18
21

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

ANALISIS Y DISEÑO DE LA INFRAESTRUCTURA TECNOLOGICA PARA LA RED DE ALTA VELOCIDAD DEL INSTITUTO DE INGENIERIA

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A N :

GUSTAVO CAMACHO PALACIOS
ARTEMIA RAMIREZ ACEVEDO
RICARDO SEPTIEN NAVA

DIRECTOR: ING. MARCO AMBRIZ MAGUEY

CD. UNIVERSITARIA 1997.

AGRADECIMIENTOS

A la Facultad de Ingeniería muy especialmente, por ser el elemento principal en nuestra formación profesional.

Al Instituto de Ingeniería y la Coordinación de Sistemas de Cómputo, en especial a Alva, Carmen, Claudia, Artemia, Eduardo, Edgar, Fer, Gustavo, Alex, Mauricio, Güendaviani, Luis, Tizoc, Daniel, así como a todos los que en ella laboran y que de alguna forma contribuyeron a la elaboración de este trabajo.

En especial al Ing. Marco Ambriz M. por su tiempo y apoyo como coordinador y director de esta tesis.

A la Ing. Cristina Casimiro, por ser una gran maestra, coordinadora y amiga. Gracias por la gran oportunidad que nos brindaste.

Al Ing. Luis Palacios, D.I Alejandro Rodríguez y D.I David Muría por su valioso apoyo e interés.

A Angustias, por pasar con nosotros los momentos mas difíciles de este trabajo y de vez en cuando ayudar a recordarnos de los inconvenientes de la profesión.

Gustavo Camacho Palacios
Artemia Ramírez Acevedo
Ricardo Septién Nava

A dios, le agradezco todo, porque alimenta mi espíritu, porque fortalece mi ser.

A mis padres.
A mis hermanos.
Porque su amor y su apoyo son pilares de mi vida.

A todos mis amigos, Esther, Alicia, Claudia Vivas, Ale, Mau, Luis, Bucio, Victor y Memo.

En especial a Claudia y Ricardo gracias por su amistad, apoyo, cariño y porque sin su apoyo y compresión no hubiera logrado terminar este trabajo.
Porque forman parte de los mejores momentos de mi vida.

Gracias a todos.

Gustavo Camacho Palacios

Agradezco y destaco sinceramente el trabajo de mis compañeros Ricardo y Gustavo quienes considero muy dedicados y competentes.

Quiero agradecer también al director de tesis tanto sus contribuciones técnicas como su paciencia y apoyo.

Es difícil enumerar la contribución exacta de cada persona ya que el trabajo tuvo una evolución significativa pero no quiero olvidar agradecer al Instituto de Ingeniería en general el haberme brindado la oportunidad de realizar este trabajo que no se limita solo al escrito si no al contacto diario con las necesidades de red del personal que ahí labora.

Por último agradezco el apoyo y comprensión de mis padres y hermanos.

Artemia Ramírez Acevedo

A Dios por darme esta oportunidad.

Mamá y papá, gracias a los dos por su gran paciencia, amor, apoyo, ejemplo de dedicación y esfuerzo, por enseñarme que cuando se quiere se pueden cumplir todas las metas que uno se propone..
que mas les puedo decir, gracias a ustedes soy lo que soy

Abulita Luz, por todo tu cariño y gran apoyo, por ser una de las personas que siempre admiraré por todo lo que fuiste, una gran persona.

A mi abuelo Ruben, por ser un ejemplo de dedicación y esfuerzo.

A mi hermano Ignacio, por enseñarme a apreciar esta vida como nadie lo ha hecho, y hacer tan especiales todos los momentos que hemos pasado juntos y espero que

A Yarid por ser esa fuerza inexplicable que hace que la vida sea especial. Gracias por estar siempre conmigo no importando las distancias y enseñarme, que uno es tan grande como los sueños que uno se atreve a vivir

A Gustavo Camacho por el apoyo y paciencia en todo este tiempo dentro del Instituto y este proyecto.

Claudia, Ruth, Clark, Rodrigo, Gux, Mauricio y Francisco por ser mas que amigos, por estar ahí incondicionalmente y compartir conmigo las mejores momentos de esta vida.

A todos ustedes por creer y apoyarme incondicionalmente gracias.

Ricardo Septién Nava

ÍNDICE

CAPÍTULO 5
DISPOSITIVOS DE INTERCONEXIÓN DE REDES 226

INTRODUCCIÓN

En la actualidad el desarrollo de la computación a nivel mundial se dirige en gran medida a la utilización de las redes de computadoras, de tal manera que se pueda compartir recursos, tanto de software como de hardware y además realizar tareas en un esquema distribuido para la solución de problemas. Este aspecto referido como computo distribuido, constituye una tecnología de punta en la computación y representa una forma eficiente de organizar el procesamiento de información de la próxima década. Por otro lado, la rápida evolución en el poder de procesamiento de los servidores y estaciones de trabajo, aunado con la reciente proliferación de múltiples aplicaciones cada vez mas sofisticadas y que demandan un incesante consumo de ancho de banda, tales como las aplicaciones con interfaces gráficas para múltiples propósitos, las nuevas y existentes aplicaciones clientes/servidor, aplicaciones de misión crítica, y por último aplicaciones multimedia, todo esto ha hecho que las redes actuales lleguen a saturarse. Es debido a esto, que las organizaciones requieren estar preparadas con una infraestructura de red adecuada para enfrentar todos estos aspectos, y que tenga una alta confiabilidad y robustez para poder soportar las crecientes necesidades de comunicación y procesamiento de información requerida por los usuarios.

Por lo anterior, hoy en día, la red del Instituto de Ingeniería de la UNAM debe experimentar cambios significativos derivados sobre todo de los requerimientos de las nuevas aplicaciones y servicios que demandan los investigadores de las diferentes áreas del Instituto. Estos cambios se están realizando por medio de la implantación de una red de cómputo de altas especificaciones, guardando ciertos lineamientos como son, el ser estándar, segura, confiable, administrable, además de ser escalable y flexible. Para llegar a este tipo de red se necesita el desarrollo de una arquitectura de red modular. Dicha arquitectura es mas que una lista de componentes de red, topologías, dispositivos etc, es la planeación de la red, donde se establecen las estrategias y anteproyectos para definir mejor los elementos de la red y la relación que mantendrán entre sí. En otras palabras, la planeación significa desarrollar una arquitectura de red.

Con el propósito de realizar una buena planeación de dicha arquitectura de red, en este trabajo se pretende llevar a cabo un estudio minucioso de las diversas nuevas tecnologías de red de área local disponibles como son **Ethernet conmutado, Fast Ethernet**, FDDI [illegible] y ATM. Lo anterior debido a que cada una de estas nuevas tecnologías [illegible] neficios específicos para un conjunto particular de aplicaciones y [illegible]os. Sin embargo, en la institución los requerimientos son diferentes dep[illegible]do de cada área o servicio, es por ello que tal vez una sola tecnología de re[illegible]o sea adecuada para todas las necesidades operacionales que demanda el Instituto. De esta manera, la arquitectura de red propuesta pretende

proveer un diseño de alto nivel, especificando tecnologías de subredes (Fast Ethernet, Ethernet conmutada, FDDI o ATM) que se consideren adecuadas a las necesidades del Instituto, los esquemas de interconexión, sistemas de cableado, de administración y control necesarios, además de los protocolos a través de los cuales se comunicarán las aplicaciones y servicios de los usuarios. Así mismo la arquitectura asentará los principales puntos de estabilidad de las subredes a través de las cuales las tecnologías de la próxima generación se integrarán dentro de la base de sistemas ya instalados. Cabe mencionar que a partir de la rigurosa definición de las interfaces entre las tecnologías se puede garantizar la flexibilidad operacional.

Finalmente se debe especificar que esta planeación de tecnología debe ser de forma **modular**, permitiendo así una ruta de migración a través de pasos o etapas controladas además de ajustarse a las necesidades presentes y futuras con un cambio mínimo de los equipos que la constituyen, a fin de ganar entre otras cosas la escalabilidad, la protección de inversión de la infraestructura actual de la red del Instituto y así salvar el mayor valor de costos, también por otro lado la minimización de los riesgos a fallos y la reducción de las interrupciones hacia la red y por tanto a los usuarios. De esta manera, se asegura guiar al Instituto hacia el futuro de la forma mas ordenada y controlada posible.

Este esquema de arquitectura de red modular permitirá a los administradores de la red y por tanto a la institución, encontrarse preparados tanto para las futuras necesidades del Instituto, además de como, las previsibles nuevas tecnologías de redes de comunicación se adecuarán para satisfacerlas.

OBJETIVOS

Este trabajo tiene como objetivo principal, el planear el crecimiento y actualizar la infraestructura tecnológica para la red de altas especificaciones del Instituto de Ingeniería, considerando las necesidades de los usuarios y las funciones propias de administración.

Selección de la arquitectura tecnológica y planeación de la configuración óptima para cada una de las etapas que comprende este trabajo.

Adecuar una metodología de selección de tecnologías y equipo de redes de computadoras para este trabajo.

Realizar la documentación de las etapas comprendidas por este trabajo en la red del Instituto de Ingeniería.

Y por último, tener una fuente de información completa de las tecnologías de red de alta velocidad actuales y protocolos de comunicación.

ORGANIZACIÓN

Este trabajo se ha organizado de la forma más modular posible, teniendo como base para su desarrollo el modelo de referencia OSI. Los capítulos son relativamente independientes y cada uno está dedicado a un determinado aspecto relacionado con el diseño de la tecnología de red necesaria para este trabajo.

1. Antecedentes
   El capítulo se inicia con una breve descripción del Instituto de Ingeniería, como son su organización y esquema de trabajo, continuando más adelante con la descripción básica de la red y como ésta ayuda al mejor desempeño de las tareas realizadas en la institución.

2. Modelo de referencia OSI
   Se explica de manera detallada cada uno de los siete niveles de que se compone el modelo de referencia OSI. Este capítulo es de suma importancia, ya que nos servirá de base para llevar a acabo un estudio organizado para llegar al objetivo planteado en este trabajo.

3. Conceptos y estándares de redes de área local
   Se da una introducción de los conceptos más relevantes utilizados en este trabajo como son los tipos de medios de transmisión, topologías, métodos de acceso al medio entre otros, asimismo de los estándares de redes más utilizados en la actualidad como son el conjunto de estándares 802.x del IEEE y el estándar de cableado estructurado (EIA-TIA 568), explicando brevemente su funcionamiento.

4. Protocolos de comunicación
   Se exponen los principales protocolos de sistemas abiertos de comunicación como son el conjunto de protocolos TCP/IP y los protocolos del modelo OSI, dando al final un punto de vista de sus ventajas y desventajas. Por último se hace una pequeña referencia a los protocolos de comunicación NetBEUI utilizado por las redes Microsoft y el conjunto de protocolos IPX/SPX utilizado en las redes Novell Netware.

5. Dispositivos de interconexión de redes
   Se plantea la forma de operación de cada uno de los dispositivos de interconexión de redes más importantes de acuerdo al modelos OSI. Además de una breve descripción de los puntos más importantes y por lo que cada uno de ellos se caracteriza.

6. Tecnologías de redes de alta velocidad
   Se trata de explicar de manera detallada la forma funcional las múltiples tecnologías de redes LAN de alta velocidad como son Fast Ethernet, 100VG-AnyLAN, FDDI/CDDI y ATM. Así como una breve descripción de las tecnologías utilizadas para redes WAN.

7. Estado actual de la red del Instituto de Ingeniería
   Se realiza una descripción mas detallada de la situación actual de la red del Instituto de Ingeniería, haciendo énfasis en los medios de transmisión, topología, protocolos de acceso al medio y de comunicación, además de los dispositivos de interconexión y los mecanismos de administración utilizados. De igual manera se hace para la Red UNAM y las tendencias a seguir por parte de esta.

8. Estudio de las soluciones por etapas para la REDII: Análisis, evaluación y selección
   En este capítulo, se adecua una metodología basada en análisis costo-efectivo que aunada con los conocimientos previamente adquiridos, nos ayudaran a la selección de cada una de las tecnologías necesarias para implantar una red de computo de altas especificaciones. En seguida, se exponen los problemas actuales y requerimientos a corto, mediano y largo plazo de la red del Instituto, dando los motivos del porqué una migración ha una red de altas especificaciones es importante.

   Posteriormente, se plantean las bases del diseño e implantación de la nueva arquitectura de red para el Instituto de Ingeniería, en esta parte, se plantean los módulos en que se compone la REDII de acuerdo a una importancia jerárquica. Una vez planteados los puntos anteriores, se definen las etapas que se llevaran a cabo en este trabajo y que forman el inicio para la red de altas especificaciones del Instituto. En el desarrollo de cada una de las etapas, se lleva a cabo un análisis y una evaluación de las posibles soluciones para cada etapa, finalizando con la selección óptima y justificando el porqué de tal selección.

9. Solución óptima para el Instituto de Ingeniería
   En este capítulo se lleva a cabo una descripción detallada de cada una de las soluciones por cada una de las etapas realizadas. Dentro de esta descripción se realiza una explicación de la configuración final de cada etapa, el porqué de esta configuración y finalmente qué beneficios se consiguieron con cada una.

10. Conclusiones
    Finalmente se estiman las metas alcanzadas de las etapas comprendidas en este trabajo. Asimismo esto servirá como base y guía para la realización de posteriores actualizaciones de la red del Instituto de Ingeniería.

CAPÍTULO 1
ANTECEDENTES

1.1 El Instituto de Ingeniería

1.1.1 Finalidad y orientación

El Instituto de Ingeniería es parte del subsistema de investigación Científica de la Universidad Nacional Autónoma de México. Las principales funciones del Instituto son desarrollar investigación para mejorar los conocimientos, métodos y criterios de ingeniería, contribuir a la formación de expertos en esta rama del saber, así como promover la mas alta calidad en la práctica profesional. Siempre teniendo encuenta las necesidades actuales y previsibles de la ingeniería nacional. Las actividades que se llevan a cabo en el instituto son: investigación técnica y aplicada, apoyo al desarrollo tecnológico y análisis de los requerimientos sociales a cuya solución puede aportar la ingeniería. Muchas veces estas actividades se llevan a cabo en colaboración con otras instituciones afines, ya sea técnicas, culturales o científicas del país y del extranjero.

La política fundamental del Instituto, desde su fundación en 1956, ha sido ocuparse de la investigación orientada a problemas generales de la ingeniería cuya importancia es mundial, y de apoyar a la vez a las instituciones privadas y públicas para mejorar la práctica de la ingeniería en México.

El Instituto de Ingeniería, es el centro de investigación más productivo del país en diversas áreas de la ingeniería. Es una comunidad de más de 1000 personas, comprendidas en: personal de investigación, estudiantes de ingeniería, técnicos de apoyo, personal secretarial y de servicios. Sus instalaciones ocupan 12 conjuntos de edificios entre laboratorios , cubículos, áreas comunes y un auditorio.

1.1.2 Organización

Las actividades del Instituto se agrupan en 12 áreas y líneas de investigación. De esta manera, los programas se forman por conjunto de proyectos específicos dentro de las áreas y líneas que mas adelante se describirán. Cabe señalar que aveces también se llevan a cabo investigaciones multidisciplinarias en las que participan personal de diversas áreas de investigación del Instituto y de otras organizaciones externas a la UNAM.

Estas 12 áreas de investigación son:

Estructuras y materiales
En esta área se llevan a cabo estudios analíticos y experimentales sobre el comportamiento de las estructuras y materiales expuestos a diversas acciones que afectan la vida útil de las construcciones. Se estudian los efectos producidos por deformaciones impuestas, sismos y vientos. De esta manera, se investiga la confiabilidad de las estructuras y se participa en la elaboración de normas y códigos que garanticen un comportamiento satisfactorio de las mismas.

Geotecnia
Se investiga la estructura y el comportamiento ya sea estático y dinámico de diversos tipos de suelo. Se desarrollan métodos de análisis y diseño estático y dinámico de túneles y presas, así como procedimientos para la evaluación de las deformaciones permanentes.

Mecánica aplicada
En esta área se desarrollan investigaciones teóricas y aplicadas para el análisis de respuesta inelástica de edificios ante soluciones sísmicas. Se estudian problemas de torsión inelástica, interacción suelo-estructura y confiabilidad estructural etc. Por otro lado, se determina el riesgo sísmico en sitios específicos, atendiendo l mecanismo de la fuente y la trayectoria de las ondas sísmicas; se evalúan los efectos de la topografía en las características de los temblores y de esta manera, se definen criterios de diseño para estructuras especiales.

Sismología e instrumentación sísmica
Se desarrollan e implantan sistemas de medición de alta precisión de temblores, se estudia la actividad general en el país y en particular la que es generada en las costas del océano Pacífico. Posteriormente se interpretan los registros sísmicos de una extensa red permanente de observación y se instrumentan estructuras para el estudio de su comportamiento dinámico durante temblores intensos. Se investigan además, movimientos en fallas activas, tanto en zonas donde existen o se construirán obras importantes.

Vías terrestres
Se realizan los estudios de sistemas de transporte en aspectos relacionados con el diseño geométrico y estructural, operación, conservación y reconstrucción de carreteras y aeropistas.

Hidráulica
En esta área se tratan los problemas de ingeniería relacionados con el aprovechamiento y control del agua. Esto se lleva a cabo a través de investigaciones sobre el comportamiento y diseño de estructuras hidráulicas.

Ingeniería ambiental
Las actividades principales de este grupo son la investigación y desarrollo de sistemas de tratamiento y potabilización de aguas residuales, convencionales y problemática. Obteniendo métodos de tratamiento aerobio y anaerobio que son aplicados en la fabricación de alimentos, empresas de transformación entre otros.

Automatización
Se desarrollan diversos aspectos de circuitería electrónica, programación y desarrollo de algoritmos, para la implantación de esquemas de control y supervisión de procesos industriales. De esta forma se apoya a las empresas que automatizan sus procesos. Además se abordan problemas de modelado, simulación, control y detección de fallas de procesos dinámicos no lineales.

Instrumentación
Este grupo realiza la investigación y desarrollo relacionado con la electrónica e instrumentación aplicada. Proporcionando asesoría y apoyo en la selección de equipo en las labores de selección de equipo de medición especializada y mantenimiento de aparatos de laboratorio

Ingeniería mecánica, térmica y de fluidos
Se lleva a cabo el estudio y diseño de mecanismos de tipo industrial para la automatización de procesos, dispositivos para la absorción de energía sísmica en edificios, diversos sistemas de engranes, etc. En lo referente a la ingeniería térmica, se estudian y diseñan sistemas termodinámicos para el aprovechamiento de energía solar. El grupo de ingeniería de fluidos analiza fenómenos transitorios y permanentes para diversas condiciones de flujo. De esta manera, se realizan estudios sobre la operación y seguridad de acueductos, investigación de los fenómenos vibratorios estacionarios en plantas hidroeléctricas entre otros.

Ingeniería de sistemas
En esta área se investigan metodologías y estudios en planeación urbana y regional, desarrollo rural, industrial, innovación tecnológica y planeación sectorial en todas sus especialidades.

Por otro lado, se hacen investigaciones en teoría de sistemas, con el fin de contribuir al perfeccionamiento de métodos y técnicas empleados en la solución óptima de problemas de ingeniería. Un esfuerzo importante se desarrolla para apoyar procesos de toma de decisiones multicriterio.

Sistemas de cómputo
Es básicamente un grupo de servicios divididos en cuatro áreas que son:

- Área de desarrollo de sistemas de información, es aquí donde se desarrollan y mantienen los múltiples sistemas de información del Instituto como son la base

de datos académicas, la base de datos de inventarios de la Secretaría Administrativa entre otras.

- Área de soporte técnico a computadoras personales y periféricos, llevan a cabo el mantenimiento preventivo y correctivo de las computadoras personales y de los periféricos. También la instalación de hardware especial y software para las PC´s de los usuarios.

  Por otro lado, prestan asesoría al personal académico referente a la compra y uso del tipo de software y hardware a utilizar.

- Área de administración de estaciones de trabajo y servidores Unix, este grupo realiza la administración de las estaciones de trabajo que prestan los múltiples servicios de Internet, así como las que se desenvuelven en tareas especificas de ingeniería. Se brinda asesoría y soporte técnico a los usuarios, además de la constante evaluación de las mejores tecnologías de software y hardware para las estaciones.

- Área de infraestructura de redes y telecomunicaciones, Se encarga de la planeación, instalación, administración, mantenimiento, operación y monitoreo de la red local del Instituto REDII. Además de mantener la seguridad tanto lógica como física de la red.

1.1.3 Antecedentes de la red de Instituto de Ingeniería

El Instituto de Ingeniería cuenta con una amplia gama de recursos de cómputo que incluyen desde computadoras personales, impresoras, scanners, múltiples periféricos, servidores y estaciones de trabajo designadas a tareas especializadas de ingeniería.

Se ofrecen además múltiples servicios de Internet para el intercambio de información y de ideas dentro de la universidad así como con otros centros de investigación tanto públicos y privados del mundo, apoyando así a la investigación científica. Cuenta además con la red local mas extensa de la UNAM, con alrededor de 350 nodos conectados. Por otro lado, se enlaza a la RedUNAM por medio de la cual se conecta a la red mundial Internet.

Esta red local con que cuenta el Instituto referida comúnmente como REDII, es una red con tecnología Ethernet de 10 Megabits por segundo, a través de un backbone de bus de cable coaxial grueso cumpliendo de esta manera con el estándar 10Base5 del IEEE 802.3. Actualmente se integran 5 edificios (1, 2, 4, 5 y 12) a este backbone principal, dentro de cada uno de los edificios se cumple con el estándar Ethernet 10BaseT y de cableado estructurado.

Se tienen 30 estaciones de trabajo, 3 servidores principales unix que brindan la mayoría de los servicios de Internet y alrededor de 300 equipos entre computadoras personales e impresoras interconectadas a esta red.

CAPÍTULO 2
MODELO DE REFERENCIA OSI

2.1 Introducción

La organización internacional de normalización ISO, creó el modelo de referencia para Interconexión de Sistemas Abiertos OSI. Este modelo proporciona un esqueleto de arquitectura de siete niveles alrededor del cual se pueden diseñar protocolos específicos que permiten a diferentes usuarios comunicarse abiertamente.

Las capas del modelo OSI se crearon teniendo en cuenta las siguientes ideas o principios :

1. Una capa se creará en situaciones en donde se necesita un nivel diferente de abstracción.
2. Cada capa deberá efectuar una función bien definida.
3. La función que realizará cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.
4. Los límites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
5. El número de capas deberá ser lo suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa y, por otra parte, también deberá ser lo suficientemente pequeña para que su arquitectura no llegue a ser difícil de manejar.

Con estos principios se espera que se dé origen a una arquitectura por niveles, con interacciones mínimas a través de las fronteras y con niveles que se puedan rediseñar fácilmente o cuyos protocolos puedan cambiarse sin modificar las interfaces con otros niveles.

Para realizar lo anterior, el modelo OSI persigue dos objetivos fundamentales. El primero tiene que ver con la comunicación de la red: los datos del emisor deben ser dirigidos y llegar al destino correctamente y en sincronía. El segundo, consiste en asegurar que los datos que se entregan sean reconocibles y estén en el formato apropiado.

Para resolver estos dos objetivos, el modelo de referencia OSI, divide los protocolos de los siete niveles en dos tipos: los protocolos que proporcionan el servicio de red y los protocolos de más alto nivel para resolver el segundo objetivo.

Por lo anterior se puede decir que las tres capas inferiores brindan los servicios de red. Los protocolos que implantan estas capas deben aparecer en cada uno de los nodos de la red. Las cuatro capas superiores ofrecen servicios propios a los usuarios finales.

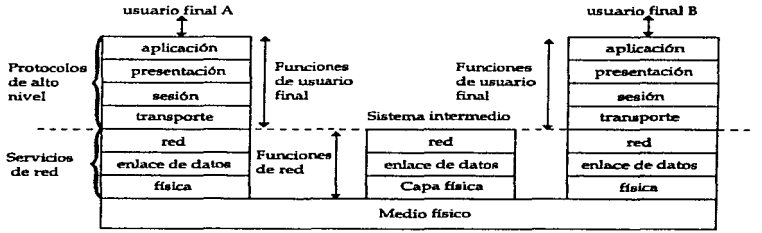


Figura 2.1 Modelo de referencia OSI

En este modelo de referencia consta de dos tipos de sistemas: los primeros, conocidos como los usuarios finales (ES: End systems) y los segundos, que son los sistemas intermedios (IS: Intermediate Systems). Los sistemas intermedios conectan dos o más subredes y realizan funciones de encaminamiento mediante el direccionamiento de paquetes entre las diversas subredes que componen una red. Los sistemas finales están conectados a las subredes y no tienen funciones de encaminamiento (los sistemas ES son básicamente una estación de trabajo de usuario, un servidor o cualquier otro nodo o dispositivo conectado a la red).

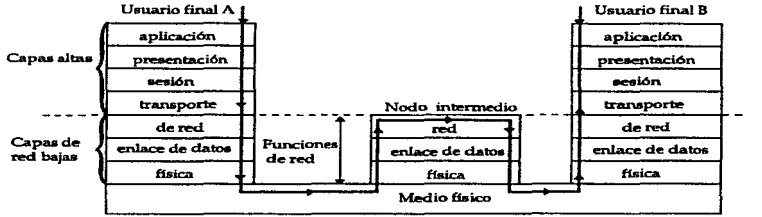


Figura 2.2 Arquitectura OSI de siete capas

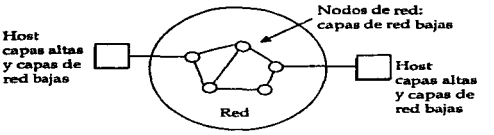


Figura 2.3 Subdivisión de capas

Las redes pueden ser del tipo de conmutación de paquetes o de conmutación de circuitos. Dentro de la categoría de conmutación de paquetes, las capas pueden ofrecer dos tipos diferentes de servicios a las capas que se encuentran sobre ellas: servicio orientado a conexión y servicio sin conexión.

- Servicios orientados a conexión: consisten básicamente en dar de alta una conexión lógica antes de transmitir los datos y posteriormente llevar a cabo la desconexión. En este tipo de operaciones, usualmente algún tipo de relación se mantiene entre las unidades de datos al ser transmitidas a través de la conexión.

- Servicios en modo sin conexión : en este tipo de operaciones no se establece ninguna conexión, por lo tanto, las unidades de datos son transmitidas como unidades independientes.

Cada uno de los servicios se caracteriza por la calidad del servicio que brinda a la capa superior; algunos de ellos son confiables en la medida que nunca pierden la información que transportan. Por lo general, un servicio confiable se realiza haciendo que el receptor notifique el haber recibido cada mensaje para que el emisor este seguro de la entrega. Cabe hacer notar que el proceso de notificación introduce un exceso de tráfico y retardos, que a menudo son convenientes, pero también son algunas veces indeseables.

Con el siguiente diagrama se observan dos trayectorias que forman un servicio completamente orientado a conexión desde las capas superiores hasta las inferiores y la otra, un servicio totalmente sin conexión. Sin embargo, es posible tener conversiones de un servicio orientado a conexión ofrecido por las capas de red o de transporte, aún cuando las capas inferiores ofrezcan un servicio sin conexión (en este caso, la capa de red o la de transporte deberán tratar la conversión), por ejemplo, un servicio de transporte orientado a conexión podría desarrollarse en una red tipo LAN, con un servicio sin conexión en la capa de enlace, por medio del establecimiento del control de flujo, de errores y funcionalidades relacionadas en la capa de red o de transporte. El mecanismo inverso de conversión sería mediante el cual se desarrolle un servicio sin conexión para las capas superiores por encima de

un servicio orientado a conexión en la capa de enlace, lo cual también se puede llevar a cabo.

Un servicio orientado a conexión puede desarrollar actividades de secuenciamiento de datos, control de error y control de flujo. Si una petición de servicio no puede ser accedida, cualquiera de las partes puede negociar el servicio dentro de una capa mas baja o rechazar la petición de conexión.

Un servicio sin conexión maneja las unidades de datos de un protocolo como entidades separadas e independientes. De esta manera las unidades de datos pueden tomar diferentes rutas para evitar nodos congestionados o con fallas. Por esta naturaleza, una red sin conexión tiene un esquema mas robusto al orientado a conexión.

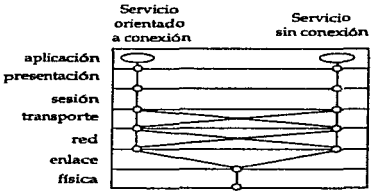


Figura 2.4 Combinación de los servicios orientados a conexión y sin conexión en el modelo OSI

Cabe hacer notar que las capas de enlace, red y de transporte soportan los servicios de orientación a conexión y sin conexión, teniendo en cuenta sus diversas conversiones. Se debe de entender que tales conversiones no son permitidas en los tres niveles superiores (capas de sesión, presentación y aplicación).

2.2 Descripción de las siete capas del modelo OSI

2.2.1 Capa 1: física

Este capa se encarga de establecer la conexión física mediante la cual los dispositivos se conectan a la red y las reglas para que los bits sean transmitidos.

Las principales funciones que desarrolla esta capa son:

- Generación de señales eléctricas, electromagnéticas u ópticas, además de la descripción de los conectores.
- Define los voltajes o niveles de luz para hacer referencia a los valores de 0 y 1 para un bit respectivamente, así como la duración de este. De tal forma que se asegure, que cuando se transmita un bit de valor 1, este se reciba con el mismo valor en el otro extremo. Además se incluyen las formas de codificación, decodificación, modulación y demodulación de la señal.
- Provee el nivel de referencia de tierra.
- Define el tipo de mecanismos de conexión (tales como plugs, sockets y pines) y la descripción de sus características.
- Provee el procedimiento para establecer, mantener y desactivar un enlace físico.

Cabe notar que el modelo OSI ve a la capa física en términos abstractos y esta no estipula los medios físicos como cable coaxial, fibra óptica, par trenzado, etc. Sin embargo, algunos estándares que usan los conceptos del modelo OSI hacen referencia a medios físicos específicos, tales como, el ISDN, IEEE, CCITT entre otros.

Las acciones de la capa física son dictadas por las funciones de control de la capa de enlace de datos y a diferencia de las demás capas del modelo OSI, la capa física no tiene otra capa por debajo, por lo que esta solo transmite bits sin tomar en cuenta su significado.

2.2.2 Capa 2: enlace de datos (Data Link)

La capa de enlace de datos debe establecer y controlar la ruta de comunicación física hacia el siguiente nodo. Por lo que la tarea principal del nivel de enlace de datos es el de establecer reglas o procedimientos que permitan la comunicación correcta y ordenada de paquetes entre nodos vecinos en una red. Es decir, sus funciones son limitadas a las ligas individuales, por lo que solo es responsable del tráfico entre nodos adyacentes (redes WAN) o estaciones sobre la misma línea (redes LAN). De esta manera convierte el medio de transmisión en una línea sin errores para la capa de red (nivel superior).

El protocolo de enlace de datos debe incorporar los procedimientos que permitan las siguientes tres fases:

1. Fase de conexión o establecimiento del protocolo, para que se permita de esta forma la comunicación entre dos extremos.
2. Fase de transferencia de datos. Donde se debe asegurar la transferencia ordenada de los paquetes de datos.
3. Terminación de la comunicación. El protocolo debe incluir procedimientos para terminar la comunicación cuando el enlace ya no se necesite o cuando se vuelve ruidoso o llega a fallar, de manera que se arruina la conexión.

Se puede decir que la capa de enlace de datos realiza las siguientes funciones :

- Sincronización lógica (no física) de el transmisor y receptor. Esto es debido a que la comunicación entre dos extremos de un enlace es, por su propia naturaleza, asincrónica. por lo que se requiere que el primer bit de cada bloque este en sincronía para funciones de reconocimiento de fin de bloque y detección de errores.

- Control de flujo de datos que cruza el enlace para prevenir que el transmisor envíe los bits de manera rápida y ocasionar que el receptor llegue a saturarse.

- Control y detección de errores. Por lo que se debe establecer un procedimiento de aceptación para indicar si los paquetes se recibieron correcta o incorrectamente, esto se realiza al definir en este nivel de enlace un campo de inicio y fin de un bloque de datos. Además para la corrección de errores se debe de incluir mecanismos para recobrar los datos perdidos, duplicados o erróneos. (detección de errores por retransmisión).

- Los paquetes deben enumerarse para asegurar la entrega ordenada al siguiente nivel de red del extremo receptor de un enlace.

- Mantiene conocimiento y control de las condiciones del enlace, como son la fase de conexión, la fase de transmisión de datos y fase de terminación para asegurar que el enlace está hecho y funciona correctamente.

- En el caso de redes tipo LAN, resuelve la competencia por el uso de un canal de comunicaciones compartido por unidades conectadas directamente al mismo.

Por lo anterior, la capa de enlace puede diseñarse para que pueda ofrecer varios servicios a la capa de red:

1. Servicio sin conexión y sin reconocimiento (Unacknowledged, datagram service). Consiste en hacer que, la máquina origen transmita tramas independientes a la máquina destino, sin que ésta proporcione una señal de reconocimiento. No establece ninguna conexión previa, ni tampoco se libera posteriormente. Si la trama se llega a perder, no se realiza ningún intento por recuperarla en la capa de enlace. Este tipo de servicios es muy conveniente cuando la tasa de error resulta muy baja y la recuperación se delega a las capas más altas. Muchas redes tipo LAN, cuentan con un servicio sin conexión y sin reconocimiento en la capa de enlace.
2. Servicio sin conexión con reconocimiento (Acknowledged, datagram service). En este servicio no se llega a la conexión, pero por cada una de las tramas transmitidas se requiere un reconocimiento de recepción de forma individual. De esta manera se sabe cuando la trama llega correctamente al otro extremo. Si la trama no llega dentro de un intervalo de tiempo especificado, entonces puede comenzar a transmitirla nuevamente.
3. Servicio orientado a conexión (Virtual circuit service). En este servicio, las máquinas origen y destino, establecen una conexión antes de transmitir algún dato. Cada una de las tramas transmitidas a través de la conexión se enumera, y la capa de enlace garantiza que cada trama transmitida sea recibida. Además, garantiza que cada una de las tramas se reciba exactamente una vez y en el orden correcto. A diferencia de un servicio sin conexión, donde se puede concebir que la pérdida de un mensaje de reconocimiento ocasione que una trama se transmita varias veces y por consiguiente se reciba también varias veces. De esta forma el servicio orientado a conexión, proporciona a los procesos de la capa de red el equivalente a un flujo de bits confiable.

NOTA: La mayoría de las redes WAN está compuesta por ligas punto a punto, mientras que las redes LAN, están construidas en base a un canal o línea compartida (multipoint broadcast channel). Obviamente, esas ligas tienen diferentes características de acceso. Esto es, en el mundo real de las redes se pueden identificar dos tipos de aplicaciones principales y sus correspondientes protocolos. En el caso de las redes WAN, el protocolo de enlace se lleva a cabo en cada enlace de una trayectoria de extremo a extremo. El nivel superior, el nivel de red puede de esta forma ignorar el enlace y suponer que un paquete que se introduce en una extremo de un enlace llega correctamente y en secuencia al otro extremo. Sin embargo, en el caso de las redes locales independientes, generalmente solo hay un enlace de red que conecta a todos los usuarios finales. Por esta razón, la existencia de la capa red sería nula si no se involucrara en esta, la retransmisión de mensajes. El

estándar en el nivel de enlace de datos en el caso de redes WAN se utiliza el HDLC. Para las redes LAN el comité IEEE ha desarrollado el estándar 802.X, el cuál suministra el nivel físico y el de enlace de datos para tres tipos de comunicacion de redes en distancias cortas.

2.2.3 Capa 3: de red

La capa de red, especifica la interfaz del usuario a través de la red, también define la conmutación/enrutamiento de redes y las comunicaciones entre redes (internetworking). Para realizar lo anterior, desarrolla cuatro funciones principales: enrutamiento, control de congestión, interconexión de redes homogéneas y heterogéneas (llevando a cabo los mecanismos de fragmentación y reensamblaje).

- El enrutamiento se encarga de encaminar los paquetes de información conforme avanzan a través de la red, es decir, guía los paquetes de datos desde el nodo origen hasta el nodo destino. Mientras que la capa de enlace de datos se ocupa del movimiento de datos entre dos nodos adyacentes.

  Los paquetes pueden restringirse a seguir una ruta orientada a conexión (circuito virtual) o estar moviéndose en modo sin conexión (o de datagrama). Es por esto que la capa de red debe de estar consiente de las diferentes rutas o caminos alternativos que existen en la red para cumplir con el objetivo. Por esta razón, la capa de red se auxilia de tablas de enrutamiento en cada nodo a lo largo de la trayectoria (estas tablas determinan las rutas de comunicación entre un transmisor y un receptor, además de tener información del estado de los nodos, etc.), y de esta manera escoge la mejor opción de ruta disponible, la cuál dependerá de varios factores como son: el congestionamiento, el número de nodos que intervienen en dicha ruta, la velocidad de los enlaces, etc.

  Para poder escoger la mejor ruta disponible, es necesario **utilizar algoritmos de enrutamiento**, los cuales son utilizados para establecer las trayectorias de enrutamiento o los valores indicados en las tablas de enrutamiento equivalentes en cada nodo a lo largo de la trayectoria; los algoritmos de enrutamiento, representan una de las áreas principales del diseño de la capa de Red. Estos algoritmos se pueden clasificar de diferentes maneras; ya sea tomando en cuenta el hecho de que las trayectorias se encuentran establecidas de manera centralizada o descentralizada, en la ultima opción es donde cada nodo lleva a cabo un algoritmo de encaminamiento específico; o bien de acuerdo con su respuesta de adaptación.

  NOTA: Las redes basadas en el enrutamiento de circuito virtual (orientadas a conexión) tienden a usar cálculos centralizados para determinar las trayectorias de enrutamiento; los paquetes de control se usan entonces para establecer la trayectoria escogida. Por otro lado, las redes de datagramas (sin conexión) usan técnicas de enrutamiento distribuido.

Algunos ejemplos de algoritmos de enrutamiento son: encaminamiento de trayectoria mínima y encaminamiento bifurcado.

Asunto	Subred Datagrama	Subred circuito virtual
Establecimiento del circuito	No es posible	Requerido
Direccionamiento	Cada paquete contiene la dirección completa de la fuente y del destino	Cada paquete contiene un número corto de circuito virtual
Información del estado	La subred no tiene la información del estado	Cada circuito virtual establecido necesita un espacio en la tabla de subred
Encaminamiento	Cada paquete se encamina independientemente	Ruta seleccionada cuando el circuito virtual se establece todos los paquetes siguen la ruta
Efecto de los fallos del nodo	Ninguno, con excepción de los paquetes que se perdieron durante la colisión	Todos los circuitos virtuales que pasan a través del equipo que falló se terminan
Control de la congestión	Difícil	Facil si un número suficiente de tampones pueden asignarse anticipadamente para cada circuito virtual establecido
Complejidad	En la capa de transporte	En la capa de red
Adecuado para	Servicio orientado a conexión y sin conexión	Servicio orientado a conexión

Tabla 2.1 Comparación de los datagramas y circuitos virtuales de subredes.

Una vez que la capa de red ha seleccionado la trayectoria de enrutamiento para cada paquete, indica a que enlace de salida se va dirigir un paquete dado.

2.2.3.1 Funciones que lleva a cabo la capa de red:

- Control de Red: Esta función se encarga de que cada nodo envíe la información de su estado a otros nodos, y de la misma forma recibir información del estado de los otros nodos para que de esta manera se determine la mejor ruta para los mensajes. Además de que aquí se asocian prioridades a los mensajes y así cumplir con el esquema de prioridades.

- Control de Congestión: Esto significa reducir los retardos de la transmisión que pueden resultar de sobrecargar algunos circuitos o un nodo en particular de la red, que al estar ocupado y deshabilitado no puede procesar los mensajes de un modo oportuno. De esta manera la Capa de Red debe adaptarse a las condiciones de tránsito y así intentar enrutar los mensajes alrededor de estos puntos o nodos de congestión. Cabe hacer notar que no todos los sistemas pueden adaptarse a las características cambiantes de las ligas y de esta forma

evitar los puntos o nodos de congestión. En algunos casos (específicamente, en sistemas tipo broadcast) se puede hacer poco para resolver este problema.

- Interconexión de redes: Esta función, el modelo OSI la lleva a cabo en la capa de red. La interconexión de redes siempre que sea necesario divide la capa de red en tres subcapas[1]:

    3a. La subcapa de acceso a la subred (SNAcP).
    3b. La subcapa de mejora de la subred (SNDCP).
    3c. La subcapa de la interconexión de redes (SNICP).

3a. La subcapa de acceso a la subred consiste en soportar el protocolo de la capa de red para la subred que específicamente se esté utilizando. Esta genera y recibe paquetes de datos y de control, lleva a cabo las funciones ordinarias de la capa de red. El software está diseñado para que funcione como el interface real de la subred que se encuentra disponible. No existe garantía de que funcione correctamente con otras subredes.

3b. La subcapa de mejora de la subred está diseñada para armonizar las subredes que ofrecen diferentes servicios.

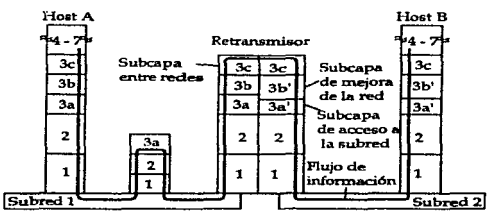


Figura 2.5 Estructura interna de la capa de red. La línea llena muestra como fluye la información desde el host A hasta el host B. El retransmisor está conectado a las dos subredes.

3c. La función principal de la subcapa de interconexión de redes es el encaminamiento extremo-extremo. Cuando llega un paquete a un retransmisor se lleva a la subcapa de interconexión de redes, este lo revisa y decide si lo reexpide o no. Si así resultara, entonces deberá indicar que subred deberá usar, esto es debido a que un retransmisor puede tener varias subredes a escoger.

[1] Para mayor información, referirse al libro de Uyless black; Redes de Computadoras; Addison Wesley p. 207.

En el caso general (que no es OSI), el proceso que lleva a cabo un retransmisor se puede realizar en cualquier capa del modelo. Los cuatro tipos de retransmisores más comunes son los siguientes:

En la capa 1 el dispositivo retransmisor se llama Repetidor. Este copia los bits individuales, entre segmentos de cable.

En la capa 2 el dispositivo retransmisor se llama Puentes. El cuál almacena y reexpide tramas entre segmentos de red tipo LAN.

En la capa 3 el dispositivo retransmisor se llama "enrutador", este almacena y reexpide paquetes entre redes que no son similares.

En la capa 4 el dispositivo retransmisor se llama compuerta o convertidor de protocolos (Gateway). Este proporciona la interconexión en las capas superiores.

2.2.3.2 Proceso de fragmentación y reensamblado

Un problema esencial en la interconexión de redes, es el que cada subred impone un tamaño máximo y formato para los paquetes que pasan a través de esta. Por lo tanto si son soportados diferentes tamaños y formatos, las subredes deben proveer el mecanismo de fragmentación y reensamblaje de los paquetes. Esto se lleva a cabo en los retransmisores llamados enrutadores[2].

2.2.4 Capa 4: de transporte

Esta capa proporciona el servicio confiable para la transmisión de datos de extremo a extremo necesario para la capa de sesión y los capas superiores, satisfaciendo así la función clave de aislar a las capas superiores de la tecnología, diseño e imperfecciones que se presentan en las capas inferiores.

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario en unidades más pequeñas (segmentos), pasarlos a la capa de red[3] y asegurar que todos ellos lleguen correctamente al otro extremo[4].

---

[2] Existen varios problemas para la interconectividad entre redes, para obtener mayor información al respecto, referirse al libro de Uyless black; Redes de Computadoras; Addison Wesley; p. 204.

[3] Bajo condiciones normales, la capa de transporte crea una conexión de red individual para cada conexión de transporte solicitada por la capa de sesión. Si la conexión de transporte solicitada por la capa de sesión necesita de un mayor caudal, la capa de transporte podría crear múltiples conexiones de red para la misma, de esta manera, dividirá los datos entre las diferentes conexiones individuales de la red que sirven a la misma sesión con objeto de mejorar dicho caudal.

[4] La función primordial de la capa de transporte, consiste en enriquecer la calidad de servicio (QOS) suministrada por la capa de red. Por esta razón, se tiene que, si el servicio de la capa de red es impecable, es decir que casi no falla, la capa de transporte puede tener un trabajo relativamente

Básicamente, se puede decir que la existencia de la capa de transporte hace posible que el servicio de transporte sea más confiable que el proporcionado por la capa de red subyacente. Ya que los paquetes extraviados, los datos dañados de la red pueden ser detectados y compensados por la capa de transporte. Además las primitivas[5] de la capa de transporte pueden ser diseñadas para ser independientes de las primitivas del servicio de la capa de red.

Se pueden distinguir dos tipos de transmisión de datos en el nivel de transporte: transmisión orientada a conexión y transmisión sin conexión (estos son muy similares a los conceptos de operación de circuito virtual y datagrama, del nivel de red).

La capa de transporte determina qué tipo de servicio debe dar a la capa de sesión, y en último término a los usuarios de la red. Por esto se han definido cinco clases de protocolos como parte del estándar del nivel de transporte. Estas clases reflejan las diferentes aplicaciones y las distintas conexiones de red

Las conexiones de red, se agrupan en distintos tipos de servicios de red dentro de las siguientes tres categorías:

1. Categoría A: consiste en un servicio que, esencialmente, se puede decir que es perfecto. La fracción de paquetes perdidos, duplicados o dañados, viene a ser despreciable. los N-RESET o fallas de señal son tan raros que pueden ser ignorados. (Las redes tipo LAN se acercan bastante a esta categoría).

2. Categoría B: en esta categoría, los paquetes individuales rara vez se pierden por lo que también pueden ser ignorados, sin embargo , de cuando en cuando la capa de red emite N-RESET debido a fallas en la señal, como consecuencia de una congestión interna, por problemas de hardware, o bien, por irregularidades del software. Depende, por consiguiente, del protocolo de transporte recolectar los pedazos, establecer una nueva conexión de red, resincronizarse y continuar, de tal manera que el N-RESET quede perfectamente oculto para el usuario de transporte. (La mayoría de las redes públicas X.25, son de categoría B).

---

sencillo. Sin embargo, por otro lado, si el servicio de la capa de red es deficiente, la capa de transporte tiene que llenar el hueco que existe entre el servicio deseado por los usuarios de la capa transporte y el servicio que la capa de red puede ofrecer.

[5] Gracias a la capa de transporte, es posible que los programas de aplicación puedan escribirse utilizando un conjunto normalizado de primitivas, y hacer que dichos programas funcionen en una gran variedad de redes, sin tener que preocuparse de la manera de tratar con diferentes interfaces que tiene cada subred y con transmisiones inseguras. Si todas las redes reales fueran perfectas y tuvieran las mismas primitivas de servicio, probablemente no se necesitaría de la capa de transporte.

3. Categoría C: Es aquí, donde el servicio de red no es lo suficientemente seguro como para que se pueda confiar en él. Las redes que entran en ésta categoría son por ejemplo, las redes tipo WAN que ofrecen un servicio puro sin conexión (datagrama), las redes de radio paquetes y varias interconexiones de redes.

   Los protocolos de transporte que deben convivir con el servicio tipo C, son los más complejos de todos y deberán resolver todos tipo de problemas que se presenten.

Por lo anterior descrito los protocolos de transporte se clasifican de acuerdo con las diferentes situaciones que se presenten. Cuanto más ineficiente es el servicio de red, será mas complejo el protocolo de transporte.

El modelo OSI ha considerado este problema y ha ideado un protocolo de transporte de cinco clases.

La clase 0: es la más sencilla. En ésta se establece una conexión de red para cada conexión de transporte que se haya solicitado, y al mismo tiempo supone que la conexión de red no comete errores. El protocolo de transporte no realiza un secuenciamiento o control de flujo, basándose en que la capa inferior de red lo haga todo correctamente.

La clase 1: es parecida a la clase 0, excepto que se ha diseñado para recuperarse de N-RESET. Si la conexión de red que se está utilizando para una conexión de transporte, alguna vez emite un N-RESET, las dos entidades de transporte se resincronizan y continúan a partir del punto en que se habían quedado. Para lograr esta resincronización, deberán utilizar y guardar un trazado de números de secuencia (algo que no es necesario en la clase 0). La clase 1, fuera de tener la facultad de recuperar los N-RESET, no llegan a proporcionar ningún tipo de control de error o de flujo adicional al que la misma capa de red proporciona.

La clase 2: al igual que la clase 0, está diseñada para ser utilizada con redes confiables (tipo A). Difiere de la clase 0 en el sentido de que dos o más conexiones de transporte pueden transmitirse (multiplexadas) sobre la misma conexión de red. Esta característica es muy útil cuando hay varias conexiones de transporte abiertas, cada una con relativamente poco tráfico, y el operador aplica una tarifa muy elevada por el tiempo de conexión por cada conexión de red abierta.

La clase 3: esta combina las características de las clases 1 y 2. permite el multiplexaje y, también, puede recuperarse de los N-RESET. Además, utiliza un control de flujo explícito.

La clase 4: está diseñada para el servicio de redes tipo C. Tiene características totalmente paranóicas y toma como hecho la ley de Murphy (si alguna cosa puede

salir mal, saldrá mal). Esta por consiguiente, deberá ser capaz de manejar paquetes que se hayan perdido, duplicado o dañado, manejo del N-RESET y cualquier otra cosa que la red pueda presentarle. Se puede notar que el hecho de tener un servicio de red sin conexión y sencillo, asocia toda la complejidad al protocolo de transporte.

La elección de la clase de protocolo que deberá utilizarse en una conexión dada, es determinada por las entidades de transporte en el momento que se establece la conexión. La parte iniciadora puede proponer una clase preferente y cero o más clases alternas. La parte contestadora entonces, eligirá de la lista proporcionada la clase de protocolo de transporte que utilizará. Si ninguna de las opciones ofrecidas es aceptable, la conexión se rechazará.

2.2.5 Capa 5: de sesión

La capa de sesión proporciona una forma por medio de la cual las capas de presentación y de aplicación establecen conexiones, estas son referidas como sesiones y transfieren datos sobre ellas en forma ordenada, repitiendo secciones que se consideran con error y permitiendo a los usuarios interrumpir el diálogo y continuar en cualquier momento posterior, intercambiando el control del diálogo entre dos entidades si se desea. Para realizar lo anterior la capa de sesión ofrece tres servicios: Administración de diálogo, sincronización y por último la administración de actividades.

- Administración de diálogo: en principio, todas las conexiones del modelo OSI son dúplex, es decir, los paquetes de información se pueden mover en ambas direcciones simultáneamente sobre la misma conexión. Sin embargo, hay varias situaciones en las que el software de las capas superiores está estructurado de tal forma que espera que los usuarios tomen turnos por lo que se convierte en semidúplex. Para este último caso, el hecho de mantener un seguimiento de a quién le corresponde el turno de hablar y hacerlo cumplir, es lo que se denomina administración de diálogo.

  Esta tarea de administración de diálogo se realiza mediante el empleo de un testigo de datos. Solamente el usuario que posee el testigo puede transmitir los datos.

- Sincronización. La sincronización se utiliza para llevar las entidades de sesión de vuelta a un estado conocido en caso de que exista un error o algún desacuerdo. Cabe hacer notar que la capa de transporte solo corrige los errores de comunicación, así como los fallos en las subredes pero no arregla los fallos que pueden ocurrir en las capas superiores.
- Administración de actividades: esta es una de las funciones estrechamente relacionadas con la sincronización. La idea de la administración de actividades

es la de permitir que el usuario divida el flujo de mensajes en unidades lógicas denominadas actividades. Cada actividad si se desea, es completamente independiente de cada una de las demás actividades.

La administración de actividades es la manera fundamental de estructurar una sesión. Por esta razón es primordial que las dos partes acuerden cuál será la estructura de la actividad.

El nivel de sesión proporciona el servicio de sincronización para sobreponerse a cualquier error que se detecte. En este servicio los usuarios pueden poner marcas de sincronización en el flujo de datos. Si se llegara a detectar un error, la conexión de la sesión podría restablecerse en un estado definido y los usuarios regresarían a un punto designado en el diálogo, se descartaría una parte de los datos transferidos y después se reiniciará a partir de ese punto. Si se desea, el nivel de sesión brinda la función de administración de la actividad. Usando esta función, el diálogo se puede segmentar en subconjuntos de actividad, donde cada uno puede ser identificado por separado si se quiere. Entonces el diálogo se puede interrumpir y continuar en cualquier momento comenzando en la siguiente actividad o sección de transferencia de datos.

2.2.6 Capa 6: de Presentación

Esta capa aísla los procesos de aplicación de la capa de aplicación de las diferencias en la representación y la sintaxis de los datos transmitidos. La capa de presentación se encarga de la preservación del significado de la información transportada, ya que cada estación puede tener su propia forma de representación interna de los datos, por lo que es necesario tener acuerdos y conversiones para poder asegurar el entendimiento entre diferentes estaciones. Estos datos a menudo toman la forma de estructuras de datos complejas. El trabajo de la capa de presentación consiste precisamente en codificar los datos estructurados del formato interno de la estación origen a un flujo de bits adecuado para la transmisión y después, decodificarlos para representarlos en el formato de la estación destino. Además el nivel de presentación debe iniciar y terminar una conexión, administrar los estados del nivel y manejar los errores.

La capa de presentación tiene las siguientes funciones principales:

- Ofrecer a los usuarios una manera de ejecutar las primitivas del servicio de sesión.
- Proporcionar una manera de especificar estructuras de datos complejas.
- Transformar los datos entre formas internas y externas

2.2.7 Capa 7: de Aplicación

Esta capa se asegura que los dos procesos de aplicación que cooperan para llevar a cabo el procesamiento de información deseado en ambos lados de la red, se entiendan entre sí. Además la capa de aplicación contiene los programas del usuario que hacen el trabajo para lo cual fueron adquiridos las computadoras. Estos programas utilizan la capa de presentación para sus necesidades de comunicación. Sin embargo, los programas que utilizan los servicios como la transferencia de archivos son tan comunes, que se han desarrollado normas para eliminar la necesidad de que cada compañía desarrolle las suyas, además de asegurar que todos ocupen los mismos protocolos normalizados.

Las actividades de estandarización de OSI se centran en los procesos comunes a todos los protocolos de aplicación los cuales son conocidos como elementos de servicio de aplicación común.

Se puede observar que el nivel de aplicación consiste de dos partes: los elementos comunes a todos los procesos que hacen la interfaz con el nivel de presentación y aquellos específicos que involucran la aplicación o aplicaciones en particular.

Se han desarrollado tres tipos de servicios y protocolos para el nivel de aplicación basados en los elementos comunes a todos los procesos: terminal virtual, protocolos para transferencia de archivos y servicios, y los de manipulación de trabajos. Además, también se han desarrollado protocolos de administración para el nivel de aplicación.

El servicio de terminal virtual: se utiliza, para ofrecer un acceso de terminal a un proceso de un usuario en un sistema remoto.

El servicio de archivo: brinda acceso remoto, administración y transferencia de información almacenada en forma de archivos.

El servicio de transferencia y manipulación de trabajos permite que se lleve a cabo el proceso distribuido de trabajos, involucrando las funciones de sumisión de trabajos, proceso de trabajo y control por monitoreo de trabajo.

CAPÍTULO 3
CONCEPTOS Y ESTÁNDARES DE REDES DE ÁREA LOCAL

3.1 Topología

El termino topología se refiere al camino en el cuál los nodos de la red son interconectados. Una topología es definida por el diseño de las ligas de comunicación y los elementos de interconexión, esto determina las diferentes rutas, que tal vez los datos utilicen para la comunicación entre cualquier par de estaciones. De esta forma las redes proveen un medio físico para interconectar los diversos dispositivos dentro de una área limitada.

La topología de una red persigue tres objetivos:
1. Proveer de un máximo posible de confiabilidad para asegurar una transmisión adecuada.
2. Conducir el tráfico por medio de la ruta mas óptima de la red entre la estación transmisora y la estación receptora.
3. Ofrecer al usuario final el mejor tiempo de respuesta posible.

Existen 4 topologías simples: bus, árbol, anillo y estrella; las cuales pueden servir como bloques para la construcción de redes que necesiten de una topología más compleja.

3.1.1 Topología de anillo

La topología de anillo, consiste en un conjunto estaciones, donde cada una es unida a la red por medio de un repetidor. Los repetidores son conectados por ligas punto a punto en un circuito cerrado. Por lo tanto, cada repetidor participa en dos ligas. Los repetidores son dispositivos relativamente simples, capaces de recibir datos que viajan a través de una liga y retransmitirlos bit por bit por la otra liga tan rápido como sean recibidos; los repetidores no cuentan con una memoria de almacenamiento o buffer. Las ligas son unidireccionales por lo que los datos son transmitidos en una sola dirección y orientados en el mismo camino.

Los datos son transmitidos por medio de paquetes, así por ejemplo, si una estación X desea transmitir un mensaje a una estación Y; la estación X dividirá el mensaje en pequeños paquetes que contienen una porción de los datos e información de control en la que se incluye la dirección de la estación destino. La estación X

esperará su turno de transmisión y entonces los paquetes serán insertados dentro del anillo uno cada vez; los paquetes fluirán en un sólo sentido a través de los repetidores. Cuando la señal es recibida por una estación, esta analiza el paquete de información y lo retransmite a la siguiente estación sobre la red. Una vez que la estación destino Y reconoce su dirección en el paquete recibido procede a copiarlo.

La topología de anillo ofrece un buen remedio para el problema de los llamados cuellos de botella, además de que la lógica para implementar esta topología es muy simple. La principal desventaja que tiene, es que ofrece un sólo canal que conecta a cada dos repetidores en el anillo; lo cuál indica que si una liga entre dos repetidores tiene una falla, toda la red se perderá.

3.1.2 Topología de bus y árbol

La topología de bus se caracteriza por tener un único medio de transmisión, al cual se unen todos los componentes de la red (no se requiere de conmutadores ni de repetidores por cada estación). Todas las estaciones se unen directamente a la línea de transmisión o bus por medio de una interfaz de hardware apropiada.

Una estación de trabajo al transmitir, inserta paquetes de información al medio de transmisión, estos paquetes se propagan por toda la longitud del bus y de esta manera son recibidos por todas las demás estaciones de trabajo unidas al medio.

La principal desventaja de la topología horizontal, es que existe un solo canal de transmisión para servir a todos los dispositivos sobre la red. En consecuencia, si se tiene una falla en el medio de transmisión se perderá el servicio en toda la red; otra desventaja que se tiene en esta topología, es la dificultad de aislar fallas de algún componente en particular que se encuentra conectado al bus. Además, la ausencia de puntos de concentración hace difícil la solución de problemas.

La topología de árbol es una generalización de la topología de bus. El medio de transmisión es un serie de ramificaciones que no cierran los ciclos. El diseño del árbol empieza en un punto conocido como la raíz (headend), de esta manera, uno o más cables empiezan a conectarse o ramificarse. Las ramas a su vez pueden conectar mas ramas para permitir realizar diseños más complejos. De la misma forma que en la topología de bus, una transmisión desde cualquier estación se propaga a través del medio y puede ser recibido por todas las demás estaciones.

Para ambas topologías, el medio es también conocido como multipunto, ya que todos los nodos sobre el bus o árbol comparten una liga de transmisión común, teniendo en cuenta que solo una estación puede transmitir a la vez, por esto se requiere de una forma de control de acceso para determinar cual estación puede transmitir la siguiente vez.

3.1.3 Topología de estrella

En la topología de estrella, cada estación es directamente conectada a un nodo central (referido de esta manera como acoplamiento en estrella) por medio de dos ligas punto a punto, cada una de transmisión en una sola dirección (una de salida y la otra de entrada al nodo central). Una transmisión desde cualquier estación de la estrella, entra al nodo central y es retransmitido por este hacia todas las ligas de salida. Aunque el arreglo de esta topología es físicamente una estrella, lógicamente se puede decir que es un bus colapsado : ya que la transmisión desde cualquier estación es recibida por todos las demás estaciones y solamente una estación a la vez puede transmitir completamente. De esta manera, las técnicas para el control de acceso al medio utilizado para la transmisión de paquetes en la topología de estrella, son las mismas utilizadas en las topologías de bus y árbol.

Existen dos maneras para la implantación de una topología en estrella. El caso de un **acoplamiento de estrella pasiva**; existe un enlace electromagnético dentro del nodo central, así cualquier transmisión de entrada se divide físicamente a todas las demás ligas de salida. En el caso de fibra óptica, la división es realizada, fusionando juntas un número de fibras, de esta manera la luz de entrada es automáticamente partida entre todas las fibras de salida; en el caso de par trenzado o cable coaxial se utiliza un acoplamiento transformador que reparte la señal de entrada en las diferentes conexiones de salida.

El otro tipo de topología de estrella, es el **acoplamiento de estrella activa**. En este caso existe una compuerta lógica digital en el nodo central, que actúa como un repetidor. Así los bits que llegan de cualquier línea de entrada, son regenerados automáticamente y repetidos sobre todas las líneas de salida. Si múltiples señales de entrada llegan simultáneamente, una señal de colisión es transmitida a todas las líneas de salida.

Esta topología es de las más utilizadas en los sistemas de comunicación de datos. El software de control no es complejo y el flujo de tráfico es simple, ya que todo el tráfico emana del nodo central que es el responsable de enrutar el tráfico a través de él, hacia los otros componentes. Además de ser el responsable de aislar fallas, lo cuál es relativamente sencillo ya que las líneas de transmisión pueden ser desactivadas independientemente y de esta manera identificar algún problema. Sin embargo, la red en estrella es vulnerable a los potenciales problemas llamados cuellos de botella y fallas en el nodo central de la estrella si el dispositivo utilizado no es debidamente seleccionado.

3.1.4 Topología de concentrador

Una variación de las topologías de bus y de anillo es la conocida como **topología de concentrador** (hub topology). Aún que esta topología tiene una apariencia de una topología en estrella, en la práctica el concentrador es simplemente un sistema de cableado de bus o anillo colapsado dentro de una unidad central. Los cables utilizados para conectar cada estación al bus o anillo son extendidos hacia afuera desde el concentrador central o hub. El **concentrador central** consiste simplemente de un conjunto de repetidores que retransmiten todas las señales recibidas desde una estación, hacia todas las demás estaciones de la misma manera que en las topologías de bus o anillo, por lo tanto, el concentrador central no desarrolla ninguna función de conmutación.

Por último cabe mencionar, que los concentradores pueden ser conectados en manera jerárquica o en cascada para formar una topología de árbol.

3.2 Medios de transmisión

3.2.1 Cable coaxial

A pesar de la creciente popularidad de los sistemas de cable de par trenzado y los cables de fibra óptica, el cable coaxial aun esta instalado en la mayoría de la redes locales existentes a causa de que por muchos años el cable coaxial fue la única opción viable que proporcionaba una transmisión segura, soportando múltiples productos para las redes de área local. Como resultado de esta base instalada, y las aplicaciones desarrolladas para esta, el coaxial es una buena alternativa actualmente, aunque a principios de los años 90 empezó a tener un declive.

3.2.1.1 Descripción física

El cable coaxial se compone de dos (o más, como se discutirá mas adelante) cables conductores contenidos en una simple envoltura. En el coaxial solo hay uno conductor sólido. Este conductor sólido (que se encuentra en el centro) es recubierto de un material dieléctrico no conductor, rodeando al material dieléctrico se coloca una malla trenzada conductora. La diferencia en la construcción de estos dos conductores, los lleva a tener características eléctricas distintas. Esta diferencia entre los dos conductores resulta en un circuito no balanceado, que ayuda a prevenir las interferencias EMI o crosstalk. Ambos conductores, tanto el central como el exterior son usualmente de cobre, cobre estañado, o cobre revestido de acero para dar firmeza.

El aislaste dieléctrico que separa el conductor interior y el conductor exterior puede hacerse de una espuma endurecida, un material sólido como el polietileno.

Estas diferencias pueden alterar la velocidad de propagación ligeramente y por eso se utilizan para diseñar cables específicos.

Los niveles de impedancia comunes para cable coaxial son de 50, 75 y 93 ohms. Estos diferentes niveles son diseñados para aplicaciones especificas únicas, esto se refleja generalmente en el hecho de que muchas aplicaciones basadas en el coaxial son especificadas por el tipo de cable coaxial que usan.

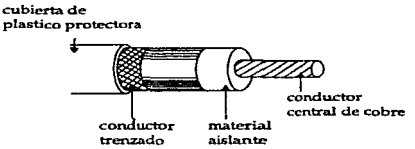


Figura 3.1 Tipo de cable coaxial

3.2.1.2 Tipos de cables coaxiales

Hay muchos tipos diferentes de cable coaxial, desde los que son usualmente diseñados para soportar aplicaciones especificas. Desafortunadamente, muchos desarrolladores de aplicaciones se decidieron por un tipo especifico de cable coaxial para cada aplicación que ellos desarrollaron. Por lo que en el mercado del coaxial no existe un estándar para los fabricantes de este. Esto es principalmente porque durante el período de gran desarrollo (los años 60's y 70's), no había muchas organizaciones de estandarización por lo que no existía el concepto de interoperabilidad. Muchos sistemas de redes estaban iniciándose y se desarrollaban como sistemas propietarios para venderse por un único vendedor, solo a través de la demanda de los usuarios y la necesidad de los vendedores esto a ocurrido con los medios de par trenzado y la fibra óptica.

3.2.1.2.1 Clasificación

Mirando los diferentes tipos de cables coaxiales disponibles hoy en día puede resultar en una confusión y algunas veces una evaluación contradictoria. Las diferencias pueden encontrarse en casi cada categoría: niveles de impedancia, tipos de conectores (jacks y plugs), diámetro del cable (AWG), número de blindajes, clasificación de cables tipo plenum, y el número de conductores centrales. Una falla en la elección de cualquiera de estos parámetros puede alterar drásticamente el manejo en la instalación de un cable en particular.

La diferencia mas común entre las características de los cables coaxiales es la clasificación RG de cables (RG: Radio Government - MIL-C-17, también RG/U: Universal). Esta clasificación indica un conjunto especifico de características físicas incluyendo la impedancia, el número AWG del conductor central, el espesor del aislante dieléctrico, el material y la configuración del blindaje, y el diámetro de la funda.

Mucha gente piensa erróneamente que la clasificación RG puede ser usado como un equivalente del AWG del par trenzado cuando se determina el tamaño del cable. Por ejemplo, el cable RG-8 (usado por las redes Ethernet de cable grueso) es aproximadamente dos veces el diámetro del cable RG-58 (usado para algunas otras redes Ethernet de cable delgado). Sin embargo, la única manera real de medir el diámetro es a través del número de clasificación AWG del conductor interior.

3.2.1.2.2 Tipos de cables coaxiales actuales

A continuación se presentara una lista de algunos tipos de los diferentes cable coaxiales disponibles hoy en día. La lista no esta basada en especificaciones técnicas, mas bien sobre los nombres comunes asociados a esto hoy en día.

Cable coaxial estándar: En el ambiente de las redes de datos, este se refiere a un cable con un único conductor central y uno o mas fundas. Un ejemplo del cable coaxial estándar es el cable RG-62 usado por las redes de área local (LAN's) IBM 3270 y ARCnet.

Coaxial Grueso (Thick coax): Es un termino aplicado al cable original coaxial, especificado para ser usado por la red Xerox Ethernet (IEEE 802.3 10Base5). El Coaxial grueso RG-8 (nonplenum) o RG-9 (plenum) consiste de un cable coaxial simple recubierto por una doble capa de aluminio y/o tipo de metal y cinta de poliester blindado.

Coaxial delgado (Thin coax): Este termino se aplica a una versión de cable coaxial especificado para Ethernet Xerox (IEEE 802.3 10Base2). El coaxial delgado es el RG-58 (nonplenum) o el RG-59 (plenum). El coaxial delgado es un forma estándar del cable coaxial consistente de un conductor central único y una malla conductora única. Este tipo de cable es también conocido como cable **thin-net**, desarrollando como una opción de cable mas delgado para Ethernet.

Coaxial Dual: El cable coaxial dual consiste de dos cables coaxiales individuales colocados en una funda común (ocasionalmente los dos cables son conectados independientemente a las mallas exteriores). No hay cambios importantes ocasionados por las características eléctricas con este arreglo físico del cable. La

razón principal para este arreglo en el cable es para ajustarse o acomodarse a redes que requieran dos conexiones independientes de los cables.

Twinax: El cable twinax es una variante importante del cable coaxial en la que hay dos conductores centrales trenzados (trenzados uno alrededor del otro) en vez del conductor sólido típico único. El cable twinax es muchas veces asociado con los productos de la red IBM 5250 Series/1 y frecuentemente son referencias como cables para datos.

Cable trunk: El cable trunk es un nombre general asociado con el Ethernet grueso (thick coax) o cable CATV.

Además de los cables coaxiales que se acaban de explicar, existen mas variantes menos comunes de cable coaxial disponibles para soportar todas los tipo la redes que usan cable coaxial que se producen hoy en día.

3.2.1.2.3 Conectores Plugs y jacks del cable coaxial

Así como hay numerosas variantes de cable coaxial, existen también un gran número de variantes de conectores para cable coaxial. Muchos tipos diferentes de conectores están disponibles con diferentes mecanismos de cerrado, como tipos de configuraciones físicas existen (como plugs de ángulo recto diseñado para conectar componentes con ángulos a 90 grados). Los componentes típicos del blindaje son de nickel-plateado con el conductor central compuesto de oro-plata para mejorar la conducción eléctrica. La siguiente lista muestra algunos de los conectores más comunes y sus cables asociados.

3.2.1.3 Aplicaciones comunes del coaxial

El uso del cable coaxial para la conexión de redes en las pasadas décadas a permitido a los fabricantes el desarrollar un gran número de aplicaciones para el cable coaxial. Estas aplicaciones corren a velocidades bajas de unos pocos megabits por segundo hasta altas velocidades (45 Mbps), son concentradas casi exclusivamente en aplicaciones de datos. El único sistema real que soporta voz, T-3, esta basado en redes de voz digital. La clasificación general de las aplicaciones de voz incluyen redes locales (LAN's), sistemas servidores y terminales, CATV (sistema de televisión por cable), sistemas de seguridad, y sistemas de datos de alta velocidad (T-3).

Redes locales LAN's de banda base: Muchos sistemas de LAN de banda base fueron originalmente desarrollados para operar sobre coaxial, ejemplos de esto son Ethernet y ARCnet. Los sistemas de banda base están disponibles en ambas

configuraciones, bus y estrella. La distancia soportada en esta configuración son típicamente de unos pocos miles de metros.

Redes locales LAN's de banda ancha: Los sistemas de LAN de banda ancha, tiene una distribución parecida a los sistemas de CATV, casi exclusivamente usan el cable coaxial como medio de comunicación. La configuración física para redes de banda ancha es de estrella (se puede ver también como una topología de árbol). Las redes LAN de banda ancha pueden soportar muchos miles de metros, desde la raíz del árbol (head-end) a una rama remota, este usa sistemas de amplificación de señales para regenerar la señal nuevamente.

Sistemas servidor-terminal: Muchos sistemas de servidor-terminal utilizan el cable coaxial para conectar los puntos del servidor a las terminales. Loa sistemas IBM 3270 y el Wang son dos ejemplos de este sistema.

3.2.1.4 Ventajas del cable coaxial

Aunque el cable coaxial ya no es considerado como el medio de transmisión preferido, hay algunas ventajas sólidas del cable coaxial. Esto es especialmente si la aplicación requiere cable coaxial o el cable de par trenzado no puede soportar las condiciones del ambiente. Algunas ventajas fuertes del coaxial incluye inmunidad a las señales de interferencia EMI, soporta una amplia variedad de sistemas de redes, una amplia base instalada fácil de unir y darle terminación.

Inmunidad al EMI: La estructura del coaxial, con el conductor central completamente cubierto por una malla conductora, brinda al coaxial una resistencia a las interferencias EMI y otras formas de interferencia de ruido.

Soporte en redes: El cable coaxial fue el medio preferido para redes de banda amplia. El coaxial provee un gran ancho de banda capaz de soportar las múltiples señales requeridas en los sistemas de banda ancha. A pesar de la popularidad del cable de par trenzado, las redes de banda base (por ejemplo, Ethernet, ARCnet) son aun soportadas sobre cable coaxial. Adicionalmente, hasta que la fibra óptica llegue a ser costeable y popular en los hogares, las redes de T.V. (CATV) seguirán utilizando cable coaxial.

Base instalada: La gran base instalada de cable coaxial ha ayudado a mantener un uso continuo en el soporte para las nuevas instalaciones con cable coaxial. Por ejemplo, muchos usuarios instalan coaxial para una nueva porción en la red existente si la red actual esta basada en cable coaxial. Dado que el cable coaxial fue el medio preferido por Ethernet por muchos años, esta base instalada no puede ser fácilmente desechada.

Simplificación en la terminación y unión: A pesar de lo voluminoso y lo poco flexible que es el cable coaxial, las uniones y terminaciones son fácil de hacer.

3.2.1.5 Desventajas del cable coaxial

Cuando los sistemas de comunicación de datos locales empezaron a desarrollarse, el cable coaxial fue la selección ideal como el medio de comunicación. Este ofrece distancias razonables, puede soportar múltiples tipos de redes y da una alta inmunidad al ruido (EMI). De cualquier manera, con el desarrollo de los sistemas de redes que soportan otro tipo de medios de cableado, las desventajas del coaxial han sido mas aparentes.

Reutilizable entre aplicaciones: Un importante punto a ser notar del coaxial es que no es lo mas ideal para los medios de comunicación entre diferentes aplicaciones. Por ejemplo, el cable usado para soportar CATV no puede soportar realmente las señales de Ethernet como fueron especificadas en el estándar Ethernet. Esto significa que los cables previamente instalados no siempre puedan ser rehusados para nuevos sistemas de redes.
Diámetro del cable: Comparándolo con el cable de fibra óptica, y aun el par trenzado, el cable coaxial es típicamente mas grueso en diámetro. Este tamaño del diámetro requiere espacio adicional en los sistemas de distribución del cableado, como son en los ductos y canaletas.

Costo en la instalación: La instalación del cable coaxial puede ser bastante cara a causa de las características físicas del cable y la topología en la instalación del coaxial en redes locales (LAN's). Entre mas grueso sea el cable coaxial decrece la flexibilidad y lo hace mas difícil para instalar en los ductos, especialmente si el ducto de distribución es pequeño o tiene muchas curvas (recodos). El cable coaxial para redes locales (LAN's) mas comúnmente instalado hoy en día es en Ethernet. Las redes Ethernet con coaxial están configuradas en una topología en bus. Esto significa que las instalaciones tienden a ser punto a punto entre los diferentes nodos del lugar (muchas veces localizados en lugares aleatorios dentro de la oficina).

Costo de los productos: El cable coaxial esta compuesto por múltiples capas de cable y material aislante. Este diseño en capas puede costar mas en la manufactura que un simple par trenzado hecho de un simple conductor cubierto de un simple aislante. Adicionalmente, los conectores plugs y jacks usados por el coaxial son típicamente voluminosos y hechos de metal. Este sistema de conectores por lo tanto son mucho mas caros para producir que un pequeño conector jack-RJ de plástico que es usado en el par trenzado sin blindar.

Limitaciones en las opciones de configuración: Dado el tamaño y la poca flexibilidad del cable coaxial, las opciones de configuración pueden ser limitadas en algunas instalaciones. Por ejemplo, en instalaciones donde el espacio en los ductos esta limitado no podrán permitir nuevas instalaciones. Esto contrasta con el gran numero de fibras ópticas y cables de par trenzado que pueden ser colocados dentro del mismo espacio.

Dificultad de mantenimiento y fallas: En las redes con cable coaxial, específicamente en la topología de bus, puede ser muy difícil el mantenimiento y la búsqueda de fallas. Por ejemplo, un cable roto en una red en bus puede deshabilitar la red completamente. Además, la localización de la ruptura puede ser difícil por el alto numero de cables derivadores (cables taps para la conexión de las estaciones) presentes en redes de bus ya que los cables derivadores pueden alterar o reflejar las señales de prueba.

3.2.2 Par trenzado

3.2.2.1 Descripción física

Las características que debe tener un cable par trenzado son:

Dos alambres de cobre aislados individualmente, los cuales son envueltos con PVC u otro tipo de plástico sintético o dieléctrico. El cobre es utilizado para transmitir datos digitales y analógicos, los cuales consisten en señales eléctricas.

El material de la envoltura consiste de un material dieléctrico que cubre al cobre de señales eléctricas conductivas externas. El par trenzado es, sin embargo, susceptible a campos magnéticos. Por esta razón, el par de alambres de cobre son encerrados individualmente dentro de un material aislante que los separa para que luego sean trenzados conjuntamente. El material aislante debe de llevar un esquema de codificación de color, el conjunto de colores representa el positivo y el negativo para cada par.

Los alambres tienen un diámetro de entre 20AWG y 26AWG. Estos son de cobre o acero cubierto por cobre. El cobre provee conductividad y el acero da firmeza. Un par de alambres actúa como una simple liga de comunicación.

Deben de mantener una proporción de trenzado circular por cada par; de entre 2 a 12 trenzados por cada 2.54 cm. El cuál ayuda a inmunizar al cable de ruido y crosstalk.

La característica de impedancia del alambre debe ser entre 90 y 110 ohms.

La envoltura exterior del cable par trenzado consiste de material dieléctrico que cubre al alambre de cobre de señales eléctricas conductivas externas, generalmente se utilizan materiales PVC o parecidos.

3.2.2.2 Tipos de cable par trenzado

Existen varios tipos de cables que tienen el nombre de par trenzado. Esos cables típicamente se diferencian en el estándar o en las características eléctricas del cable, Entre los más importantes se encuentran :

Par trenzado sin blindar (UTP: Unshielded Twisted Par): El par trenzado sin blindar, es el cable par trenzado típico, este no lleva ningún tipo de blindaje de metal siendo de esta manera más susceptible a interferencias electromagnéticas (EMI) o crosstalks.

Par trenzado blindado (STP: Shielded Twisted Par): Se llama así por que consta de una capa envolvente de malla trenzada o un conductor sólido, ambos de metal, el cuál es conectado a tierra por medio de cualquiera de los alambres de la malla o un alambre de drenado en el caso de conductor sólido. De esta forma se protege al cable par trenzado de las interferencias electromagnéticas (EMI) o crosstalk, las cuales causan interrupciones en la señal de comunicaciones, causando bits erróneos. Cabe notar que un escudo escaso altera las características eléctricas del cable.

Par trenzado Plenum Rating: Es llamado así por su característica de ser un cable aislado por un material que ha sido certificado para no exhalar humo tóxico cuando se quema o se calienta[6]. Por lo que es instalado a través de los ductos de calefacción o aire acondicionado en las oficinas. Los cables de tipo plenum no alteran las características eléctricas del conductor. Sin embargo decrementa la flexibilidad del cable debido a que incrementa su diámetro, además de que aumenta el costo. Se encuentra en versiones UTP y STP

Cables especiales: Esta categoría, incluye cualquier tipo de cable que mantenga las características físicas del par trenzado y sea manufacturado con un requerimiento específico conocido.

---

[6]Hay que tener en cuenta que existen varios tipos de cables par trenzado que son aislados con materiales del tipo PVC o una funda similar, por su bajo costo y características físicas (flexibilidad). Infortunadamente, el PVC y plásticos similares, exhalan humo extremadamente tóxico al quemarse o calentarse.

3.2.2.3 Estándares para cables par trenzados

3.2.2.3.1 El estándar AWG (American wire gauge)

Este estándar es una forma en la cuál se clasifica al cable par trenzado por el diámetro de los alambres que conforman los pares, este diámetro es medido en unidades AWG (es decir 24AWG, o 24 gauge).

Estándares Aplicables	EIA/TIA TSB-36 AWG	Categoría 3 24AWG	Categoría 4 24AWG	Categoría 5 24AWG
	Impedancia	100 ohms	100 ohms	100 ohms
	Frecuencia	1-16 Mhz	1-20 Mhz	1-100 Mhz
	Atenuación (máx.)			
	4 Mhz	17 dB/M'	13 dB/M'	13 dB/M'
	10 Mhz	30 dB/M'	22 dB/M'	20 dB/M'
	16 Mhz	40 dB/M'	27 dB/M'	25 dB/M'
Consideraciones Eléctricas	31.25 Mhz	-	-	36 dB/M'
	100 Mhz	-	-	67 dB/M'
	N.E.X.T* (min.)			
	4 Mhz	32 dB/M'	47 dB/M'	53 dB/M'
	10 Mhz	26 dB/M'	41 dB/M'	47 dB/M'
	16 Mhz	23 dB/M'	38 dB/M'	44 dB/M'
	31.25.Mhz	-	-	40 dB/M'
	100 Mhz	-	-	32 dB/M'

*Near-End Crosstalk

Tabla 3.1 Características

Las medidas comunes de AWG para cables tipo par trenzado son 22, 24 y 26. El AWG es una medida inversa donde el grado mas alto pertenece al cable de diámetro menor. Como el diámetro del cable incrementa, también se incrementa la distancia sobre la cual una señal puede viajar sin tener un incremento de perdida significante. Por esta razón, el cable tipo 22AWG es usualmente reservado para aplicaciones que requieran de una alta velocidad de transmisión de datos y que estos viajen a una gran distancia. El 24AWG es típicamente utilizado para aplicaciones de datos y voz. El cable 26AWG es caracterizado para transmisiones de distancia reducida.

3.2.2.3.2 El estándar EIA/TIA 568 - TSB-36

Dentro del estándar EIA/TIA 568 existe un boletín de especificación adicional llamado :

EIA/TIA Boletín de sistema técnico TSB-36 (Technical Systems Bulletin) en el cuál se definen las características de transmisión de alto desempeño para cables par trenzado sin blindar UTP. Encontrándose bajo es suplemento las especificaciones de los cables UTP categorías 3, 4 y 5.

3.2.2.4 Características de transmisión

Un par de alambres puede ser utilizado para transmitir datos de señales digitales como analógicas. Para señales analógicas se requiere de un amplificador cada 5 o 6 kilómetros, para señales digitales se utilizan repetidores cada 2 o 3 kilómetros.

Comparado con otros medios de transmisión, el par trenzado esta limitado en distancia, ancho de banda (bandwidth) y proporción de datos transmitidos.

Los factores más importantes que influyen para la selección de una configuración para una aplicación específica que utiliza cable par trenzado son los siguientes:

- La distancia que el cable va a cubrir.
- La cantidad de EMI dentro de la ruta que el cable va a cubrir.
- La proporción de conducto de aire, o carencia de uno, para la distribución de la ruta del cable.
- La fuerza física que tal vez tenga lugar sobre el cable.

En adición a las diferencias básicas en las características físicas del cable par trenzado puede haber diferentes características eléctricas permitidas por el mismo tipo de cable físico. Por ejemplo los proveedores AT&T y Northern Telecom ofrecen un alto desarrollo de datos en versiones de 24AWG par trenzado sin blindar. Este cable incrementa grandemente la distancia permitida para la transmisión de una LAN encima de un cable convencional con las mismas características físicas (es decir que el par trenzado sin blindar UTP convencional). Esto es que estos cables especiales permiten altas velocidades en la transmisión de datos para operar sobre par trenzado sin blindar.

Varias medidas han sido tomadas para reducir los impedimentos del cable par trenzado tales como: cubrir los alambres con una malla metálica para reducir la interferencia el tipo conocido STP. El trenzado de los alambres reduce la interferencia a baja frecuencia, y el uso de diferentes longitudes del trenzado en pares adyacentes reduce el crosstalk. Otra técnica es el uso de una línea de transmisión balanceada. Con una línea desbalanceada, un alambre tiene potencial a tierra; con una línea balanceada ambos alambres tienen un potencial por arriba del potencial de tierra, llevando señales con la misma amplitud pero fase opuesta.

3.2.2.5 Aplicaciones más comunes del par trenzado

El cable par trenzado ha llegado a ser una parte fundamental en cualquier tipo de construcción de sistema de cableado. Ya que es el medio para diferentes tipos de aplicaciones que van desde los sistemas PBX a redes locales LANs.

Sistema de redes de área local LAN:
Las redes de área local comúnmente llamadas LAN's han llegado a ser la forma más común de instalación para redes de computadoras hoy en día. Ellas ofrecen un amplio rango de opciones de configuración para conectar una gran variedad de dispositivos de cómputo. Algunas de las más comunes redes locales funcionan sobre par trenzado incluyendo las siguientes estándares:

Estándar	Cable par trenzado que utiliza
IEEE 802.3 Ethernet	Par trenzado blindado o sin blindar
IEEE 802.5 Token ring	Par trenzado blindado
ARCnet	Par trenzado sin blindar
Appletalk	Par trenzado blindado o sin blindar
Star LAN	Par trenzado sin blindar

Tabla 3.2 Tipo de cable par trenzado utilizado por las redes LAN mas comunes

3.2.2.6 Ventajas del par trenzado

Múltiples recursos del producto: Existe actualmente una gran demanda por el cable par trenzado. Con muy pocas excepciones. Cada construcción tiene una cierta cantidad de par trenzado instalado, en respuesta a la demanda universal por este producto, una multitud de vendedores son actualmente disponibles para proveer productos de par trenzado. A continuación mencionamos algunas de las ventajas del par trenzado.

Bajo costo: Dado el gran número de proveedores que venden y además dan servicio para par trenzado, viene a darle una característica orientada al mercado, ya que cables y productos que se venden para este cable son completamente universales y tiene un grado altamente competitivo en las áreas de mercado.

Planificación de configuración simplificada: La mayoría de los sistemas de voz o datos con par trenzados, son cableados en una configuración de tipo estrella con un concentrador central. Esta topología es muy fácil para planear y modelar. Además de que se ofrece un gran aprovechamiento de la configuración de red simplificando así la instalación.

Personal de instalación calificado: Dado el gran número de proveedores que dan soporte al par trenzado y a la gran demanda de los productos, existe una gran cantidad de personal calificado, disponible para instalaciones de par trenzado. Las compañías telefónicas, han desarrollado procedimientos detallados y conjuntos de instrucciones para capacitar personal de instalación.

Instalación fácil: El cable par trenzado, es relativamente fácil de instalar en muchas situaciones, incluyendo nuevas construcciones y renovación del cableado en edificios. esto es debido a su pequeño diámetro y extrema flexibilidad.
Resolución de problemática simplificada: La configuración de topología tipo estrella con un concentrador central en las instalaciones de par trenzado, hace que sea fácil predecir los defectos en la instalación y ayuda a simplificar la solución. Ya que en una topología como esta, si un cable llega a dañarse, es muy fácil aislarlo y repáralo por separado.

Proveedores de soporte y equipo: La tendencia por coaxial a cambiado drásticamente en los años recientes. Predominantemente como resultado de la demanda de los consumidores, muchos vendedores han tenido que modificar sus sistemas de interconexión para poder soportar cualquiera de los tipos de par trenzado : par trenzado blindado (Shielded) o par trenzado no blindado (unshielded). Los productos tales como adaptadores de medios permiten al par trenzado remplazar segmentos de cable coaxial en diferentes arquitecturas. Nuevos estándares de interconexión de redes, tales como el IEEE 10BaseT, permiten a sistemas como ethernet soportar par trenzado blindado en ambientes que solo hace pocos años podían requerir cable coaxial delgado. Cada vez más vendedores están reorganizando la apelación universal de cables de par trenzado y diseñando nuevos sistemas que soporten este medio de transmisión.

3.2.2.7 Desventajas del cable par trenzado

Limitación en el rendimiento de datos: El cable par trenzado, mientras que ofrece varias ventajas, tiene varias desventajas. Una de las mas importantes es la imperfección que envuelve en el rendimiento de los datos en comparación con otros tipos de medios de transmisión. Mientras que el cable coaxial y la fibra óptica pueden ofrecer proporciones de transmisión arriba de 45 a 600 megabits por segundo (Mbps) el par trenzado está limitado de 16 a 20 Mbps.

Limitaciones de distancia: En los ambientes de sistemas de voz analógicos PBX pueden soportar hasta miles de pies entre la terminal telefónica y el procesador PBX. Sin embargo más sistemas de datos son restringidos a cientos de pies de distancia entre la estación de trabajo del usuario final y el concentrador central de proceso. Esta restricción frecuentemente puede poner varias limitantes sobre la configuración de sistemas de datos, si la construcción del sistema de cableado no fue diseñada originalmente pensando en las limitaciones del cable par trenzado.

Susceptibilidad a interferencias: El par trenzado es muy susceptible a EMI. Las señales EMI pueden ser causadas por varias razones incluyendo líneas de poder, maquinaria no blindada u otro par trenzado. El resultado de esta susceptibilidad puede incrementar errores sobre una señal de comunicaciones. Para sobreponerse

a esto, existen el tipo de cable par trenzado blindado (Shielded twisted par). Sin embargo, estos sistemas aun no proveen estabilidad e inmunidad a EMI que el coaxial y la fibra óptica ofrecen hoy en día.

3.2.3 Fibra óptica

Para transportar cualquier señal es necesario un medio de transmisión, por ejemplo para transportar voz podemos utilizar microondas, señales eléctricas, etc. Pero en el caso de transportar señales que llevan información importante, debemos de elegir un medio seguro para hacerlo.

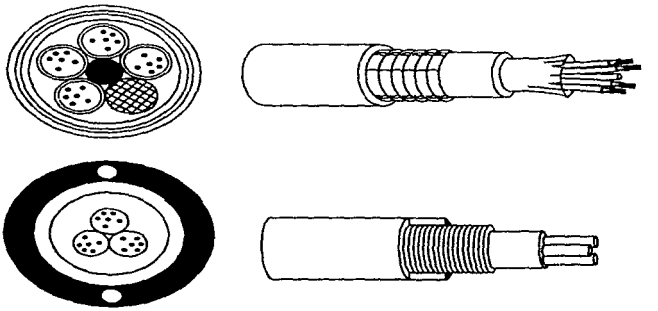


Figura 3.2 Cables OSP y de cinta vertical

La esencia de la fibra óptica es la canalización de los rayos de luz a través de "caminos de fibra óptica" y la generación de frecuencias de luz apropiadas.

Una de las tecnologías más importantes en transmisión de información ha sido el desarrollo de sistemas de comunicación por fibra óptica. Las partes principales de los sistemas de comunicación de fibra óptica son el transmisor, la fibra y el receptor.

La razón por la cual la fibra óptica se volvió económicamente viable, fué en parte que el **láser**, construido en 1959, había alcanzado cualidades suficientemente buenas en lo que a expectativa de vida y precio se refiere y por otra parte que las fibras ópticas habían alcanzado bajos valores de atenuación.

Gracias a los trabajos de Charles Kao, la técnica de procesamiento de la fibra óptica se incrementó drásticamente hacia la mitad de la década de 1960, por lo que la pureza de la materia prima aumentó y la atenuación disminuyó. De una atenuación de 1000 dB/km, hacia 1980 había sido reducida a 0.2 dB/km. Como una comparación se puede mencionar que los cables coaxiales comunes tienen una atenuación de 5 dB/km (alrededor de 20 dB/km, a las más altas frecuencias usadas en la actualidad).

No sólo se ha mejorado el comportamiento óptico de los cables de fibra, sino también su comportamiento mecánico, es decir, su capacidad para soportar tirones, compresiones, torciones y flexiones.

3.2.3.1 Descripción física

La fibra óptica es una especie de filamento mucho más delgado que un cabello, flexible, generalmente las fibras esta hechas de sílice (combinación de silicio y oxigeno), y algún tipo de vidrio, pero este vidrio es de muy alta calidad, el cual es capaz de transportar rayos de luz en su interior de una manera determinada.

La fibra óptica consiste de dos porciones sólidas: el núcleo y el revestimiento, estas dos porciones no pueden ser separadas. La luz viaja a través del núcleo mientras el revestimiento guarda la luz contenida dentro del núcleo. Esto es realizado para tener índices diferentes de refracción entre el núcleo y el revestimiento.

El núcleo que consiste de vidrio o cuarzo, tiene un índice de refracción mas alto que el revestimiento de vidrio, cuarzo o plástico que lo rodea.

A su vez la superficie del revestimiento esta protegida por otras 4 capas más que son: Recubrimiento primario, aire o petrolato, recubrimiento secundario y una cubierta protectora.

Recubrimiento primario. Cuando la fibra es manufacturada, esta es inicialmente protegida con un recubrimiento primario. Este es típicamente hecho de acrílico y existe sobre todas las fibras virtualmente. El propósito del recubrimiento primario es para darle más fuerza a la fibra, durante el cableado, el empalme y al poner los conectores. El diámetro de esta capa primaria es de aproximadamente 250 µm.

También tiene aire o petrolato entre la cubierta primaria y el recubrimiento secundario, esto es para que se encuentre libre y manejable. El recubrimiento secundario que mide aproximadamente 1 mm.

Por último tiene una cubierta protectora que mide 2.5 mm aproximadamente. La fibra queda entonces protegida contra esfuerzos mecánicos debidos al cableado, instalación, cambios de temperatura, etc.

El tamaño de la fibra óptica es dado con dos números: El diámetro del núcleo y el diámetro del revestimiento, respectivamente. Por ejemplo 62.5/125 μm es una fibra con un núcleo de 62.5 μm y tiene un diámetro de revestimiento de 125 μm.

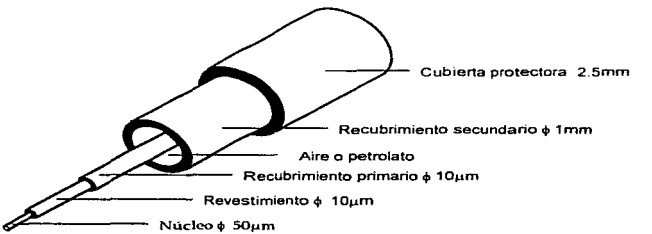


Figura 3.3 Descripción física de un cable de fibra óptica

Transmisión

La fibra óptica transmite una señal codificada irradiando luz por medio de reflexión interna total. Esta puede ocurrir en cualquier medio transparente que tenga un índice alto de refracción que lo rodee, en efecto, la fibra óptica actúa como una guía de onda para frecuencias en el rango de 10^{14} a 10^{15} Hz el cual cubre el espectro visible y parte del espectro infrarrojo.

La forma de propagación es llamada multimodo porque se refiere a la variedad de ángulos que refleja. Cuando el radio del núcleo de la fibra es reducido pocos ángulos serán reflejados. Para reducir el radio del núcleo al de una guía de onda, solamente un ángulo o un modo podrá pasar.

Debido a la manera de transmisión es como se clasifican a las fibras, sólo que para fines prácticos nos referiremos a la de índice escalonado como multimodo.

Los modos de transmisión de la fibra óptica son los siguientes:

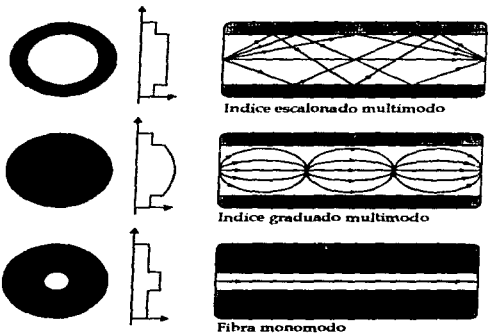


Figura 3.4 Índice escalonado multimodo, Índice graduado multimodo y fibra monomodo

3.2.3.3 Tipos de fibras ópticas

Existen dos clases de fibras la monomodo y la multimodo.

Monomodo: Se dice que una fibra óptica es monomodo cuando sólo consideramos una frecuencia de luz para transmitir, ya que el diámetro del núcleo es muy pequeño.

La fibra monomodo presenta grandes ventajas en cuanto a distancia, por ello es preferida por las grandes compañías de comunicaciones.

Las razones de preferencia son :

- Garantía de la instalación una sola vez por 20 años de vida.
- Funcionalidad al costo más bajo, ofreciendo una transmisión con un ancho de banda máximo.
- Capacidad de actualización para servicios futuros de consumo de gran ancho de banda.
- Calidad de transmisión superior por la ausencia de ruido.
- Compatibilidad con tecnología óptica integrada.

Sólo que esta es más cara que cualquiera otro tipo, esto es porque necesita de una fuente de luz láser.

Multimodo: Se dice que una fibra óptica es multimodo, si bien el diámetro del núcleo o los índices de refracción del núcleo y de la cubierta son mayores que los límites establecidos para la operación en monomodo.

Cuando se trabaja en multimodo habrá muchos rayos de luz diferentes (cada una de ellos viajando con un ángulo de reflexión distintos, pero siempre menores que el ángulo crítico) viajando a lo largo del núcleo.

Las fibras multimodo tienen principal utilidad en distancias cortas, tal es el caso de las redes locales. Y para tener mayor referencia de esta utilidad conviene revisar la tabla siguiente:

	Multimodo	Monomodo
Diámetro del núcleo (μm)	50 a 125	2 a 8
Diámetro del revestimiento (μm)	125 a 440	15 a 60
Ancho de banda	ancho más de 200 Mhz/km	muy ancho de 3 a 50 Ghz/km
Empalme	difícil	difícil
Aplicación típica	Liga de datos en redes	líneas de telecomunicaciones
Costo	no muy caro	muy caro
Fuente de luz	láser o LED	láser

Tabla 3.3 Características principales de los tipos de fibra óptica monomodo y multimodo

Se observa que la gran diferencia en cuanto a redes locales radica en lo caro del tipo monomodo y esto se debe principalmente a la fuente de luz, esto es algo que se revisa a continuación.

3.2.3.4 Transmisores ópticos

El transmisor óptico convierte las variaciones de las señales eléctricas en variaciones de potencia luminosa. Las variaciones en la intensidad luminosa se obtienen por modulación digital, la cual es más común.

Existen dos tipos diferentes de fuentes de luz que son usados en los sistemas de fibra óptica. Los diodos láser (LD) y los diodos emisores de luz (LED) se usan como convertidores electro-ópticos, estos son dispositivos de estado sólido que emiten luz cuando una corriente es aplicada. El láser tiene un ancho de banda de aproximadamente 1000 Ghz, el diodo emisor de luz aproximadamente 10 000 Ghz.

El gran ancho de banda de las fuentes de luz no es una gran desventaja teniendo en cuenta las demandas de comunicaciones que existen o que pueden existir en el futuro.
La característica de transferencia de un LED es lineal, mientras que la de un LD es no lineal. Tanto para el LD como para el LED la longitud de onda se elige para que exista un baja atenuación en la fibra y para que caiga dentro del rango de sensibilidad del detector. A continuación se comparan el LD y LED

	LD	LED
Longitud de onda	800-900 nm	800-900 nm
Ancho espectral	1-2 nm	30-40 nm
Potencia de salida disponible	5-15 mW	1-5 mW
Pérdida de inserción	3 dB	15-20 dB
Frecuencia de modulación	1000 Mhz	50-100 Mhz
Expectativa de vida	10^{4} a 10^{5} horas	10^{5} a 10^{6} horas

Tabla 3.4 Tabla de comparación del LD y LED

Aún cuando el diodo emisor de luz, en muchos aspectos, tiene un comportamiento inferior al del diodo láser, su dependencia con la temperatura es mucho menor y sobre su rango de temperaturas de 100 K (grados Kelvin), su potencia de salida varia en un factor menor que 2. En consecuencia no se necesita ninguna, o muy poca, estabilización de temperatura. Más aún se puede obtener un LED con una buena expectativa de vida, a un precio mucho más bajo que el correspondiente al láser.

3.2.3.5 Tipos de cable/fibra

En cualquier aplicación práctica de tecnología de la guía de onda óptica, las fibras necesitan ser incorporadas en algún tipo de estructura de cable. La estructura de cable variara enormemente, dependiendo si el cable es subterráneo o ductos intraedificios o submarinos. Diseños diferentes de cables son requeridos para cada tipo de aplicación, pero fundamentalmente los principios de diseños del cable son requeridos para cada caso. El objetivo de manufacturar cables ha sido que los cables de fibra óptica deberían instalarse con el mismo equipo, técnicas de instalación y precauciones como las que son usadas en cables convencionales. Estas requieren diseños de cables especiales por propiedades mecánicas de las fibras de vidrio.

Un cable óptico consiste principalmente de varias fibras ópticas y a veces, de algunos conectores metálicos. Estos quedan bien protegidos contra las influencias metálicas y químicas y en alguna forma protege a la fibra también contra los cambios bruscos de temperatura.

En los cables de telecomunicaciones se usan generalmente una lamina de aluminio y vaselina como protección contra la humedad y alambre de acero para aumentar la resistencia a la tracción.

En algunos cables se usan conductores metálicos para alimentar eléctricamente a los repetidores y con propósito de supervisión del funcionamiento.

Una propiedad mecánica importante es la máxima carga axial permisible sobre el cable, ya que este factor determina la longitud del cable que puede ser instalado confiablemente. En cables de cobre los alambres por si mismos son generalmente los miembros principales de transportación y carga del cable, y elongaciones de más del 20% son posibles sin fractura. Por otro lado, fibras ópticas sumamente fuertes tienden a romperse a elongaciones de 4%, mientras fibras típicas de buena calidad de 0.5% a 1%. Desde que la fatiga estática ocurre muy rápidamente a niveles de tensión arriba del 40% de la elongación permisible y muy despacio abajo del 20% del limite de rompimiento, elongaciones durante la manufactura e instalación debería estar limitado a 0.1 a 0.2%.

Existen varios tipos de cable que están disponibles para proteger las fibras y cumplir con los requisitos de instalación, este entorno de instalación es el que van a determinar la selección del tipo de cable, la clase de vaina y los diseños de núcleo de aire o núcleo de relleno

El cable de planta externa (OSP). Se usa para la instalación aérea, subterránea y enterrada directa además para el cable de entrada al edificio. En este cable pueden ir fibras monomodo o multimodo. Ofrece también distintos diseño de núcleo de cable, cinta y trenzado y con una variedad de opciones de vaina.

El cable de cinta vertical. Es semejante al cable OSP en diseño, pero es construido de materiales pirorretardantes y valorado para edificios.

El cable para edificio de guía de luz (LGBC). Esta diseñado para usarse en distribuciones dentro de edificios, son típicamente utilizados en conductos ascendentes y en planos. El cable contiene desde una hasta doce fibras individuales codificadas por color, las fibras se encuentran flotando libremente dentro de un tubo separador y en el centro se encuentra un bloque contra agua y esta cubierto por una envoltura que protege de los rayos ultravioleta.

3.2.3.6 Conectores

Los conectores son usados para unir los cables de fibra a los equipos terminales, y realizar diferentes tipos de arreglos en las redes (topologías). En este caso varias terminales son conectadas entre sí y además estas a uno o más servidores.

Lo sistemas de fibra óptica permiten una expansión rápida en varias áreas. Los conectores entonces toman un papel importante, ya que estos tiene que estar bien diseñados, de tal manera que permitan facilidad y rapidez de instalación, a un costo muy bajo, manteniendo su rendimiento alto.

3.2.3.6.1 Fenómenos de pérdidas en los conectores

Separamos los factores que causan las pérdidas ópticas en dos categorías. La primera incluye factores Extrínsecos a la fibra, como el "offset" lateral entre núcleos, reflexión, resultados inexactos relacionados directamente al diseño del conector y control de fabricación. La segunda categoría, factores intrínsecos , son relacionados directamente a las propiedades particulares de dos fibras ópticas que están siendo interconectadas. Estos factores incluyen mal ajuste en el núcleo, desigualdad en los índices de contorno y forma elíptica del núcleo.

Además de estos factores, la eficiencia del acoplamiento de un conector también puede depender de la longitud de onda de la fuente óptica, y en el caso de fibras multimodo, del espaciamiento relativo de la fuente óptica y las características de la atenuación de modo diferencial de las fibras.

3.2.3.7 Empalme

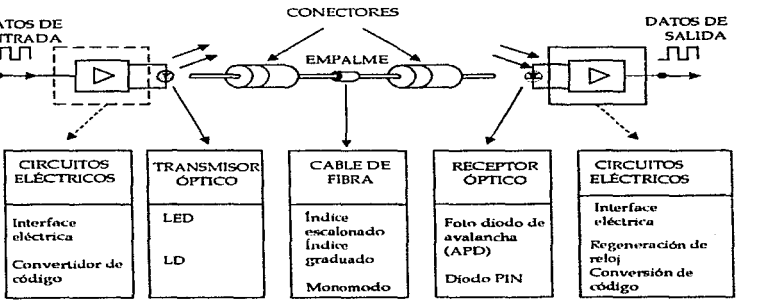


Figura 3.5 Enlace de fibra óptica

Un empalme es una unión permanente de dos cables ópticos. Las mas importantes exigencias para un empalme son:

- ejecución fácil, rápida y barata
- baja atenuación

El empalme puede ser pegado usando elementos simples, pero este método toma tiempo. Generalmente el empalme se realiza por fusión usando aparatos especiales obteniéndose buenos resultados por medio de la fusión con arco eléctrico

Las dos superficies del cable desmantelado son acercados, puestas en intimo contacto y fusionadas por medio de un arco eléctrico de corta duración. La tensión superficial del vidrio fundido tiende a ajustar el posicionamiento de los extremos de la fibra.

Tanto el método de fusión como el de pegado dan bajas atenuaciones del orden de 0.1 a 0.2 dB por empalme.

3.2.3.8 Aplicaciones

La fibra óptica pueden ser usadas para señalización, transmisión de información e incluso en aplicaciones de control. En este tipo de aplicaciones de corto alcance las pérdidas se pueden considerar como tolerables. Los estudios realizados demuestran que en estas aplicaciones pueden admitirse pérdidas de entre 50 y 100 decibeles por kilómetro.

Para demostrar la capacidad de la fibra óptica en comunicaciones de voz, video y señales de datos computarizados, se realizó en 1977 una instalación en Chicago por la Bell Telephone System conectando dos oficinas centrales. Se utilizaron láseres y LEDs para transmitir la luz y fotodiodos de avalancha para convertir de nuevo en señales eléctricas. El sistema tuvo tanto éxito, que a partir de entonces se desplegaron grandes esfuerzos hacia el uso de la fibra óptica .

Dado que el ambiente actual de las redes está en constante cambio y las aplicaciones de computación de mayor complejidad requieren de mayores velocidades de transmisión de datos se debe tener un cableado capaz de aceptar esta tarea. El cableado de fibra ofrece estas cualidades

En cuanto a sistema de redes de área local LAN: ofrece un rango grande de opciones de configuración, como las mostradas en la tabla 3.5.

Topología
Bus
Anillo
Estrella

Tabla 3.5 Topologías que se pueden realizar con cable de fibra óptica

3.2.3.9 Ventajas

Las principales ventajas de la fibra óptica sobre los sistemas de cableado son la baja atenuación, y el ancho de banda tan grande disponible. Y como la atenuación es baja, pueden ser alcanzadas distancias grandes entre repetidores.

Podemos decir que no es peligroso el cableado con fibra óptica, ya que no existe el riesgo que una chispa pueda provocar un incendio, o algo similar. Aun que siempre debemos tener precaución con los conectores (pero una vez que estos quedan conectados ya no hay riesgo)

También ofrece ventajas significantes en cuanto al tamaño y al peso ya que un sistema de fibra reduce hasta 30 veces su tamaño con respecto al cable de cobre, con ello también se beneficia su funcionamiento, dado que podemos cablear en lugares o edificios muy reducidos, sin tener la limitante de construir nuevamente el edificio para tener una red funcionando.

Debido a que la fibra es un medio dieléctrico, es inmune a la electricidad, a la interferencia electromagnética (EMI) y a la interferencia de frecuencias de radio (RFI), la retroreflexión no existe.

La fibra es el medio más económico para transmisión de varios canales de voz, vídeo y datos de alta calidad a largas distancias, es por ello que la transmisión vía fibra óptica abre un nuevo concepto en los sistemas de comunicación. La tabla que se muestra a continuación nos presenta una comparación ente cables de fibra óptica contra cables de cobre de alto rendimiento.

	Fibra óptica	Coaxial
Distancia de transmisión	1000m (MM) o10,000m (SM)	200m
Distancia de transmisión para LANs	2000m	500m
Ancho de banda	500Mbps (MM) a multigigabit (SM)	100Mbps
Ancho de banda para LANs	200 Mhz/Km	100Mbps
Retroreflexión	Ninguna	44dB
EMI	Ninguna	Problema

Tabla 3.6a Tabla comparativa entre cable de fibra óptica y cable coaxial

	Fibra óptica	Coaxial
RFI	Ninguna	Problema
Fallas a tierra, rayos eléctricos.	Ninguna	Gran Problema
Seguridad	Segura	Gran Problema
Apoyo de multimedios	Sí	Cuestionable
Facilidad de identificación de fallas/pruebas de instalación	Simple	Difícil
Duración (tiempo de vida)	10 a 15 años	3 a 5 años

Tabla 3.6b Tabla comparativa entre cable de fibra óptica y cable coaxial

3.2.3.10 Desventajas

La desventaja que puede existir es la fragilidad (para el caso de cables de unión). Pero en general debido a la tabla que se presenta en el punto anterior no podemos hablar de desventajas propiamente (ya que es con respecto a los medios ya existentes), otro aspecto que cabe mencionar es que este medio (fibra óptica) se estaría desperdiciando en el caso de utilizar muy poco este canal, es decir transportar poca cantidad de información, por lo que puede resultar en ciertos casos caro.

A continuación se apuntan algunas limitantes que se tienen, pero aclarando que utilizando otros medios estos límites se incrementan (referirse tabla)

Existen dos factores que limitan la utilidad de la fibra óptica para comunicaciones. La primera es la atenuación, esta es siempre un nivel de transmisión máximo y un nivel mínimo útil recibido . La diferencia entre estos es la perdida total, la cual es debido a la atenuación de la fibra. La atenuación de la fibra es expresada en dB/km, limita la máxima distancia entre el transmisor y el receptor.

El otro factor limitante es el ancho de banda. La fibra óptica tendrá un ancho de banda máximo para señales que son transmitidas mediante la fibra sin distorsión. El ancho de banda limita el valor a el cual la señal puede cambiar su intensidad u otros parámetros de la señal, y así el valor para el cual la información puede ser transmitida.

3.2.4 Medios de transmisión para redes inalámbricas

Todos los medios de transmisión mencionados anteriormente han sido para transmitir la información. Sin embargo los datos pueden ser transmitidos usando frecuencias electromagnéticas (radio) o rayos infrarrojos, a través de espacios libres, como sistemas satelitales o de radio.

3.2.4.1 Radio

Radio transmisión de baja frecuencia se utilizada en lugar de enlaces de cable fijos, para cubrir áreas de transmisión más cortas. Utilizando bases de transmisión y recepción en tierra.

En este tipo de transmisión, un radio transmisor conocido como estación base, es localizado al lado del punto de terminación de cable fijo. proveyendo una liga sin alambrado físico entre cada computadora y el sitio central.

Múltiples estaciones base pueden ser utilizadas para aplicaciones que requieren una área de cobertura mayor o una densidad alta de usuarios. El área de cobertura de cada estación base es restringida, al estar limitada su potencia de salida. De esta manera la estación base provee solo los canales suficientes para soportar la carga total de esa área. Para cubrir un área mas amplia, es llevado a cabo un arreglo de múltiples estaciones base, lo que es llamado una estructura de celda. En la práctica, el tamaño de cada celda varia y es determinado por algunos factores como la densidad terminal y el terreno local.

En la estructura de celdas, cada estación base opera utilizando una banda diferente de frecuencias que la utilizada por sus vecinos, sin embargo, el campo de cobertura de cada estación base es limitado, por lo que hace posible reutilizar la banda de frecuencia en otras partes de la red. Normalmente, la proporción de datos utilizable disponible para cada una de las computadoras dentro una celda es de decenas de miles de bits por segundo.

Un arreglo similar puede ser utilizado dentro de una construcción para proveer ligas sin cordones para equipos basados en computadoras dentro de cada oficina. En tales casos una o más estaciones base son localizados sobre cada uno de los pisos y conectada a la red fija. Cada estación base entonces provee ligas sin cordón a la red fija para todos las computadoras en su campo de cobertura. Claramente, esto evita cablear cada vez que una nueva computadora sea instalada o que sea movida a otro punto dentro del edificio. Las desventajas que se pueden observar, es el costo de proveer una unidad de radio para convertir los datos de entrada en una señal de radio. Así también, la proporción de datos de transmisión es frecuentemente mas baja que la ofrecida por un cable fijo.

Este tipo de medios de transmisión, puede ser caro comparado a la instalación de cableado de alambre fijo para cada aplicación. De aquí que el radio es frecuentemente utilizado para proveer una liga sin cordón entre un punto de terminación de la red con alambre fijo y las computadoras distribuidas.

3.3 Protocolos de control acceso al medio

Todas las redes locales consisten en una colección de dispositivos que deben compartir la capacidad de transmisión de la red. Por esta razón es necesario tener un control de acceso al medio de transmisión para que dos dispositivos particulares puedan intercambiar datos cuando sea requerido dentro de un esquema centralizado o distribuido.

En un esquema centralizado, se designa un controlador con la suficiente autoridad para garantizar el acceso a la red. De esta manera, una estación que desee transmitir deberá esperar a recibir el permiso del controlador. En una red decentralizada, las estaciones colectivas desarrollan una función de control de acceso al medio para determinar dinámicamente el orden en el cuál transmitirán las estaciones.

En general se puede clasificar a las técnicas de control de acceso en síncronas y asíncronas. Con las técnicas síncronas, una capacidad especifica es dedicada para realizar una conexión (se utiliza en redes locales de circuitos conmutados, cabe mencionar que no son muy óptimos para redes LANs y WANs por que las necesidades de transmisión de las estaciones se puede decir que son impredecibles). Otra forma de realizar una conexión mas eficazmente para redes locales, serían las técnicas asíncronas. Las cuales se pueden subdividir en tres categorías : round robin, reservación y contención.

- **Round Robin:**

Esta técnica es basada en la filosofía de darle a cada quien un turno. Cada estación en turno se le da la oportunidad de transmitir. Durante este turno la estación puede declinar la transmisión o puede transmitir sujeto a un cierto límite. El control en esta técnica puede ser de modo distribuido o centralizado.

- **Reservación:**

En esta técnica, el tiempo sobre el medio de transmisión es dividido dentro de ranuras (frames). Una estación que desea transmitir, reserva ranuras futuras para un período indefinido. La reservación de las ranuras puede llevarse a cabo de una manera distribuida o centralizada.

- **Contención:**

Con esta técnica no se ejerce el control para determinar que estación tiene derecho a transmitir. Todas las estaciones contienden por el tiempo. Esta técnica es necesariamente distribuida..

	Topología en Bus	Topología en anillo
Round Robin	Token Bus (IEEE 802.4)	Token Ring (IEEE 802.5, FDDI)
Reservación	DQDB (IEEE 802.6)	FDDI-II
Contención	CSMA/CD (IEEE 802.3)	

Nota : DQDB y FDDI-II protocolos para trafico de circuitos conmutados no son completamente especificados en los estándares y pueden ser distribuidos o centralizados. todos los demás protocolos MAC son protocolos distribuidos.

Tabla 3.7 Relación entre el control de acceso al medio y el tipo de topología

Las técnicas que han sido adoptadas para ser utilizadas en topologías de bus y árbol son :

- CSMA/CD Carrier Mense Multiple Access with Collision Detection (Acceso Múltiple con Censo de Portadora/Detección de Colisiones).
- Control Token Bus (Control Token).
- Reservación Centralizada.

Mientras que para las topología de anillo son :

- Token Ring. (control token)
- Inserción de Registros.
- Anillo Ranurado (slotted ring).

	Centralizado	Distribuido
Round Robin	Polling	Token bus Token ring Delay Token implícito (implicit token)
Reservación	Reservación centralizada (Centralized reservation)	Reservación distribuida (Distributed reservation)
Contención		CSMA/CD Anillo ranurado (Slotted ring) Inserción de registros (Register insertion)

Tabla 3.8 Técnicas de control de acceso al medio

3.3.1 CSMA/CD

El método de acceso al medio CSMA/CD es únicamente utilizado en redes de tipo bus. Con esta topología, todos las estaciones son conectadas directamente al mismo cable o medio de transmisión. Por lo tanto este medio es utilizado para transmitir todos los datos entre cualquier par de estaciones. El medio, dicho de esta manera sirve para operar en un modo de **acceso múltiple** (multiple access mode MA).

Todos los datos son transmitidos por una estación que primero encapsula los datos dentro de un paquete de información (frame) con la dirección de la estación destino en el encabezado de cada paquete; el paquete es entonces transmitido o difundido sobre el medio. Todos las estaciones conectadas a el medio, detectan en cualquier momento que un paquete está siendo transmitido de esta forma, cuando la estación requerida como destino detecta que el paquete de información que actualmente es transmitido tiene su propia dirección en el encabezado, continua por leer la información contenida dentro de este y responde de acuerdo a el protocolo de comunicación definido. La dirección del remitente es incluida como parte del encabezado del paquete, así que el receptor puede dirigir su respuesta a la estación originaria.

Con este tipo de técnica, es posible que dos o mas estaciones transmitan un paquete sobre el medio cuando este se encuentra ocupado por otro paquete, causando de esta manera que los paquetes de las estaciones transmisoras sean corrompidos al ocurrir una colisión de paquetes. Para reducir la posibilidad de este suceso, antes de que un paquete sea transmitido, cada estación fuente primeramente escucha eléctricamente el medio, lo que es llamado **censo de señal de portadora** (CS carrier sense) para detectar si un paquete esta siendo transmitido actualmente. Si una señal de portadora es censada o detectada, la estación detiene su intento de transmitir hasta que el paquete que esta en el medio haya sido transmitido completamente, solo entonces la estación fuente tratará de enviar su paquete. De la misma forma, dos estaciones deseosas de transmitir un paquete pueden determinar simultáneamente que no existe actividad de transmisión sobre el medio (paquetes sobre el bus), y de aquí ambos empiecen a transmitir sus paquetes al mismo tiempo. De esta forma también ocurrirá una colisión.

La estación fuente simultáneamente monitorea la señal del medio a la vez que transmite los datos de un paquete. Si las señales de los datos transmitidos y los monitoreados son diferentes, la estación asume que ha ocurrido una colisión, esta operación es llamada **detección de colisión** (CD collision detection). De esta manera al detectar la colisión, la estación cesa la transmisión de el paquete de datos y da seguimiento a la colisión transmitiendo un bit de patrón aleatorio por un corto período de tiempo, el cual es conocido como **señal de secuencia de congestión** (jam sequence). Esta señal asegura que todas las estaciones se hallan percatado de que ha ocurrido una colisión. Después de que todas las estaciones envueltas en la colisión conocen el suceso, esperan durante un pequeño intervalo de tiempo aleatorio antes de intentar retransmitir los paquetes afectados.

De esta manera se puede concluir, que el protocolo de acceso al medio para bus CSMA/CD es probabilístico y depende de la carga de la red.

3.3.2 Control token

Otra manera de control de acceso para compartir el medio de transmisión es por el uso de un control (permiso) de señal (token). Esta señal (token) es pasada desde una estación a otra, de acuerdo a un conjunto de reglas entendidas y apegadas por todas las estaciones conectadas a el medio. Una estación solo puede transmitir su frame cuando tiene posesión de la señal token y después que ha transmitido el paquete de información pasa la señal token a otra estación permitiéndole el acceso al medio de transmisión.

La secuencia de operación de la técnica de control token es la siguiente:

- Primero se establece un estructura de anillo lógico, con el cual se ligan todas las estaciones conectadas al medio físico, además, es creada una señal única de control de permiso (control token).
- La señal de control token es pasada de una estación a otra, recorriendo el anillo lógico hasta que esta señal llega a una estación que espera enviar un paquete o paquetes de información.
- La estación que espera para la transmisión cuando es poseedor de la señal de token, envía su paquete o paquetes de información a través del medio físico. Una vez concluida la transmisión de paquetes de información pasará la señal de control a la siguiente estación en el anillo lógico.

La función de monitoreo dentro de los estaciones activas conectados al medio físico, proveen un fundamento para la inicialización y la recuperación de la conexión del anillo lógico y de la perdida de la señal token.

Aunque las funciones de monitoreo son normalmente efectuadas entre todas los estaciones sobre el medio, solo una estación a la ves acarrea la responsabilidad de recuperación y reinicialización.

El medio físico no necesariamente debe tener una topología de anillo; una señal de token puede ser también utilizada para control de acceso a una red en bus. En esta topología se hace un arreglo de anillo lógico como se demuestra en la figura.3.6.

Con una topología de anillo físico, la estructura del anillo lógico **token-passing ring** es la misma estructura que la del anillo físico, con el orden de la señal token pasando en el mismo orden de la estructura física de las estaciones conectadas. Con una estructura de red en bus, el orden del anillo lógico es diferente al orden del las estaciones conectadas al medio. Además, con un control de acceso al medio de tipo token sobre una estructura de bus, todas las estaciones no necesariamente deben estar conectadas dentro del anillo lógico. Esto significa que una estación conectada al bus pero no conectada dentro del anillo lógico, puede operar solo en

estado de recepción, teniendo en cuenta que nunca será propietaria de la señal token, por lo tanto nunca podrá trasmitir. Otra característica del método de acceso al medio con señal de token, es la de poder asociar una prioridad con la señal de token, por medio de esto se permite transmitir primero a los paquetes con mayor prioridad.

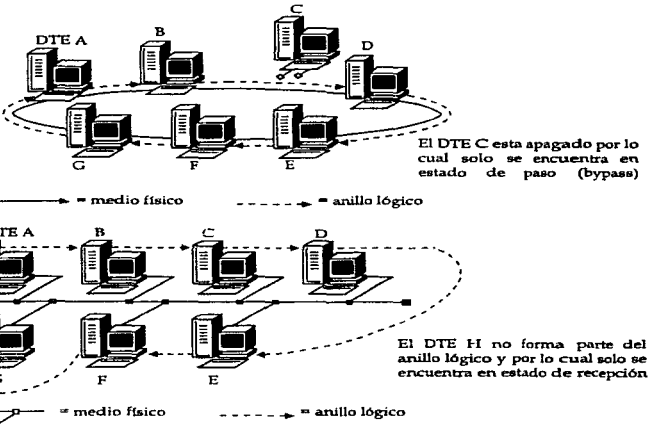


Figura 3.6 Control de acceso al medio a través de control token
(a) token ring
(b) token bus

3.3.3 Anillo ranurado

Es llamado así, por que sobre el anillo circulan continuamente varios paquetes (frames) de longitud fija llamados ranuras.

En el anillo ranurado, cada ranura contiene un bit en el encabezado el cuál indica si una ranura se encuentra llena o vacía. Inicialmente todas las ranuras se inicializan como vacías. Cuando una estación desea transmitir deberá repartir los datos en varios paquetes o frames con una longitud fija y entonces esperará a que llegue

una ranura vacía en este momento marcara la ranura como llena e insertará los datos sobre la ranura; así de esta manera hasta que la ranura vaya llegando

La estación no podrá transmitir otro paquete hasta que la ranura ocupada regrese, de esta manera insertará los paquetes de datos como la ranura vaya llegando. Una ranura hace un viaje redondo para ser marcada de nuevo como vacía por la estación transmisora. Cada estación conoce el número total de ranuras existentes sobre el anillo, de esta manera puede llenar o vaciar el bit como va llegando.

La principal desventaja de el anillo ranurado es su desperdicio de ancho de banda. Primero cada paquete de datos debe ser de una longitud lo suficientemente pequeña para poder adaptarse a la ranura, resultando con esto una gran cantidad de sobrecarga. Segundo, una estación puede enviar solo un paquete por viaje redondo a la vez. Si solo una estación tiene paquetes a transmitir, varias ranuras circularán vacías. Su principal ventaja es su simplicidad.

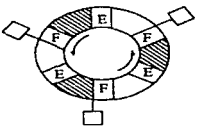


Figura 3.7 Anillo ranurado

Cabe mencionar que los métodos de acceso al medio tales como: **Centralized Reservation** sirven para la transferencia de archivos, audio y facsimile.

3.3.4 Registro de inserción

Esta técnica deriva su nombre del **registro de cambio** asociado con cada nodo conectado al anillo. El registro de cambio, el cual es igual en tamaño a la longitud máxima del frame, es utilizado temporalmente, manteniendo frames que circulan por el nodo. En adición, cada nodo tiene un **buffer** para almacenar los frames producidos localmente. En la figura 3.8 se muestra el registro de intercambio y el buffer para un nodo.

A continuación, se explican los dos casos principales que se pueden tener en el anillo de registro de inserción.

El primer caso, se considera cuando una estación no tiene datos para enviar, por tal motivo se realiza simplemente el manejo de frames de datos que circulan por su posición. Cuando el anillo se encuentra vacío, la posición del **apuntador de**

entrada del registro de cambio se encuentra en la parte mas a la derecha de éste registro, lo cuál indica que el registro está vacío. Cuando los datos llegan provenientes del anillo, estos son insertados bit por bit en el registro de cambio y el apuntador de entrada va cambiando de posición bit por bit hacia la izquierda. Cada paquete de datos recibido desde el anillo empieza con un campo de encabezado de direccionamiento, tan pronto como este campo se encuentre completamente dentro del registro de cambio, la estación puede determinar si es o no el destinatario del paquete. En caso de que no sea la estación destino, el paquete será retransmitido al anillo, al intercambiarlo bit por bit hacia la salida del registro de cambio. Si durante este lapso de tiempo, no llega un paquete adicional, el apuntador de entrada retornará a su posición inicial, es decir, a la parte mas a la derecha del registro de cambio; de otra manera, un segundo frame empezará a acumularse en el registro de cambio al mismo tiempo como el primero es enviado fuera hacia el anillo[7].

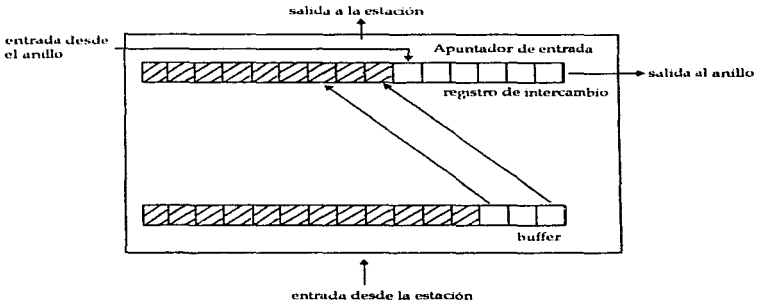


Figura 3.8 Anillo de inserción de registro

Si un frame llegase con la dirección de la estación en cuestión, la estación tiene dos acciones para elegir. Primero, puede desviar el resto del frame para él mismo y borrar los bits del campo de dirección, de esta manera se purga el frame del anillo., o una segunda alternativa, es retransmitir el frame mientras se copian los datos del frame hacia la estación local en cuestión.

[7] En este caso, se pueden hacer dos observaciones. Primero, se puede implicar que mas de un frame puede encontrarse sobre el anillo al mismo tiempo. Segundo, se tiene una serie de paquetes con huecos entre ellos pasando por el nodo de una estación, lo que permite poder insertar nuevos paquetes al anillo.

Ahora considerando el segundo caso principal, en el cuál, la estación tiene datos para transmitir. Un frame para ser transmitido es colocado en el buffer de salida. Si la línea se encuentra vacía y el registro de cambio también esta vacío, el frame puede ser transferido inmediatamente del buffer hacia el registro de cambio. Si el frame consiste de una longitud de n bits, menor que el tamaño máximo de frame estipulado en el anillo, y si al menos n bits están vacíos en el registro de cambio, los n bits son transferidos-en-paralelo a la porción vacía del registro de cambio adyacente inmediato para llenar la porción y al mismo tiempo el apuntador de entrada es ajustado.

La técnica de **registro de inserción** refuerza una eficiente forma de imparcialidad. Tanto como el anillo se encuentre ocioso, una estación con muchos datos a ser transmitidos pueden ser enviados frame tras frame, utilizando enteramente el ancho de banda del anillo. Sin embargo, si el anillo se encuentra ocupado, una estación encontrará que, después de enviar un frame, el registro de intercambio no acomodará otro frame. La estación deberá esperar hasta que exista un hueco entre mensajes lo suficientemente grande para poder colocar el suyo, teniendo entonces que acumular los frames locales hasta poder enviarlos. Como un refinamiento al método, ciertamente se pueden establecer nodos con registros de cambio con una mayor prioridad, los cuales tienen una longitud mas grande que la del mínimo registro de intercambio (el cuál, es de tamaño igual a la longitud del frame).

La principal ventaja de esta técnica, es que lleva a cabo la utilización máxima del anillo de entre cualquiera de los otros métodos; sin embargo, permite como en el sistema de token, la utilización de frames de longitud variable. Permitiendo al igual que la técnica de anillo ranurado múltiples frames sobre el anillo al mismo tiempo. La principal desventaja que se tiene, es el mecanismo de purgado sobre el anillo, esto es, el permiso de múltiples frames sobre el anillo requiere que el reconocimiento de la dirección sea primero antes de que el frame sea removido por el transmisor o por el receptor, esto nos lleva a que si una dirección del frame es alterada, el frame puede circular indefinidamente. Una posible solución es el uso de un código de detección de error sobre el campo de direccionamiento.

3.4 Estándares de redes

Historia de la Interconexión de Redes (Internetworking)

Las redes se han venido desarrollando desde finales de los años 70's y principios de los 80's, hasta nuestros días; un amplio rango de diferentes tipos de redes han sido propuestas e implementadas. Al principio cada compañía fabricante tenía sus propias arquitecturas y protocolos, a causa de estas diferencias entre los proveedores, solo podían ser conectadas las computadoras del mismo fabricante. Estas redes eran llamadas sistemas propietarios o sistemas cerrados.

Para evitar esta situación, se tomaron mejores iniciativas a través de varios organismos internacionales de estandarización con el propósito de formular y aceptar un conjunto de estándares para las redes, con lo que se formo lo que hoy se llaman sistemas abiertos. Y aun que los estándares imponen algunas limitaciones para los desarrolladores de los sistemas, los estándares son la mejor respuesta para resolver el problema de la intercomunicación de diversos equipos de comunicación y programas de diferentes proveedores.

3.4.1 Estándares de IEEE

Uno de los organismos que tuvo un mayor desempeño en esta actividad fue el IEEE el cuál desarrolló la serie de estándares conocido como IEEE 802.x para redes de área local (LAN). El cuál ha sido adoptado por ISO como un estándar internacional.

El estándar 802.x está integrado por varios subcomités, lo que proporciona una mayor flexibilidad para cubrir las diferentes necesidades de los diseñadores de redes. Estos subcomités están organizados de la siguiente manera:

802.1 Interfaces de alto nivel HLI (High Level Interface HLI) (y puentes MAC)
802.2 Control de Enlace Lógico (LLC) (Logical Link Control)
802.3 Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
802.4 Token Bus
802.5 Token Ring
802.6 Redes de Área Metropolitana (MAN) Metropolitan Area Networks
802.7 Broadband Technical Advisory Group
802.8 Fiber Optic Technical Advisory Group
809.9 Integrated Data and Voice Networks
809.10 LAN security
809.11 Redes inalámbricas (wireless LANs)
809.12 100VG Anylan

Los subcomités del IEEE abarcan las 2 capas inferiores del modelo de referencia OSI: la capa física y la capa de enlace de datos.

3.4.1.1 Interface de redes de alto nivel (802.1)

Este subcomité trata asuntos comunes a través de todos los subcomités 802 de redes LAN, en las que se incluyen: el sistema de direcciones, administración de las redes y puentes. Además de la relación entre las normas 802.X del IEEE y el Modelo de Referencia OSI .

3.4.1.1.1 Sistema de direcciones del IEEE 802

Las redes locales, al ser de tipo multipunto, hace que cada estación conectada sobre la red examine cada paquete que se transmite por esta. Por lo que es necesario que cada paquete contenga dos campos de dirección: un campo con la dirección de la estación destino y otro con la dirección de la estación fuente.

Para prevenir que cada estación interrumpa sus actividades por cada paquete que examina, es necesario, que las interfaces de red filtren los paquetes que no contienen su dirección en el campo destino.

Por lo anterior el subcomité 802.1 llevó a cabo la estandarización del sistema de direcciones para redes locales. El cuál se llevó a cabo al establecer una longitud de 48 bits (El rango de una dirección entera por lo tanto es de 6 octetos) para cada dirección. El argumento de 48 bits es suficiente para proveer un identificador global único para cada dispositivo de red. Por tanto cada dispositivo de red que se comunicará con otros tiene una dirección física única, la cuál es asignada por el fabricante en el momento de la fabricación de cada dispositivo (esta dirección es referida también como dirección física, dirección de hardware, o dirección MAC).

Actualmente la organización IEEE es la autoridad administrativa universal para la asignación y manejo de bloques o rangos de direcciones. Cuando un fabricante desea fabricar equipo que se enlazará en red, primeramente debe contactar a la autoridad global para obtener un bloque de direcciones , cada bloque consta de 2^{24} direcciones o sea 48 bits (6 octetos).

Al fabricante se le asignan tres octetos de valor fijo (24 bits), esta porción de valor fijo de direcciones es referido también dentro de la industria como código del vendedor u OUI (organizationally unique identifier). Los otros tres octetos o 24 bits identificadores son asignados por el fabricante para cada uno de sus productos.

Actualmente los 24 bits de valor fijo (OUI) tienen una estructura adicional (2 bits de control). El primer bit puede representar un grupo/individual . Si el bit es 0, la dirección se refiere a una estación particular o individual, de otra manera, si el bit es 1, la dirección se refiere que el resto del campo de la dirección se refiere a un grupo lógico de estaciones que necesita mayor resolución. El segundo bit es el bit, Universal/ Local. Si el bit es 0, quiere decir que la dirección fue establecida por la autoridad administrativa universal (significa que los siguientes 22 bits fueron asignados por el IEEE). Si el segundo bit tiene valor de 1, el campo OUI fue asignado en forma local[8].

[8] Este tipo de asignación local del OUI puede causar problemas de direccionamiento, si se descifra como si se tratara de una dirección asignada por el IEEE.

Por lo tanto la autoridad global asigna 22 bits de valor fijo, un bit para indicar grupo/individualidad y un ultimo para indicar Universal/Local.

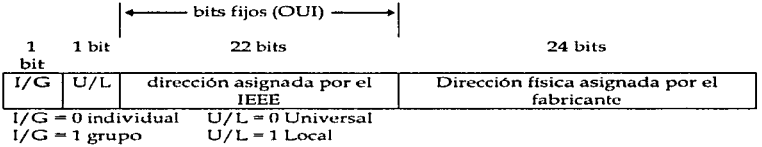


Figura 3.9 Esquema de direccionamiento del IEEE 802

Si un fabricante se quedara sin direcciones físicas, el IEEE tiene capacidad de asignarle un segundo OUI identificador. Cabe hacer notar que si sigue la tasa actual de crecimiento es posible que en un futuro se lleguen a agotar los OUIs.

3.4.1.1.2 Direcciones multicast y broadcast

Una dirección **multicast** permite a un solo frame ser recibido por un grupo seleccionado de estaciones. El software de red puede establecer que la configuración de una interfaz de red de una estación escuche una dirección especifica de multicast. Esto hace posible para un conjunto de estaciones, se le asigne a un grupo multicast al cual le ha sido dado una dirección multicast especifica. Un solo paquete enviado a la dirección multicast asignada ha ese grupo entonces será recibido por todas las estaciones en ese grupo.

También existe un caso especial de dirección multicast conocida como dirección broadcast o de difusión, la cual es una dirección donde los 48bits de dirección son establecidos en valor de 1 (uno). Todas las interfaces Ethernet que observen un frame con esta dirección destino leerán el frame recibido y lo entregaran al software de la capa de red de la estación.

3.4.1.1.3 802.1A

Dentro de otros subcomités tenemos el 802.1A, el cuál es responsable de proveer una arquitectura con manejo en red, consistente con el modelo OSI (providing a network management architecture consistent).

3.4.1.1.4 802.1B

El subcomité 802.1B,desarrolla protocolos de manejo y administración de redes LAN/MAN. Estos estándares tienen por objeto ser un complemento para los estándares de administración de sistemas OSI.
Tales como el CMIP (Common Managment Information Protocol) y SMNP (Simple Management Network Protocol), entre otros. ?

3.4.1.1.5 802.1D

Define el estándar para encaminamiento por medio de puentes(encontrándose bajo consideración por el IEEE), el cuál provee un mecanismo de encaminamiento distribuido sobre múltiples redes LAN conectadas a través de estos dispositivos. Este estándar para puentes (bridges) ha adoptado el algoritmo de enrutamiento **Spanning tree**, el cuál es utilizado por puentes para redes locales tipo Ethernet.

El subcomité 802.1D pretende incorporar al estándar algunos aprovechamientos de encaminamiento del protocolo de IBM para redes tipo anillo llamado **source routing** el cual forma parte del protocolo 802.5

3.4.1.1.6 802.1G

El subcomité 802.1G ha estado trabajando para desarrollar un estándar para encaminamiento de puentes remotos (remote bridges) en redes de área amplia WANs. El comité ha adoptado para los puentes remotos la utilización del algoritmo de encaminamiento **spanning tree** (adoptado como un estándar para puentes de redes de área local).

3.4.1.2 IEEE y la capa de enlace de datos (data link level)

Los protocolos en el nivel de enlace de datos llevan a cabo la tarea de transmisión eficaz de frames o bloques de datos entre dos nodos adyacentes (sin nodos de conmutación intermedios).

Las funciones principales de la capa de enlace de datos son:
- Sincronización lógica del transmisor y receptor.
- Control de flujo de datos.
- Control y detección de errores.
- Secuenciamiento de los paquetes de datos para garantizar una entrega ordenada.

El estándar IEEE divide el nivel de la capa de enlace de datos (data link layer) en dos subniveles: El nivel Control de Acceso al Medio MAC (subcomités 802.3, 802.4,

802.5 y 802.12) y el nivel Control Lógico de Enlace LLC (subcomité 802.2)[9]. Cabe hacer notar que la capa de enlace en redes locales difiere en tres características de la capa de enlace tradicional (WAN):

Las funciones asociadas en el nivel de enlace de datos para realizar la transmisión y recepción entre estaciones conectadas a una red local son las siguientes:

Proveer uno o más puntos de acceso a servicio SAPs (interfaz lógica entre dos niveles o capas adyacentes) para soportar la característica multiacceso del enlace.

Deberá realizar algunas funciones del nivel 3 del modelo OSI referido como la capa de red. (se explica mas adelante).

En la transmisión, lleva a cabo el ensamblado de datos dentro de un frame o paquete con los campos correspondientes a las direcciones[10] y el método CRC (para detección de errores).

En la recepción, lleva a cabo el desensamblaje del paquete (frame), desarrollando el reconocimiento de las direcciones y la validación con el método CRC.

Administración del acceso al medio compartido de las redes locales para llevar a cabo la transmisión.

Las dos primeras funciones son desarrolladas por el subnivel LLC, las últimas tres son desempeñadas por el subnivel de control de acceso al medio (MAC).

Esta subdivisión del nivel de enlace de datos se llevo a cabo por las siguientes razones:

Con esta subdivisión se satisface la lógica requerida para administrar el acceso al medio compartido para redes multipunto (enlace único para todas las estaciones unidas a la red local) ya que no esta contemplada dentro del nivel de enlace de datos tradicional.

El subnivel LLC sirve como interface para los protocolos de las capas superiores (principalmente para la capa red) y de esta manera aísla los niveles superiores de las acciones especificas llevadas a cabo por la subcapa MAC como son el control de acceso al medio. De esta forma se tiene la utilización de un mismo subnivel LLC(IEEE 802.2) para varias opciones a escoger del subnivel MAC (802.3, 802.4, 802.5 y 802.12). Teniendo con esto una mayor flexibilidad de los niveles inferiores del modelo OSI, además de poder soportar diversas opciones de pilas de protocolos en las capas superiores. Lo que llena las expectativas de los diseñadores de redes.

---

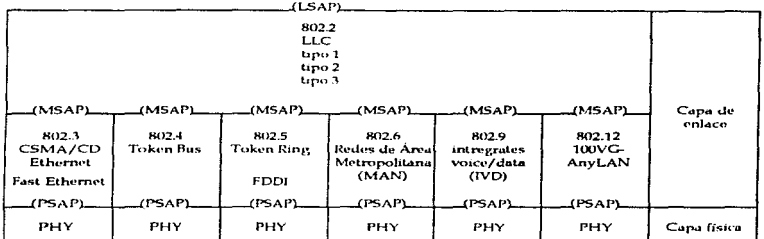
[9]Cabe hacer notar que la subdivisión del nivel 2 no es llevada a cabo en el modelo tradicional de OSI.

[10]Los campos para direcciones fuente y destino se llevan a cabo en el subnivel MAC. De esta manera cada subcomité (802.3, 802.4 y 802.5) pueda definir sus direcciones de manera independiente al subnivel LLC.

Cabe señalar que dentro de los estándares definidos por el IEEE también se han definido las características para el nivel físico como son:

Tipo de medio para las respectivas topologías que soportan las diferentes opciones de subnivel de MAC[1].
- Codificación/descodificación de señales.
- Transmisión/recepción de bits.
- Preámbulo de generación/remoción (para la sincronización), etc.

Protocolos de IEEE para redes LAN para los niveles inferiores del modelo OSI, se conforman de la siguiente manera:



LLC: Control de Enlace Lógico
MAC : Control de Acceso al Medio
LSAP : LLC Punto de Acceso al Servicio
MSAP : MAC Punto de Acceso al Servicio
PSAP : Punto de Acceso Físico.
PHY : medio físico.
Tipo1 servicio sin-conexión-sin-reconocimiento
Tipo2 servicio orientado a conexión
Tipo3 servicio sin-conexión-con-reconocimiento

Figura 3.10 Protocolos de redes LAN del IEEE

Como se puede observar en la tabla anterior, la división MAC/LLC del nivel de enlace de datos (link level) provee varias ventajas esenciales. Primero, controla el acceso al canal compartido entre los dispositivos (subcapa MAC). Segundo, provee un esquema descentralizado que reduce la susceptibilidad de errores en la red. Tercero, brinda una interface más compatible con las redes de área amplia (WAN wide area network), partiendo de la idea de que el LLC es un subconjunto del

[1]En el modelo de referencia OSI no se definen ningún tipo medio físico.

protocolo HDLC. Además el LLC es independiente de un método de acceso al medio, mientras que el MAC es un protocolo específico dependiente del diseño. El resultado de esta división hace más fácil el diseño de las redes, al proveer una interfaz con mayor flexibilidad para las redes locales.

3.4.1.2.1 Control de Enlace Lógico LLC (802.2)

El **Control de Enlace Lógico** (LLC: logical link control) es basado en el protocolo **Control de Enlace de Datos de Alto Nivel** HDLC (high-level data link control). El LLC, define los campos que permiten a múltiples protocolos de niveles superiores compartir el uso del enlace de datos.

Este se comunica con la capa de red por medio de las interfaces llamadas LSAPs (link service access points)[12].

El LLC puede ser especificado en tres partes:

1. La interface con la estación, especificando el servicio que la subcapa LLC (y por tanto la red LAN) proveerá al suscrito en la red.

2. El protocolo LLC, especificación de las funciones LLC.

3. La interface con el subnivel MAC, especificando los servicios que LLC requiere para desarrollar su función.

De acuerdo al estándar 802 se definen dos categorías generales de operación en el control de enlace de datos. El primero es una operación **sin-conexión** que provee un servicio suficiente con un mínimo de complejidad de protocolo. Esto es muy útil y eficiente cuando los protocolos de las capas superiores (capa de red, capa de transporte etc.) proveen el control de error, control de flujo y funciones de secuencia. También es muy útil cuando no se requiere garantizar la entrega de datos. La segunda categoría es la operación **orientada-a-conexión**, esta provee las funciones similares al protocolo HDLC. Estos dos tipos de operaciones son reflejadas en las especificaciones tanto de los servicios LLC y el protocolo LLC.

Por lo anterior, la subcapa LLC provee tres tipos servicios :

- Tipo 1: Servicio **sin-conexión-sin-reconocimiento** (Unacknowledge connectionless service). Este es un servicio de datagrama que simplemente permite el envío y recepción de frames LLC, sin ninguna forma de

[12] LSAPs son direcciones de enlace de datos lógicos puntos de acceso. Una sola dirección MAC puede tener múltiples direcciones LSAPs. Estas múltiples direcciones habilitan múltiples conexiones punto-final (end-point) entre dos nodos de una red local.

reconocimiento (acknowledge) para asegurar la entrega ya que en este servicio, los paquetes (frames) llevan la información completa de la dirección fuente y dirección destino. De manera que no se garantiza que los paquetes lleguen intactos o en el orden adecuado. Este tipo de servicio, soporta transmisiones punto-a-punto, multipunto y broadcast.

- Tipo 2: El servicio **orientado a conexión** provee un estilo de conexión de circuito virtual entre LSAPs (puntos de acceso a servicio de capa de enlace LSAPs). Con esto provee una medida por la cuál un usuario puede hacer una petición o ser notificado del establecimiento o terminación de una conexión lógica. Este servicio también provee control de flujo, funciones de secuencia, y control de errores. Soporta direccionamiento punto-a-punto. Este servicio incluye un conjunto de primitivas de petición, indicación, respuesta y confirmación para establecer una conexión lógica entre LSAPs, una vez que una conexión es establecida los bloques de datos son intercambiados ya que la existencia de una conexión lógica garantiza que todos los bloques de datos serán entregados, por lo que no existe la necesidad para el reconocimiento (acknowledgment) de cada bloque de datos individual (por medio de indicación y confirmación de primitivas). El control de flujo puede ser controlado en cualquier dirección, esto es un mecanismo de control de flujo local que especifica la cantidad de datos que pueden ser pasados a través del SAP.

- Tipo 3: Servicio **sin-conexión-con-reconocimiento** (Acknowledge connectionless service): este es también un servicio sin conexión, pero con reconocimiento (acknowledge) Con el que se provee un mecanismo por el cuál cada usuario puede enviar una unidad de datos y recibir un reconocimiento (acknowledgment) que indica que los datos fueron entregados sin la necesidad de establecer una conexión lógica. Además lleva a cabo la corrección de datos erróneos por medio de la retransmisión de paquetes que contienen los datos erróneos, esto libera a los niveles superiores de esta tarea. Soporta transferencias punto-a-punto.

La especificación de los tres tipos de servicios fueron el resultado de permitir al protocolo LLC ser utilizado para soportar los diversos requerimientos de los usuarios. El servicio **sin-conexión-sin-reconocimiento** (Unacknowledge connectionless) es el servicio más simple y requiere de una implantación mínima. Se puede utilizar en casos donde los protocolos de niveles superiores (usualmente el de transporte) proveen un control de error y control de flujo punto-a-punto, de manera que este servicio mínimo es todo lo que se necesita.

El servicio **sin-conexión con reconocimiento** (Acknowledge connectionless) puede ser muy útil en algunos ambientes de tiempo real (algunos ejemplos son las redes locales en empresas e industrias donde las funciones de tiempo son críticas, o las

funciones de seguridad como alarmas son necesarias que se transmitan en tiempo real).

3.4.1.2.1.1 Funciones de la capa de red realizados por el nivel de enlace de datos de redes LAN

Las redes de área local, al ser redes multipunto se tiene la ausencia de nodos de conmutación intermedia (todos los nodos son adyacentes entre sí), hace que una red local no requiera del nivel 3 del modelo OSI referente a la "capa de red", ya que las funciones esenciales de dicha capa pueden ser incorporadas dentro de la capa 2 (capa de enlace):

- **Servicio sin conexión** (Connectionless): Un servicio que no requiere la sobrecarga de establecer una conexión lógica, es necesaria para eficientar el soporte del tráfico altamente interactivo.
- Servicio **Orientado-a-conexión**: Un servicio orientado a conexión es utilizado usualmente.
- Servicio de **Multiplexaje**: Generalmente un solo enlace físico une una estación a la red local; esto deberá ser posible para proveer transferencia de datos con múltiples puntos terminales/finales sobre el enlace.

Como no se requiere llevar a cabo un enrutamiento en las redes locales, las 3 funciones antes mencionadas son llevadas a cabo fácilmente (por el nivel 2). Por último también se lleva a cabo la tarea de :

Multicast, broadcast: el nivel de enlace deberá proveer un servicio para enviar un mensaje a múltiples estaciones y de esta manera tomar ventaja de la naturaleza de acceso múltiple de una red local.

3.4.1.2.2 Protocolos de acceso al medio MAC (802.3, 802.4, 802.5)

3.4.1.2.2.1 IEEE 802.3 Estandarización de la tecnología Ethernet CSMA/CD

La tecnología Ethernet es también llamada red de bus CSMA/CD. Cabe mencionar que el método de control acceso al medio CSMA/CD y el formato del frame Ethernet es idéntico para todas las variedades de velocidad en la que ellos operan y los medios soportados por Ethernet. Sin embargo, las velocidades 10Mbps y 100Mbps individualmente tienen diferentes tipos de medios los cuales pueden usar diferentes componentes de conexión, y por tanto tienen diferentes guías de configuración.

3.4.1.2.2.1.1 Operación de Ethernet

Cada estación equipada con Ethernet, opera de forma independiente de todas las demás estaciones sobre la red (no existe un controlador central). Todas las estaciones unidas en un sistema Ethernet son conectadas a un sistema de señal compartido, también llamado medio compartido o bus (backbone). Las señales Ethernet son transmitidas serialmente es decir, un bit a la vez, sobre el canal de señal compartido el cual es recibido por cada estación conectada al bus. Para transmitir datos una estación primero escucha el canal, cuando el canal este desocupado o vacío la estación transmite sus datos en forma de un frame Ethernet.

Después de cada transmisión de un frame (paquete de bits), todas las estaciones sobre la red deberán contender de igual forma para obtener la oportunidad de transmitir el siguiente frame. Esto asegura que el acceso al canal de transmisión compartido sea claro, y que ni una sola estación pueda bloquear a las demás estaciones. El acceso al canal compartido es determinado por un método de control de acceso (MAC) llevado a cabo en cada interfaz Ethernet localizado en cada máquina. Ethernet ocupa un mecanismo de control de acceso al medio llamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Ethernet opera como un sistema de entrega de frames con el **mejor esfuerzo**. Para mantener la complejidad y el costo de la red LAN a un nivel razonable, no garantizando la entrega eficaz de los datos.

Parámetros	10Base5[13]	10Base2[5]	10BaseT[5]	10Base36[5]	10BaseF[5]
Medio de transmisión	coaxial	coaxial	par trenzado UTP	coaxial	fibra óptica
Diámetro de cable (mm)	10	5	0.4-0.6 (26-22 AWG)	0.4-1.0	
Tasa de transmisión de datos (Mbps)	10	10	10	10	10
Longitud max. del segmento	500	200	100 al disp. central	1800	
Técnica de señal utilizada	Baseband manchester	Baseband manchester	Baseband manchester	Broadband (DPSK)	Baseband Manchester
Extensión máxima de la red (m)	2500	925	500	3600	2000

Tabla 3.9a Opciones de medios para la capa física de Ethernet

[13] El comité ha desarrollado una notación concisa para reconocimiento de la tecnología utilizada para su desarrollo:
<Tasa de transmisión > <método de señal> <máx. long. por segmento en cientos de metros>

Parámetros	10Base5[14]	10Base2[5]	10BaseT[5]	10Base36[5]	10BaseF[5]
Nodos por segmento	100	30	núm. de puertos del concentrador		
Numero máximo de nodos	1024	1024			
distancia min. entre estacione	múltiplos de 2.5m	0.5m			
topología	bus	bus	estrella (concentra-dor)	bus	estrella (concentra-dor)

Tabla 3.9b Opciones de medios para la capa física de Ethernet

3.4.1.2.2.1.2 10 Base 5

La especificación 10BASE5 es el estándar 802.3 original. El cuál especifica un cable coaxial Baseband a 10Mbps. La máxima longitud de un segmento de cable es de 500 metros. con un máximo de 100 nodos o estaciones permitidas por segmento.

La longitud de la red puede ser extendida utilizando repetidores. El estándar permite un máximo de cuatro repetidores en la ruta entre dos estaciones cualquiera, extendiendo la ruta efectiva de la red a una longitud de 2.5 Km.

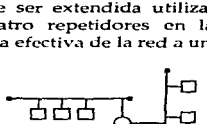


Figura 3.11 Configuración Banda Base

3.4.1.2.2.1.3 10Base 2

La versión 10BASE2 también llamada **Cheapernet**. Esta provee la utilización de un cable coaxial delgado (thinner coaxial cable) con la misma tasa de transmisión a 10Mbps. El cable coaxial delgado utiliza componentes electrónicos de menor costo, resultando con perdida en la longitud. El segmento de longitud máximo con cable

[14] El comité ha desarrollado una notación concisa para reconocimiento de la tecnología utilizada para su desarrollo:
<Tasa de transmisión > <método de señal> <máx. long. por segmento en cientos de metros>

coaxial delgado es de 200 metros con un máximo de 30 nodos por segmento (es ideal para conectar dispositivos de bajo costo como son estaciones de trabajo y computadoras personales).

3.4.1.2.2.1.4 10BaseT

Otra opción es la conocida como **StarLAN**, con la que se especifica una versión de operación con cable par trenzado sin blindar UTP operando a 10Mbps, utilizando un alambrado de estrella o topología de concentrador. Esta opción es substancialmente mas baja en costo que las dos opciones de cable coaxial.

Las estaciones conectadas al repetidor multipuertos vía un enlace punto-a-punto consiste de dos pares de par trenzado, cada par de alambres forma un segmento de enlace (uno de transmisión y otro para recepción). La tasa de transmisión de datos es de 10Mbps utilizando la codificación llamada Manchester.
En consecuencia de la alta tasa de transmisión de datos y la baja calidad de transmisión proporcionado por cable par trenzado sin blindar (UTP), la longitud de enlace de una estación al concentrador es limitado a 100 metros. Como una alternativa, un enlace de fibra óptica puede ser utilizado. En este caso, la longitud máxima es de 500 metros. Debe hacerse notar que la conexión entre un repetidor y el próximo es un enlace que aparece el mismo como un enlace de estación ordinario, en efecto, no se hace distinción entre una estación y un repetidor. En el sistema 10BASET, todos los repetidores multipuertos funcionan de la misma manera como un repetidor ordinario de los sistemas 10BASE5 o 10BASE2. Una ventaja de utilizar repetidores y el uso de la tasa de transmisión de datos a 10Mbps es que el sistema 10BASET puede ser mezclada con los sistemas 10BASE2 y 10BASE5.

Las reglas de configuración para mas de un concentrador son las siguientes :

- Un máximo de cuatro concentradores en la ruta de datos entre dos estaciones cualquiera.
- Los segmentos de cable UTP no deberán ser mayores de 100 metros

Medios de transmisión	numero de dispositivos conectados	Longitud máxima (m)
dos cables de par trenzado	2	100
dos cables de fibra óptica	2	500
cable coaxial (10BASE5)	30	185
cable coaxial (10BASE2)	100	500

Tabla 3.10 Conexiones permisibles para un repetidor multipuertos 10BASET

La ruta de transmisión máxima permitida entre dos estaciones cualquiera es de cinco segmentos y un conjunto de cuatro repetidores. Un segmento es uno de los

dos siguientes : segmento de enlace punto-a-punto o un segmento coaxial 10BASE2 o 10BASE5. El número máximo de segmentos de cable coaxial en una ruta es de tres segmentos.

3.4.1.2.2.1.5 10BaseF

El sistema 10BASE-F es el estándar de medio de fibra óptica para redes Ethernet, es el más frecuentemente usado actualmente para cubrir largas distancias (hasta 2 km entre repetidores). Es también usado para inter e intra backbone de edificios (por costumbre no es instalado para la conexión directa a las estaciones por el alto costo del cableado de la fibra óptica).

Ethernet utiliza pulsos de luz en lugar de corriente eléctrica para el envío de las señales. El uso de pulsos de luz provee un mejor aislamiento eléctrico para los equipos con terminación de enlace con fibra óptica. Mientras que el equipo Ethernet usado en segmentos de medio metálico tiene solamente protección de circuitos diseñado para riesgos eléctricos internos. El medio de fibra óptica es totalmente no-conductivo. Este completo aislamiento eléctrico provee inmunidad para un mayor número de riesgos eléctricos incluyendo el efecto llamado "lighting strikes", de los diferentes niveles de corriente de tierra eléctrica que pueden ser encontrados en la conexión de instalaciones separadas. Además de que este completo aislamiento eléctrico es esencial cuando los segmentos Ethernet viajan a la intemperie a través de la parte exterior de las instalaciones para enlazar dos edificios separados.

La mejor ventaja que da un segmento de enlace de fibra óptica 10BaseFL es la gran distancia a la que este puede extenderse. Otra ventaja es que el medio de fibra óptica puede soportar velocidades de transmisión mucho más altas que 10Mbps. Cuando se diseña una red con el enlace de bus backbone basado con medio de fibra óptica con enlace a concentradores de 10Mbps, cuando se lleve a cabo una actualización en el futuro se pueden cambiar los concentrador de 10Mbps por otros a 100Mbps y no existe la necesidad de cambiar el esquema de cableado de fibra óptica.

3.4.1.2.2.1.6 Los estándares FOIRL y 10BaseF

El uso más común para el tipo de medio de fibra óptica es el enlace entre segmentos. Existen dos tipos de enlace entre segmentos con fibra óptica en uso, el segmento original **Fiber Optic Inter-Repeater Link** (FOIRL) y el nuevo segmento 10BaseFL.

La especificación original FOIRL del estándar Ethernet de principios 1980's provee un segmento de hasta 1000 metros entre dos repetidores únicamente. Cuando se

hizo costeable realizar enlaces individual entre las estaciones y los puerto de un concentrador repetidor por medio de fibra óptica, los vendedores crearon salidas de interfaz FOIRL MAUs para permitir que se hiciera la conexión, aunque una conexión repetidor-a-DTE no fue especificamente descrita en el estándar FOIRL.

Para cubrir con este y otros aspectos de la conexión Ethernet con fibra óptica, el conjunto de estándares llamados 10BaseF para medios de fibra óptica fueron desarrollados. Este conjunto de estándares incluye especificaciones revisadas para un segmento de enlace de fibra óptica que permitirá conectar directamente a las estaciones. El conjunto completo de especificaciones 10BaseF incluye tres tipos de segmentos:

- 10Base-FL: el estándar 10BASE-FL reemplaza las anteriores especificaciones FOIRL, y este es diseñado para interoperar con el equipo basado en FOIRL existente. 10 Base-FL provee un segmento de enlace de fibra de hasta 2000 metros de longitud, previendo que solamente equipo 10BaseFL sea usado en el segmento. Si equipo de 10BASE-FL es combinado con equipo basado en FOIRL, entonces la longitud máxima de segmento puede ser de 1000 metros.

  Un segmento 10 Base-FL puede ser conectado entre dos estaciones, dos repetidores o entre una estación y un puerto de repetidor. El tipo 10BaseFL es la especificación mas ampliamente usada de las especificaciones de fibra óptica 10BaseF, y el equipo esta disponible por un gran número de distribuidores.

- 10Base-FB: Las especificaciones 10Base-FB describen un segmento backbone (espina dorsal) de señal síncrona que permite que el limite de número de repetidores que pueden ser usados en un sistema Ethernet a 10 Mbps pueda ser excedido. Los enlaces 10Base-FB típicamente realizan la unión entre concentradores repetidores, y son usados para enlazar concentradores repetidores de señal síncrona 10BaseFB especiales juntos en un sistema backbone repetido que puede expandirse hasta largas distancias. Un enlace individual de 10BaseFB puede ser de hasta 2000 metros de longitud. Este sistema tiene una limitación en el mercado y el equipo esta disponible solo con pocos vendedores.

- 10Base-FP. El sistema de fibra pasiva provee un conjunto de especificaciones para un segmento combinado de fibra óptica que enlaza múltiples computadoras sobre un sistema de medio de fibra óptica sin el uso de repetidores. Los segmentos 10Base_FP pueden ser de hasta 500 metros de longitud. El uso de un solo empalme en estrella pasiva de 10Base-FP puede enlazar hasta 33 computadoras. Este sistema no ha sido ampliamente adoptado y el equipo no esta disponible.

3.4.1.2.2.1.7 10BROAD36

Otra opción del tipo banda amplia a 10Mbps ha sido adicionada, 10BROAD36, el cual provee un soporte para un mayor número de estaciones sobre distancias más amplias que las versiones banda base, a un mayor costo.

3.4.1.2.2.1.8 Extendiendo redes Ethernet con concentradores

Ethernet fue diseñado para ser expandido de manera fácil para cubrir las necesidades de las redes en cualquier sitio particular. Para ayudar a la expansión del sistema Ethernet, los vendedores de interconexión de redes venden los dispositivos llamados concentradores (hubs) que proveen múltiples puertos ethernet. A partir de este dispositivo proveen un elemento central con el sistema de cableado en bus de manera interna.

Existen dos clases principales de concentradores: **concentrador repetidor** y **concentrador conmutador**.

Cada puerto de un *concentrador repetidor* realiza un enlace *individual de segmento* de medio Ethernet, la estructura del concentrador une estos enlaces individuales para crear una gran red que opera como una sola red local Ethernet. El total del conjunto de segmentos y repetidores en la red LAN Ethernet deberán conocer las especificaciones del tiempo de viaje redondo (RTT). El segundo tipo de concentradores provee un esquema de conmutación de paquetes, típicamente basado en un esquema de puertos de puente.

El punto importante que ha ser tomado es que cada puerto del concentrador conmutador provee una conexión a un sistema de medio Ethernet que opera como una red Ethernet separada o independiente de las otras (un dominio de colisión por cada puerto o sea cada puerto tiene un ancho de banda de 10Mbps). A diferencia de un *concentrador repetidor* el cual combina puertos individuales como segmentos, al combinar segmentos conjuntamente para crear una sola LAN extensa (es decir, todo el esquema del concentrador repetidor es un dominio de colisión es decir todo el esquema del concentrador repetidor con todos los segmentos que une comparten el ancho de banda de 10mbps). Un concentrador conmutador hace posible la división de un conjunto de sistemas de cableado ethernet dentro de múltiples LANs que son enlazadas en conjunto por medio de los componentes electrónicos de conmutación de paquetes que lleva dentro el concentrador. Las reglas de tiempo de viaje redondo (RTT) para cada LAN llegan hasta el puerto del concentrador conmutador. Esto permite enlazar un gran número de redes LAN ethernet individuales en forma conjunta.

Una sola red Ethernet LAN puede consistir de únicamente de un solo segmento de cable que enlaza cierto número de computadoras, o puede consistir de un *concentrador repetidor* que enlaza varios segmentos de medio conjuntamente. Todas las redes Ethernet LANs pueden ser enlazadas conjuntamente utilizando concentradores de conmutación de paquetes de tal forma se puede extender el sistema de red. Mientras que una red LAN ethernet individual puede generalmente soportar algunas docenas de computadoras. El sistema total de redes LAN ethernet enlazado por medio del mecanismo de conmutación de paquetes puede soportar varios miles de cientos de máquinas.

3.4.1.2.2.1.9 Nuevas especificaciones del 802.3

Por último se hace notar que la velocidad de transmisión original del estándar 802.3 Ethernet es de 10 Mbits/seg, pero las nuevas implantaciones como el 100BaseT, transmiten hasta 100 Mbits/seg en cable de par trenzado para tipos de datos (esta tecnología se estudiara en un capítulo posterior).

3.4.1.2.2.2 IEEE 802.4 Token Bus

El estándar token bus se caracteriza por tener un control de acceso al medio del tipo determinístico por estar basado en el tipo de control de acceso al medio con token, además de la habilidad de poder poner prioridades a la transmisión de paquetes. Bajo condiciones normales, la operación de este tipo de red es muy parecido a las redes token ring. Sin embargo existen diferencias en los métodos de control de acceso al medio (broadcast para el bus y secuencial para el anillo), los procedimientos que utiliza para el manejo y administración del anillo lógico, tales como inicialización y perdida del token, son manejados de manera diferente en ambos tipos de redes.

Las redes tipo token bus normalmente utilizan cable coaxial como medio de transmisión, operando en modo broadband o un modo de baseband modificado llamado **carrierband**.

La modulación y los circuitos de la interface, desarrollan las siguientes funciones:
- codificación de datos de transmisión (modulación).
- descodificación de datos de transmisión (demodulación).
- generación de señal de reloj.

El modo carrierband es el mismo baseband en el aspecto de que cada transmisión ocupa el ancho de banda (bandwidth) completo del cable, la diferencia radica en que en el modo carrierband todos los datos son primeramente modulados antes de que se transmitan. Además se puede mencionar que el formato del frame utilizado por este estándar es muy parecido al utilizado por los frames de tipo token ring.

Existe una interfaz estándar entre el modulo de interfaz física (PIM) y el DTE conectado. En algunos casos, el PIM es integrado sobre la tarjeta de comunicación dentro del DTE.

La topología utilizada para este estándar es de bus físico o tipo árbol, por otro lado, las estaciones son organizadas en forma de un anillo lógico. El estandar token bus especifica tres tipos de opciones para la capa física. El primero es un sistema broadband, el cual soporta canales de datos a 1, 5 y 10 Mbps con anchos de banda de 1.5, 6 y 12 Mhz respectivamente. El estándar recomienda el uso de un sistema dividido de un sólo cable con un traductor de frecuencia principal (la configuración de cable dual o doble también es permitida).

El segundo esquema es conocido como **carrierband** o **broadband de un solo canal** (single-channel broadband)[15]. El esquema carrierband especifica las tasas de transmisión en 1, 5 y 10 Mbps.

La más reciente adición al nivel físico del estándar 802.4 es una especificación de fibra óptica, en la que se especifican tres tasas de transmisión: 5, 10 y 20 Mbps.

La especificación de fibra óptica del estándar 802.4 puede ser utilizado con cualquier topología que sea lógicamente un bus. Esto es, una transmisión desde una estación cualquiera sea recibida por todas las demás estaciones, y si dos estaciones transmiten al mismo tiempo, una colisión ocurrirá. El estándar recomienda el uso de estrellas (activas o pasivas).

Cabe mencionar que esta norma no se implementa frecuentemente en el entorno de redes LAN. Siendo su mayor aplicación en las industrias de manufactura (fabricas automatizadas) y otras relacionadas con las industrias de control de procesos.

Parámetros	carrierband de fase continua	carrierband de fase coherente		broadband		fibra óptica
Tasa de transmisión (Mbps)	1	5	10	1	5	5, 10, 20
Ancho de banda (bandwidth)	N.A	N.A	N.A	1.5 Mhz	6 Mhz	270nm
centro de frecuencia	5 Mhz	7.5 Mhz	15 Mhz	*	*	800-900nm

Tabla 3.11a Opciones de la capa física para el estándar 802.4

[15]La señal carrierband significa que el espectro entero de el cable es dedicado a una sola ruta de transmisión para señales analógicas.

Parámetros	carrierband de fase continua	carrierband de fase coherente	broadband	fibra óptica
Modulación	manchester/ fase continua FSK	Fase coherente FSK	Multinivel duobinary AM/PSK	On-Off
Topología	bus (omni-direccional)	bus (omni-direccional)	bus direccional (árbol)	estrella pasiva u activa
Medio de transmisión	cable coaxial (75 ohms)	cable coaxial (75 ohms)	cable coaxial (75 ohms)	fibra óptica

Tabla 3.11b Opciones de la capa física para el estándar 802.4

3.4.1.2.2.3 IEEE 802.5 Token Ring

También llamada 802.1 de ANSI 1985, define los protocolos de acceso, cableado e interfaces para las LANs en anillo con testigo. IBM popularizó esta norma. Utiliza un método de acceso con testigo o token y se cablean físicamente en una topología en tipo estrella pero formando un anillo lógico. Los nodos se cablean a una unidad de acceso múltiple central (concentrador MAU) que repite las señales de una estación a la siguiente. Las unidades de acceso múltiple (MAUs) se cablean conjuntamente para extender la red, lo cuál implica el anillo lógico.

Este tipo de red es una concatenación de enlaces punto a punto (no broadcast como en el caso de ethernet aunque pueden realizar un broadcast de red local de manera secuencial con los enlaces punto a punto formando un circulo). La tecnología de redes en anillo es digital a diferencia de las redes ethernet donde el método de acceso al medio CSMA/CD puede ser analógico. Otra característica de las redes en anillo es su tiempo de respuesta ya que es determinístico aún bajo condiciones donde existe mayor carga.

Como se mencionó, las redes locales token ring son concatenaciones de enlaces punto a punto donde cada estación actúa como un repetidor, proveyendo a la señal la amplificación necesaria y la corrección necesaria de la misma. Los enlaces pueden ser realizados con cualquier tipo de medio, cable coaxial, par trenzado[16] blindado y fibra óptica.

El tamaño mínimo de un anillo deberá ser de un kilómetro (este tamaño es muy extenso sobre todo cuando se desean conectar pocas estaciones de trabajo dentro de un solo cuarto, por esta razón, se instala una estación especial designada como "monitor activo", el cuál adiciona un retraso de almacenamiento de 24 bits para el anillo. Este almacenamiento también compensa cualquier fase jitter acumulada

[16]Para redes token ring IBM, el cable par trenzado es el ideal. La fibra óptica puede ser utilizada para extender la red sobre grandes distancias.

sobre el anillo. El monitor activo es indispensable para el buen funcionamiento del anillo. El monitor activo no es una estación con dispositivos de red especial, de hecho cualquier estación sobre el anillo puede ser monitor activo y que las otras estaciones del anillo son designadas estaciones pasivas. La selección de que estación debe ser estación activa se lleva a cabo mediante el procedimiento de inicialización.

El estándar 802.5 especifica tres opciones de tasa de transmisión: 1 Mbps, 4 Mbps y 16 Mbps. La configuración a 1Mbps utiliza cable par trenzado UTP. Inicialmente, las configuraciones de 4 y 16 Mbps utilizaban cable STP. La demanda en el mercado hizo que estas configuraciones soportaran también cable UTP. Varios dispositivos soportan el uso de cable UTP para anillos de 4 y 16 Mbps (IBM en un principio no soportaba los 16Mbps sobre UTP. mas adelante al hacer equipo con Synoptics Communications propuso el estándar a IEEE 802.5). Las estaciones a 16Mbps no esperan el regreso del frame de datos para poner la señal de token otra vez sobre la red. Con este mecanismo, llamado el "**early token release mechanism**", dos frames pueden ser transmitidos simultáneamente sobre la red token ring.

Parámetros de token ring	tipo 1 y tipo 2	tipo 3
Núm. máximo. de dispositivos por anillo	260	96
Núm. mínimo. de dispositivos por anillo	2	2
tasa de transmisión de datos probados	16 Mbps	4 Mbps
Estación a una sola MAU[17] LAN	300 metros	100 metros
Estación a múltiples MAU LAN	100 metros	45 metros
Máximo número de MAUs por LAN	12	2
distancia entre MAU y MAU	200 metros	120 metros
distancia entre estaciones	no especificado	no especificado

Tabla 3.12 Reglas de cableo para redes token ring

Aunque el número máximo de estaciones con cable tipo 1 y tipo 2 son 260 estaciones permitidas, el número recomendado es de 100. El límite máximo de estaciones sobre el anillo es debido a la acumulación del clock jitter. También la distancia máxima entre estación y el MAU es de 300 metros.

[17]MAU unidad de acceso multiestación (no confundirlo con el dispositivo MAU para ethernet) es un centro de cableo donde pueden ser conectadas varias estaciones. Contienen dos puertos finales llamados ring in y ring out, estos sirven para interconectar múltiples MAUs juntos.

3.4.1.2.2.3.1 Tamaño del anillo

Una red token ring que utiliza cable STP, tal como los cables de IBM tipo 1 y tipo 2, tiene un número máximo de estaciones que pueden ser conectadas en un solo anillo limitado a 260 (aumentar el numero de estaciones arriba de este numero causa problemas en el jitter clock haciendo fallar al anillo). para tener el mínimo anillo utilizable, el número mínimo de estaciones son dos.

En este estándar solo se especifica el tipo de medio par trenzado blindado (STP) con tasas de transmisión de 4 y 16 Mbps utilizando el método Manchester diferencial de codificación de señal.

Por último se puede mencionar que el estándar X3T9 referente a la **Interfaz de Datos Distribuido por Fibra** (FDDI: Fiber Distributed Data Interface y CDDI) se basa en el protocolo de anillo con testigo 802.5 token ring. Pero este estándar X3T9 fue desarrollado por el Comité de normas acreditadas (ASC, Accredited Standards Commitee). Además el estándar X3T9 es compatible con el estándar 802.2 control de enlace lógico (LLC) y asi con otras normas 802.x referentes a la conexión de red.

3.4.1.3 Otros estándares del IEEE

3.4.1.3.1 802.6 Red de área metropolitana (MAN: Metropolitan Area Networks)

La norma 802.6 del IEEE para redes de áreas metropolitana (MAN Metropolitan area network) define un protocolo de alta velocidad en el cual las estaciones enlazadas comparten un bus doble de fibra óptica que utiliza un método de acceso llamado Bus dual de cola distribuida (DQDB: Distributed Queue Dual Bus). Este bus ofrece tolerancia a fallos para mantener activas las conexiones en caso de que falle o llegue a romperse el bus. La norma MAN se designa para proporcionar servicios de datos, voz y video en una área metropolitana de aproximadamente 50 kilómetros, con una velocidad de transmisión de datos de 1.5, 45 y 155 Mbps. El DQDB es el protocolo subyacente de acceso para SMDS (Servicio de Conmutación de Datos Multimegabit, Switched Multimegabit Data Service), que ofrecen la mayoría de las compañías de telecomunicaciones públicas como una forma de construcción de redes privadas en áreas metropolitanas. DQDB es una red de transmisión de celdas conmutadas con una longitud fija de 53 bytes, por lo tanto, es compatible con la ISDN de banda ancha (ISDN-B) y el Modo de Transferencia Asíncrono (ATM: Asynchronous Transfer Mode). La conmutación de celdas tiene lugar en el nivel de control de enlace lógico 802.2.

Los servicios MAN son tanto orientados como no orientados a la conexión, y/o isócronos (video en tiempo real). El bus tiene una serie de ranuras de longitud fija

donde se sitúan los datos para su transmisión sobre el bus. Así, cualquier estación que necesite transmitir, simplemente sitúa los datos en una o más ranuras. No obstante, para acomodar datos isócronos sensibles al tiempo, se reservan unas ranuras a intervalos regulares para garantizar que los datos lleguen a tiempo y en orden (secuencial).

3.4.1.3.2 802.7: Grupo asesor para técnicas de banda ancha

Este comité proporciona consejos técnicos a otros subcomités en técnicas de conexión de redes de banda ancha.

3.4.1.3.3 802.8: Grupo asesor para técnicas de fibra óptica

Grupo que ofrece consejo a otros subcomités de redes que utilizan fibra óptica como una alternativa a las redes actuales basadas en cables de cobre.

3.4.1.3.4 802.9: Redes integradas por voz/video

El grupo de trabajo 802.9 del IEEE trabajan en la integración de tráfico de voz, datos y video en LAN 802.X y en Redes digitales de servicios integrados (ISDNs, Integrated Services Digital Networks). Los nodos definidos en las especificaciones incluyen teléfonos, computadoras, además de codificadores/descodificadores (codecs) de video. Las especificaciones se han llamado Integración de Datos y Voz, o IVD (Integrated Voice and Data). El servicio proporciona un flujo multiplexado que puede llevar información de datos y voz por los canales que conectan las dos estaciones sobre cables de par trenzado de cobre. Se definen varios tipos distintos de canales entre los que se incluyen los canales dúplex no conmutados a 64 Kbits/seg., de conmutación de circuitos o de conmutación de paquetes.

3.4.1.3.5 802.10: Seguridad de red

Este grupo trabaja en la definición de un modelo normalizado de seguridad que interopera sobre distintas redes e incorpora métodos de autentificación y cifrado.

3.4.1.3.6 802.11: Redes inalámbricas

Este comité define las normas para redes inalámbricas. Trabaja en la normalización de diversos medios como: la radio de espectro expandido, radio de banda estrecha, rayos infrarrojos y transmisiones sobre líneas de potencia. El comité también trabaja en la normalización de interfaces inalámbricas para redes informáticas, donde los usuarios se conectan a sistemas de computadores que usan computadoras basadas en lápices, asistentes digitales personales (PDSs, Personal Digital Assistants) y otros dispositivos portátiles. Se han planeado dos enfoques

para las redes inalámbricas: Planteamiento distribuido y el planteamiento de punto de coordinación.

En el planteamiento distribuido, cada estación de trabajo controla su acceso a la red. En cambio, en el planteamiento de punto de coordinación, un concentrador central perteneciente a una red cableada controla las transmisiones de las estaciones de trabajo inalámbricas. El comité 802.11 favorece las redes con planteamiento distribuido.

3.4.1.3.7 802.12: LAN de Acceso de prioridad por demanda (100VG-AnyLAN)

Este comité define una de las normas de Ethernet a 100 Mbits/seg con el método de acceso de prioridad por demanda (Demand Priority Access Method) propuesto por Hewlett-Packard y otros fabricantes. El cable especificado es de par trenzado de cuatro hilos de cobre. El método de acceso al medio llamado "método de prioridad por demanda" utiliza un concentrador central para controlar el acceso al canal de comunicación compartido. Las prioridades están disponibles para soportar la distribución de la información multimedia en tiempo real (este estándar se estudiará mas a detalle en el capítulo 7).

3.4.2 Estándar de cableado estructurado EIA/TIA 568

3.4.2.1 Cableado estructurado

Un sistema de cableado estructurado consiste en una infraestructura de cableado flexible que puede soportar múltiples computadoras y sistemas de telefonía de un modo independiente de su fabricante. En el cableado estructurado cada estación es alambrada hacia un punto central utilizando una topología en estrella facilitando el sistema de interconexión y administración. Este aprovechamiento permite la comunicación virtualmente con cualquier dispositivo, donde sea y en cualquier momento. Un plan de alambrado bien diseñado puede incluir varias soluciones de cableado independientes con diferentes tipos de medios instalados para cada estación de trabajo para soportar y desarrollar requerimientos.

La especificación actual[18] ANSI/EIA/TIA-568 es el estándar de cableado estructurado de telecomunicaciones comerciales.

El propósito del estandar EIA/TIA 568 es:
- Establecer un estándar de cableado de telecomunicaciones para que soporte un ambiente no propietario (multiproveedor o sistema abierto).

[18]American National Standars Institute (ANSI), Electronic Industry Association (EIA) y Telecommunications Industry Association (TIA).

- Facilitar la planeación e instalación de un sistema de cableado estructurado en organizaciones comerciales.
- Establecer el desempeño y criterios técnicos para diferentes sistemas de cableado.

El estándar EIA/TIA 568 especifica los siguientes puntos:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente corporativo.
- Recomendaciones de topologías y distancias.
- Parámetros de los medios los cuales determinan el desempeño.
- Asignaciones de pines para conectores para asegurar la interconectividad.
- El tiempo de vida de un sistema de cableado para telecomunicación (es?) de 10 años.

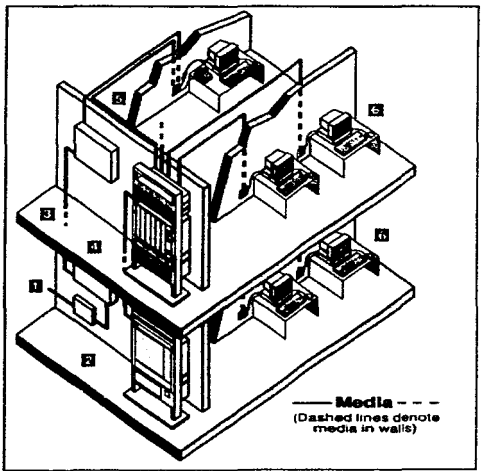


Figura 3.12 Descripción de los seis subsistemas de un sistema de cableado estructurado (fuente ANIXTER, http://anixter.neog.com)

El EIA/TIA 568, describe seis subsistemas de un sistema de cableado estructurado:

1. Entrada a la Estructura (Building entrance facilities)
2. Habitación de equipo (Equipment room)
3. Cableado de bbackbone (Backbone Cabling)
4. Armario(Closet) de telecomunicaciones (Telecommunications Closet)
5. Cableado horizontal (Horizontal Cabling).
6. Área de trabajo (Work Area).

1. Entrada a la estructura:
Es donde la parte externa del servicio de telecomunicaciones entra al edificio y se interconecta con los sistemas de telecomunicaciones internos del edificio o de la estructura. En una ambiente de campus o multi-edificios. La entrada de telecomunicaciones puede también contener la interconexión del backbone entre edificios (buildings backbone interconnects).[19]

2. La habitación de equipo:
Es el área en un edificio donde está localizado el equipo de telecomunicaciones. Partes de, o todo el sistema de cableado de telecomunicaciones termina en esta área[1]. Esta área es generalmente de mayor complejidad que los armarios de telecomunicaciones. Algunas o todas las funciones de un armario de telecomunicaciones pueden ser provistas por la habitación de equipo.

3. Cableado del backbone (Backbone Cabling):
4.
Este provee la interconexión entre closets de telecomunicación, habitaciones de equipo y entrada de la estructura. Este consiste del backbone, cross-connects[20] principales y intermedios, terminaciones mecánicas y patch cords o jumpers utilizados para conexiones backbone-backbone, Esto incluye:

- Conexión vertical entre pisos (risers).
- Cables entre habitaciones de equipo y entradas de la estructura.
- Cables entre edificios (interconexión de edificios o interbuilding).

Tipos de medios de cable reconocidos y distancias máximas para el backbone (Maximum Backbone distancies):

El backbone debe ser una topología en estrella. La longitud máxima por enlace es dependiente del tipo de medio utilizado.

---

[19]Los requerimientos de diseño son definidos en el estándar EIA/TIA-569.
[20]Productos de Conectores-Cruzados (Cross-Connect Products). Estos productos de conectores cruzados proveen un principio de terminación para cable mientras establece un campo para movimientos de administración, adiciones o cambios. Existen dos tipos de equipos conectores cruzados : Patch Panels y Punch-down blocks.

Tipo de cable	Distancia
100 ohm UTP (24 o 22 AWG)	800 metros (Voz)
150 ohm STP	90 metros (Datos)
Fibra óptica Multimodo 62.5/125 mm	2000 metros
Fibra óptica monomodo (Single mode) 8.3/125 mm	3000 metros

Tabla 3.13 Distancias permisibles para el tipo de cable

Nota: las distancias de cableado del backbone son dependientes de la aplicación. Las máximas distancias especificadas en la tabla están basadas en aplicación de transmisión de voz para UTP, transmisión de datos para STP y fibra. La distancia de 90 metros para aplicaciones STP con un espectro ancho de banda (bandwidth) de 20Mhz a 300Mhz. Una distancia de 90 metros también se aplica a cable UTP a un espectro de ancho de banda (bandwidth) de 5Mhz-16MHz para CAT 3, 10Mhz CAT4 y 20Mhz-100Mhz para CAT5.

Las distancias actuales dependen del tipo de sistema, velocidad de datos y especificaciones del proveedor para los sistemas electrónicos y los componentes asociados. En la actualidad el estado-del-arte de la facilidades de distribución usualmente incluye una combinación de cables del tipo de cobre y fibra óptica para el backbone.

Otros requerimientos del diseño :

- Topología en estrella.
- No mas de dos niveles de jerarquía de cross-connects (hierarchical levels of cross connects)
- No son permitidos los derivadores de puente (Bridges taps).
- Cableado de interconexión de tablas de parcheo principales e intermedios no deberán exceder la longitud de 20 metros.
- Evitar la instalación en áreas donde puedan existir equipos que generen altos niveles de interferencia EMI/RFI.
- El nivel de tierra eléctrica deberá soportar los requerimientos definidos en el estándar EIA/TIA 607.

4. Armario de Telecomunicaciones:
Es un área dentro del edificio, en el que se localizan el equipo de sistema de cableado de telecomunicaciones. Las funciones que toman lugar en el armario[12] incluyen los terminadores mecánicos y/o cross connects para interconexión de los puntos de cableado horizontales y(backbone.

5. Cableado Horizontal
El cableado horizontal es la porción del sistema de cableado que se extiende desde la caja de contactos del área de trabajo (outlets) hasta el armario de telecomunicaciones. El Cableado Horizontal es una topología en estrella, que consiste de lo siguiente:

- ·Cableado Horizontal
- ·Contactos de telecomunicación en el área de trabajo (outlets de telecomunicaciones)
- ·Cable terminador
- ·conexión cruzada (Cross-connection).

Tres tipos de medios son reconocidos como opciones para el cableado horizontal, cada una tiene una extensión de distancia máxima de 90 metros.

El subsistema horizontal permite el uso de :
- ·4 pares de 100 ohms de cable UTP para voz (24AWG).
- ·4 pares de 100 ohms UTP/STP.
- ·2 pares de 150 ohms STP.
- ·cable coaxial de 50 ohm (10Base2). Este no es muy recomendado para nuevas instalaciones.
- ·cable de fibra óptica 62.5/125 mm. para datos.

En adición a los 90 metros de cableado horizontal, un total de 10 metros es permitido para el área de trabajo, la tabla de parcheo del closet de telecomunicaciones y los cables jumper.

Cada área de trabajo permitirá tener un mínimo de dos contactos de telecomunicación (enchufes u outlets), uno para voz y otro para datos.

6. Área de Trabajo
Interconecta al cableado horizontal a los contactos de telecomunicaciones en la pared para los dispositivos de los usuarios. El cableado del área de trabajo esta diseñado para ser relativamente simple para la conecxión. La máxima distancia permisible para los cables de parcheo es de 3 metros, basado sobre el mismo tipo de cable que es utilizado para el Cableado Horizontal.

Los componentes son :
- ·Equipo terminal (estación, teléfonos, impresora etc.).
- ·Cables de Parcheo- cordones modulares, cables adaptadores para PC's, jumpers para fibra, etc..
- ·Adaptadores- baluns, etc. Deberán ser externos a el conector de telecomunicaciones (outlet communications)

Por último, ISO actualmente esta desarrollando un estándar de sistema de cableado sobre base internacional con el titulo **Generic Cabling for Customers premises Cabling** ISO/IEC 11801.

3.4.3 Redes inalámbricas

Las redes inalámbricas son una nueva herramienta para los diseñadores de enlace de redes, es basada en tecnología inalámbrica. Los segmentos de redes locales inalámbricas pueden ser totalmente utilizables en ambientes donde el sistema de cableado es difícil de implementar (depósitos aislados, áreas de recepción o departamentos donde los grupos de trabajo se mueven frecuentemente). Esta tecnología aun esta en sus primeros desarrollos y contiene un número de limitaciones en las que se incluyen el ancho de banda (bandwidth), ésta tecnología se esta desarrollando de manera rápida y se piensa que llegará a ser más popular cuando el precios de los dispositivos que utiliza para su implantación bajen.

Actualmente las redes locales inalámbricas usan una de tres tecnologías: rayos infrarrojos, propagación de espectro (spread spectrum), o radio de banda corta (narrowband radio).

3.4.3.1 Redes locales inalámbricas por medio de rayos infrarrojos

Las redes locales inalámbricas basadas en rayos infrarrojos ofrecen varias ventajas para los usuarios, ya que pueden igualar las velocidades de redes locales basadas en sistema de cableado (incluyendo la velocidad de 16Mbps que ofrece token ring). Su precio y radio de desarrollo son mucho más favorables que las redes locales basadas en la tecnología de propagación de espectro. Un tercer beneficio es que las señales de rayos infrarrojos ofrecen una mayor seguridad que las señales ofrecidas por propagación de espectro.

Una limitante de esta tecnología es que requiere una clara línea de señal entre los transmisores y receptores. Cuando las redes locales inalámbricas basadas en rayos infrarrojos son utilizadas para llevar a cabo conexiones extramuros como la tarea de conexión de edificios que cruzan un pequeño parque por ejemplo, sus señales son susceptibles a interrupciones durante condiciones ambientales adversas. Otra limitante, es que puede transmitir solo sobre distancias limitadas de aproximadamente 100 pies.

A principios de 1994 la Asociación de Datos por Infrarrojo (Infrared Data Association) introdujo un estándar de codificación y descodificación por medio de rayos infrarrojos. Este conjunto de especificaciones asegura que en el año de 1995 existirá interoperabilidad entre productos basados en infrarrojos desarrollados para computadoras móviles (actualmente Apple ha anunciado que tendrá soporte para este estándar).

Línea de Señal (Line-of-sight): La variedad de tecnología de infrarrojos Line-of-sight es limitada a lugares como oficinas donde no existan obstrucciones físicas

para la señal entre las estaciones de usuarios. Aun que la naturaleza punto a punto de esta tecnología restringe la distancia alrededor de 100 pies , la velocidad de transmisión puede igualarse a las redes basadas en el sistema de cableado que se encuentre en dicha instalación.

Infrarrojos por diseminación (Scatter infrarred): La tecnología de redes locales de infrarrojos por diseminación rebota las señales lejos de las paredes y del techo para iluminar un área de aproximadamente 100 pies. Esta característica produce una señal con una velocidad relativamente baja.

Rayos infrarrojos reflexivos (reflective infrared): En sistemas reflexivos, dispositivos (transceivers) ópticos son montados cerca de las estaciones PC y son dirigidos hacia un spot común sobre el techo de la oficina. Esta propuesta trabaja bien en un ambiente con techos altos.

Ventajas	Desventajas
Iguala velocidades de redes locales basadas en sistema de cableado.	Es susceptible a interrupciones por condiciones ambientales adversas
	Requiere una clara línea de señal

Tabla 3.14 Resumen de ventajas y desventajas

3.4.3.2 Redes locales inalámbricas por medio de propagación de espectro de radio

Desarrollado por los militares para brindar un transmisión eficaz y segura, la tecnología de propagación de espectro utiliza una de dos técnicas para "propagar" datos sobre varias frecuencias. La técnica de **secuencia directa de acceso múltiple por división de código** (secuencia directa CDMA) este opción representa cada bit por un bit patrón llamado "chip". Unos (1s) y ceros (0s) son representados por chips que son inversos uno del otro. Cada bit es propagado sobre un espectro de amplia-frecuencia (wide-frecuency) cuando es transmitido. El receptor colapsa cada chip atrasado dentro de un solo bit. Por que todas las señales que no son igualadas son eliminadas, dando como resultado una señal libre de interferencias.

En los Estados Unidos, un canal de 83Mhz de amplitud es disponibles desde 2.4000 a 2.4835 Ghz para operaciones sin licencia. Esta banda de frecuencia es dividida dentro de canales (referidos también como hops) de 82 1-Mhz. Los adaptadores se sintonizan en un canal especifico durante un corto período de tiempo y entonces se mueven a un diferente canal (hop). Los canales son visitados en un orden predefinido, como es especificado por la secuencia de canalización. Todas las estaciones participantes dentro de la misma red usan el misma secuencia de

canalización y sincronizan sus temporizadores de canal. Cuando la interferencia esta presente, esta usualmente afecta solo a unos pocos canales.

Las secuencias de canalización son diseñadas de manera que canales sucesivos se encuentren separados por varios Mhz.

El FCC autorizó que tres bandas de frecuencia separadas se establecieran aparte para redes locales basadas en radio comercial: 902-928 Mhz, 2.4- 2.5 Ghz, y 5.8 -5.9 Ghz. Muchos de los primeros productos para redes inalámbricas fueron diseñados para trabajar en el rango de banda industrial, científico y médico (ISM) sin licencia de 902-928 Mhz. En 1993, la tendencia cambió cuando más compañías ofrecieron productos en las otras dos bandas ISM mas altas. Cabe hacer notar que mientras más alta sea la frecuencia seleccionada, más altos son los costos de los dispositivos. Además de que no importa que banda de frecuencias se utilice el resultado es el mismo.

La tecnología de propagación de espectro puede transmitir sus señales de baja frecuencia a través de materiales de construcción comunes y de esta manera cubrir una mayor área que otras alternativas de redes locales inalámbricas. Mientras que la inmunidad virtual a señales de interferencia y la seguridad significante que provee, complementa su propagación de espectros a un rango extenso, la mayor limitante de esta tecnología ha sido su considerable consumo de ancho de banda (bandwidth) que da como resultado una relativamente baja velocidad de transmisión comparada con otras tecnologías de redes inalámbricas.

Problemas de interferencia con la tecnología de propagación de espectros
Existen algunos problemas con la interferencia cuando son instalados dos equipos de propagación de espectro uno al lado del otro. Otras formas de emisión electromagnética y maquinaria pesada también afectan el rendimiento de la propagación de espectros.

Ventajas	Desventajas
No es requerida una licencia FCC	Distancia limitada (1watt de poder tiene un limite de cobertura de alrededor de 800pies)
Una alta inmunidad a interferencia	posibles conflictos de frecuencia con múltiples redes locales en un ambiente alto - levantamiento (high-rise)
No es requerida una línea de señal	

Tabla 3.15 Resumen de ventajas y desventajas

3.4.3.3 Redes inalámbricas de radio de banda corta

El uso dedicado de redes locales de radio de banda corta, tienen una licencia de ancho de banda (bandwidth) de 18 a 19GHz, el cual es asignado por el FCC. Debido a que el ancho de banda utilizado por la tecnología de radio de banda corta es mayor que el rango de propagación de espectro, la tasa de transmisión es generalmente mayor que aquellas encontradas en la tecnología de propagación de espectros. Esta tecnología no puede atravesar muros de metal o muros concreto presente dentro de una estructura, pero su alta frecuencia lo habilita cubrir un radio de 5000 pies[3].

3.4.3.4 Especificaciones del comité 802.11 redes inalámbricas

El comité 802.11 ha sido el que desarrolló de las especificaciones para redes inalámbricas que soportarán punto-a-punto, ad-hoc, y la infraestructura de redes locales interconectadas vía un punto de acceso con una red existente con sistema de cableado. Los protocolos desarrollados permitirán al usuario móvil andar con toda libertad por todo un campus mientras mantiene la misma conexión a los recursos de red. Estos protocolos también permitirán el poder de conversación, los cuales serán disponibles dentro de pequeños dispositivos de computadoras móviles para comunicarse por largos periodos de tiempo con una sola carga de batería.

El comité esta definiendo los protocolos para redes inalámbricas del rango de 900MHz, 2.4GHz, y bandas de frecuencia infrarroja. Además también define diferentes especificaciones físicas (PHY) para protocolos que dependen del medio. Existen diferentes especificaciones PHY para cada banda de frecuencia soportada por el estándar 802.11. Existen especificaciones de control de acceso al medio (MAC) para redes inalámbricas ad-hoc e infraestructuras de redes inalámbricas. Un solo protocolo MAC independiente del medio provee una interface de red unificada entre diferentes PHY inalámbricos y redes con sistema de cableado.

Los requerimiento de usuario para redes locales inalámbricas establecidas por el 802.11 (Marzo de 1992) incluyen el soporte para todos los anchos de banda (bandwidth) de 1Mbps o más en las siguientes áreas de aplicación:

- Transferencia de archivos y control remoto.
- Carga de programas (program loading)
- Paginación de programas (program paging)
- Proceso de transacción
- Multimedia
- Control y monitoreo de manufactura
- Manejo de material
- Sistemas carentes de tolerancia.

Concentradores o puntos de acceso

Como en las redes alambradas, los concentradores o puntos de acceso permiten a múltiples estaciones conectarse los servidores o con otras estaciones. En el caso de redes inalámbricas, sin embargo, los concentradores llevan a cabo dos tareas adicionales:

1. Puede proveer una conexión a un backbone para las unidades inalámbricas.
2. Un número de concentradores localizados estratégicamente puede extender el rango para cada estación con acceso a la red.

A diferencia de redes alambradas como 10BaseT, algunas redes inalámbricas pueden ser establecidas sin utilizar concentradores del todo.

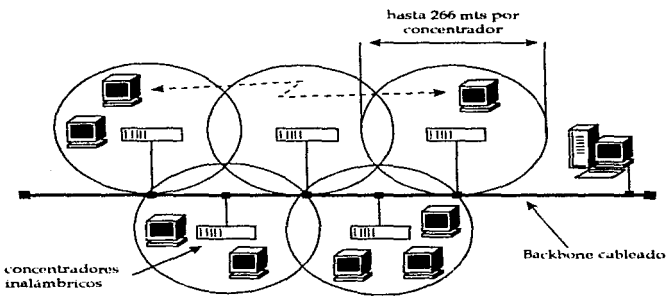


Figura 3.13 Bus realizado con concentradores inalámbricos

3.4.3.5 Puentes entre edificios para la interconexión de redes locales inalámbricas

Existen varios puentes de propagación de espectro los cuales pueden conectar edificios con una distancia de separación de hasta 3 millas a una velocidad de hasta 2Mbps. Un ejemplo de esta tecnología es la desarrollada por AirLAN/puentes, el cual transmite en la banda 902 a 928MHz, este dispositivo soporta tanto redes Ethernet como Token ring, además de ser compatible con muchos sistemas operativos en red. A una tasa de transmisión de 2Mbps este dispositivo puede

transmitir correo electrónico entre los edificios, pero tiene limitantes al transmitir archivos de datos de gran longitud.

Para enviar y recibir señales de datos, los puentes inalámbricos requieren de antenas espaciales. Dependiendo de los requerimientos de distancia y las demandas físicas del sitio, el tipo de antenas usados variará dependiendo de las bases del caso.

Factores de retraso en la implantación de redes locales inalámbricas

Existe un número de razones por las cuales las redes locales inalámbricas aun no ha llegado a ser popular.

El alto costo del equipo aunado con la rápida declinación de los precios de los dispositivos Ethernet basados en cableado, ha dado como resultado muy difícil la justificación de una red local inalámbrica.

Una segunda razón por la cuál las redes locales inalámbricas no han llegado a ser tan populares es que el estándar ha sido desarrollados de manera lenta. El IEEE 802.11 ha tomado su tiempo de finalización de especificaciones, y las corporaciones han llegado a ser poco dispuestos a investigar productos que puedan resultar ser propietarios.

3.4.3.6 Redes híbridas: inalámbricas y cableadas

Hace pocos años la compañía AT&T introdujo una red inalámbrica basada en propagación de espectro, WaveLAN, como un reemplazo inalámbrico para redes locales con sistema de cableado ; el cual falló. La diferencia de precios entre los dos sistemas(inalámbrico y cableado) fue y es aún muy grande para justificar grandes redes locales inalámbricas, excepto donde las condiciones hacen imposible llevar a cabo un sistema de cableado convencional. Actualmente, el mercado de productos AT&T cuenta con una solución híbrida para ambientes difíciles que necesitan ser conectados a una red local con sistema de cableado.

Cuando las compañías se muevan con tendencias a las redes que incorporan todas las partes de una compañía, la tecnología de redes inalámbricas tendrán una tarea mas importante y significativa. Mientras tanto, durante los próximos años la tarea se mantendrá dentro de redes híbridas, proveyendo segmentos de red inalámbricos donde el sistema de cableado convencional no es fácil de implantar. La tecnología inalámbrica esta ligada a jugar un papel mucho más significativo, sobre redes de área amplia antes de que tome ventaja en redes locales.

La tecnología infrarrojos ofrece velocidades de transmisión consistente con los sistemas de redes cableadas; desafortunadamente, las distancias de transmisión son limitadas y los usuarios de la red frecuentemente deben estar situados con una línea de señal para este tipo de red para que su funcionamiento se lleve apropiadamente. La tecnología de propagación de espectro ofrece menos velocidad de transmisión (alrededor de 2Mbps), pero brinda grandes distancias, al mismo tiempo mas soporte por parte de los vendedores. La técnica roaming pionera por Xircom permite a los usuarios moverse a través del edificio mientras su señal es pasada por acceso de estación en estación.

CAPÍTULO 4
PROTOCOLOS DE COMUNICACIÓN

4.1 Sistemas abiertos: TCP/IP y OSI

El escoger protocolos de red para sistema abierto es muy importante, ya que son la base para integrar todos los recursos de cómputo de una institución, haciéndolos disponibles a todos. Existen varios estándares que satisfacen estos requerimientos. Aunque estas soluciones de sistemas abiertos no están aún disponibles totalmente, las personas que estén planeando implantar un sistema abierto tienen que seleccionar sistemas que soporten sus necesidades actuales y futuras.

4.1.1 La diversidad de la computación

Las redes de computadoras son una componente indispensable en el mundo de la computación. Actualmente, tanto ingenieros, científicos como trabajadores de oficina, dependen de las computadoras personales y estaciones de trabajo que se conectan mediante redes (LANs), para compartir recursos, tanto dentro, como fuera de la institución. Al conectarse a otras redes, se tiene acceso a computadoras centrales (mainframes), minicomputadoras, supercomputadoras y al procesamiento en paralelo, para aprovechar el poder de procesamiento de estos equipos. Las tecnologías para interconectar estos sistemas son diversas, complejas y frecuentemente incompatibles.

Los estándares para la comunicación son parte de la solución a este problema de sistemas incompatibles. Hoy en día, existen dos conjuntos principales de estándares de protocolos de comunicación de datos, el primero es el conjunto de protocolos TCP/IP y el segundo es el modelo de **Interconexión de Sistemas Abiertos** (OSI: Open System Interconnection) de la ISO.

4.1.2 ¿Por qué dos conjuntos de Protocolos?

TCP/IP y OSI proveen varias capacidades similares: la interconexión de computadoras tanto en redes locales (LAN) como en redes de área amplia (WAN), enrutamiento de la información entre las redes, retransmisión confiable de datos, transferencia de archivos, acceso remoto a computadoras, y el correo electrónico. Sin embargo, hay algunas diferencias, con respecto al despliegue, la disponibilidad de aplicaciones y características técnicas en los dos conjuntos de protocolos. El gobierno de los Estados Unidos ha apoyado el desarrollo de ambos, dando apoyo financiero directo al desarrollo de TCP/IP como una solución inicial o temprana para resolver la incompatibilidad de los sistemas de red, Y ha

colaborado con la industria para desarrollar e implementar estándares internacionales para OSI, creando sistemas abiertos globales adaptativos.

4.1.3 El desarrollo de TCP/IP

El conjunto de protocolos de TCP/IP, es más viejo que OSI y se ha usado durante varios años. TCP/IP se implementó sobre **Internet**; varios miles de redes y varios millones de computadoras son usadas por investigadores, en universidades e instituciones, tanto publicas como privadas, para el intercambio de información y colaboración. Los protocolos TCP/IP fueron incluidos en el sistema operativo UNIX, específicamente en la versión de la Universidad de Berkeley o UNIX BSD, que es muy popular en estaciones de trabajo para uso científico, diseño y aplicaciones gráficas.

El gobierno federal respaldó el desarrollo del UNIX BSD, y continúa apoyando a TCP/IP indirectamente a través de **Red de la Fundación Nacional de las Ciencias** (NSFNET: National Science Foundation Network), **NSI** (NASA Science Internet), la **Red de Ciencias de Energía** (ESnet: Energy Sciences Network), y mediante **la Agencia de Proyectos Investigación Avanzada de la Defensa** (DARPA: Defense Advanced Research Projects Agency), estas organizaciones patrocinan la investigación para la mejora de los servicios de la red. El **UNIX BSD** y **TCP/IP** ha sido usado por estudiantes en universidades, especialmente en los Estados Unidos, por mas de una década; como resultado, TCP/IP es entendido por muchos usuarios, integradores sistemas, y desarrolladores.

TCP/IP está implantado más ampliamente que OSI. Esta popularidad pudo surgir de la fácil disponibilidad de las implantaciones comerciales de TCP/IP las cuales pueden proveer soluciones sobre TCP/IP sin tener que invertir grandes cantidades en el desarrollo de los protocolos. Con una inmediata recuperación o reembolso de sus inversiones, los desarrolladores pueden concentrar recursos para mejorar sus productos de redes basados en TCP/IP.

4.1.4 El desarrollo de OSI

El éxito de TCP/IP como una solución para las comunicaciones de datos entre sistemas de computadoras heterogéneas puede ser la causa de la lentitud del desarrollo de aplicaciones para OSI. OSI es la norma internacional aceptada para comunicaciones de datos, sin embargo, está esperando llegar a ser el reemplazo de TCP/IP. OSI se creo para el uso de un número creciente de países alrededor el mundo: la Comunidad Europea legisla OSI; el Gobierno de Estados Unidos ordena OSI (y los gobiernos estatales siguen); Australia tiene adoptado OSI, como tiene Japón, Taiwan, y los Países Nórdicos. OSI es aceptado también por otros grupos con alcance internacional, tal como la Confederación Mundial de Grupos de Usuarios MAP/TOP.

Los estándares OSI fueron creados y evolucionaron en un proceso abierto, visible a los usuarios y suministrados en todo el mundo. Además, los estándares de OSI son sometidos a un proceso riguroso de pruebas que mejora la calidad de sus productos. Las ventajas y desventajas de TCP/IP y OSI están en la facilidad de las comunicaciones de datos entre computadoras heterogéneas. TCP/IP y OSI, pueden interactuar por medio compuertas (gateways), y complementarse el uno al otro. El protocolo de OSI para el enrutamiento de paquetes (CLNP), que corresponde al IP, se despliega en un segmento importante y creciente del Internet compuesto en su mayoría por TCP/IP. CLNP es un protocolo más robusto que IP y tiene un campo mas grande y versátil para direccionar. Un gran número de compuertas (gateways) existen para interoperar con el correo electrónico (SMTP) de TCP/IP y el Sistemas de Manejo de Mensajes referido comúnmente como X.400; El protocolo de TCP/IP para transferir archivos (FTP) se utiliza de manera rutinaria sobre el Internet, el protocolo de OSI para el traslado de archivos, acceso y gestión (FTAM) se usan también sobre el Internet; algunos de los primeros servicios de directorios de OSI (X.500) están siendo utilizados sobre Internet.

Una de las razones de la popularidad de TCP/IP puede ser su bien conocida **Interface de Programación de Aplicaciones** (API): **sockets** y **streams**. Los productos comerciales tienen que ser implantados usando TCP/IP para distribuir servicios a través de la red; por ejemplo, SQL accede a bases de datos relacionales, los servicios de archivos en red permiten montar sistemas de archivo remotos, se permite el despliegue gráfico en sistemas remotos. X-Windows y los sistemas de ventanas propietarias operan sobre TCP/IP.

OSI provee APIs equivalentes que pueden ser usados por los mismos vendedores de software, dando las mismas características de TCP/IP y otras adicionales, tales como el acceso a SQL y las interfaces con ventanas (windows), además otras especificaciones están siendo desarrollados para ser integradas dentro de la capa de servicios de la arquitectura OSI de una manera estándar, haciendo que la capa de servicios sea más robusta y compleja.

Los servicios de aplicación más importantes de TCP/IP son: la Transferencia Simple de Correo (SMTP: Simple Mail Transfer Protocol), Transferencia de Archivos (FTP), y Acceso remoto (Telnet). Cabe decir, que los servicio de aplicación de OSI, actualmente proveen una funcionalidad mayor que los servicios de TCP/IP, por ejemplo, el servicio de correo electrónico (X.400) de OSI provee una estructura con la cual puede manejar todos los tipos de información existentes, no solo es un sistema de mensajes personales; los servicios de terminal virtual de OSI soportan más que una simple terminal de carácter (formatos, tipos de páginas, y modos de barra de desplazamiento de ventana "scroll bar"); el servicio de directorios distribuido de OSI (X.500) es mucho más robusto y eficiente que el equivalente de TCP/IP, que es un servicio centralizado de directorios (Whois).

OSI también provee capacidades técnicas mejoradas sobre TCP/IP. Por ejemplo, el espacio de direccionamiento de TCP/IP es de 32 bits (que se esta agotando rápidamente) mientras que en OSI las direcciones de red comprenden 160 bits, un tamaño que proveerá un direccionamiento global en el futuro. Los protocolos de enrutamiento de OSI soportan un tipo de enrutamiento jerárquico, reduciendo la cantidad de información de enrutamiento que fluye en la red y que debe almacenarse en los nodos de conmutación. Cabe hacer notar que los servicios de conmutación de OSI deberán proveer un mecanismo de transición sobre el Internet como el espacio de direcciones limitado de TCP/IP.

OSI se construyó pensando en el futuro, mejorando las aplicaciones existentes y nuevas aplicaciones están siendo desarrolladas aun para proveer servicios adicionales a los usuarios. Las aplicaciones del **Sistema de Manejo de Mensajes** (MHS, X.400) proveerá seguridad y servicios de directorios estándares, conjuntamente con la capacidad del intercambio de datos electrónicos (EDI). Las aplicaciones FTAM están siendo mejoradas para poder transferir o manejar diferentes tipos de documentos, para facilitar las operaciones remotas sobre directorios y proporcionar operaciones de reinicio y recuperación. Las aplicaciones de Terminal Virtual están empezando a extenderse con diferentes tipos de terminales.

4.1.5 Se necesitan más mejorías

Tanto TCP/IP como OSI necesitan mejorías en las arquitecturas de sus capas superiores. TCP/IP utiliza unas técnicas de codificación anticuadas para los protocolos de las capas superiores, que son inferiores a la solución de OSI, el cual utiliza ASN.1. TCP/IP usa un tipo de direccionamiento referido como de "**bien conocidas**" para conectar los servicios de red; mientras que OSI confía en un directorio de nombres para encontrar la dirección para un servicio determinado. Pero por otro lado OSI forza a una estructura arbitraria de tres capas (sesión, presentación y aplicación) en sus capas superiores, creando construcciones ineficientes y haciendo que ciertas operaciones, como la encriptación, sean más difícil de lo necesario. Ninguna arquitectura provee la flexibilidad deseada para construir nuevos servicios de aplicación.

Ambas arquitecturas TCP/IP y OSI tienen deficiencias, como es la **seguridad**, **multicasting** y **multimedia**. En TCP/IP se están empezando a desarrollar estándares o propuestas para poder tener correo privado, incluyendo un sistema para una distribución certificada para el apoyo de un servicio de autenticación general, y también están bajo consideración propuestas para proveer seguridad en los servicios para la administración de red y enrutamiento. Kerberos, un sistema de autentificación por medio de llaves, con integridad y confidencialidad ,se ha desarrollado en el Instituto Tecnológico de Massachusetts (MIT) bajo el Proyecto Atena; el cual está siendo implementado en cientos de lugares en Internet. Los estándares de OSI están bajo desarrollo para la autenticación, la confidencialidad,

e integridad en la red, transporte, liga, y capas de aplicación, pero las soluciones tomaran varios años para estar listas.

Los protocolos de **multicasting** de área amplia están siendo considerados para Internet. OSI tiene un gran conjunto de capacidades para multimedia incluidos en los estándares de correo electrónico, mientras que en TCP/IP simplemente desarrollaron extensiones para soportar multimedia por medio de SMTP. Cabe mencionar que los protocolos de TCP/IP y OSI tienen capacidades para tiempo real, y servicios de multimedia.

4.1.6 ¿Como seleccionar un sistema abierto?

Se recomienda que las instituciones u organizaciones que instalen una nueva red o adquieran nuevos servicios de comunicación de datos, se apeguen a los protocolos provistos por OSI. Donde existan requerimientos específicos que van más allá de las capacidades disponibles de los productos OSI actuales, deberán complementarse con los otros protocolos de red actuales, mientras no se hayan terminado los protocolos de OSI completamente, comúnmente esto significa que se acepte soluciones propietarias

Puede haber ejemplos donde adquirir productos TCP/IP sea conveniente; por ejemplo, para agregarlos a una red grande ya existente con TCP/IP. Sin embargo, si la adquisición es de una tamaño importante, entonces los sistemas deberían adquirirse con la capacidad dual para manejar tanto TCP/IP como OSI, y los enrutadores deberían actualizarse para poder enrutar datos de TCP/IP como de OSI. Además, estos sistemas (frecuentemente llamados 'host duales') deberían incluir software para poder retransmitir aplicaciones entre TCP/IP y OSI. Estas capacidades se llaman frecuentemente 'aplicaciones de compuerta' (application gateways) o, mas específicamente, 'compuertas SMTP-X.400' para el correo electrónico y 'compuerta FTP-FTAM' para la transferencia de archivos, entre otros. De esta manera se están dando los primeros pasos para que las redes soporten trafico tanto de TCP/IP como de OSI y faciliten el intercambio de información entre computadoras OSI y TCP/IP. Una vez que estas capacidades estén funcionando, las futuras adquisiciones pueden convertirse para ocupar OSI en el lugar de TCP/IP.

A veces, la instalación de TCP/IP junto con OSI podría tener sentido cuando se instala una nueva red; por ejemplo, la adquisición de una red grande de enrutadores, servidores, y estaciones de trabajo que se tienen que integrar con algunas computadoras existentes más viejas en la red. Frecuentemente, una instalación de TCP/IP pueden existir para computadoras más viejas que no puedan manejar los protocolos OSI y tampoco puedan ser actualizadas. En estos casos, la manera de migración es directa: adquiera enrutadores (llamados enrutadores duales) capaces de conmutar datos entre OSI y TCP/IP además agregar algunos host-duales que tengan aplicaciones de compuerta. La nueva red

apoyará entonces el intercambio de información entre computadoras viejas existentes y los nuevos productos OSI.

4.2 TCP/IP

4.2.1 Introducción

El conjunto de protocolos TCP/IP fue desarrollado por el Departamento de Defensa de los Estados Unidos para permitir la comunicación entre sistemas independientes y multivendedor para compartir recursos a través de una interred común que utiliza una tecnología de conmutación de paquetes. TCP e IP son dos de los principales protocolos de este conjunto, por lo que la familia entera se refiere usualmente como TCP/IP. Los protocolos soportan los servicios tradicionales desde sus inicios, como la transferencia de archivos, el correo electrónico, y las sesiones remotas. Lo que hace interesante al conjunto de protocolos de TCP/IP es su adopción casi universal, así como su tamaño y el crecimiento que ha tenido sobre Internet.

4.2.2 Historia de TCP/IP

La historia de TCP/IP explica la historia de Internet. A fines de los años 60's y principios de los 70's, los centros de cómputo operaban de manera autónoma. En esos días, las redes no eran diseñadas para permitir que compartieran recursos entre usuarios de diferentes redes. Los usuarios tenían que ser capacitados para cada tipo de computadora y de red. Para solucionar este problema, el Departamento de Defensa creó la **Agencia de Proyectos de Investigación Avanzada** (ARPA: Advanced Research Projects Agency). Su objetivo principal fue el de proveer una red de comunicación entre computadoras que, a parte de poder sobrevivir un ataque nuclear, permitiera accesos remotos a computadoras distantes, compartición de archivos, y, aunque no estaba en el plan original de la red de ARPA, el correo electrónico. La red de ARPA fue nombrada ARPANET. Otros de los objetivos de ARPANET fue el permitir el acceso desde computadoras de propósito general (que ahora llamamos de escritorio) a computadoras especializadas (que ahora llamamos servidores). Estos son los principios del modelo **cliente-servidor**, que se usa actualmente en la mayoría de los servicios como en la transferencia de archivos (FTP), Telnet, y el e-mail.

La Internet global se inició alrededor de 1980 cuando ARPA comenzó utilizar en sus máquinas conectadas a sus redes los nuevos protocolos TCP/IP. ARPANET, se convirtió rápidamente en la columna vertebral del nuevo Internet, y fue utilizada para realizar muchos de los primeros experimentos con TCP/IP. La transición hacia la tecnología Internet se completó en enero de 1983, cuando la Secretaría de Defensa ordenó que todas las computadoras conectadas a redes de largo alcance utilizaran los protocolos TCP/IP. Al mismo tiempo, la Agencia de Comunicación de la Defensa (DCA), dividió ARPANET en dos redes separadas, una para la

investigación futura y otra para la comunicación militar. La parte de investigación conservó el nombre de ARPANET; la parte militar, que era un poco más grande, se conoció como red militar MILNET.

Para alentar a los investigadores universitarios a que adoptaran y utilizaran los nuevos protocolos, ARPA puso a su disposición una implantación de bajo costo. En ése tiempo, la mayor parte de los departamentos universitarios de ciencias de la computación utilizaban una versión del sistema operativo UNIX, conocido como UNIX Berkeley o UNIX BSD. Al proporcionar fondos a Bolt Beranek de Newman, Inc. (BBN), para implementar sus protocolos TCP/IP en la utilización de UNIX y al proporcionar fondos a Berkeley para integrar los protocolos a su sistema de distribución de software, ARPA fue capaz de llegar a más del 90% de los departamentos universitarios de ciencias de la computación.

La distribución de UNIX BSD se volvió popular ya que ofrecía mucho más que protocolos básicos TCP/IP. Además de los programas normales de aplicación TCP/IP, Berkeley ofrecía un grupo de utilidades para servicios de red que se parecían a los servicios de UNIX utilizados en una sola máquina. La principal ventaja de las utilidades Berkeley reside en su parecido con el UNIX normal.

El éxito de la tecnología TCP/IP y de Internet entre los investigadores de ciencias de la computación guió a que otros grupos la adoptaran. Dándose cuenta de que la comunicación por red pronto sería una parte crucial de la investigación científica, la Fundación Nacional de Ciencias tomó un papel activo al expandir el Internet para llegar a la mayor parte posible de científicos. Iniciando en 1985, se comenzó un programa para establecer redes de acceso distribuidas alrededor de sus seis centros con supercomputadoras. En 1986 se aumentaron los esfuerzos para el enlace de redes al proporcionar fondos para una nueva red de área amplia que sirviera de columna vertebral, llamada **NSFNET**, que eventualmente alcanzó todos los centros con supercomputadoras y los unió a ARPANET. Por último, en 1986, la NSF proporcionó fondos para muchas redes regionales, cada una de las cuales conecta en la actualidad importantes instituciones científicas de investigación en cierta área entre ellas la UNAM. Todas las redes con fondos de la NSF utilizan los protocolos TCP/IP y todas forman parte de la Internet global.

A siete años de su concepción, Internet había crecido hasta abarcar cientos de redes individuales localizadas en los Estados Unidos y el resto del mundo. Conectaba casi 20,000 computadoras en universidades, así como a centros de investigación privados y gubernamentales. El tamaño y la utilización de Internet ha seguido creciendo mucho más rápido de lo esperado. A finales de 1987, se estimó que el crecimiento había alcanzado un 15% mensual. En 1994, la Internet global incorporaba más de 3 millones de computadoras en 61 países.

La adopción de los protocolos TCP/IP y el crecimiento de Internet no se ha limitado a proyectos con fondos del gobierno. Grandes corporaciones

computacionales se conectaron a Internet, así como muchas otras grandes corporaciones, incluyendo: compañías petroleras, automovilísticas, empresas electrónicas, compañías farmacéuticas y de telecomunicaciones. Las compañías medianas y pequeñas se comenzaron a conectar en los años noventa. Además, muchas compañías han utilizado los protocolos TCP/IP en sus redes corporativas, aunque no han optado por ser parte de la Internet global.

La rápida expansión ha presentado problemas de escala no contemplados en el diseño original y ha motivado a los investigadores a encontrar técnicas para manejar grandes recursos distribuidos. Por ejemplo, en el diseño original, los nombres y direcciones de todas las computadoras conectadas a Internet se guardaban en un solo archivo que se editaba a mano y luego se distribuía a cada sitio en Internet. A mediados de los ochenta, fue obvio que una base central no sería suficiente. Primero, las solicitudes de actualización del archivo pronto excederían la capacidad de procesamiento del personal disponibles. Segundo, aunque existiera un archivo central apropiado, la capacidad de la red era insuficiente para permitir la distribución frecuente a cada sitio o el acceso por línea de cada sitio.

4.2.2.1 Crecimiento y tecnologías del futuro

Tanto la tecnología TCP/IP como Internet continúan evolucionando. Se siguen proponiendo nuevos protocolos. La NSF añadió una considerable complejidad al sistema, al introducir una red de columna vertebral, redes regionales y cientos de redes a nivel de campus. Otros grupos alrededor del mundo se conectan día con día a Internet. Sin embargo, el cambio más significativo no viene de la adición de conexiones de redes, sino del tráfico adicional.

Cuando nuevos usuarios se conectan a Internet y aparecen nuevas aplicaciones, los patrones de tráfico cambian. Cuando los físicos, químicos y biólogos comenzaron a utilizar Internet, intercambiaban archivos de datos sobre sus experimentos. Dichos archivos parecían muy grandes comparados con los mensajes de correo electrónico. Cuando Internet se volvió más popular y los usuarios comenzaron a buscar información utilizando servicios como gopher y el Web, el tráfico se incremento de nuevo.

Para incorporar el crecimiento de tráfico, la capacidad de la columna vertebral NSFNET ya se había incrementado tres veces, aumentando su capacidad aproximadamente 840 veces en comparación con la original; En 1995 se incrementó en un factor de 3. En la actualidad, es difícil visualizar un fin de la necesidad de mayor capacidad.

En la tabla 4.1 se resume la expansión de Internet y se ilustra un componente importante del crecimiento: el cambio en la complejidad, surge porque muchos grupos autónomos manejan partes de la Internet global. Los diseños iniciales para

muchos subsistemas dependen de un manejo centralizado. Se necesita mucho esfuerzo para extender dichos diseños e incorporar el manejo descentralizado.

	número de redes	número de computadoras
1980	0	10^2
1990	10^3	10^5
1997	10^6	10^8

Tabla 4.1 Crecimiento de Internet

4.2.3 Dependencia de los protocolos TCP/IP

En la figura 4.1, se muestra la dependencia entre los principales protocolos TCP/IP que se examinarán. Cada protocolo está colocado directamente arriba de los protocolos que utiliza.

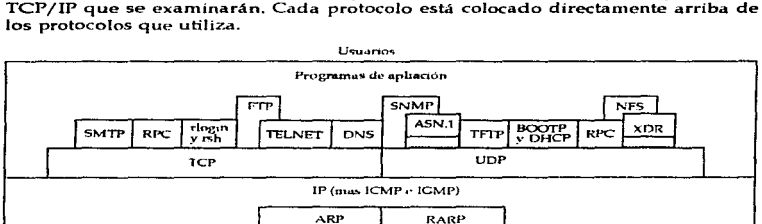


Figura 4.1 Dependencia entre los principales protocolos TCP/IP de más alto nivel.

La capa inferior representa todos los protocolos de control que proporciona el hardware, como por ejemplo ethernet, FDDI, ATM, etc.

La segunda capa está integrada por ARP y RARP. No todas las máquinas o tecnologías de red los utilizan. ARP es el más utilizado en Ethernet; RARP casi siempre se emplea en máquinas que no tienen disco.

La tercera capa contiene al IP (Internet Protocol), además del Protocolo de Mensaje de Error y Control Requerido (ICMP), y el Protocolo de Administración de Grupos Opcionales de Multibroadcast (IGMP).

El TCP y el UDP componen la capa de transporte. Existen nuevos protocolos de transporte pero ninguno se ha adoptado ampliamente aún.

La capa de aplicación ilustra las complejas dependencias entre los diversos protocolos de aplicación. Por ejemplo, FTP emplea las definiciones de la terminal virtual de red de TELNET para definir la comunicación en su conexión de control y al TCP para formar conexiones de datos. Así pues, el diagrama muestra que el FTP depende de TELNET y del TCP. El sistema de nombres de dominio (DNS) se vale del UDP y del TCP para la comunicación, de modo que el diagrama muestra ambas dependencias. NFS depende de los protocolos de representación externa de datos (XDR) y de la llamada de procedimientos remotos (RPC). RPC aparece dos veces porque puede utilizar el UDP o el TCP.

Como XDR y ASN.1 tan sólo describen las convenciones sintácticas y las representaciones de datos, no utilizan ni el TCP ni el UDP, en el diagrama se muestras como sistemas que no dependen de otros protocolos. Se han omitido varios detalles en el diagrama, por ejemplo, el IP depende del BOOTP/DHCP o varios protocolos dependen del DNS.

4.2.4 TCP/IP: protocolos de la capa de red y de transporte

4.2.4.1 IP: Protocolo de Internet (Protocolo de interconexión de redes)

El protocolo de la capa de red en TCP/IP es **Protocolo Internet** (IP: Internet Protocol), fue introducido a principio de los años 80's. A partir de esa fecha, otras redes lo han adoptado[21], por lo que es uno de los dos protocolos más importantes utilizados en la capa de red. El protocolo IP se define como un sistema de entrega de paquetes **sin conexión**, no confiable, y de tipo de **mejor esfuerzo** (A diferencia del protocolo X.25 que es orientado a conexión), por lo tanto los datagramas son transportados de manera transparente a las estaciones, pero sin seguridad. [22]

El término del protocolo IP no confiable se refiere a que la entrega de datagramas no es garantizada. Esto es debido a que no lleva a cabo ninguna relación con el control o confiabilidad del flujo, por lo que no existe capacidad para verificar que un datagrama enviado sea recibido correctamente. Tampoco tiene un algoritmo de verificación para el contenido de los datos de un datagrama, solamente realiza una suma de verificación para la información contenida en el encabezado del datagrama. Estas funciones de verificación y control de flujo se dejan a otros componentes de los protocolos de TCP/IP. El protocolo IP tiene solamente la capacidad de hacer una estimación del mejor enrutamiento para mover un

---

[21] El Protocolo Internet (IP) es el protocolo principal del modelo OSI, así como parte integral del TCP/IP. Aunque en su nombre lleva la palabra internet, su uso no se restringe a Internet. Es cierto que en Internet todas las estaciones lo deberán utilizar y entender. Pero este protocolo puede ser usado en redes dedicadas que no tengan ninguna relación con internet. IP define un protocolo no una conexión.

[22] Al poner todos los mecanismos de seguridad en la capa de transporte fue posible tener conexiones de extremo a extremo fiables, incluso cuando las redes subyacentes no brinden mucha seguridad.

datagrama al siguiente nodo a lo largo de una ruta, pero no verifica en forma inherente que la ruta seleccionada sea la más rápida o la más eficiente. Las tareas principales del protocolo IP son el esquema de direcciones y la administración del proceso de fragmentación de los datagramas.[23]

4.2.4.1.1 El protocolo IP proporciona tres definiciones importantes:

1. Define el formato de un datagrama de información: formato del encabezado con información relativa al datagrama y de los datos que llevará a través de las redes TCP/IP.
2. El software de IP define las funciones de enrutamiento, seleccionando una ruta disponible por donde los datos serán transmitidos.
3. Incluye un conjunto de reglas que le dan forma al esquema de entrega de datagramas sin conexión y con el mejor esfuerzo. Estas reglas establecen las características en que las estaciones y enrutadores (gateways) deben de procesar los datagramas, como y cuando se deberá de generar un mensaje de error, bajo que condiciones los paquetes deben ser descartados y como recuperarse de los problemas que pueden ocurrir.

4.2.4.1.2 Actividad de un datagrama

Cuando una aplicación debe enviar un datagrama hacia la red, lleva a cabo los siguientes pasos: primero, construye el datagrama IP (dentro de las longitudes legales estipuladas por la implantación local de IP). Se calcula la suma de verificación para los datos del encabezado y a continuación se elabora el encabezado IP. En seguida, se deberá determinar el primer salto en la ruta hacia el destino, a fin de enrutar el datagrama a la máquina destino directamente por la red local, o a una compuerta (gateway) si se trata de la interred. Si el enrutamiento es de importancia la información de encaminamiento se añadirá al encabezado utilizando una opción. Finalmente, el datagrama se envía a la red.

Conforme el datagrama pasa por la red, cada compuerta lleva a cabo una serie de pruebas. Después de que la capa de red en la compuerta ha retirado el encabezado, la compuerta comprueba la suma de verificación y revisa la integridad del datagrama. Si las sumas de verificación no coinciden, el datagrama se descartará y se envía un mensaje de error al dispositivo emisor por medio del protocolo ICMP. A continuación, el campo de tiempo de vida se disminuye y verifica. Si el datagrama ya expiró, el datagrama se descartará y se enviará un mensaje de error al emisor. Después, determina el siguiente salto de la ruta, ya sea mediante análisis de la dirección destino o de una instrucción específica de

[23] El protocolo IP tiene una capacidad de paquete máximo de 65,535 bytes (64Kb). Además de que puede dividir en forma automática un datagrama de información en datagramas más pequeños si es necesario (fragmentación).
El protocolo IP se ocupa del direccionamiento del datagrama mediante la dirección completa Internet de 32 bits, aun cuando las direcciones del protocolo de transporte utilicen 8 bits.

enrutamiento dentro del campo de opciones del encabezado IP. Se reconstruye el datagrama con un nuevo valor de tiempo de vida y de suma de verificación.

Si es necesario realizar fragmentación debido a un incremento de la longitud[24] del datagrama o por alguna limitación del software, se divide el datagrama y los nuevos datagramas se ensamblan con la información correcta de encabezado. Si se requiere un enrutamiento especial o una marca de tiempo también se añade. Y por ultimo, el datagrama se devuelve a la capa de red.

Cuando el datagrama finalmente se recibe en el dispositivo destino, el sistema realiza un cálculo de la suma de verificación para comprobar la suma del encabezado, suponiendo que las dos sumas coinciden, verifica la existencia de otros fragmentos del datagrama original (en el caso de que se haya efectuado fragmentación). Si se requieren más datagramas para reensamblar el mensaje completo, el sistema espera la recepción de todos los fragmentos, haciendo funcionar entre tanto un temporizador para asegurarse de que los datagramas llegan en un plazo razonable. Aún cuando todas las partes del mensaje completo hallan llegado, si el dispositivo no puede reensamblarlas antes de que el temporizador de tiempo llegue a cero, el datagrama será descartado y se enviará un mensaje de error al emisor. Finalmente, el encabezado IP se retira y el mensaje se pasa a las capas superiores. Si se requería alguna respuesta, ésta se genera entonces y se devuelve al dispositivo emisor.

4.2.4.1.3 MTU de la capa de red y el mecanismo de fragmentación

Cada tecnología de conmutación de paquetes establece un límite superior fijo para la cantidad de datos que puede transferir en una trama física[25]. Se hace referencia a estos límites como la **Unidad de Transferencia Máxima** (MTU: maximum transfer unit), de una red

En realidad un datagrama[26] debe pasar a través de muchos tipos de redes físicas (tal vez con diferentes MTUs) conforme viaja a través de una interconexión de redes (internet) para llegar a su destino final.

El diseño de una interconexión de redes es ocultar la tecnología de red subyacente y hacer la comunicación conveniente para el usuario. Así en lugar de diseñar datagramas que se ajusten a las restricciones de la red física, el software IP selecciona un tamaño de datagrama más conveniente desde el principio y

[24]Cuando se añade información adicional al datagrama en relación con el enrutamiento o el registro de marca de tiempo la longitud de un datagrama puede aumentar. El manejo de todas estas condiciones es el punto fuerte del protocolo Internet (IP), para los cuales practicamente todos los problemas tienen un sistema de resolución.
[25]Ethernet limita a 1,492 octetos mientras que FDDI permite aproximadamente 4,470 octetos por trama.
[26]Se debe recordar que los datagramas viajan encapsulados en tramas de capa física.

establece una forma para dividir datagramas en pequeños fragmentos, cuando el datagrama necesita viajar a través de una red que tiene una MTU pequeña. Las pequeñas piezas dentro de un datagrama dividido se conocen con el nombre de fragmentos y el proceso de división de un datagrama se conoce como mecanismo de fragmentación.

En la práctica, el protocolo IP deberá ser capaz de adaptar el tamaño de los datagramas para cada tipo de red que el datagrama atraviese. El protocolo IP no limita los datagramas a un tamaño pequeño, ni garantiza que los datagramas grandes serán entregados sin fragmentación. El emisor puede seleccionar cualquier tamaño de datagrama que considere apropiado; la fragmentación y el reensamblado se dan automáticamente sin que el emisor deba realizar ninguna acción especial ya que la fragmentación generalmente se lleva a cabo en un enrutador a lo largo del trayecto entre la fuente del datagrama y su destino final.

El protocolo IP de cada nodo intermedio en la red, deberá ser capaz de dividir datagramas en fragmentos y recibirlos, para transmitir los fragmentos sobre una subred hacia el siguiente nodo o estación. Y cada nodo final IP deberá ser capaz de reensamblar los mensajes fragmentados.

En una interconexión de redes TCP/IP, una vez que un datagrama se ha fragmentado, los fragmentos viajan como datagramas separados hacia su destino final donde serán reensamblados.

Fragmentar un datagrama significa dividirlo en varios segmentos que mantienen el mismo formato que el datagrama original. Es decir, cada fragmento de un mensaje contiene su propio y completo encabezado de información de protocolo IP unido con el campo de identificación del mensaje original, el cual puede ser usado para reconocer todos los fragmentos del mensaje original. Cada fragmento individual de un mensaje puede llegar a su destino por diferentes rutas. Una vez que todos los fragmentos individuales llegan a su destino, se puede reensamblar el mensaje original, por medio de un campo del encabezado IP de cada fragmento, el cuál indica el lugar que ocupa éste en el orden del mensaje original, de esta forma se reensambla el datagrama completo.

Si el emisor original desea prevenir a un datagrama de ser fragmentado, posiblemente por que el destino no es capaz de reensamblarlo, el emisor puede establecer la opción de no fragmentar (DF bit) en el encabezado del mensaje, el cual indica que no se debe llevar a cabo fragmentación alguna.

4.2.4.1.4 Temporizador y reensamblado

Cuando el primer datagrama de un mensaje que se dividió llega a su destino, se inicia un sincronizador de reensamblaje (temporizador de reensamblaje). Si no se

han recibido todas las piezas o partes de un datagrama completo cuando el temporizador llega a un valor predeterminado, todos los datagramas que se hayan recibido se descartaran sin procesar el datagrama. De esta manera, la probabilidad de perder un datagrama aumenta con la fragmentación ya que la perdida de un solo fragmento provoca la perdida del datagrama completo.

El siguiente es un resumen de las principales características del Protocolo Internet (IP)

- Protocolo sin conexión.
- Fragmentación (división) de paquetes si es necesario.
- Esquema de direccionamiento por medio de direcciones Internet (actualmente de 32 bits)
- Direcciones de protocolo de transporte de 8 bits.
- Máximo tamaño de paquete es de 65535 bytes (64Kb)
- Contiene solo un verificador de información del encabezado, no contiene chequeo de datos.
- El Tiempo de vida de un paquete es finito.
- Entrega **con el mejor esfuerzo** (best-effort delivery).

4.2.4.1.5 Esquema de direcciones IP

Las redes TCP/IP se pueden definir como redes virtuales, formadas al interconectar redes físicas a través de enrutadores. Las direcciones IP son el componente esencial para ocultar los detalles de las redes físicas y hacer que Internet parezca una sola entidad uniforme.

4.2.4.1.6 Identificadores universales

Un servicio universal de comunicaciones es el esquema que permite que cualquier computadora se comunique con cualquier otra computadora en toda la red, para llevar a cabo esto, se necesita un método global para identificar cada computadora que se conecte a dicha red.

Los identificadores de computadoras host pueden ser: nombres, direcciones o rutas. Aunque estas definiciones son intuitivas, pueden ser confusas; los nombres, direcciones y rutas representan a identificadores de host a nivel más bajo. En general, las personas prefieren nombres fáciles de recordar para identificar a los hosts, mientras que el software trabaja más eficientemente con direcciones de forma binaria o numérica. En esta sección solo se explicaran el esquema de direcciones binarias y en la sección de Sistemas de Nombre de Dominio DNS (Domain Name Service), los nombres además, de como se lleva a cabo la transformación de las direcciones binarias a nombres.

4.2.4.1.7 Tipo de direcciones IP

Los diseñadores de TCP/IP eligieron para las direcciones IP un esquema análogo al direccionamiento en las redes físicas, en el que cada host en Internet tiene asignada una dirección de número entero de 32 bits, llamada, dirección Internet o dirección IP.

En una dirección IP de un host se encuentra codificada la identificación de la red a la que se conecta y también la identificación única de dicho host en la red en cuestión. En el caso más sencillo, cada host conectado a Internet tiene asignando un identificador universal de 32 bits (dirección IP) como su dirección dentro de la red.

Conceptualmente, cada dirección esta dividida en dos partes: netid, hostid, donde netid es el identificador de una red y hostid es el identificador de un host dentro de esa red. En la práctica, cada dirección IP debe tener una de las primeras tres formas mostradas en la figura 4.2

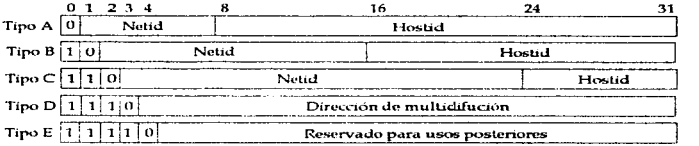


Figura 4.2 Las cinco formas de direcciones en Internet (IP)

Se puede determinar el tipo de dirección IP según los primeros cinco bits de orden, de los cuales solo son necesarios los dos primeros bits para distinguir entre los tres tipos de red primarios (redes tipo A, B y C).

Las direcciones de red tipo A, se utilizan para redes que tienen más de 2^{16} hosts, asignándose 7 bits al campo netid y 24 bits al campo hostid.

Las direcciones de red tipo B, se utilizan para redes de tamaño mediano que tienen entre 2^8 y 2^{16} hosts, asignándose 14 bits al campo netid y 16 bits al hostid.

Las direcciones de red tipo C, se utilizan en redes que tienen redes con menos de 2^8 hosts, asignándose 21 bits al campo netid y sólo 8 bits al hostid.

Las direcciones IP se han definido de tal forma que es posible extraer rápidamente los campos hostid o netid, de manera que los enrutadores que utilizan el campo

netid de una dirección para poder decidir a dónde enviar un paquete puedan trabajar de manera más eficiente.

Debido a que las direcciones IP tienen codificado los identificadores tanto de una red y un host en dicha red, se puede especificar una computadora individual o la conexión a la red. Por lo tanto, un enrutador que conecta "*n*" número de redes, debe tener "*n*" número de direcciones IP distintas, una para cada conexión de red que tenga.

Las direcciones IP se pueden utilizar para referirse a redes, así como a hosts individuales. Por regla, una dirección que tiene todos los bits del campo hostid igual a 0, se reserva para hacer referencia a la red misma en sí.

Una ventaja del esquema de direccionamiento IP es que éste incluye una dirección de broadcast que hace referencia a todos los hosts conectados a la red. De acuerdo con el estándar, cualquier dirección que tenga en el campo hostid consistente de solamente unos (1), está reservada como dirección de broadcast. En muchas tecnologías de red (por ejemplo, Ethernet (capa 2 del modelo OSI)), el broadcast puede ser tan eficiente como la transmisión normal; en otras, el broadcast encuentra apoyo en el software de red, pero requiere substancialmente un mayor retraso que una transmisión simple. Algunas redes inclusive no cuentan con la función de broadcast. Por lo tanto, tener una dirección IP de broadcast no garantiza la disponibilidad o la eficiencia de la entrega por broadcast.

Técnicamente, la dirección de broadcast que describimos en el párrafo anterior se conoce como dirección de broadcast dirigida, debido a que contiene tanto una identificación válida de red como el campo hostid de broadcast, proporcionando un mecanismo poderoso, que permite que un sistema remoto envíe un solo paquete y que este será dirigido a toda la red especificada. La mayor desventaja de el broadcast dirigida es que requiere un conocimiento de la dirección de red.

Existe otra forma de dirección de broadcast, llamada dirección de broadcast limitada o dirección de broadcast de red local, esta forma, proporciona una dirección de broadcast para la red local, independientemente de la dirección IP, esta dirección de broadcast limitada consiste de treinta y dos bits con valor de unos (1). Un host sin disco de arranque puede utilizar la dirección de broadcast limitada como parte de un procedimiento de arranque antes de conocer su dirección IP o la dirección IP de la red local.

En general, el software de TCP/IP interpreta los campos que consisten en ceros (0) como si fuera "esta". Por lo tanto una dirección IP con el campo de hostid en ceros se refiere a "este" host, y una dirección IP con netid en ceros se refiere a "esta" red.

Existen dos extensiones importantes al esquema de direccionamiento IP, el direccionamiento de subredes y el direccionamiento "sin tipo". Estos clases de direccionamiento se discuten en la siguiente sección con más detalle.

4.2.4.1.8 Desventaja del direccionamiento IP

Codificar la información de la red en una dirección IP tiene algunas desventajas. La más obvia es que las direcciones se refieren a las conexiones de red, no a la computadora. Así, por ejemplo, si una computadora se cambia a otra red, su dirección IP debe cambiar, ya que la dirección original contiene el identificador de la red en la que estaba conectada primeramente.

Otra debilidad del esquema de direccionamiento, es que cuando una red tipo C crece hasta tener más de 255 hosts, tiene que cambiar su dirección a una tipo B, y no hay forma de hacer la transición de manera gradual.

La desventaja más importante es en el manejo del enrutamiento. Como el enrutamiento utiliza la parte de identificación red (netid) de la dirección IP, el camino tomado por los paquetes que viajan hacia un host con muchas direcciones IP dependen de la dirección utilizada.

4.2.4.1.9 Notación decimal con puntos

La mayor parte del software TCP/IP que muestra una dirección IP o que requiere que una persona introduzca una dirección IP, utiliza la forma de notación decimal con puntos. Esta notación se escribe como cuatro campos de enteros decimales separados por puntos, en donde cada entero proporciona el valor de un octeto de la dirección IP, por ejemplo, la dirección:: 10000100 11111000 110101 11110101

se escribe en notación decimal con puntos, de la siguiente manera: 132.248.53.245

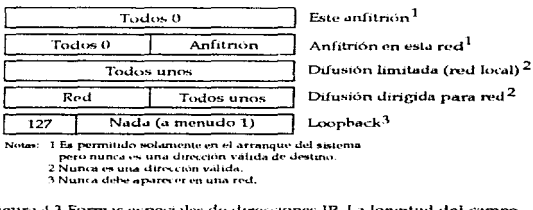
Es importante entender la relación entre los tipos de direcciones IP y los números decimales con puntos. En la tabla 4.2 se resumen el rango de valores para cada tipo de red.

Tipo	Direcciones más bajas	Direcciones más altas
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tabla 4.2 Rango de valores decimales con punto que corresponden a cada tipo de direcciones IP. Algunos valores están reservados para propósitos especiales.

No todas las direcciones posibles en el rango son asignadas a los tipos de red. Por ejemplo, la dirección 127.0.0.0, valor del rango tipo A, se reserva para hacer referencia a la red misma (referida también como dirección loopback); y está diseñada para utilizarse en las pruebas de TCP/IP y para la comunicación de los procesos internos de un host (maquina local). Cuando algún programa utiliza la dirección loopback como destino, el software que utiliza TCP/IP regresa los datos (al host mismo) sin generar tráfico a través de alguna red.

El protocolo IP utiliza sólo unas cuantas combinaciones de ceros (0) (se refiere al host) o unos (1) (se refiere a la red). En la figura 4.3 se listan las posibles combinaciones.



Notas: 1 Es permitido solamente en el arranque del sistema pero nunca es una dirección valida de destino.
2 Nunca es una dirección valida.
3 Nunca debe aparecer en una red.

Figura 4.3 Formas especiales de direcciones IP. La longitud del campo de red de una broadcast dirigida depende del tipo de dirección de red.

4.2.4.1.10 Autoridad de direcciones Internet

Para garantizar que el campo de red dentro de una dirección de Internet es único, todas las direcciones de Internet son asignadas por una autoridad central, llamada INTERNIC.

Una vez que una organización obtiene un prefijo de red, puede escoger cómo asignar un sufijo único a cada host de su red sin tener que contactar a la autoridad central.

Solamente es esencial para la autoridad central asignar direcciones IP para redes que están (o estarán) conectadas a la red global Internet. De esta manera, una corporación individual, es decir sin conectarse a la red global Internet, puede asignar de manera independiente a INTERNIC las direcciones únicas de red dentro de su propia red TCP/IP aislada, y esto funcionara adecuadamente siempre y cuando nunca se conecte al mundo exterior (red global Internet).

4.2.4.1.11 Orden de octetos de red

Para permitir el intercambio de datos binarios entre máquinas con diferente arquitectura, los protocolos TCP/IP requieren del ordenamiento estándar de octetos para los enteros dentro de los campos del protocolo, ya que de otra forma, si se hiciera la copia directa de octetos de una máquina otra puede cambiar el valor del número y su significado, por esto un host debe convertir todos los datos binarios de su forma interna a un orden estándar de octetos de red antes de enviar un paquete y debe hacer la conversión de orden de octetos de red al orden interno cuando reciba paquetes. Esto es muy importante en una red como Internet ya que los paquetes llevan números binarios que especifican información importante, como son las direcciones de origen, destino y la longitud de los paquetes.

El estándar de Internet para el orden de los octetos especifica que la parte de los enteros que se envía primero es el octeto más significativo (por ejemplo, el tipo Big Endian)[27]. Si se consideran los octetos en un paquete mientras viajan de una máquina a otra, un entero binario en dicho paquete tiene su octeto más significativo cerca del comienzo del paquete y su octeto menos significativo cerca del final.

4.2.4.1.12 Subredes IP

Para tener una idea completa del esquema de direccionamiento IP, a continuación se explican cuatro extensiones de esté, los cuales permiten que una localidad utilice una sola dirección IP para varias redes físicas. Además se explicará con más detalle el esquema de subred IP, el cual forma parte del estándar TCP/IP.

Las direcciones IP de 32 bits se deben asignar de manera tal, que todos los hosts de una red física tengan un prefijo en común, este prefijo es la parte de identificación de red de una dirección IP (netid) y la parte restante como la parte de identificación del host (hostid).

La ventaja que se tiene al dividir una dirección IP, en una parte de red y otra de host, es que los enrutadores solo tienen que examinar la parte de red de la dirección IP (netid), cuando tienen que tomar decisiones de enrutamiento, manteniendo en su interior tablas de enrutamiento que contienen solamente direcciones de red y no de hosts.

Para entender las extensiones o nuevos esquemas de direccionamiento, es importante tener en cuenta que las organizaciones tienen la libertad de manejar o

[27] Existen principalmente dos maneras de almacenar enteros de 32 bits, la primera, llamada Little Endians, la dirección más baja de memoria contiene el octeto de orden bajo del entero; la segunda, llamada Big Endian, la dirección más baja de memoria guarda el octeto de orden alto del entero.

modificar las direcciones y rutas, siempre y cuando dichas modificaciones permanezcan ocultas para las demás localidades.

Las extensiones, son esquemas de direccionamiento que surgen debido a que los diseñadores originales del sistema de direcciones IP, no tomaron en cuenta en un principio el gran crecimiento que se iba a tener[28], en especial las redes de tipo LAN. El insuficiente rango de direcciones que tomaron en cuenta (rango de direcciones muy pequeño con respecto al crecimiento actual) se hace más evidente en redes tipo B, debido a que no existen suficientes prefijos (netid) para cubrir todas las redes de tamaño mediano en Internet.

Una solución es poder minimizar las direcciones de red, por lo tanto, muchas redes físicas deben compartir el mismo prefijo IP de red. Para minimizar las direcciones tipo B, se deben utilizar emulaciones de direcciones tipo C, teniéndose que modificar los procedimientos de enrutamiento, tomándose en cuenta que todas los hosts que se conecten a las redes afectadas deben entender las normas utilizadas.

La idea de compartir (subdividir) una dirección de red IP entre muchas redes físicas no es nueva y hay varios métodos para llevarlo a cabo, entre los más comunes, se encuentran:

- **Enrutadores transparentes**: Generalmente se utilizan en redes clase A. Por medio de un enrutador transparente se puede extender una red de área amplia a muchos hosts de una red local, dando como resultado, que cada host parezca tener una dirección IP en la WAN.

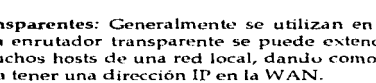


Figura 4.4 Enrutador transparente que extiende una red WAN a muchos hosts en una localidad. Cada host parece tener una dirección IP en la red WAN

- **ARP sustituido** (proxy ARP): En esta técnica se hace la transformación de un solo prefijo IP de red en dos direcciones físicas. Sólo se lleva a cabo en redes que utilizan ARP (protocolo de resolución de direcciones).

[28] El gran aumento que se tiene en las redes da como consecuencia, que se requiera más trabajo administrativo para el manejo de las direcciones de red, que las tablas de enrutamiento sean bastante extensas y que el rango de direcciones actual llegue a su fin.

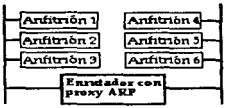


Figura 4.5 La técnica de ARP sustituto (ARP hack) permite que una dirección de red se comparta entre dos redes físicas.

- **Subredes IP estándar**: Es la técnica más utiliza para permitir que un solo prefijo de dirección de red abarque varias redes físicas, es también referido como el **direccionamiento de subred, enrutamiento de subred o utilización de subredes**, siendo la manera más general, además de que forma parte del estándar IP (por esta razón, se explica a continuación).

4.2.4.1.13 Direccionamiento de subred (Subredes IP estándar)

La manera de entender el direccionamiento de subred es por medio de un ejemplo, supóngase que en una localidad se tiene asignada una sola dirección de red IP tipo B, pero se tienen varias redes físicas. Sólo los enrutadores locales saben que existen muchas redes físicas y por tanto saben cómo se debe enrutar el tráfico entre ellas; por otra parte, los enrutadores en otros sistemas autónomos remotos enrutan todo el tráfico como si sólo hubiera una red física. En la figura 4.6 se muestra un ejemplo.

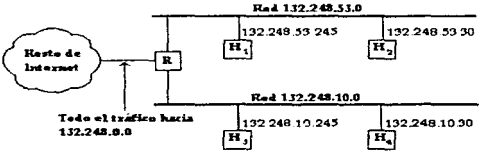


Figura 4.6. En esta figura, se demuestra una localidad con dos redes físicas que utilizan el direccionamiento de subred (mismo netid), para poder etiquetarlas con una sola dirección de red tipo B. El enrutador R acepta todo el tráfico para la red 132.248.0.0 y elige una red física, basándose en el tercer octeto de la dirección.

En este ejemplo, el administrador asigna a todas las máquinas de una de las redes físicas, una dirección con la forma 132.248.53.X, y a las otras máquinas dentro de la otra red física, una dirección 132.248.10.X, donde X representa un número entero pequeño, utilizado para identificar un host específico. Para escoger una red física,

R examina el tercer octeto de la dirección de destino, enrutando los datagramas que tengan el valor 53 hacia la red 132.248.53.0 y los que tengan el valor 10 hacia la red 132.248.10.0 .

Conceptualmente, el agregar subredes sólo cambia ligeramente la interpretación de direcciones IP. En vez de dividir la dirección IP de 32 bits en un prefijo de red (netid) y un sufijo de host (hostid), el direccionamiento de subred divide la dirección en una **porción de red** y una **porción local.** La interpretación de la porción de red permanece igual que en las redes que no utilizan el direccionamiento de subred, identificando una localidad, posiblemente con muchas redes físicas, y la porción local identifica una red física y un host en dicha localidad.

En el ejemplo anterior, para lograr que el enrutamiento entre las redes físicas sea eficiente, el administrador de la localidad debe utilizar un octeto de la porción local a fin de identificar una red física y otro octeto para identificar un host en dicha red, como se muestra en la figura 4.7.

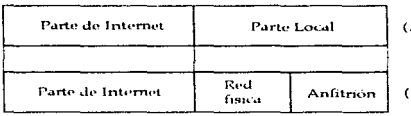


Figura 4.7 (a) Interpretación conceptual de una dirección IP de 32 bits siguiendo el esquema original de direcciones IP, y (b), interpretación conceptual de direcciones que utilizan el esquema de subred de la figura 10.3. La porción local se divide en dos partes que identifican una red física y un host dentro de dicha red.

El direccionamiento de subredes da como resultado una forma de direccionamiento jerárquico que lleva al correspondiente enrutamiento jerárquico. El nivel superior del enrutamiento jerárquico (por ejemplo, otras redes autónomas (remotas) en Internet), utilizan los primeros dos octetos cuando se enruta y el siguiente nivel (por ejemplo, el sitio local) utiliza un octeto adicional. Finalmente, el nivel más bajo (por ejemplo, la entrega a través de la red física, a el host específico) utiliza toda la dirección.

La ventaja de utilizar el direccionamiento jerárquico es que se puede incorporar un gran crecimiento, ya que significa que una ruta no necesita saber muchos detalles sobre el sitio distante, lo mismo que sobre destinos locales. Una desventaja es que la selección de una estructura jerárquica es difícil, además de que también, es difícil cambiar una jerarquía previamente establecida.

El estándar TCP/IP para el direccionamiento de subred reconoce que no todas las localidades tienen la misma necesidad de una jerarquía de direcciones; por lo que permite que se tenga flexibilidad al poder escoger cómo asignarlas. Por ejemplo, se podría utilizar de la parte local de 16 bits, 8 bits para el identificador de red y los otros 8 bits restantes para el identificador del host, permitiéndose hasta 256 redes, con 256 hosts cada una[29], o utilizar 3 bits para identificar una red física y los 13 bits restantes para identificar un host de dicha red, permitiendo de otra manera incluso, 8 redes con hasta 8192 hosts cada una. Pero una vez que se escoja una partición para una red en particular, todos los hosts y enrutadores conectados a ella deben utilizarla; si no lo hacen, los datagramas se pueden perder o enrutar de manera equivocada.

4.2.4.1.14 Implantación de subredes por medio de máscaras

El estándar de subredes de IP especifica que una localidad que utiliza el direccionamiento de subred, debe escoger una máscara de subred de 32 bits para cada red física.

Los bits en la máscara de subred se indican como 1, si la red trata al bit correspondiente de la dirección IP como parte de la dirección de red física, o se indican como 0, si se trata al bit como parte del identificador de host. Por ejemplo, la máscara de subred de 32 bits:

11111111 11111111 11111111 00000000

En este ejemplo, se especifica que los tres primeros octetos identifican a la red física y el cuarto a un host en dicha red. Una máscara de subred debe tener 1 para todos los bits que correspondan a la porción de red de la dirección.

El estándar no restringe a las máscaras de subred para seleccionar bits contiguos de la dirección. Por ejemplo, una red puede tener asignadas la máscara:

11111111 11111111 00011000 01000000

La cual selecciona los primeros dos octetos, dos bits del tercer octeto y un bit del cuarto, aun que esto hace confuso la asignación de direcciones de hosts y la tabla de enrutamiento, por lo que se recomienda que se utilicen máscaras contiguas de subredes.

Especificar máscaras de subredes de forma binaria es molesto y favorece los errores, por lo tanto, la mayor parte del software permite representaciones

[29] En la práctica, el límite es de 254 subredes con 254 anfitriones cada una, debido a que las direcciones de anfitrión de todos 1 y todos están reservadas para la difusión, y no se recomiendan las subredes con todos 1 o todos 0.

alternativas, por ejemplo notación hexadecimal o decimal, aunque la notación decimal es más popular, por ejemplo, la máscara en binario:
11111111 11111111 11111111 00000000

su representación en decimal es:

255.255.255.0

que es más corta y se comprende mejor.

4.2.4.1.15 Evolución del direccionamiento IP: IPv6 e IPng

Existen cuatro razones principales por las que tiene que evolucionar el TCP/IP:

- **Nuevas tecnologías de comunicación y computación**: Cuando una nueva computadora de alta velocidad esta disponible, generalmente se conecta a la red, ya sea como host o como enrutador. También sucede con las nuevas tecnologías de redes de alta velocidad, en cuando están disponibles se les empieza a utilizar para transportar paquetes IP (entre las tecnologías más importantes se encuentra ATM).
- **Nuevas aplicaciones**: Generalmente crean una demanda de infraestructura o servicios que los protocolos actuales no pueden proporcionar. Por ejemplo, las aplicaciones que tienen que ser en tiempo real.
- **Incremento en el tamaño y la carga**: El tamaño de Internet se ha duplicado durante varios años de manera exponencial. Sorprendentemente, la carga de tráfico ha crecido más rápido que el número de redes, hay varias causas para esto, pero la más importante, son las nuevas aplicaciones que transfieren imágenes y vídeo en tiempo real que generan más trafico que las aplicaciones que transfieren solo texto.
- **Nuevas políticas**: Se refiere a las nuevas reglas de administración y asignación de los recursos de las nuevas redes, ya que al crecer se necesitan nuevas reglas para poderse regular

En la actualidad se esta utilizando la versión 4 de los Protocolos Internet (IPv4) [30], esta se ha mantenido casi sin cambios desde su introducción a finales de los setenta, demostrando que su diseño es flexible y poderoso, al poderse adaptar a las tecnologías, tanto de LANs como de computadoras, que han surgido durante todo este tiempo. Sin embargo, a pesar de su diseño, IPv4 debe ser reemplazado y las principales razones son:

[30] Las versiones 1,2 y 3 nunca se asignaron formalmente y la versión 5 se asigno al protocolo ST.

- El inminente agotamiento del rango de direcciones, aunque en un principio se pensó que con un espacio de 32 bits era más que suficiente, actualmente no puede adaptarse al crecimiento proyectado de Internet.
- Soporte a nuevas aplicaciones, como por ejemplo, audio y vídeo en tiempo real, los cuales necesitan que sea garantizado un retardo determinado.
- La nueva versión de IP debe proporcionar un mecanismo que haga posible asociar un datagrama con una reservación de fuente pre-asignada.
- También deberá incluír mecanismos con la capacidad de poder autentificar al emisor.

El IETF (Internet Engineering Task Force) ha trabajado en la formulación de una nueva versión del IP, el cual tiene que ser un estándar abierto. Se han propuesto varios diseños, uno de los cuales haría al IP más sofisticado, incrementándose el costo por la complejidad del procesamiento. Otro diseño propone utilizar el protocolo CLNS de OSI, modificado. Un tercer diseño propone conservar la mayor parte de las ideas del IP, y hacer extensiones para adaptarlo a direcciones amplias, uno de estos diseños es el conocido como SIP (Simple IP), la versión extendida del SIP ha sido llamada Simple IP Plus (SIPP), el cual es la base para la próxima versión IP.

El termino IPng se utiliza para referirse a todas las discusiones y propuestas para una próxima versión del IP, mientras que el término IPv6 se ha utilizado para referirse a una propuesta específica que proviene del IETF.

El protocolo IPv6 conserva muchas de las características del IPv4, sin embargo tiene cambios significativos, los cuales se describen a continuación.

Los cambios introducidos para el IPv6 pueden agruparse en cinco categorías:

- **Rango de direcciones más amplio**: El nuevo tamaño de las direcciones es el cambio más notable. El IPv6 cuadruplica el tamaño de las direcciones del IPv4, teniendo un cambio de 32 bits a 128 bits.
- **Formato de encabezado flexible**: El IPv6 utiliza un formato de datagrama incompatible y completamente nuevo. A diferencia del IPv4, que utiliza un encabezado de datagrama de formato fijo en que todos los campos excepto las opciones ocupan un número fijo de octetos en un desplazamiento fijo, el IPv6 utiliza un conjunto de encabezados opcionales.
- **Opciones mejoradas**: Como el IPv4, el IPv6 permite que un datagrama incluya información de control opcional. El IPv6 incluye nuevas opciones que proporcionan capacidades adicionales no disponibles en el IPv4.

- **Soporte para asignación de recursos**: El IPv6 reemplaza la especificación del tipo de servicio del IPv4 con un mecanismo que permite la pre-asignación de recursos de la red. En particular el nuevo mecanismo soporta aplicaciones de vídeo en tiempo real que requieren una garantía de ancho de banda y retardo.
- **Prevención para extensión de protocolo**: Posiblemente el cambio más significativo en el IPv6 es el cambio de un protocolo que especifica completamente todos los detalles a un protocolo que pueda permitir características adicionales. La capacidad de extensión tiene la posibilidad de permitir que el IETF se adapte a los protocolos para cambiar el hardware de redes subyacente o nuevas aplicaciones.

El IPv6 utiliza, a diferencia del IPv4, una fragmentación de extremo a extremo.

4.2.4.1.16 Tamaño del rango de dirección de IPv6

En la IPv6, cada dirección ocupa 16 octetos (4 veces el tamaño de una dirección IPv4). El amplio espacio de direcciones garantiza que el IPv6 pueda tolerar cualquier esquema de asignación de direcciones razonable. Teniendo un espacio de direcciones mayor que 3.4 x 10. [18]

Por otro lado, aun que se resuelve el problema de tener suficientes direcciones, surge otro problema, que es el manejo del tamaño de las direcciones nueva. Obviamente, la notación binaria se puede manejar de manera práctica o sencilla, tampoco, la notación decimal con punto hace que las direcciones sean lo suficientemente compactas. Una forma de ayudar a tener una notación mas corta, es utilizar la notación **hexadecímal con dos puntos**, en la cual el valor de cada cantidad de 16 bits se representa en forma hexadecimal separada por dos puntos, por ejemplo:

La dirección IP en notación decimal es: 104.230 140.100.255.255.255.255.0.0.17.128.150.10.255.255
En forma hexadecimal: 68E6:8C64:FFFF:FFFF:0:1180:96A:FFF

Además, de que esta notación hexadecimal tiene algunas ventajas para mayor información referirse al Comer Douglas E.; TCP/IP 3ª; Prentice Hall.

4.2.4.1.17 Los tres tipos básicos de dirección IPv6

El IPv6 asocía una dirección con una conexión de red especifica, no con una computadora específica. Así, la asignación de direcciones es similar que el IPv4. Un enrutador IPv6 tiene dos o más direcciones, y un host IPv6 con una conexión a red, necesita sólo una dirección. El IPv6 también conserva y extiende la jerarquía de direcciones del IPv4 en la que una red física es asignada a un prefijo. Sin

embargo, para hacer la asignación de direcciones y la modificación más fácil, el IPv6 permite que varios prefijos sean asignados hacia una interfaz determinada.

Además de permitir varias direcciones simultáneas por conexión de red, el Ipv6 expande y, en algunos casos, unifica las direcciones especiales del IPv4. En general, una dirección de destino en un datagrama cae dentro de una de las tres categorías siguientes:

Unibroadcast La dirección de destino especifica una sola computadora ya sea host o enrutador; el datagrama deberá enrutarse hacia el destino a lo largo de la trayectoria más corta.

Grupo El destino es un conjunto de computadoras en las que todas comparten un solo prefijo de dirección (por ejemplo, si están conectadas a la misma red física), el datagrama deberá enrutarse hacia el grupo a través de la trayectoria más corta y, después, entregarse exactamente a cada uno de los miembros del grupo.

Multibroadcast El destino es un conjunto de computadoras, posiblemente en múltiples localidades. Una copia del datagrama deberá entregarse a cada miembro del grupo que emplee hardware de multibroadcast o de broadcast si están disponibles.

4.2.4.1.18 Asignación propuesta de espacio de dirección IPv6

La cuestión sobre cómo dividir el espacio de direcciones ha generado muchas discusiones. Hay dos temas centrales: cómo administrar la asignación de direcciones y cómo transformar una dirección en una ruta. El primer tema se enfoca en el problema práctico de construir una jerarquía de autoridad. A diferencia de la Internet actual, la cual utiliza una jerarquía de dos niveles de prefijos de red, asignados por la autoridad de Internet (INTERNIC) y sufijos de host asignados por la organización de manera individual, el gran espacio de direcciones en el IPv6 permite una jerarquía de multiniveles o jerarquías múltiples. El segundo tema se enfoca en la eficiencia computacional. Independientemente de la jerarquía de autoridad que asigne direcciones, un enrutador debe examinar cada datagrama y elegir una trayectoria hacia el destino correcto. Para mantener bajo el costo de los enrutadores de alta velocidad, el tiempo de procesamiento requerido para elegir una trayectoria debe mantenerse lo mas bajo posible.

4.2.4.2 Protocolo de Mensajes de Control de Error: ICMP

El nivel de red IP contiene un módulo llamado **Protocolo de Mensajes de Control de Error** (ICMP, Internet Control Message Protocol). La responsabilidad del ICMP

es la de proveer los mensajes de estado y diagnóstico para el protocolo IP[31], considerando ciertas actividades en la red.

El ICMP notifica al IP cuando los datagramas no pueden ser entregados, cuando las compuertas (gateways) dirigen el tráfico sobre rutas cortas, o cuando los enrutadores (los enrutadores en TCP/IP son también llamados gateways) no tienen el suficiente espacio de memoria de almacenamiento para redireccionar (forward) las unidades de datos de protocolo. El ICMP también notificará a la estación origen (transmisor) si el destino es inaccesible. Además de ser el responsable del manejo o creación de un mensaje de tiempo-excedido en el evento de que el tiempo de vida (life time) de un datagrama expire. El ICMP desarrolla ciertas funciones de edición en el caso de que el encabezado un datagrama IP sea erróneo. Todas las funciones antes mencionadas son realizadas por el ICMP para lo cual envía diferentes tipos de mensajes dependiendo de los siguientes eventos.

4.2.4.2.1 Prueba de acceso

Para cerciorarse si dos estaciones pueden comunicarse, el ICMP soporta los mensajes de **solicitud de eco** y **respuesta de eco** (este proceso es mejor conocido como ping). El receptor de un mensaje de "solicitud de eco" deberá retornar un mensaje de "eco de respuesta". Las dos unidades de datos de protocolo (PDUs, protocol data units) son utilizados para determinar si los dos destinos pueden ser accesibles desde uno a otro.

4.2.4.2.2 Reporte de destino no accesible

Cuando un enrutador no puede direccionar o entregar un datagrama IP, envía el mensaje de **destino no accesible**.

4.2.4.2.3 Disminución en la tasa de transmisión del origen.

El ICMP también provee mensajes de **fuente/congestión** (source/quench) los cuales permiten tanto a una estación como a un enrutador (gateway) detener la transmisión de datagramas o reducir la tasa de transmisión. Este tipo de mensaje es utilizado si un enrutador (gateway) no tiene la capacidad suficiente en memoria para almacenar los datagramas recibidos, por lo tanto el enrutador (gateway) envía este tipo de mensaje ICMP a la estación responsable y de esta manera no congestionar al enrutador.

[31] Cada uno de los mensajes ICMP es encapsulado en un paquete IP.

4.2.4.2.4 Solicitud de cambio de ruta

En el caso especial, cuando un enrutador detecta que una estación utiliza una ruta no óptima para la transmisión, el enrutador le envía a la estación un mensaje ICMP del tipo **redireccionar** solicitando que cambie sus rutas.

4.2.4.2.5 Tiempo excedido

El ICMP tiene el mensaje de **tiempo excedido**. Un enrutador envía este mensaje cuando el campo de tiempo de vida del datagrama llega a cero (debido a rutas circulares o excesivamente largas, es lo que hace que el tiempo de vida de un datagrama llegue a cero) o cuando el temporizador de ensamblado del enrutador expira mientras el enrutador espera los fragmentos.

4.2.4.2.6 Problema de parámetros

Cuando un enrutador o una estación receptora encuentra problemas que no son cubiertos con los mensajes ICMP de error anteriores, envía un mensaje de **error de parámetros**. Una causa posible del problema ocurre cuando los parámetros o argumentos para una operación son incorrectos.

4.2.4.2.7 Estimación del tiempo de tránsito.

ICMP también soporta los mensajes de **estimación de tiempo de tránsito** (time stamp) y mensaje de **respuesta de estimación de tiempo** (time stamp reply messages). Estos proveen datos para examinar y calcular las características de retraso de la red, sincronización del reloj entre equipos etc.

4.2.4.2.8 Obtención de máscara de red

Para aprender la máscara de una subred (subnet mask) utilizada en la red local, una máquina puede enviar un mensaje de **solicitud de máscara** de subred a un enrutador y recibir un mensaje de **respuesta de máscara** de subred. La máquina que hace la solicitud puede enviar directamente el mensaje (si conoce la dirección del enrutador) o transmitir el mensaje por broadcast .

4.2.4.3 TCP: Protocolo de Control de Transmisión

En la mayoría de las aplicaciones abiertas distribuidas se requiere de un servicio de transporte de mensajes eficaz. Para lo cuál en la arquitectura TCP/IP, el protocolo de transporte orientado a conexión es conocido como **Protocolo de Control de Transmisión** (TCP, Transmission Control Protocol), y el servicio que ofrece a los usuarios a través de los protocolos de aplicación es un servicio de transporte de flujo eficiente, lo que permite a una aplicación asegurarse que un datagrama enviado sobre una red, se recibió totalmente.

El protocolo TCP reside en la capa de transporte, encima del protocolo en la capa de red, pero debajo de las capas superiores y sus aplicaciones. El protocolo TCP reside solo en dispositivos que realmente procesen datos de información (en una compuerta o gateway no existe capa TCP, por que simplemente lleva a cabo la tarea de enrutamiento de datagramas), asegurándose de que los datos de información vayan desde la fuente hacia las estaciones destino. Debido a que TCP es un protocolo independiente de propósitos generales asumiendo muy poco sobre el sistema inmediato inferior de comunicación hace que se pueda adaptar para utilizarse con una gran variedad de sistemas de entrega de paquetes, incluyendo el servicio de entrega de datagramas IP. Lo que lo hace una de sus ventajas.

El protocolo TCP maneja el flujo de datos provenientes de las capas superiores, así como los datagramas de llegada provenientes de la capa IP. El protocolo TCP debe ser capaz de manejar la terminación en una aplicación de una capa superior, así como fallas en las capas inferiores, TCP también debe de mantener una tabla de estado de todos los flujos de datos hacia dentro y fuera de la capa de TCP. El aislamiento de estos servicios en una capa independiente (capa de transporte) permite que el diseño de los protocolos de las capa de superiores no se preocupen de la tarea de control de flujo y de la confiabilidad del mensaje.

4.2.4.3.1 Conexión full dúplex

Las conexiones proporcionadas por el servicio de flujo TCP/IP permiten la transferencia concurrente en ambas direcciones (full dúplex). El servicio de flujo permite que un proceso de aplicación termine el flujo en una dirección mientras los datos pueden continuar moviéndose en la otra dirección.

4.2.4.3.2 Transferencia de memoria intermedia

Normalmente el protocolo TCP decide cuando un nuevo segmento es transmitido. Para hacer más eficiente la transferencia y minimizar el tráfico en la red, el software del protocolo TCP emisor por lo general, recolecta los datos suficientes de flujo de datos pequeños para llenar un segmento razonablemente largo antes de transmitirlo a través de la red. De manera similar si un programa de aplicación

genera flujos de datos muy largos, el software de TCP puede dividir cada flujo en partes más pequeñas para su transmisión.

En el lado destino, el protocolo TCP receptor almacena los datos recibidos en un segmento en una memoria de almacenamiento asociada con la aplicación en cuestión, poniéndolos a disposición del programa de aplicación receptor una vez que el segmento en la memoria asociada este completo y los datos sean verificados[32].

4.2.4.3.3 Control de flujo por medio de ventanas deslizantes

El protocolo TCP visualiza el flujo de datos de los procesos de usuario como una secuencia de octetos (bytes) que divide en segmentos para su transmisión. Por lo general, cada segmento viaja a través de la red como un solo datagrama IP.

El TCP utiliza un mecanismo especializado de **ventana deslizable de tamaño variable** para solucionar dos problemas importantes: la transmisión eficiente y el control de flujo. El mecanismo de ventana del TCP hace posible enviar varios segmentos antes de que llegue un reconocimiento de mensaje. El método de TCP de ventana deslizable también soluciona el problema de control de flujo de extremo a extremo, al permitir que el receptor restrinja la transmisión hasta que tenga espacio suficiente en memoria intermedia para recibir más datos.

El mecanismo TCP de ventana deslizable opera a nivel de octeto, no a nivel de segmento ni de paquete. Los octetos de flujo de datos se enumeran de manera secuencial. Tomando en cuenta que el receptor tiene que tener una ventana similar para poder reensamblar de nuevo el flujo. Sin embargo, es importante hacer notar que las conexiones TCP son de tipo full dúplex, por lo tanto, el software TCP en cada extremo mantiene dos ventanas por cada conexión, una se desliza a lo largo del flujo de datos que envía, mientras la otra se desliza a lo largo de los datos que recibe.

El protocolo TCP permite que el tamaño de la ventana varíe. Con lo que cada reconocimiento de mensaje, que informa cuántos octetos se recibieron, contiene además un aviso de ventana del receptor, en el que especifica cuántos octetos adicionales de datos está preparado a aceptar el receptor (tamaño actual de la memoria intermedia del receptor). En respuesta del aumento en el aviso de la ventana, el transmisor aumenta el tamaño de ventana deslizable y procede la envío de octetos. De manera que el tamaño de la ventana cambia en el momento que la ventana se mueve hacia adelante.

[32] El protocolo TCP lleva a cabo una verificación de integridad de datos y de información de encabezado por medio de una suma de verificación de 16 bits.

4.2.4.3.4 Control de congestionamiento

Tener un mecanismo para el flujo de datos es esencial en un ambiente de interconexión de redes , en donde las estaciones pueden ser de diferentes capacidades y velocidades. Además el protocolo TCP debe implantar un control de flujo extremo a extremo para garantizar una entrega confiable, ya que los protocolos de red necesitan un control de flujo que permita que los sistemas intermedios como enrutadores (compuertas) controlen un emisor que envíe más tráfico del que el enrutador puede manejar.

La sobre carga en dispositivos intermedios se conoce como congestionamiento. TCP no cuenta con un método explícito de control de congestionamiento pero lo resuelve de otra forma. El protocolo TCP puede ayudar a evitar el colapso por congestionamiento al reducir automáticamente la velocidad de transmisión siempre que ocurra un retraso. Para esto, el estándar TCP ahora recomienda la utilización de dos técnicas: **arranque lento** y la **disminución multiplicativa**.[33]

4.2.4.3.5 Opción del tamaño máximo de segmento

No todos los segmentos que se envían a través de una conexión son del mismo tamaño. Sin embargo, ambos extremos de la conexión necesitan acordar el tamaño máximo de los segmentos que transferirán. Esto es de vital importancia, ya que en estaciones conectadas por redes de área local de alta velocidad es especialmente importante escoger un tamaño máximo de segmento que llene los paquetes o de otra manera no aprovecharán el ancho de banda . Es decir, si dos puntos extremos residen en la misma red física, el TCP por lo general acordará un tamaño máximo de segmento de tal forma que los datagramas IP resultantes correspondan con la MTU (maximum transfer unit) de la red. Si los puntos extremos no residen en la misma red física, pueden intentar descubrir la MTU mínima a lo largo del camino entre ellos o pueden escoger un tamaño máximo de segmento de 536 (tamaño máximo asignado por omisión de datagrama IP).

Por otro lado, los tamaños de segmento muy grandes también pueden producir un bajo desempeño, esto es debido a que los grandes segmentos dan como resultado grandes datagramas IP. Cuando estos datagramas viajan a través de una red con una MTU pequeña, el protocolo IP debe fragmentarlos. A diferencia de un segmento TCP, un fragmento no se puede confirmar o retransmitir en forma independiente, de manera que todos los fragmentos deben llegar o de lo contrario se tendrá que retransmitir todo el datagrama. Por lo que aumentar el tamaño de segmento por arriba del rango de fragmentación disminuye la probabilidad de que lleguen los datagramas, lo que disminuye la eficiencia.

---

[33] Douglas E. Commer; Internetworking with TCP/IP. Principles, Protocols, and Architectures. 2a. edición; Prentice Hall.

En teoría, el tamaño óptimo de segmento, es cuando los datagramas IP que llevan los segmentos son tan grandes como sea posible sin requerir fragmentación en ninguna parte a lo largo de la ruta entre el emisor y el receptor.[34]

4.2.4.3.6 Temporizadores

Al igual que la mayor parte de los protocolos basados en conexión, los temporizadores son un aspecto importante de TCP. El uso de un temporizador asegura que no se espere más tiempo del necesario de un reconocimiento de mensaje o un mensaje de error. Si el temporizador expira, se supone una transmisión incompleta. Por lo general un temporizador que termina antes del envío de un mensaje de reconocimiento de mensaje causará la retransmisión del datagrama a partir de la estación emisora.

El protocolo TCP maneja los retrasos variables en la red al utilizar un algoritmo adaptable de retransmisión. En esencia, el TCP monitorea el desempeño de cada conexión y deduce valores razonables para la terminación del temporizador. Para recolectar los datos necesarios para un algoritmo adaptable, el TCP registra la hora de envío y la hora de recepción del reconocimiento de mensaje para los datos en el segmento (tiempo de viaje redondo, RTT round trip time). Siempre que obtiene una nueva muestra de viaje redondo, el TCP ajusta su noción de tiempo de viaje redondo promedio para la conexión, y actualiza el tiempo para el temporizador.

Los temporizadores pueden crear algunos problemas en el protocolo TCP, ya que en este las especificaciones de TCP prevén el reconocimiento de mensaje solamente del datagrama con el número de más alto valor recibido sin error, pero las recepciones fragmentadas no se pueden manejar correctamente. Si un mensaje se compone de varios datagramas que por su naturaleza llegan fuera de orden, la especificación indica que TCP no puede realizar un reconocimiento de mensaje de recepción del mensaje hasta que se reciban todos los datagramas. Por lo tanto, aun si todos los datagramas se han recibido con éxito, excepto uno que se encuentre a la mitad de la secuencia, el temporizador puede llegar a su fin y provocar que se tengan que volver a enviar todos los datagramas. En el caso de mensajes largos puede generar un aumento en el tráfico de la red. Además de que puede empeorar la situación en el congestionamiento de dispositivos intermedios.

Los problemas de retransmisión pueden surgir cuando las redes tienen grandes retrasos que provocan la retransmisión prematura. Es por esto que el protocolo TCP detecta los paquetes duplicados al asignar a cada uno un número de secuencia y forzar al receptor a recordar qué números de secuencia recibe. En el caso de que el receptor TCP reciba datagramas duplicados, el TCP receptor descartará cualquier datagrama duplicado, sin la emisión de mensajes de error.

[34] Este punto del tamaño óptimo de segmento esta aún en investigación.

4.2.4.3.7 Puertos y Sockets

Los números de puerto son utilizados para el esquema de direccionamiento al nivel de capa de transporte, por lo tanto todas las aplicaciones de capa superior que utilizan TCP (o UDP) tienen un número de puerto que las identifica. Como el campo de número de puerto es de 16 bits, una estación puede teóricamente establecer hasta 65535 diferentes conexiones TCP[35] al mismo tiempo.

Se han adoptado algunas reglas convencionales para permitir una mejor comunicación entre varias implantaciones de TCP. Esto permite que el número de puerto realice la identificación del tipo de servicio que un sistema TCP está solicitando de otro (Los números de puerto se pueden cambiar de manera local pero puede causar problemas[36]).

Típicamente, los números de puerto mayores a 255 se reservan para uso privado de la máquina local, pero números inferiores a 255 se utilizan para procesos de uso frecuente. La Autoridad de Números Asignados de Internet (Internet Assigned Numbers Authority) publica una lista de los números de puerto de uso frecuente, tales números son:

Núm. de puerto	Nombre del proceso	Clave UNIX	Descripción
0			Reservado
1	TCPMUX		Multiplexador de servicio de puerto TCP
5	RJE		Entrada de tarea remota
7	ECHO	echo	Eco
9	DISCARD	discard	Descartar
11	USERS	systat	Usuarios activos
13	DAYTIME	daytime	Hora hábil
15		netstat	Programa de estado de red
17	QUOTE	qotd	Cita del día
19	CHARGEN	chargen	Generador de caracteres
20	FTP-DATA	ftp-data	Protocolo de transferencia de archivos (
21	FTP	ftp	Protocolo de transferencia de archivos
23	TELNET	telnet	Conexión de terminal
25	SMTP	smtp	Protocolo de transferencia de correo sencillo
42	NAMESERVER	name	Nombre del host servidor
43	NICNAME	whois	¿Quién está ahí?
53	DOMAIN	nameserver	Servidor de nombre de dominio

Tabla 4.3a número de puerto y nombre de proceso asociado

[35] UDP también utiliza números de puerto para el direccionamiento. Haciendo notar que TCP y UDP, cada uno tiene su propio espacio de direcciones, es decir, el número de puerto 511 en TCP no es el mismo que el número de puerto 511 en UDP. El rango de validación del número de puerto es restringido por la estación misma pero se ha llevado a cabo una convención en el establecimiento de números de puerto.

[36] Por ejemplo, para el servicio de ftp que utiliza el puerto 21, se puede utilizar otro número de puerto.

Núm. de puerto	Nombre del proceso	Clave UNIX	Descripción
77		rje	Cualquier servicio RJE probado
79	FINGER	finger	Finger
80	HTTP	http	Servidor de Web
93	DCP		Protocolo de control de dispositivo
95	SUPDUP	supdup	Protocolo SUPDUP
101	HOSTNAME	hostnames	Servidor de nombre de host NIC
102	ISO-TSAP	iso-tsap	ISO-TSAP
103	X400	x400	Servicio de correo X.400
104	X400-SND	x400-snd	Envío de correo X.400
111	SUNRPC	sunrpc	Llamada a procedimiento remoto de SUN
113	AUTH	auth	Servicio de autentificación
117	UUCP-PATH	uucp-path	Servicio de trayecto UUCP
119	NNTP	nntp	Protocolo de transferencia de noticias USENET
129	PWDGEN		Protocolo generador de clave de acceso
139	NETBIOS-SSN		Servicio de sesión NETBIO

Tabla 4.3b número de puerto y nombre de proceso asociado

TCP utiliza la conexión (no el puerto del protocolo) como elemento fundamental. Una conexión completa tiene dos puntos extremos. Esto permite que un puerto se pueda utilizar para varias conexiones al mismo tiempo (multiplexaje). Es decir, si la estación emisora desea tener mas de una conexión con la misma aplicación, los números de puerto fuente serán diferentes aún cuando los números de puerto destino de la aplicación pueden ser iguales.

Cada circuito de comunicación dentro y fuera de la capa TCP se identifica en forma única mediante la combinación de dos números: La dirección IP (número de red, el número de estación) y el número de puerto utilizado por el TCP, determinando un punto final de comunicación (o socket). Existe un socket tanto en la estación emisora como en la receptora debido a que la dirección IP es única en toda la Internet y los números de puerto son únicos para cada aplicación en una estación, dando como resultado que el número de socket es único para toda la Internet. Esto permite que un proceso se comunique con otro a través de la red basándose enteramente en el número de socket.

4.2.4.3.8 Puertos Pasivos y Activos

El protocolo TCP tiene dos métodos para establecer una conexión: activo y pasivo.

El establecimiento de conexión activo, ocurre cuando TCP emite una solicitud para conexión, basado en una instrucción proveniente de un protocolo de nivel superior que proporciona el número de socket.

Una conexión pasiva se establece cuando el protocolo de nivel superior instruye al software TCP que espere la llegada de solicitudes de conexión de un sistema remoto (por lo regular provenientes de una instrucción de apertura de conexión activa). Cuando TCP recibe esta solicitud, le asigna un número de puerto. Esto permite que la conexión se realice rápidamente, sin tener que esperar el proceso activo.

4.2.4.3.9 Actividad de un mensaje

El mensaje se origina en una aplicación de una capa superior pasándola al protocolo TCP, el cuál recibe un flujo de bytes y los ensambla en segmentos TCP. La información del encabezado se añade en el proceso de ensamblar el segmento, cada segmento tiene incluido una suma de verificación dentro del encabezado, así como un número de secuencia en el caso de que el mensaje completo se lleva a partir de más de un segmento. La longitud de un segmento por lo general es determinada por TCP o por un valor establecido por el administrador del sistema.

Si es requerida una comunicación de dos vías (como FTP o Telnet), se establece una conexión (circuito virtual) entre las estaciones emisora y receptora, antes de pasar el segmento al protocolo IP para su enrutamiento, este proceso se inicia en el software TCP enviando una petición de conexión TCP a la máquina receptora. En el mensaje aparece un número único (conocido como dirección de puerto TCP o número de socket) que identifica la conexión de la estación emisora. El software TCP de la estación receptora asigna su propio número único de puerto o socket y lo devuelve a la estación emisora. Estos dos números únicos definen entonces la conexión entre las dos estaciones hasta que se llegue a la conclusión del circuito virtual.

Una vez establecido el circuito virtual, TCP envía el segmento al software del protocolo IP, el que a su vez lo envía a la red en forma de datagrama[37]. Una vez que el datagrama llega al software IP de la máquina receptora pasa el segmento recibido a la capa TCP de la misma estación receptora, donde se procesa y pasa a las aplicaciones superiores, mediante el uso de un protocolo de capa superior.

---

[37] Cabe hacer notar que los segmentos de TCP viajan encapsulados dentro de datagramas IP, que a su vez están encapsulados en tramas de red física.

Si el mensaje completo es a partir de más de un segmento de largo, el software TCP receptor lo reensambla a partir de los números de secuencia contenidos en cada encabezado de segmento recibido. Si algún segmento es erróneo (tarea de chequeo a partir de la suma de verificación), el TCP devuelve un mensaje con el número de secuencia defectuoso. A continuación el TCP emisor puede volver a enviar el segmento erróneo.

Si para todo el mensaje solamente se utiliza un segmento, después de comparar la suma de verificación del segmento con un valor recién calculado, el TCP receptor puede generar ya sea un reconocimiento de mensaje (ACK) o una solicitud de reenvío del segmento y enrutarlo de regreso a la capa emisora.

4.2.4.3.10 En resumen los principales características de TCP

- Provee un circuito virtual bidireccional full dúplex.
- El usuario ve la transmisión de datos como un flujo de datos (no en bloques).
- Transmisión de datos eficaz utilizando:
  números de secuencia,
  sumas de verificación (checksums),
  reconocimiento de mensajes (acknowledgements), y
  retransmisión de segmentos después de que el temporizador de reconocimiento a expirado.
- Principio de ventana deslizante para mayor eficiencia.
- Funciones de datos urgentes y de empuje.
- El dirección de transporte utiliza un esquema de número de puerto de 16 bits.
- Terminación de conexión de manera formal (graceful connection shutdown) elegante.

4.2.4.4 Protocolo de Datagrama de Usuario (UDP: User Datagram Protocol)

El **Protocolo de datagramas de usuario** UDP proporciona un servicio de entrega sin conexión y no confiable, es decir, no emplea acuses de recibo para asegurarse de que llegaron los mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad a la que fluye la información entre las máquinas, por lo tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden, además, los paquetes pueden llegar más rápido de lo que el receptor los pueda procesar. Utiliza el protocolo IP para transportar los mensajes entre las máquinas[38].

[38] Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de una computadora anfitrión.

El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación, permitiendo que varios programas de aplicación que se ejecutan en una misma computadora envíen y reciban datagramas en forma independiente. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. En cada mensaje UDP, además de tener los datos, contiene tanto el número de puerto de destino como el número de puerto de origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe un reconocimiento.

Un programa de aplicación que utiliza el UDP acepta toda la responsabilidad para el manejo de problemas de confiabilidad, incluyendo la pérdida, duplicación y retraso de los mensajes, la entrega fuera de orden y la pérdida de conectividad. Varios programas de aplicación que utilizan UDP, olvidan implementar estas tareas, por lo que en redes de área local, que son altamente confiables y de baja demora, no se percibe este problema, pero cuando se utilizan en redes más grande generalmente tiene graves problemas.

Siguiendo un modelo por capas, el UDP es un protocolo de transporte, que reside sobre la capa del Protocolo Internet. Conceptualmente, los programas de aplicación acceden el UDP, que utiliza el IP para enviar y recibir datagramas como se muestra en la figura 4.8.

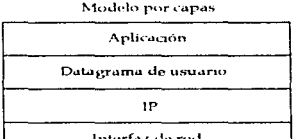


Figura 4.8 Estratificación por capas de UDP entre programas de aplicación e IP

UDP está fuertemente integrado al protocolo IP, lo cual rompe con la premisa de que la estratificación por capas permite una separación de funcionalidades (que es el objetivo del modelo OSI), esto se debe por razones prácticas, ya que es imposible identificar plenamente un programa de aplicación de destino sin especificar la máquina de destino y por que se debe de realizar, de manera eficaz, la transformación de direcciones utilizadas por el UDP y el IP.

El multiplexaje y el demultiplexaje entre UDP y los programas de aplicación lo hace a través del mecanismo de puerto. Este mecanismo es parecido al que utiliza TCP.

4.2.4.4.1 Resumen de las características de UDP

En resumen, las principales características de UDP son:

- Menos complejo que TCP.
- Orientado a no conexión.
- Direccionamiento por medio de puertos.
- Verificación de datos.
- Envío con el mejor esfuerzo.

4.2.4.5 Protocolo de Resolución de Direcciones: ARP

4.2.4.5.1 Direcciones Físicas y Lógicas de Red

En el esquema de direcciones de TCP/IP, a cada nodo se le asigna una dirección lógica de 32 bits. El esquema de direccionamiento lógico permite que las redes TCP/IP se comporten como una red virtual. De esta manera se puede utilizar tan solo esta asignación de direcciones para llevar a cabo el envío y recepción de paquetes. Pero se debe tomar en cuenta que dos máquinas a nivel físico, solo se pueden comunicar, una con otra, *solo si cada una, conoce la dirección física de red de la otra máquina.* Por tanto para hacer posible la comunicación entre máquinas debe existir un procedimiento que permita realizar el mapeo entre una dirección IP a una dirección física correcta, lo cual es necesario para enviar un paquete a través de la red física.

4.2.4.5.2 La Resolución de Direcciones

El problema de mapear direcciones de alto nivel (como las direcciones IP) en direcciones físicas se conoce como **problema de asociación de direcciones** y se ha resuelto de muchas maneras. Algunos grupos de protocolos cuentan con tablas en cada máquina que contienen pares de direcciones, direcciones de alto nivel y físicas. Otros solucionan el problema al codificar direcciones de hardware en direcciones de alto nivel. Basarse en cualquier de estos enfoques sólo hace que el direccionamiento de alto nivel sea de manera delicada.

4.2.4.5.3 Dos tipos de direcciones físicas

Hay dos tipos básicos de direcciones físicas, ejemplificadas por las direcciones Ethernet que tienen direcciones físicas grandes y fijas, y las direcciones proNET, que tiene direcciones físicas pequeñas y fáciles de configurar. La resolución de direcciones para redes Ethernet es difícil, en tanto que la resolución para redes tipo proNET es de manera sencilla.

Hay tres posibilidades básicas para convertir una dirección IP en una dirección física:

- Conversiones estáticas: se llevan a cabo usando una tabla. Esta tiene la desventaja que cuando ocurre una alteración en la red una nueva tabla debe ser generada.
- Conversión mediante asociación directa: este método hace uso de alguna función o fórmula para realizar la conversión de una dirección IP (dirección internet) a una dirección física. Por ejemplo, una estación con dirección Ethernet 80-04-00-60-00-01 es usada en la dirección IP 89.60.00.01, donde parte de la dirección Ethernet es usada para la dirección internet correspondiente. Cabe mencionar, que es posible que esta conversión no tenga una correspondencia uno a uno; por ejemplo, si dos direcciones Ethernet coinciden en los campos usados para la conversión, entonces ambos hosts tendrán la misma dirección IP.
- Conversión dinámica: este método involucra que se tenga que hacer una petición a la red. Lo que implica que este esquema de conversión solo se pueda llevar a cabo en redes que cuentan con mecanismos de broadcast . De esta manera, la modificación de las direcciones Ethernet llegan a ser transparentes en la red.

El tercer esquema de conversión es el mas adecuado para seguir. **El Protocolo de Resolución de Direcciones** *(ARP)* fue diseñado para este propósito y es utilizado para realizar la petición a la red.

4.2.4.5.4 Resolución por medio de la conversión dinámica

Para entender por qué la definición de direcciones es difícil para algunos tipos de redes, consideremos la tecnología Ethernet. A cada interfaz Ethernet (tarjeta de red) se le asigna una dirección física de 48 bits única. En consecuencia, cuando la interfaz falla y se necesita reemplazarla, la dirección física de la máquina cambia. Además, como la dirección física Ethernet es de 48 bits, no hay posibilidad de codificarla directamente en una dirección IP de 32 bits. [39]

[39] Debido a que la transformación directa es más conveniente y eficiente que la asignación dinámica, la próxima generación de IP se esta diseñando para permitir que las direcciones físicas de 48 bits se puedan codificar directamente en direcciones IP.

Los diseñadores de los protocolos TCP/IP encontraron una solución creativa para el problema de la asociación de direcciones en redes como Ethernet, que tiene capacidad de broadcast . La solución permite agregar nuevas máquinas a la red, sin tener que recompilar el código y no requiere tener una base de datos centralizada. Para evitar la definición de una tabla de conversiones, los diseñadores utilizan un protocolo de bajo nivel para resolver direcciones en forma dinámica, conocido como **Protocolo de Resolución de Direcciones** (ARP, Address Resolution Protocol), el cual proporciona un mecanismo eficaz y sencillo de mantener.

El método que se sigue en la resolución por medio de la conversión dinámica con el protocolo ARP se lleva a cabo de manera simple, ver figura 4.9, por ejemplo: cuando una estación *A* requiere resolver la dirección IP de una estación B *(IB)*, transmite en un paquete especial (por medio de broadcast o broadcast) que pregunta a la estación que posea la dirección IP *IB*, que responda con su dirección física (*PB*). Por la naturaleza del mecanismo de broadcast, todas las estaciones de la red física incluyendo la estación *B*, reciben el paquete de solicitud ARP, pero sólo la estación *B* reconoce su propia dirección IP (*IB*) y de esta manera envía un paquete de respuesta que contiene su dirección física *PB*. Cuando *A* recibe la respuesta, utiliza la dirección física obtenida para enviar el paquete de datos directamente a la estación *B*.

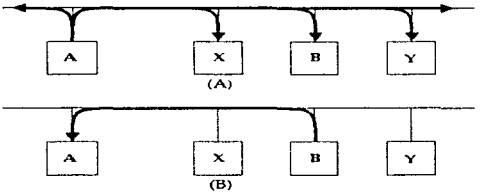


Figura 4.9 Protocolo ARP. Para determinar la dirección física PB de B, desde su dirección IP, IB, (A) el anfitrión A transmite por broadcast una solicitud ARP que contiene IB a todas las máquinas de la red, y (B) el anfitrión B envía una respuesta ARP que contiene el par (IB, PB)

4.2.4.5.5 Memoria intermedia para la resolución de direcciones

Puede parecer extraño que para que *A* envíe un paquete a *B*, primero, tenga que transmitir un broadcast que llegue a *B*. Podría parecer aún más extraño que A transmita por broadcast la pregunta ¿cómo puedo llegar hasta ti?, en lugar de sólo transmitir por broadcast el paquete que quiere entregar. Pero existe una razón importante para este intercambio. La broadcast es demasiado cara para utilizarse cada vez que una maquina necesita transmitir un paquete a otra, debido a que

requiere que cada maquina en la red procese dicho paquete. Para reducir los costos de comunicación, las estaciones que utilizan ARP, mantienen una memoria intermedia de las asignaciones de direcciones IP a direcciones físicas recientemente adquiridas, para que no tengan que utilizar ARP varias veces. Siempre que una estación recibe una respuesta ARP, ésta guarda la dirección IP del transmisor, así como la dirección física correspondiente, en su memoria intermedia, para utilizarla en búsquedas posteriores. Cuando transmite un paquete, una estación siempre busca, en su memoria intermedia, una asignación antes de enviar una solicitud ARP. Si una estación encuentra la asignación deseada en su memoria intermedia ARP, no necesita transmitir una broadcast a la red.

4.2.4.5.6 Implantación de ARP

Funcionalmente ARP esta dividido en dos partes. La primera parte, mapea una dirección IP a una dirección física cuando se envía un paquete. La segunda parte, contesta las peticiones de otras máquinas.

4.2.4.5.7 Encapsulamiento e identificación ARP

Para identificar que la trama transporta un mensaje ARP, el transmisor asigna un valor especial al campo de tipo en el encabezado de la trama y coloca el mensaje ARP en el campo de datos de la misma. Cuando llega una trama a una estación, el software de red utiliza el campo de tipo de trama para determinar su contenido. En la mayor parte de las tecnologías se utiliza un solo valor para el tipo de todas las tramas que transportan un mensaje ARP, el software de red en el receptor debe examinar el mensaje ARP para distinguir entre solicitudes y respuestas.

4.2.4.6 Protocolo de Réplica de Resolución de Direcciones: RARP

El protocolo RARP (Reverse Address Resolution Protocol) es utilizado para el caso inverso al protocolo ARP, es decir, sirve para obtener la dirección IP (dirección Internet) a partir de la dirección física[40] de la máquina (dirección MAC).

Cabe señalar que este protocolo es utilizado por las estaciones carentes de disco duro, estas ocupan el protocolo RARP a fin de obtener su correspondiente dirección IP apartir de un servidor de RARP, de esta manera poderse comunicar con los protocolos TCP/IP.

RARP es una adaptación del protocolo ARP ya que utiliza el mismo formato de paquete ARP pero con diferentes códigos de operación. El mensaje RARP enviado para solicitar una dirección IP es un poco más general, permitiendo así, que una estación solicite la dirección IP de una estación tercera a partir de la dirección física

[40] La dirección Ethernet o dirección MAC usualmente se obtiene de la memoria del controlador físico o tarjeta de red de la estación misma.

de la tercera. También lo permite cuando se trabaja con múltiples tipos de redes físicas.

Un mensaje de petición RARP se transmite por medio de broadcast (broadcast) especificando que la estación es transmisora y receptora, además de proporcionar su dirección física en el campo de dirección de hardware objetivo. Por la naturaleza de la broadcast , todas las máquinas de la red reciben la petición. Una de las estaciones en la red debe tener activo el servicio de RARP (servidor de RARP) el cual responde a la petición utilizando la tabla que contiene las direcciones IP correspondientes a las direcciones Ethernet. Cambian el tipo de mensaje de petición a respuesta y la envían de regreso a la maquina originaria. La máquina en cuestión recibe respuesta de todos los servidores RARP, aunque solo sea necesaria una respuesta.

La comunicación que se lleva a cabo entre una máquina que solicita el servicio de RARP y el servidor de RARP se lleva a cabo utilizando solamente una red física.

Recientemente el mecanismo RARP ha sido reemplazado por el protocolo BOOTP, este lleva a cabo un mecanismo mucho más simple de inicialización de carga de estaciones sin disco duro basado en datagramas IP.

4.2.5 TCP/IP: Protocolos del nivel de aplicación

4.2.5.1 Protocolos de arranque y autoconfiguración: BOOTP Y DHCP

4.2.5.1.1 Introducción

Una computadora conectada a una red TCP/IP o a Internet necesita saber su dirección IP antes de que pueda enviar o recibir datagramas, además, requiere información adicional como la dirección de un enrutador, la mascara de la subred y la dirección de un servidor de nombres. A continuación se analizara dos protocolos que permiten a un sistema determinar su dirección IP sin utilizar RARP.

4.2.5.1.2 Una alternativa a RARP

Las máquinas sin disco por lo general contienen información de arranque en sus PROMs. En vista de que éstos, a fin de reducir costos, deben conservarse pequeños y consistentes entre muchos modelos de estaciones de trabajo sin disco, es imposible incluir un protocolo completo como TCP/IP en un chip. También es imposible incrustar una dirección IP, porque el chip se podría emplear en muchas máquinas distintas de la misma red. Esto obliga a una estación de trabajo sin disco recién arrancada determine su propia dirección IP a partir de otras máquinas de la red.

Para superar algunas de las dificultades de RARP, se desarrollo el **BOOT-strap Protocol** (BOOTP), y más recientemente, el **Dynamic Host Configuration Protocol** (DHCP) que es una extensión y el sucesor de BOOTP.

Dado que BOOTP utiliza UDP e IP, se debe implementar como un programa de aplicación. Como RARP, BOOTP trabaja bajo el esquema de cliente-servidor y requiere sólo de un intercambio de paquetes. No obstante, BOOTP es mas eficiente que RARP pues con un sólo mensaje BOOTP especifica muchos aspectos necesarios para el arranque, que incluye una dirección IP de la computadora, la dirección de un enrutador y la dirección de un servidor.

4.2.5.1.3 Utilización de IP para determinar una dirección IP

Para determinar la dirección IP de una computadora sin disco, BOOTP utiliza las capacidades de broadcast de IP. Recuérdese que IP habilita varias direcciones especiales de red que se difunden a todas las máquinas de la red. Esto le permite a la computadora enviar un mensaje aun cuando no conozca la dirección de la máquina destino o la suya propia.
Las direcciones de broadcast IP, como 255.255.255.0, permiten que se envíe un mensaje a todas las máquinas de una subred, a pesar de que no se tenga dirección de red fuente o destino.

4.2.5.1.4 Política de transmisión BOOTP

BOOTP coloca todas las tareas de comunicaciones en las computadoras sin disco. Especifica que todos los mensajes UDP que se envíen sobre la red utilicen sumas de verificación y que se establezca el bit de no fragmentar. Esto tiende a reducir el número de datagramas perdidos, mal interpretados o duplicados.

BOOTP utiliza un conjunto de temporizadores para manejar la pérdida de un mensaje. Cuando éste se envía, un temporizador se inicia. Si cuando el temporizador expira no se ha recibido respuesta, se vuelve a enviar el mensaje. El protocolo estipula que el temporizador se establece con un valor aleatorio, el cual va aumentando cada vez que el alcanza un valor máximo, después de lo cual se vuelve a determinar un nuevo valor aleatorio. Esto impide un tráfico masivo si varias máquinas fallan simultáneamente e intentaran difundir mensajes BOOTP simultáneamente.

4.2.5.1.5 Procedimiento de arranque de dos pasos

BOOTP utiliza un procedimiento de arranque de dos pasos. No proporciona una imagen de memoria a los clientes - sólo proporciona al cliente la información necesaria para obtener una imagen. El cliente entonces utiliza un segundo protocolo (por ejemplo, TFTP) para obtener la imagen de memoria. Aunque el procedimiento de dos pasos parece innecesario, permite una clara separación de configuración y almacenamiento. Un servidor BOOTP no necesita correr en la misma máquina que almacena las imágenes de memoria. De hecho, el servidor BOOTP opera desde una simple base de datos que sólo conoce los nombres las máquinas con las imágenes de memoria de estas.

4.2.5.1.6 Las necesidades de una configuración dinámica

Como RARP, BOOTP fue diseñado para un ambiente relativamente estático en el que cada host tiene una conexión de red permanente. Un administrador crea un archivo de configuración BOOTP que especifica un conjunto de parámetros BOOTP para cada host. El archivo no cambia con frecuencia pues la configuración generalmente se mantiene estable. Por lo común, una configuración no registra cambios durante semanas.

Con la llegada de redes inalámbricas y computadoras portátiles (como las laptops y las notebooks), se ha vuelto posible transportar a las computadoras de una localidad a otra rápida y fácilmente. BOOTP no se adapta a esta situación pues la información que contiene de configuración no se puede cambiar rápidamente. Así pues, sólo proporciona una transformación estática desde un identificador de host hacia parámetros para el host. Además, un administrador debe introducir un conjunto de parámetros para cada host y luego almacenar la información en un archivo de configuración de servidor BOOTP-BOOTP no incluye una forma para asignar dinámicamente valores a máquinas individuales. En particular, un administrador debe asignar cada host a una dirección IP.

Los parámetros de asignación estática trabajan bien si las computadoras se mantienen en localidades fijas y el administrador tiene suficientes direcciones IP para asignar a cada computadora una dirección IP única. Sin embargo, en los casos en los que las computadoras se mueven con frecuencia o que el número de computadoras físicas exceda el de direcciones IP de hosts disponibles, la asignación estática generará sobrecargas excesivas.

4.2.5.1.7 Configuración dinámica de la estación de trabajo

Para manejar la asignación de direcciones dinámica de manera automática, se diseño el Protocolo de Configuración Dinámica de Anfitrión (DHCP: Dynamic Host Configuration Protocol), el nuevo protocolo extiende a BOOTP de dos

formas. En primer lugar, el DHCP permite que una computadora adquiera toda la información que necesita en un solo mensaje. Por ejemplo, además de una dirección IP, tiene una mascara de subred. En segundo lugar, el DHCP permite que una computadora posea una dirección IP en forma rápida y dinámica. Para utilizar el mecanismo de asignación de direcciones dinámico DHCP, un administrador debe configurar un servidor DHCP supliendo un conjunto de direcciones IP. Cada vez que una computadora nueva se conecta a la red, la computadora contacta al servidor y solicita una dirección. El servidor selecciona una de las direcciones especificadas por el administrador y la asigna a la computadora.

Para ser completamente general, el DHCP permite tres tipos de asignación de direcciones; un administrador selecciona cómo responderá el DHCP a cada red o a cada host. Como BOOTP, el DHCP permite la configuración manual, mediante la cual el administrador puede configurar una dirección específica. El DHCP también permite la configuración automática, por medio de la cual el administrador permite a un servidor DHCP asignar una dirección permanente cuando una computadora es conectada por primera vez a la red. Por último, el DHCP permite una configuración dinámica completa, con la cual el servidor "presta" una dirección para una computadora por tiempo limitado.

Como en BOOTP, el DHCP utiliza la identidad del cliente para decidir cómo proceder. Cuando un cliente contacta un servidor DHCP, envía un identificador, por lo general, la dirección de hardware del cliente. El servidor utiliza el identificador del cliente y la red a la que el cliente se ha conectado para determinar cómo asignar el cliente y la dirección IP. Así, el administrador tiene un control completo sobre la forma en que se asignan las direcciones. Un servidor puede configurarse para asignar direcciones a computadoras específicas de manera estática (como BOOTP), mientras permite a otras computadoras obtener dinámicamente direcciones de manera permanente o temporal.

4.2.5.1.8 Asignación dinámica de direcciones IP

La asignación dinámica de direcciones es el más significativo y novedoso aspecto del DHCP. A diferencia de la asignación de direcciones estática, utilizada en BOOTP, la asignación de direcciones dinámica no es una transformación uno a uno, y el servidor no necesita conocer la identidad de un cliente a priori. En particular un servidor DHCP puede ser configurado para permitir que una computadora arbitraria obtenga una dirección IP y comience la comunicación. Así, el DHCP permite diseñar sistemas que se autoconfiguren.

Para hacer posible la autoconfiguración, un servidor de DHCP comienza con un conjunto de direcciones IP que el administrador de red asigna al servidor para su manejo. El administrador especifica las reglas bajo las que operará el servidor. Un

cliente DHCP negocia el uso de una dirección intercambiando mensajes con un servidor. En el intercambio, el servidor proporciona una dirección para el cliente y el cliente verifica que la dirección sea aceptable. Una vez que el cliente ha aceptado una dirección, puede comenzar a utilizarla para comunicarse.

A diferencia de la asignación de direcciones estática, que asigna permanentemente cada dirección IP a un host específico, la asignación de direcciones dinámica es temporal. Decimos que un servidor DHCP arrienda una dirección a un cliente por un período de tiempo finito. El servidor especifica el período de arrendamiento cuando asigna la dirección. Durante el período de arrendamiento, el servidor no arrendará la misma dirección a ningún otro cliente. Al final del período de arrendamiento, sin embargo, el cliente debe renovar el arrendamiento o dejar de usar la dirección.

El tiempo óptimo de arrendamiento depende en particular de la red y de las necesidades de un host. Por ejemplo, para garantizar que las direcciones puedan reciclarse con rapidez, las computadoras en una red utilizadas por estudiantes debe tener un corto período de arrendamiento (por ejemplo, una hora). En contraste, la red de una compañía podría utilizar un período de arrendamiento de un día o de una semana. Para adaptarse a todos los posibles ambientes, el DHCP no especifica un período de arrendamiento fijo y constante. De hecho, el protocolo permite que un cliente solicite un período de arrendamiento específico y permite a un servidor informar al cliente que el período de arrendamiento está garantizado. Así, un administrador puede decidir durante cuánto tiempo podrá asignar cada servidor una dirección a un cliente. En el caso extremo, el DHCP reserva un valor infinito para permitir un arrendamiento por un período de tiempo indeterminadamente largo, como si fuese la asignación de direcciones permanente utilizada en BOOTP.

4.2.5.1.9 DHCP y nombres de dominios

Aun cuando puede asignar direcciones IP a una computadora que lo demande, el DHCP no automatiza por completo todo el procedimiento requerido para conectar un host permanente a TCP/IP. En particular, el DHCP no interactúa con el sistema de nombre de dominio. Así, la asignación entre un nombre de host y la asignación DHCP de la dirección IP del host se deben manejar de manera independiente.

Se necesita mecanismos adicionales para soportar nombres de host permanentes. En particular, los nombres de los hosts permanentes requieren de una coordinación entre DHCP y DNS. Un servidor DNS debe cambiar la asignación, nombre-a-dirección cada vez que un host reciba una dirección IP y retirar la asignación cuando expire el arrendamiento. Actualmente se esta trabajando para que se pueda interactuar el DHCP con el DNS. De momento, no hay protocolos para actualizaciones DNS dinámicos.

4.2.5.2 Sistema de Nombres de Dominio: DNS

4.2.5.2.1 Introducción

TCP/IP utiliza una dirección de 32 bits para enrutar un datagrama a un destino. Como usuario final resulta más fácil dejar a un lado estas direcciones de 32 bits y en su lugar emplear nombres comunes, ya que estos últimos son mucho más fáciles de recordar. Para ello hay varios métodos, uno emplea un archivo ASCII en la máquina emisora que tiene los nombres y direcciones correspondientes. Una limitación importante de este sistema es que la máquina solamente será capaz de enrutar hacia otras que tengan registrada en este archivo, lo que resulta imposible mantener cuando existen muchas máquinas destino.

Otro método es que la resolución de dirección se lleve a cabo en otra máquina, que actúe como servicio de directorio. Hoy en día hay dos de estos procedimientos en uso común: el Servicio de Nombres de Dominio (DNS) y el Servicio de Información de Red (NIS) que ahora forma parte de NFS.

4.2.5.2.2 Nombres para las máquinas

Aun cuando la diferencia entre *dirección* y *nombre* es significativa intuitivamente, resulta artificial. Los nombres sólo son útiles si el sistema puede transformarlos de manera eficiente para referirse al objeto que denotan. Así, podemos pensar en una dirección IP (números, por ejemplo: 132.248.53.245) como en un *nombre de bajo nivel* y decimos que el usuario prefiere utilizar *nombres de alto nivel* (palabras, por ejemplo: pumas.iingen.unam.mx) para las máquinas.

La forma de los nombres de alto nivel es importante pues determina cómo son traducidos los nombres a nombres de bajo nivel o cómo conducen a objetos, también determinan la forma en que se autoriza la asignación de nombres. Cuando sólo se tiene unas cuantas máquinas interconectadas, la selección del nombre es fácil y cualquier forma será suficiente. En Internet, donde hay millones de máquinas conectadas, la selección de nombres se vuelve difícil.

4.2.5.2.3 Espacio de nombres planos

En un principio, al conjunto de nombres utilizados en Internet se le conocía como **espacio de nombres planos** en el que cada nombre de una máquina consistía de una secuencia de letras sin ninguna estructura. Esta lista era administrada por una unidad central llamada **Network Information Center** (NIC), y determinaba si un nombre nuevo era apropiado. Después el NIC fue reemplazado por el **INTERnet Network Information Center** (INTERNIC).

La mayor ventaja del espacio de nombres plano es que los nombres eran convenientes y cortos; la mayor desventaja es que el espacio de nombres plano no podía generalizarse para grandes conjuntos de máquinas. Uno de los problemas principales, es que si la base de nombres está localizada en una sola localidad, el tráfico de la red hacia dicha localidad se incrementaría enormemente.

4.2.5.2.4 Nombres jerárquicos

La manera más óptima de que el sistema de nombres se adapte al crecimiento rápido y extenso del conjunto de nombres, es que se organice de manera descentralizada el mecanismo de asignación de nombres, mediante el cual se delega la autoridad de partes del sistema de espacio de los nombres y se reparte la responsabilidad de traducción de los nombres y direcciones. Las redes TCP/IP utiliza dicho esquema.

4.2.5.2.5 Delegar autoridad para los nombres

Un esquema de nombres jerárquico funciona como una administración extensa. El espacio de nombre es subdividido en el nivel superior y dándoles la autoridad de las subdivisiones a los agentes designados. Por ejemplo, se debe seleccionar el espacio de nombres para subdividirlos en base a un *nombre de localidad* y delegar a cada localidad la responsabilidad de mantener los nombres dentro de esta partición.

La sintaxis de la asignación jerárquica es: *local.localidad*

Donde *localidad* es el nombre de la localidad autorizada por la autoridad central, *local* es la parte del nombre controlado por la localidad y, el punto (.) es un delimitador empleado para separarlos. Cuando la máxima autoridad añade una nueva localidad, *X*, ésta añade *X* a la lista de localidades válidas y delega a la localidad *X* la autoridad sobre todos los nombres que terminen con ".*X*".

4.2.5.2.6 Autoridad para los subconjuntos de nombres

En un espacio jerárquico de nombres, la autoridad puede ser subdividida en cada nivel. La localidad en sí puede consistir en varios grupos administrativos y la autoridad de la localidad puede elegir subdividir sus espacios de nombres entre los grupos. La idea es conservar subdividido el espacio de nombres hasta que cada subdivisión sea lo suficientemente pequeña como para que se pueda administrar.

Sintácticamente, subdividir el espacio de nombres introduce otra partición del nombre. Por ejemplo:

local.grupo.localidad

Dado que el nivel superior delega autoridad, el nombre de grupo no tiene que concordar en todas las localidades. La localidad de una universidad podría elegir nombres de grupo como *ingeniería, ciencia, arquitectura,* etc.

En una red TCP/IP, la jerarquía de nombres de máquinas se asigna de acuerdo con la estructura de la organización que obtiene la autoridad para dividir el espacio de nombres y no necesariamente de acuerdo con la estructura de las interconexiones de red física.

Por supuesto, en muchas localidades la jerarquía organizacional corresponde a la estructura de las interconexiones físicas de la red.

4.2.5.2.7 Nombres de dominio TCP/IP de Internet

El mecanismo que implanta una jerarquía de nombres de máquinas para las redes TCP/IP se conoce como **Sistema de Nombres de Dominio** *(DNS: Domain Name System).* El DNS tiene dos aspectos conceptuales independientes. El primero es abstracto: especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto a los nombres. El segundo es concreto: especifica la implantación de un sistema de computación distribuido que transforma eficientemente los nombres en direcciones.

El sistema de nombres de dominio se vale de un esquema de nombres jerárquicos, conocido como **nombre de dominio**. Un nombre de dominio consiste en una secuencia de nombres separados por un carácter delimitador, el punto ".", cada una de las cuales son secciones particulares del nombre debiendo representar localidades o grupos, en el sistema de dominios, a cada sección se le llama *etiqueta.* Así, el nombre de dominio

iingen.unam.mx

contiene tres etiquetas: *iingen, unam, mx*. Cualquier sufijo de una etiqueta en un nombre de dominio es llamado también *dominio.* En el ejemplo de arriba, el dominio de nivel inferior es *iingen.unam.mx* (el nombre de dominio para el Instituto de Ingeniería de la UNAM), el segundo dominio es *unam.mx* (el nombre de dominio para UNAM) y el nivel superior de dominio es *mx* (el nombre de dominio para México). Los nombres de dominio están escritos con la etiqueta local primero y el dominio superior al último.

4.2.5.2.8 Nombres de dominio oficiales y no oficiales de Internet

El Servicio de Nombre de Dominio, como su nombre lo indica, funciona dividiendo a Internet en un conjunto de dominio o redes, que a su vez se pueden dividir en subdominios. Esta estructura se parece a un árbol, como se muestra en

la figura 4.10. El primer conjunto de dominios se le llama dominios de nivel superior. Hay seis dominios de nivel superior de uso común:

- **arpa** para organizaciones específicas de Internet
- **com** para empresas comerciales
- **edu** para organizaciones educativas
- **gov** para organizaciones gubernamentales
- **mil** para organizaciones militares
- **org** para organizaciones no comerciales

Además de estos dominios de nivel superior, hay dominios de nivel superior dedicados para cada país conectado. Estos se identifican normalmente por medio de una abreviatura del nombre del país, como **.mx** para México y **.ca** para Canadá. Por conveniencia, estos dominios de nivel superior del país por lo general se omiten en los diagramas de la estructura de Internet, de lo contrario existirían cientos de dominios de nivel superior. La división de dominios a veces se repite por debajo del dominio de país, por lo que puede haber una extensión **.com** acoplada con **.mx** para mostrar un dominio comercial mexicano.

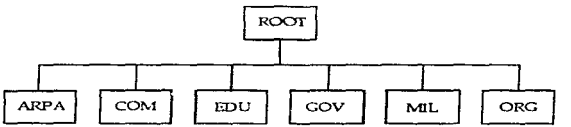


Figura 4.10 La estructura del dominio Internet

Por debajo de los dominios de nivel superior hay otro nivel para organizaciones individuales, dentro de cada dominio del nivel superior. Todos los nombres de dominio están registrados en el Centro de Información de Red (NIC) y son únicos para la red. Normalmente estos nombres son representativos de la empresa u organización.

Hay dos formas de identificar un destino. Si el destino está en la interred, se utilizará el *nombre absoluto*. Este es único y sin ambigüedades, especificando el dominio de la máquina destino. Un *nombre relativo* se puede utilizar ya sea en el interior del dominio local, donde el servidor de nombre sabrá que el objetivo está dentro del dominio y por lo tanto no necesita enrutar el datagrama a la interred, o cuando el servidor de nombre conoce el nombre relativo y lo puede expandir y enrutar correctamente.

4.2.5.2.9 Asociación de nombres de dominio en direcciones

Además de las reglas para la sintaxis del nombre y la delegación de autoridades, el esquema de nombres de dominio incluye un sistema distribuido, confiable y de propósito general para asociar nombres y direcciones. El sistema está distribuido en el sentido técnico, esto significa que un conjunto de servidores, que opera en varias localidades de manera conjunta, resuelve el problema de la asociación de nombres en direcciones. Es eficiente en el sentido de que la mayor parte de los nombres se puede asociar localmente; solo uno pocos requieren tráfico de Internet. Es de propósito general puesto que no se encuentra restringido a nombres de máquina. Por último, es confiable ya que una sola falla de una máquina prevendrá al sistema para que opere correctamente.

El mecanismo de dominio para la asociación de nombres en direcciones consiste en sistemas independientes y cooperativos llamados *servidores de nombres*. Un servidor de nombres es un programa servidor que ofrece la asociación nombre-a-dirección, asociando los nombres de dominio en direcciones IP. A menudo, el software servidor se ejecuta en una sola máquina, y a la máquina se le conoce como servidor de nombres. El software cliente llamado, **resolvedor de nombres** (*name resolver*), utiliza uno o más servidores de nombres cuando traduce un nombre.

La forma más fácil de entender cómo trabaja un servidor de dominio es imaginándolo como una estructura de árbol que corresponde a la jerarquía nombrada, como se muestra en la figura 4.11. La raíz del árbol es un servidor que reconoce el dominio de nivel superior y sabe qué servidor resuelve cada dominio. Teniendo un nombre por resolver, la raíz puede resolver el servidor correcto para este nombre. En el siguiente nivel, un conjunto de servidores de nombre proporciona respuestas para un dominio de nivel superior (por ejemplo, *mx*). Un servidor en este nivel sabe qué servidor puede resolver cada uno de los subdominios bajo su dominio. En el tercer nivel del árbol, el servidor de nombres proporciona respuestas para el subdominio (por ejemplo, *unam* bajo *mx*). El árbol conceptual continua con un servidor en cada nivel para el que se ha definido un subdominio.

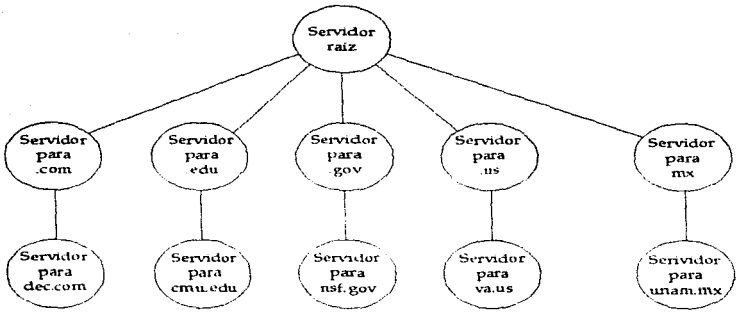


Figura 4.11 Arreglo conceptual del servidor de nombres de dominio en un árbol que corresponde a la jerarquía de nombre. En teoría, cada servidor conoce la dirección de todos los servidores de bajo nivel para todos los subdominios dentro del dominio que maneja.

Los enlaces en el árbol conceptual no indican conexiones físicas de red. De hecho, muestran qué otros servidores de nombres conoce y contacta un servidor dado. El servidor por sí mismo puede localizarse en una localidad cualquiera dentro de Internet. De esta manera, el árbol de servidores es una abstracción que emplea Internet para comunicarse.

En la práctica, la relación entre una jerarquía de nombres y el árbol de nombres no resulta tan sencilla como nuestro modelo lo plantea. El árbol de servidores tiene pocos niveles pues un sólo servidor físico puede contener toda la información para partes extensas de una jerarquía de nombres. En particular, las organizaciones a menudo reúnen información de todos los subdominios desde un solo servidor. La figura 4.12 muestra una organización más realista de servidores para la jerarquía de nombres que la figura 4.11.

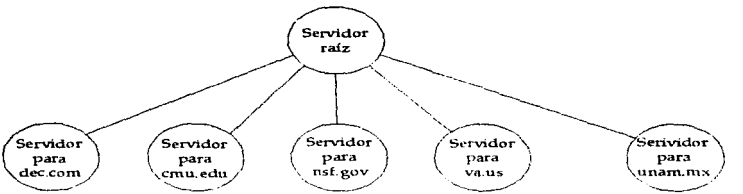


Figura 4.12 Una organización realista de los servidores para la jerarquía de nombres de la figura 4.11. Dado que el árbol es extenso y plano, pocos servidores necesitan conectarse cuando se resuelve un nombre.

Un servidor raíz contiene información acerca de la raíz y de dominios de nivel superior y cada organización utiliza un sólo servidor para sus nombres. Dado que el árbol de servidores es poco profundo, en la mayoría de los casos, dos servidores necesitan contactarse para resolver un nombre como *pumas.iingen.unam.mx*: el servidor raíz y el servidor para el dominio *unam.mx* (esto quiere decir que el servidor raíz sabe qué servidor maneja *unam.mx* y toda la información de dominio reside en un servidor).

4.2.5.2.10 Desempeño del cache: clave de la eficiencia

El costo de una búsqueda para nombres locales puede ser muy alta si se resuelve enviar cada solicitud hacia el servidor raíz. Incluso si las solicitudes pueden ir directamente hacia el servidor que tiene autoridad para el nombre, la búsqueda de nombres puede representar una pesada carga para Internet. Así, para manejar el desempeño global de un sistema servidor de nombres, es necesario reducir los costos de búsqueda para nombres no locales.

Los servidores de nombres de Internet utilizan una memoria inmediata de nombres (name caching) para optimizar los costos de búsqueda. Cada servidor mantiene una memoria inmediata de los nombres utilizados más recientemente, así como un registro de dónde fue obtenida la información para la asociación del nombre. Cuando un cliente interroga a un servidor a fin de resolver el problema de un nombre, el servidor verifica primero si tiene autoridad para el nombre de acuerdo con el procedimiento estándar. Si no es así, el servidor verifica su memoria inmediata para ver si el problema del nombre se resolvió recientemente. Los servidores reportan la información almacenada en memoria inmediata a los clientes, pero la marcan como una asignación **no autorizada** y entrega el nombre de dominio del servidor, S, desde el cual obtiene la asignación. El servidor local también envía información adicional que le indica al cliente la asignación entre S y

una dirección IP. De esta manera, los clientes reciben respuestas rápidamente, pero la información podría no estar actualizada.

4.2.5.3 Acceso remoto: telnet y rlogin

4.2.5.3.1 Introducción

El programa telnet (telecommunications network) pretende proporcionar conexión remota o capacidad de terminar virtual a través de una red y para tener acceso a muchos servicios públicos, que incluyen catálogos de bibliotecas y otros tipos de bases de datos. En otras palabras, un usuario de la máquina A debería ser capaz de registrarse en la máquina B desde cualquier parte de la red, y por lo que respecta al usuario, aparecer como si estuviera sentado frente a la maquina B. El servicio telnet se proporciona a través del TCP.

Telnet se creó debido a que en un tiempo el único método para permitir que una máquina tuviera acceso a otra era estableciendo un enlace mediante dispositivos de comunicaciones como módems o redes en puertos dedicados. Esto es un poco más complicado de lo que parece a primera vista, por la amplia variedad de terminales y computadoras existentes, cada una con sus propios códigos de control y características de terminal. Con varias conexiones remotas activas, el CPU del servidor puede generar una cantidad exorbitante de tiempo administrando las conversiones.

4.2.5.3.2 Protocolo TELNET

El conjunto de protocolos TCP/IP incluye un protocolo de terminal sencillo, llamado *telnet*. Telnet permite a un usuario de una localidad establecer una conexión TCP con un servidor de acceso a otro. Telnet transfiere después las pulsaciones de teclado directamente desde el teclado del usuario a la computadora remota como si hubiesen sido hechos en un teclado unido a la máquina remota. Telnet también transporta la salida de la máquina remota de regreso a la pantalla del usuario. El servicio se llama transparente (transparent) porque da la impresión de que el teclado y el monitor del usuario están conectados de manera directa a la máquina remota.

Telnet ofrece tres servicios básicos. El primero, define una **terminal virtual de red** *(network virtual terminal)* que proporciona una interfaz estándar para los sistemas remotos. Los programas clientes no tienen que comprender los detalles de todos los sistemas remotos, se construyen para utilizarse con la interfaz estándar. En segundo, telnet incluye un mecanismo que permite al cliente y al servidor negociar opciones, asimismo proporciona un conjunto de opciones estándar (por ejemplo, una de las opciones controla si los datos que se transfieren a través de la conexión se valen del conjunto de caracteres ASCII estándar de siete bits o de un conjunto

de caracteres de ocho bits). Por último, telnet trata con ambos extremos de la conexión de manera simétrica. En particular, telnet no fuerza la entrada de cliente para que ésta provenga de un teclado, ni al cliente para que muestre su salida en una pantalla. De ésta manera, telnet permite que cualquier programa se convierta en cliente, además, cualquier extremo puede negociar las opciones.

En la figura 4.13, se ilustra la forma en que los programas de aplicación implantan un cliente y servidor de telnet.

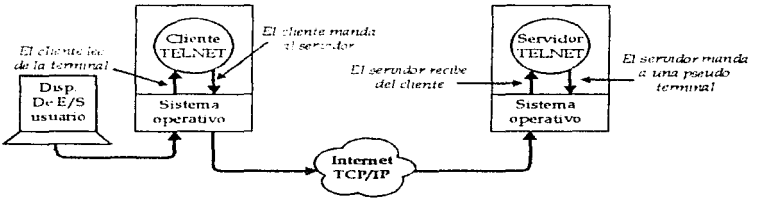


Figura 4.13 Trayectoria de los datos en una sesión de terminal remota con TELNET conforme viaja del teclado del usuario al sistema operativo. La adición de un servidor TELNET a un sistema de tiempo compartido suele requerir la modificación del sistema operativo.

Como se muestra en la figura, cuando un usuario invoca a telnet, un programa de aplicación en la maquina del usuario se convierte en un cliente. El cliente establece una conexión TCP con el servidor por medio de la cual se comunicarán. Una vez establecida la conexión, el cliente acepta los pulsos de teclado del usuario y los manda al servidor, al tiempo que acepta caracteres de manera concurrente que el servidor regresa y despliega en la pantalla del usuario. El servidor debe aceptar una conexión TCP del cliente y después transmitir los datos entre las conexión TCP y el sistema operativo local.

4.2.5.3.3 Adaptarse a la heterogeneidad

Para hacer que telnet interopere entre tantos sistemas como sea posible, debe adaptar los detalles de las computadoras heterogéneas y los sistemas operativos.

Para adaptar la heterogeneidad, telnet define cómo deben mandarse las secuencias de datos y comandos a través de Internet. La definición se conoce **como terminal virtual de red** (NVT: network virtual terminal). Como se ilustra en la figura 23.2, el software cliente traduce las pulsaciones de teclado y las secuencias de comandos que vienen de la terminal del usuario a formato NVT y las envía al servidor. El software del servidor traduce los datos y comandos que acaban de llegar de

formato NVT al formato que el sistema remoto requiere. Para devolver los datos, el servidor remoto traduce del formato de una máquina remota a NVT y el cliente local traduce del formato NVT al formato de la máquina local.

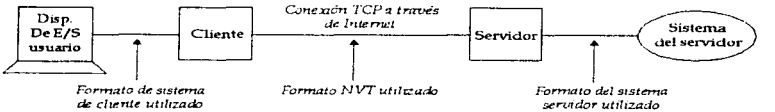


Figura 4.14 Telnet utiliza el formato Terminal Virtual de Red (NVT: Network Virtual Terminal).

4.2.5.3.4 Rlogin (BSD de UNIX)

Los sistemas operativos que se derivan de BSD de UNIX incluyen un servicio de acceso remoto, llamado **rlogin**, que soporta a hosts confiables. Permite que los administradores del sistema elijan un conjunto de máquinas en las que se compartirán nombres de acceso y protecciones de acceso a archivos, y establezcan equivalencias entre los usuarios de los accesos. Los usuarios pueden controlar el acceso a sus cuentas autorizando un acceso remoto basado en un host remoto y un nombre de usuario remoto. De este modo, es posible para el usuario tener un nombre de acceso *X* en una máquina y *Y* en otra, es incluso ser capaz de hacer el acceso remoto de una de las máquinas a la otra sin teclear una clave de acceso en cada ocasión.

4.2.5.4 Transferencia y acceso a archivos: FTP, TFTP, NFS

4.2.5.4.1 Introducción

A continuación se examinaran los protocolos de acceso y transferencia de archivos, describiendo su diseño.

El **Protocolo de Transferencia de Archivo** (FTP: File Transfer Protocol) permite que un archivo de un sistema se copie a otro sistema. No es necesario en algunos casos que el usuario se registre como usuario completo en la máquina a la que desea tener acceso, como en el caso de TELNET. Una vez establecida la conexión con la máquina remota, FTP lo habilita para copiar a su máquina uno o más archivos.

El **Protocolo Trivial de Transferencia de Archivos** (TFTP: Trivial File Transfer Protocol) es un protocolo de transferencia de archivos muy sencillo, sin complicaciones, que carece totalmente de seguridad.

El **Servidor de Archivos en Red** (NFS: Network File Server) es un conjunto de protocolos desarrollado por la empresa Sun Microsystems para habilitar en forma transparente a varias máquinas de acceso a los directorios de las demás máquinas. Esto se lleva a cabo utilizando un esquema de sistemas de archivos distribuidos.

4.2.5.4.2 FTP: el principal protocolo de TCP/IP para la transferencia de archivos

La transferencia de archivos se da entre las aplicaciones TCP/IP utilizadas con mayor frecuencia, y que cuenta con mucho mayor tráfico en red. Existían protocolos de transferencia de archivos estándar para ARPANET antes de que comenzara a funcionar el TCP/IP. Estas versiones tempranas de software de transferencia de archivos evolucionaron hasta llegar al estándar actual, conocido como **Protocolo de transferencia de archivos** (FTP: File Transfer Protocol).

4.2.5.4.2.1 Características del FTP

Dado un protocolo de transporte de extremo a extremo como el TCP, la transferencia de archivos podría parecer trivial. Sin embargo, como se ha señalado, los detalles de autorización, el nombre y la representación entre máquinas heterogéneas hace que el protocolo sea complejo. Además, el FTP ofrece muchas facilidades que van más allá de la función de transferencia misma.

- **Acceso interactivo.** Aunque el FTP está diseñado para usarse mediante programas, la mayor parte de las implantaciones proporciona una interfaz interactiva que permite a las personas interactuar fácilmente con los servidores remotos.
- **Especificación de formato (presentación).** El FTP permite al cliente especificar el tipo y formato de datos almacenados. Por ejemplo, el usuario puede especificar si un archivo es de texto o binarios, así como, si los archivos de texto esta en ASCII o EBCDIC.
- **Control de autenticación.** El FTP requiere que los clientes se autoricen a sí mismos con el envío de un nombre de conexión y una clave.

4.2.5.4.2.2 Modelo de proceso FTP

Como en otros servidores, la mayor parte de las implantaciones de servidores FTP permiten el acceso concurrente de varios clientes. Los clientes se valen del TCP para conectarse a un servidor. Un proceso sencillo de servidor maestro espera las conexiones y crea un proceso esclavo para manejar cada conexión. Sin embargo, a diferencia de casi todos los servidores, el proceso esclavo no ejecuta todos los cómputos necesarios. Por el contrario, el esclavo acepta y maneja la *conexión de control* de cliente, pero utiliza un proceso (o procesos) adicional para manejar una **conexión de transferencia de datos** separada. La conexión de transferencia de

datos, que también usa el TCP como protocolo de transporte, transporta todas las transferencias de datos.

Por lo general, el cliente y el servidor crean un proceso separado para manejar la transferencia de datos. Cabe mencionar, que los detalles precisos acerca de la arquitectura de proceso dependen de los sistemas operativos, en la figura 4-15, se ilustra el concepto:

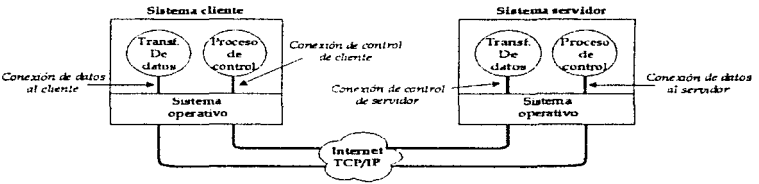


Figura 4.15 Un cliente y un servidor FTP con una conexión de control TCP entre ambos y una conexión TCP separada entre sus procesos de transferencia de datos asociados.

4.2.5.4.2.3 El FTP desde el punto de vista del usuario

Por lo general, FTP se inicia con el nombre o con la dirección de la máquina destino. Igual que para telnet, deberá ser posible convertir el nombre en una dirección IP para que tenga éxito el comando. La máquina destino también se puede especificar desde la línea de comandos de FTP. El proceso que sigue FTP cuando se establece una conexión es el siguiente:

1. *Registro de entrada*: verifica identificación y contraseña del usuario
2. *Define directorio*: identifica el directorio de inicio
3. *Define modo de transferencia de archivo*: define el tipo de transferencia
4. *Inicia transferencia de datos*: habilita los comandos de usuario
5. *Detiene la transferencia de datos*: cierra la conexión

4.2.5.4.2.4 Acceso FTP anónimo

Para habilitar la capacidad de transferencia de archivos, FTP requiere un identificación y contraseña de usuario, pero existe un método más liberal para permitir acceso general a un archivo o directorio, conocido como **FTP anónimo**. Este elimina la necesidad de una cuenta de registro de entrada en la máquina remota, y permite por lo general un registro de entrada anónima mediante una contraseña que puede ser "**invitado**" o el nombre de registro de entrada real de usuario.

4.2.5.4.2.5 TFTP: Protocolo Trivial de Transferencia de Archivos

Aunque el FTP es el protocolo de transferencia de archivos más generalizado en TCP/IP, también es el más complejo y difícil de programar. Muchas aplicaciones no necesitan de la funcionalidad completa que ofrece el FTP.

El conjunto de protocolos TCP/IP contiene un segundo protocolo de transferencia de archivos que proporciona un servicio menos sofisticado. Se conoce como **Protocolo Trivial de Transferencia de Archivos** (TFTP: Trivial File Transfer Protocol) y se diseño para aplicaciones que no necesitan interacciones complejas entre el cliente y servidor. El TFTP restringe las operaciones a transferencia de archivos sencilla y no proporciona autentificación. Como es más restrictivo el software TFTP resulta mucho más pequeño que el FTP.

El tamaño reducido es importante para muchas aplicaciones. Por ejemplo, los fabricantes de dispositivos sin disco pueden codificar al TFTP en la memoria de sólo lectura (ROM) y usarlo para obtener una imagen de memoria inicial cuando se encienda la máquina. La ventaja de utilizar el TFTP es que permite al código de arranque emplear los mismos protocolos TCP subyacentes que el sistema operativo utiliza una vez que empieza la ejecución. De este modo es posible para una computadora arrancar desde un servidor en otra red física.

A diferencia del FTP, el TFTP no necesita un servicio de transporte de flujo confiable. Corre bajo UDP o cualquier otro sistema de entrega de paquetes no confiable utilizando tiempos límite y retransmisión para asegurar que los datos lleguen. El lado que envía transmite un archivo de tamaño fijo (512 octetos) bloquea y espera un acuse de recibo para cada bloque antes de enviar el siguiente. El receptor envía un acuse de recibo para cada bloque cuando le llega.

4.2.5.5 Correo electrónico: SMTP, MIME Y 822

El **correo electrónico** o **e-mail** es el servicio de aplicación más ampliamente utilizado. E-mail es popular porque ofrece un método rápido y conveniente de transferir pequeñas notas o grandes documentos de información.

El protocolo para la entrega de correo difiere de los otros protocolos descritos anteriormente, en los que se enviaban los paquetes directamente a sus destinos, sin embargo, en el caso del correo electrónico, el sistema debe proporcionar los medios cuando la máquina remota o las conexiones de la red han fallado.

Para manejar las entregas con retraso, el sistema de correo utiliza una técnica conocida como encolamiento/almacenamiento (*spooling*). Cuando el usuario envía un mensaje de correo, el sistema coloca una copia en su área de almacenamiento privado (*spool*) junto con la identificación del emisor, recipiente, máquina de destino y hora de depósito. El sistema, entonces, inicia la transferencia hacia la máquina remota como una tarea subordinada o secundaria, permitiendo al emisor que continúe con otras actividades, figura 4.16.

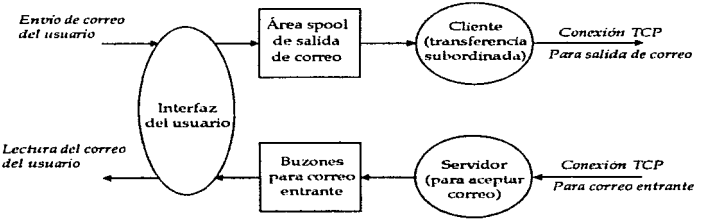


Figura 4.16 Componentes conceptuales de un sistema de correo electrónico. El usuario invoca una interfaz de usuario para depositar o recuperar correo; todas las transferencias se dan en un proceso subordinado.

El e-mail utiliza el sistema de nombre de dominios (DNS) para transformar el nombre de la máquina de destino en una dirección IP y luego trata de establecer una conexión TCP hacia la máquina destino. Si tiene éxito, el proceso de transferencia envía una copia del mensaje a la máquina destino, el cual almacena la copia en el área de proceso spool del sistema remoto, el cliente entonces desecha la copia local. Si no se puede establecer la conexión o si esta falla, el proceso de transferencia registra la hora en que se intentó la entrega y termina el proceso. El proceso de transferencia subordinado realiza de manera periódica un barrido a

través del área spool, en busca de correo no enviado. Si encuentra que el mensaje de correo no se puede entregar después de un tiempo prolongado, el software de correo devuelve el mensaje al emisor.

4.2.5.5.1 Relación entre el enlace de redes y el correo electrónico

Muchos sistemas de computadoras comerciales pueden enviar correo electrónico desde localidades que no están conectadas a Internet. Esto es posible con el uso de **compuertas de correo** (mail gateway), a veces llamadas **mail bridges o mail relay** para transferir mensajes. En cada sistema, la máquina del emisor no establece contacto directamente con la máquina del receptor, sino que envía el correo a través de una o más maquinas intermedias que completan el envío.

La principal desventaja de utilizar compuertas de correo es que reduce la confiabilidad. Una vez que la máquina del emisor transfiere un mensaje a la primera máquina intermedia, se descarta la copia local. Así, mientras el mensaje está en tránsito, ni el receptor ni el emisor tienen una copia. Si se dan fallas en las máquinas intermedias esto puede provocar una pérdida del mensaje sin que se informe ni al emisor ni al receptor. También se puede dar una pérdida de mensajes si las compuertas de correo enrutan el correo de manera incorrecta. El punto importante es que el emisor y el receptor dependen de máquinas sobre las que pueden no tener ningún control.

La mayor ventaja de las compuertas de correo es su interoperabilidad. Las compuertas de correo proporcionan conexiones entre el estándar TCP, el sistema de correo TCP/IP estándar y otros sistemas de correo, así como entre redes de redes TCP/IP, como Internet, y redes que no soportan los protocolos de Internet.

4.2.5.5.2 Estándares TCP/IP para el servicio de correo electrónico

El objetivo de TCP/IP es proporcionar interoperatibilidad a través de un amplio rango de sistemas de computadoras y redes. Para extender la interoperatibilidad del correo electrónico, TCP/IP divide sus estándares de correo en dos grupos. Un estándar especifica el formato para los mensajes de correo, frecuentemente se refieren al formato de mensaje de correo como "822" ya que el RFC 822 contiene el estándar. El otro especifica los detalles del intercambio de correo electrónico entre dos computadoras. Mantener los dos estándares separados para el correo electrónico hace posible construir compuertas de correo que conecten redes de redes TCP/IP con algunos sistemas de entrega de correo de otros vendedores, siempre y cuando utilicen el mismo formato de mensaje para ambos.

El correo electrónico esta dividido en dos partes: un encabezado y un cuerpo de mensaje, separados por una línea en blanco. El estándar TCP/IP para los mensajes de correo especifica el formato exacto de los encabezados de correo así como el

significado de interpretación de cada campo del encabezado; la definición del formato del cuerpo se deja al emisor. En particular, el estándar especifica que los encabezados contienen texto que es posible leer, dividido en líneas que consisten en palabras clave, seguidas por dos puntos y por un valor. Algunas palabras clave son necesarias, otras son opcionales y el resto no tiene interpretación.

El formato de los mensajes de correo ha sido seleccionado para facilitar el proceso y realizar el transporte a través de máquinas heterogéneas, mantener el formato del encabezado de correo sin cambios permite utilizarlo dentro de un amplio rango de sistemas. La restricción de los mensajes al formato de sólo texto evita los problemas de seleccionar una representación binaria estándar y traducir entre la representación estándar y la representación de la máquina local.

4.2.5.5.3 Direcciones de correo electrónico

Dentro de Internet, las direcciones tienen una forma simple y fácil de recordar:

parte_local@nombre_dominio

Donde **nombre_dominio** es el nombre del dominio de un destino de correo en donde el correo debe ser entregado y **nombre_local** es la dirección de un buzón en la máquina. Por ejemplo, dentro de Internet, una dirección de correo electrónico valida es:

ricardo@pumas.iingen.unam.mx

Sin embargo, las compuertas de correo vuelven las direcciones complejas. Cualquiera que éste fuera de Internet debe direccionar el correo hacia la compuerta de correo más cercana o tener el software que lo haga de manera automática.

4.2.5.5.4 Protocolo de transferencia de correo simple (SMTP)

Además del formato de los mensajes, el conjunto de protocolos TCP/IP especifica un estándar para el intercambio de correo entre máquinas. Es decir, el estándar especifica el formato exacto de los mensajes de un cliente en una máquina que lo utiliza para transferir correo hacia el servidor en otra. El protocolo de transferencia estándar se conoce como **Protocolo de transferencia de correo simple** (SMTP: Simple Mail Transfer Protocol). El SMTP es más sencillo que el **Protocolo de transferencia de correo** (MTP: Mail Transfer Protocol) original. El protocolo SMTP se enfoca específicamente en cómo transferir el sistema de entrega de correo subyacente de los mensajes a través de un enlace de una máquina a otra. No especifica de qué manera acepta el sistema de correo los mensajes de correo de un usuario o cómo presenta al usuario la interfaz de usuario del correo entrante. El SMTP tampoco especifica en qué forma se almacena el correo o con qué frecuencia el sistema de correo trata de enviar mensajes.

El SMTP es sorprendentemente sencillo. La comunicación entre un cliente y un servidor consiste en texto ASCII que es posible leer. Aun cuando el SMTP define rígidamente el formato de los comandos, los usuarios pueden leer fácilmente una transcripción de interacciones entre un cliente y un servidor. Inicialmente, el cliente establece una conexión de flujo confiable con el servidor y espera que el servidor envíe un mensaje *220 READY FOR MAIL*. (Si el servidor está sobrecargado, deberá retardar el envío del mensaje 220 temporalmente.)

4.2.5.5.5 La extensión MIME para datos no ASCII

Para permitir la transmisión de datos no ASCII a través de e-mail, la IETF definió la **Extensión del Correo Internet Multipropósito** (MIME: Multipurpose Internet Mail Extension). La MIME no cambia al SMTP ni lo reemplaza, de hecho, la MIME permite que los datos arbitrarios sigan codificándose en ASCII y luego se envíen por medio de mensajes e-mail estándar. Para adaptarse a tipos y representaciones arbitrarias de datos, cada mensaje MIME incluye datos que informan al recipiente del tipo de datos y de la codificación utilizada. La información de MIME reside en el encabezado de correo 822, la línea del encabezado MIME que especifica la versión de MIME utilizada, el tipo de datos que se envían y la codificación empleada para convertir los datos en ASCII.

El estándar define siete tipos de contenidos básicos, los subtipos válidos para cada uno y las codificaciones de transferencia. Además de los tipos estándar y los subtipos, MIME permite a un emisor y a un receptor definir tipos de contenido privado. La siguiente tabla lista los siete tipos de contenidos básicos.

Tipo de contenido	Se utiliza cuando los datos en el mensaje son:
text	Texto (por ejemplo, un documento)
image	Imagenes estáticas o imagenes generadas en computadora
audio	Grabaciones de audio
video	Grabaciones de vídeo que incluyen movimiento
application	Datos para un programa
multipart	Mensajes múltiples de los que cada uno tiene una codificación y un tipo de contenido diferentes
message	Mensajes e-mail completos (por ejemplo, un memorándum que se está enviando) o una referencia externa a un mensaje (por ejemplo, un servidor FTP y un servidor Web)

Tabla 4.4 Tipos de contenidos básicos.

4.2.5.5.5.1 Mensajes MIME multipart

El tipo de contenido multipart de MIME es útil pues añade una flexibilidad considerable. El estándar define cuatro posibles subtipos para un mensaje multipart, cada uno proporciona una funcionalidad importante. El subtipo *mixed* permite que un solo mensaje contenga submensajes independientes, de los que cada uno tiene un tipo independiente y una codificación diferente. Los mensajes multipart mezclados hacen posible incluir textos, gráficos y audio en un solo paquete, o permitir el envío de un memorándum con segmentos de datos adicionales asociados, similares a los enclosures (datos adicionales) incluidos en una carta de negocios. El subtipo *alternative* permite que un solo mensaje incluya varios representaciones de los mismos datos. Algunas alternativas de los mensajes multipart son útiles cuando se envía un memorándum a muchos recipientes de los que no todos utilizan el mismo hardware o software de sistema. Por ejemplo, se puede enviar un documento como texto en ASCII y con formato, permitiendo que los recipientes que tienen computadoras con capacidades gráficas seleccionen la opción con formato. El subtipo *parallel* permite que un solo mensaje incluya subpartes que deben ser vistas juntas (por ejemplo, subpartes de audio y vídeo que deben presentarse de manera simultánea). Por último, el subtipo *digest* permite que un solo mensaje contenga un conjunto de otros mensajes (por ejemplo, la colección de mensajes e-mail de una discusión).

4.2.5.6 Sistemas de Archivos en Red (NFS: Network File System)

Varios métodos para compartir discos en red han sido desarrollados. El **Sistema de Archivos en Red** (NFS: Network File System) de SUN ha emergido como el mas claro estándar de compartición de discos entre sistemas UNIX, y se esta extendiendo hasta en sistemas NO UNIX.

4.2.5.6.1 La tecnología de NFS

NFS fue desarrollado e introducido al mercado por SUN Microsystem Inc., que ha tomado la filosofía de sistemas distribuidos y abierto. Así, desde el inicio, NFS fue diseñado para que permitiera conectar computadoras de diferentes fabricantes con muy diferentes sistemas operativos corriendo sobre estas, este hecho fue probablemente la gran ventaja sobre otros productos como Remote File System de AT&T (RFS) y Andrew File System (AFS).

Las especificaciones de los protocolos de NFS han sido publicadas y una referencia de la implantación para UNIX esta disponible a un bajo costo. Muchos fabricantes de sistemas UNIX han llevado este sistema, o una variante de esta, a sus computadoras y pagan el uso de las licencias a la empresa Sun Microsystems. Así, cuando menos en el mundo del sistema operativo UNIX, NFS ha sido el estándar

de facto para la distribución de archivos y se encuentra disponible para prácticamente cualquier sistema UNIX.

4.2.5.6.2 Los modos de operación y aplicación

NFS es comúnmente proporcionado como una extensión del sistema operativo ofrecido por el fabricante y debe ser adquirido como un extra. La mayoría de las estaciones de trabajo son la excepción a esto, e incluyen los protocolos y los comandos de NFS y TCP/IP como parte de la configuración básica. Los productos de NFS están disponibles para otros sistemas operativos como son: MS-DOS, UNIX, VMS, MVS, etc.

NFS permite el acceso a programas para leer y escribir en archivos que están en el servidor de NFS. Este acceso es transparente para el programa, sin la necesidad de alterarlos, prepararlos o ponerles parámetros especiales, antes de operarlos sobre NFS. Los archivos que están en el servidor de NFS están disponibles a la computadora cliente de NFS, la cual monta los sistemas de archivos (o secciones) desde los sistemas de archivo del servidor de NFS, y hacerlos estos como un sistema de archivos propios.

Un aspecto de la transparencia es la velocidad con la que se accede los datos sobre la red, que debe ser tan alta que no halla diferencia perceptible en el acceso hecho desde un disco local. La meta original de NFS fue tener o lograr el 80% de la velocidad, comparándola con el acceso en un disco local. Así, es posible acceder con NFS sobre un servidor de NFS dedicado, con un disco muy rápido, bajo ciertas circunstancias, tener un mejor rendimiento, que el que se logra en maquinas que tienen discos duros baratos y lentos. Las estaciones de trabajo de alto desempeño, en particular las que operan sin disco duro, pueden usualmente leer o escribir a una velocidad de varios miles de Kilobytes por segundo sobre NFS.

Las implantaciones de NFS sobre sistemas UNIX pueden operar como cliente y servidor al mismo tiempo. Dos computadoras pueden así compartir sus archivos, siempre y cuando el administrador de la red permita la configuración.

NFS es algunas veces llamado como un "Sistema de distribución de archivos", pero una terminología mas correcta seria "Sistema de archivos en red" que es el significado de las iniciales de NFS (Network File System). NFS no distribuye sistemas de archivos en la red, pero convierte los accesos locales en pedidos a uno o mas servidores.

Este concepto no es nuevo, este ha sido usado exitosamente en muchos otros sistemas. Muchas soluciones han sido desarrollados para sistemas UNIX en los últimos 10 años. El sistema de archivos en red también ha sido implementado para otros sistemas operativos en particular para PC's sobre MS-DOS.

4.2.5.6.3 Inicios

NFS fue anunciado en 1984, la primera implantación sobre una estación de trabajo SUN fue introducida al año siguiente. Este producto tenía el numero de versión 2.0 y contenía implementado un cliente y un servidor, junto con el nuevo **Sistema de Archivo Virtual** (VFS: Virtual File System), una estructura para asociar sistemas de archivos en UNIX, el servicio de directorios llamado Yellow Page (YP). El llevarlo al System V mostró que era posible hacer disponible NFS en prácticamente cualquier maquina UNIX. En el mismo año, Sun emitió una nueva versión de NFS, la 3.0, en la que se mejoro el protocolo de YP. Además, Sun liberó la primera implementaron de NFS para PC's bajo MS-DOS (PC-NFS), en el mismo año.

La versión 3.2 fue introducida en 1987, esta ofrecía la posibilidad de manejar archivos en redes amplias. También incorporo el **Remote Execution Service** (REX), un servicio de red que lo habilitaba al usuario para inicializar procesos en otras máquinas (procesos que accedían a archivos locales vía NFS).

La versión 4.0 de NFS, liberada en 1989, que contiene funciones de encriptación, es usado para garantizar que los archivos accedidos no puedan ser robados.

4.2.5.6.4 Producto y Protocolo NFS

Se debe distinguir entre el producto NFS y el protocolo NFS:

- El producto NFS consiste de un rango de protocolos que tienen diferentes funciones. Otras tareas deben realizarse en la red además del acceso de archivos (por ejemplo, la gestión de área). NFS usualmente define un protocolo para cada una de estas tareas.

- El protocolo de NFS es un protocolo dentro del producto de NFS que es usado para acceder archivos y que ha dado su nombre al producto NFS.

4.2.5.6.5 Campos de aplicación de NFS

Al igual que todos los mecanismos, el acceso de archivos en red tiene ventajas y desventajas que determinan la aplicación y el alcance.

NFS permite accesos opcionales a bloques de archivos sobre el disco duro, sin la interpretación de la estructura interna.

Se debe señalar que NFS no es muy bueno como servidor de bases de datos.
Las áreas preferidas de aplicación para NFS son el desarrollo, la automatización de oficinas y diseño, donde los datos accedidos mas comunes son archivos de códigos fuente, bibliotecas de objetos, rótulos, etc.

4.2.5.6.6 Alternativas a NFS

Naturalmente, como un producto, NFS tiene competidores. En particular hay dos productos que son similares usados en redes de área local sobre sistemas UNIX:

4.2.5.6.6.1 RFS

El **Sistema de Archivos Remoto** (RFS: Remote File System) fue liberado por AT&T junto con el System V Release 3 en 1986. Este sistema nunca tuvo el éxito de NFS, algunas de las razones son:

- Funcionalidad desde el punto de vista del usuario: Casi idéntico a NFS. Ambos productos ofrecen una conexión transparente y no son visibles a los usuarios y sus aplicaciones. En RFS también, los sistemas de archivos son montados localmente sobre el servidor. Diferente a NFS, RFS permite el acceso a archivos especiales.
- *Soporta sistemas sin disco*: No provisto para este. Aunque en principio es posible, RFS no incorpora arreglos para proveer una implantación para sistemas sin disco.
- *Manejo:* Conceptualmente, semánticamente y sintácticamente diferentes. El subsistema de RFS es manejado por una computadora designada para este propósito, mientras que las redes con NFS, con excepción de NIS consiste del manejo de computadoras independientes.
- Uso en ambientes no UNIX: A diferencia de NFS, RFS solo se diseño para trabajar bajo sistemas UNIX. La integración con MS-DOS, VMS u otro sistema operativo es prácticamente imposible. De cualquier manera, los sistemas UNIX usados en redes con RFS pueden estar basados en diferentes arquitecturas.
- Preservación de la semántica de los sistemas de archivos en UNIX. Mejor que NFS. El protocolo de RFS no usa las primitivas de acceso a archivos, pero también maneja las llamadas al sistema de UNIX para generar dinámicamente procesos en el servidor. Esto habilita el acceso a archivos especiales.
- Desempeño: Se determina por la configuración. Los protocolos de transporte orientados a conexión son generalmente usados, esto conduce a costos de procesos mas altos. El tamaño de los paquetes usado es generalmente mas pequeño que en NFS.
- Independencia del protocolo de transporte usado: Es alta. Los módulos de RFS usa la **Interfaz de Nivel de Transporte** (TLI: Transport Level Interface) y la Interface Proveedora de Transporte (TPI: Tranport Provider Interface) en System V.
- Seguridad: Mejor que NFS. Como en NFS, los identificadores de usuarios y grupos son usados para autentificar la información. Sin embargo, estos ID's pueden protegerse para evitar que se sobrepongan o desactivarlos usando tablas de conversión en el servidor.

- Protección contra fallas: Peor que NFS. Un reinicio transparente después de que el servidor tiene una caída es imposible.
- Abierto: Los fuentes de código de RFS están disponibles bajo un System V con licencia. De cualquier manera , AT&T nunca a publicado los protocolos.

Por último cabe mencionar que el System V Release 4 permite la conexión entre RFS y NFS y que otro sistema parecido a RFS y NFS es el **Sistema de Archivos Andrew (AFS: Andrew File System).**

4.2.5.6.7 Funcionamiento de NFS

4.2.5.6.7.1 Protocolos de NFS

El producto NFS está formado por varios protocolos, uno solo de los cuales se conoce como protocolo NFS. Los protocolos del producto NFS están diseñados como un conjunto de capas, similar al modelo OSI. En la figura 4.17 se comparan las capas del producto NFS con las capas OSI.

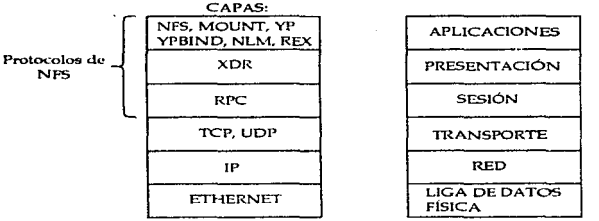


Figura 4.17 Capas del producto NFS

NFS utiliza los protocolos de TCP/IP, el protocolo de IP para la entrega de paquetes en la red, y los protocolos TCP o UDP los utiliza para transportar los paquetes.

NFS esta basado en dos protocolos principales, similares pero distintos: MOUNT y NFS. El servidor de NFS utiliza el protocolo MOUNT para identificar cuales filesystem están disponibles y para que hosts; este utiliza el protocolo NFS para hacer que estos filesystems sean disponibles para los clientes específicos.

Toda la comunicación entre el cliente de NFS y el servidor de NFS se basa sobre el sistema de Sun Microsystems de **Llamadas a Procedimientos Remotos** (RPC:

Remote Procedure Call), con estos programas corriendo sobre una computadora se puede llamar a subrutinas que son ejecutadas en otra computadora. Los RPC usan el **Sistema de Representación de Datos Externos** de Sun Microsystems (XDR:eXternal Data Representation) para permitir el intercambio de información entre clases de computadoras. Por velocidad y simplicidad, Sun construyó NFS sobre el protocolo de Internet UDP (User Datagrama Protocol).

UDP es rápido pero informal: "informal" significa que la red no garantiza que el paquete UDP transmitido siempre sea entregado, o que estos se entregaran en orden. NFS para evitar este problema, requiere que el servidor de NFS reconozca cada RPC mandado con el código de resultado, en el que se indica, si el comando se completo exitosamente o no. Si el cliente de NFS no obtiene reconocimiento dentro de un tiempo determinado, este retransmite el comando original.

De otra manera, si el cliente de NFS no recibe ningún reconocimiento, este vuelve a retransmitir una y otra vez, cada vez duplicando el tiempo. Si el filesystem fue montado con la opción de **soft**, las peticiones eventualmente se harán. Si el filesystem fue montado con la opción de **hard**, el cliente continua enviando peticiones hasta que sea reinicializado u obtenga un reconocimiento.

4.2.5.6.7.2 Llamadas a procedimientos remotos (RPC: Remote Procedure Call)

El protocolo de Llamada de Procedimiento Remoto (RPC) actúa como capa de sesión y como el intercambiador de mensajes para todas las aplicaciones basadas en NFS. RPC está compuesto de un conjunto de procedimientos que se pueden incorporar en aplicaciones de alto nivel, para manejar cualquier acceso requerido a la red. Los procedimientos remotos no son más complicados en su uso que los procedimientos locales.

Un RPC funciona sobre la red entre un cliente y un servidor. En la figura 4.18 aparece el proceso que sigue RPC. Empieza con la activación del procedimiento por el cliente, desde el cual se envía un mensaje de solicitud al servidor. Después de recibir el mensaje y extraer la solicitud, el servidor ejecuta el procedimiento solicitado y ensambla un mensaje de respuesta con los resultados. Al recibir la respuesta, el cliente desensambla el mensaje y continúa con la ejecución normal de la aplicación. Cada uno de los pasos del procedimiento es controlado por rutinas dentro de la biblioteca RPC (que está vinculada con las aplicaciones).

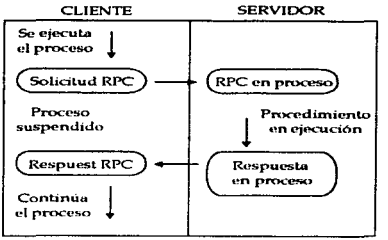


Figura 4.18 Ejecución de una RPC

Los mensajes RPC se pueden enviar mediante TCP o UDP (o incluso, cualquier otro protocolo que proporcione la misma funcionalidad). Típicamente, RPC se utiliza con UDP porque no es necesario un protocolo basado en conexión. Por lo general UDP es más rápido.

La ejecución de un RPC consiste de los siguientes pasos:

(1) Activación por el programa cliente. Los parámetros de petición son empaquetados dentro de un paquete de datos.
(2) Envía la petición y se desempaquetan los parámetros en el programa servidor.
(3) Ejecución de la petición (el procedimiento) en el servidor.
(4) Los resultados son empaquetados y reenviados al cliente.
(5) Los resultados son desempaquetados por el cliente y continua la ejecución normal del programa.

4.2.5.6.7.3 XDR: Representación de Datos Externos

La Representación de Datos Externos (XDR: External Data Representation) es el método por el cual se codifican los datos dentro de un mensaje RCP (y en otros sistemas de protocolos).

XDR se emplea para asegurarse de que los datos de un sistema son compatibles con otros. Se podría pensar que no se requiere una definición formal, pero considere el caso de una máquina basada en EBCDIC comunicándose con una basada en ASCII. XDR habilita a ambos extremos para que conviertan sus representaciones de datos local a un formato común, eliminando cualquier duda sobre el significado de los datos.

4.2.5.6.7.4 Protocolo NFS

El protocolo NFS está compuesto de un conjunto de procedimientos RPC. No es un protocolo en el sentido convencional de definir un complejo proceso de saludo entre dos máquinas. En vez de ello, se trata de un método para comunicar información sobre un procedimiento que se ejecutará. NFS utiliza UDP.

NFS se diseño para ser un protocolo sin estado, lo cual significa que las máquinas que utilizan NFS no tienen que mantener tablas de estado para emplear el protocolo. También se diseño para ser robusto, es decir, que después de una falla (una conexión o una máquina) el sistema se recupera rápida y fácilmente.

4.2.5.6.7.5 Protocolo MOUNT

El producto NFS maneja el procedimiento de montaje de sistemas de archivo como un tema por separado, utilizando el protocolo Mount, el cual emplea UDP.

El protocolo mount se ocupa en devolver un identificador de archivo del servidor al cliente, permitiéndole a éste el acceso a un área del sistema de archivo del servidor. El protocolo no sólo devuelve el identificador de archivo, sino también el nombre del sistema de archivo en el cual reside el archivo solicitado. Mount esta compuesto por un conjunto de procedimientos que facilitan las comunicaciones entre el cliente y el servidor, diseñados especialmente para tratar con archivos.

Una vez que se realiza un montaje, NFS puede continuar operando sin volverse a referir al montaje para nada. Esto le permite a mount continuar modificando sus tablas internas sin afectar las sesiones en marcha; sin embargo, puede causar problemas si un cliente se congela y vuelve a conectarse, debido a que el servidor aún tendrá listadas las conexiones originales en sus tablas internas de montaje.

4.2.5.6.7.6 Servicio de Ejecución Remota (REX)

El **Servicio de Ejecución Remoto** (REX: Remote Execution Service) está diseñado para permitirle a un usuario ejecutar comandos sobre otras máquinas con todas sus variables de ambiente, sin incurrir en sobrecargas de procesos, como telnet, rlogin o rsh. REX utiliza un demonio llamado rexd, que se ejecuta sobre el servidor y emplea los servicios de NFS. REX se usa comúnmente cuando ciertas aplicaciones están instaladas sólo en algunas máquinas, pero deben estar disponibles para todos los usuarios.

REX tiene una ventaja importante sobre otras utilerías UNIX en relación con este tipo de servicio. Permite acceso a los datos de la máquina local mientras se está ejecutando el comando sobre la máquina remota. Lo anterior le da a un usuario la capacidad de ejecutar una aplicación sobre otra máquina, mientras tiene acceso a

los archivos de datos de la máquina local. También permite emplear los recursos de otra máquina sin iniciar un proceso de shell del usuario o sin registrarse en la máquina remota.

4.2.5.7 Protocolos de administración de red

Los protocolos de administración de red son utilizadas para obtener información de los dispositivos conectados a la red y así los administradores de la red puedan detectar, corregir o prevenir los posibles problemas que puedan ocurrir en la red. Actualmente los dos protocolos de administración que se utilizan ampliamente son: el **Protocolo Simple de Administración de Red** (SNMP: Simple Network Management Protocol) y el **Protocolo Genérico de Información de Administración**[41] (CMIP: Common Management Information Protocol). CMIP, es mas general y mas antiguo que SNMP y es parte de los estándares OSI y a sido adoptado por ISO, la ITU (antes CCITT) y otros. La comunidad Internet desarrollo SNMP como parte del conjunto de protocolos TCP/IP. Uno de los objetivos de estos estándares abiertos, SNMP y CMIP es el de conseguir la interoperatibilidad de las herramientas y productos de administración de la red.

Los dos protocolos se basan en los mismos conceptos fundamentales de almacenamiento de datos, en los que la información de administración se recoge y almacena para utilización posterior por una aplicación de administración.

4.2.5.7.1 Administración en Internet: SNMP

El SNMP es un protocolo básico de administración de red, el cuál es el protocolo de entorno de administración más ampliamente implantado actualmente. Trabaja sobre el Protocolo de Datagramas de usuario (UDP), que forma parte del conjunto de protocolos TCP/IP como se muestra en la figura 4.19. Casi todos los vendedores de software y hardware de administración lo soportan, lo que justifica su popularidad, aun que, no es tan robusto como el CMIP de la ITU-T/OSI.

En 1987 se introdujo el Protocolo básico de supervisión de enrutadores[42] (SGMP: Simple Gateway Monitoring Protocol) como producto interno para la administración de redes TCP/IP. Este no solo incluía el protocolo de comunicación entre entidades de administración de red (protocolos de administración de la red), si no que además, definía que variables se iban a utilizar.

---

[41] Para mayor información referirse a: Uyless Black; OSI A model for computer communications standars; Prentice Hall; pp 489-491.

[42] Recordar que en TCP/IP a un enrutador se le conoce como gateway

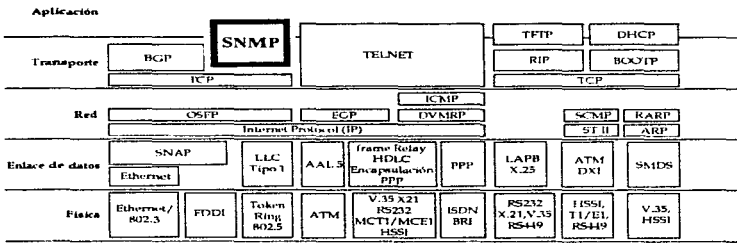


Figura 4.19 Nivel de operación del protocolo SNMP con respecto al modelo TCP/IP

De 1988 a 1990, muchos vendedores implantaron el sucesor del SNMP, el Protocolo Básico de Administración de Red (SNMP). En el documento RFC[43] 1157 se define el protocolo para que los administrados (clientes) se comuniquen con agentes (servidores). En el protocolo no se define ni cómo ni qué información de administración de red guardan, obtienen o manejan los agentes. tampoco se define como se recoge, distribuye y presenta a los gestores la información de administración. En le RFC 1158, la **Base de Información de Administración** (MIB II: Management Information Base) define un conjunto de base de variables que representan un recurso o dispositivo administrado.

En 1989, la discusiones sobre administración de red en ISO recibieron una amplia atención por parte de la comunidad Internet. Un comité de trabajo intentó definir una arquitectura que permitiera la utilización de los **Servicios y Protocolos Genéricos de la información de Administración** sobre TCP/IP (CMOT: Common Management Information Services and protocols). La premisa que se tuvo en cuenta era que el paso a OSI sería más sencilla en el futuro si se utilizaba una administración de red al estilo OSI. CMOT utiliza la misma MIB II para definir los objetos administrados. Aunque CMOT recibió mucha atención al principio, se ha utilizado ampliamente hoy en día.

La administración de red SNMP se implementa mediante el modelo cliente/servidor. Los servidores están definidos como entidades que poseen el recurso. Los clientes son elementos que necesitan servicios del recurso. En el

[43] Las Peticiones de comentarios (RFC: Request for Comments) son documentos que contienen ideas, especificaciones, notas u otras informaciones sobre normas de Internet propuestas o en funcionamiento.

contexto SNMP, los servidores se llaman agentes, por que poseen la base de información de administración (MIB) Los clientes se llaman gestores, por que solicitan servicios del agente para supervisar y controlar la red. El agente se comunica directamente con el sistema operativo o los niveles de trabajo en la red para obtener y manejar la información de administración de la red. Como esta comunicación con el sistema operativo y los niveles de la red dependen mucho de la implantación, no existe una norma para ella. Del otro lado, el agente expone la información a los clientes en forma de objetos MIB II por medio del protocolo SNMP.

En cada entidad de red que deba administrarse o supervisarse debe ejecutarse un agente (servidor). Lo habitual es tener agentes de SNMP ejecutándose en enrutadores, además de los servidores importantes, como los servidores de archivos y de correo. De esta manera se permite la supervisión de las conexiones de red con los servidores, también pueden existir agentes SNMP dedicados que supervisen hardware o aplicaciones especificas.

El administrador o la estación de administración (cliente) es el software de aplicación que se ejecuta en el centro de operaciones de la red. Se comunica con los agentes SNMP para recoger o distribuir la información de administración de la red en forma de variables MIB.

El SNMP modela toda las funciones del agente como modificaciones o inspecciones de variables. Las variables pueden recuperarse o modificarse. La supervisión del estado de la red se consigue principalmente mediante consultas. Se comprueba la información de los sistemas de forma ordenada y periódica.

SNMP es un protocolo de solicitud/respuesta que refleja un sencillo paradigma de búsqueda/almacenamiento. Un administrador está restringido a las operaciones de recuperación (get) y modificación (set) sobre los datos de la MIB del agente. Las operaciones más complicadas sobre un sistema agente se consigue mediante el manejo adecuado de la operación de recuperación (set)

Existen tres criterios por los que se diseño SNMP de esta forma:

- Minimizar el número y complejidad de las funciones de administración que lleva a cabo el agente de administración. Esto supone unos menores costos de desarrollo y una implantación más sencilla de los agentes SNMP para los desarrolladores de herramientas de administración de red.
- Funcionalidad fácilmente expandible de la supervisión y control para incorporar aspectos adicionales, no previstos de las operaciones y administración de la red.
- Arquitectura independiente de los hosts o enrutadores (gateway) conectados.

4.2.5.7.1.1 Base de Información de Administración II (MIB II)

SNMP no especifica qué datos, objetos o variables se utilizan en la administración de la red, o cómo se representa la información de administración de la red. En su lugar, SNMP utiliza la MIB II de Internet como definición de dicha información. La MIB II está definida aparte de SNMP, lo que permite que otros protocolos (por ejemplo, CMOT) utilicen la misma MIB II para proporcionar la administración de la red.

La separación entre la definición de la información de administración de la red (objetos administrados) y los protocolos utilizados para supervisar o administrar dicha información presenta las siguientes ventajas:

- Se pueden añadir objetos nuevos sin cambiar el protocolo que los administre.
- Múltiples protocolos pueden administrar los mismo objetos.

4.2.5.7.1.2 Protocolos Simple de Administración de Red II (SNMP II)

Una mejora del SNMP es el SNMP II (Simple Network Management Protocol II). Este no ha sido adoptado tan ampliamente, debido principalmente a la falta de un trayecto de migración para los productos SNMP existentes. Estos son algunos de los aspectos notables de SNMP II:

- Mejoras en la seguridad.
- Capacidad de transferencia masiva de datos.
- Interacción de un administrador con otro administrador.
- Soporte de protocolo expandido (es decir, transporte)
- Definición mejorada de los objetos administrados.
- Manejo de los errores mejorado.
- informes de excepciones configurables (es decir, discriminadores).
- Utilización de menos memoria.

Para la comunicación entre SNMP y SNMP II se utiliza un gateway proxy, porque SNMP II no es compatible con SNMP.

4.3 Protocolos OSI del nivel de aplicación

4.3.1 Sistema de manejo de mensajes (X.400/MOTIS)

4.3.1.1 Introducción

En el pasado, una variedad de sistemas propietarios de correo electrónico fueron desarrollados para sus computadoras y sistemas. La incompatibilidad entre estos sistemas, limita la habilidad para transferir correo entre los usuarios de los distintos sistemas. Las recomendaciones CCITT **X.400** para el **Sistema de Manejo de Mensajes** (MHS: Message Handling Systems) (ISO 10021) proporciona estándares para interconectar sistemas de correo electrónico a fin de facilitar un servicio global y vencer las limitaciones técnicas de los sistemas existentes.

4.3.1.2 Estándares

El Comité Consultivo Internacional para telegrafía y telefonía (CCITT), definió la norma **MHS X.400** como un sistema electrónico para el intercambio de mensajes entre sistemas de almacén y reenvío de correo que se ejecuta en una amplia variedad de plataformas. En la terminología del Modelo de Referencia OSI, X.400 se llama **Sistema de Intercambio de Texto Orientado a la Mensajería** (MOTIS: Message Oriented Text Interchange System). El objetivo del estándar es proporcionar compatibilidad entre productos de diversos vendedores e interfaces además de servicios de mensajería pública y privada.

4.3.1.3 Conceptos básicos

Los estándares X.400 están definidos en términos de un número de componentes fundamentales, mostrados en la figura 4.20, que pueden ser combinadas en varias configuraciones físicas para realizar el servicio de MHS. El MHS consiste de un **Sistema de Transferencia de Mensajes** (MTS: Messages Transfer System) y un (potencialmente grandes) número de **Agentes de Usuario** (UA: User Agents).

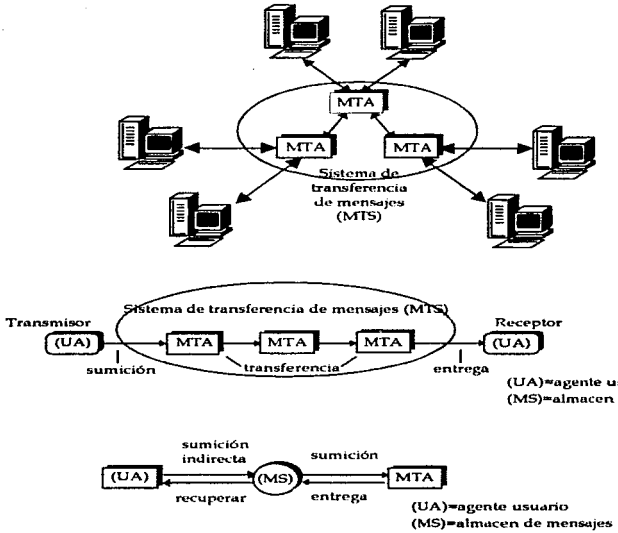


Figura 4.20 Modelo funcional del MHS

UA: El UA es el software que corre en la computadora de cada usuario conectado al sistema X.400. Proporciona las funciones para: creación y lectura de mensajes o visualización de una lista. Cada UA se comunica con otros a través del sistema y cada UA tiene un nombre único[44]. MHS agrupa los UA en clases basándose en los tipos de mensajes que se pueden procesar. Estos UA se denominan UA cooperadores. Hay un UA por cada usuario.

IPM: Diferentes tipos de UAs pueden ser soportados. El UA definido inicialmente por los estándares es para el **Mensaje Interpersonal** (IPM: Interpersonal

[44] Los usuarios pueden utilizar el servicio X.500.

Messaging), como puede ser el correo electrónico. Un estándar adicional fue creado específicamente para el **Intercambio de Datos Electrónicos** (EDI: Electronic Data Interchange) en 1990.

El transmisor y el receptor: El mensaje es creado por el **transmisor**, y es enviado al MTS por medio del UA. El MTS provee el servicio de transferencia como una aplicación independiente para almacenar y reenviar mensajes. El MTS determina si la entrega del mensaje es posible y de esta forma **entrega** el mensaje al receptor por medio de los recipientes del UA.

MTA: Un MTA acepta mensajes de las UAs y los encaminan a otros MTAs. Cada UA esta conectado a solo un MTA. El MTA debe traducir la información de dirección del mensaje y determinar cómo se enruta el mensaje, para hacer esto el MTA contiene un agente del sistema de servicios de directorio X.500. Se necesita la traducción de la dirección, debido a los diferentes tipos de redes posibles dentro de una institución. Los MTA empaquetan el mensaje y lo enrutan con la dirección que han traducido. Entonces, envía el mensaje a la MTA del receptor. El conjunto de varios MTA se denomina **Sistema de Transferencia de Mensajes** (MTS).

Direcciones O/R: El principal centro de las operaciones del MHS y el enrutamiento de mensajes por los MTAs son las direcciones jerárquicas para los usuarios. X.400 define un nombramiento global y un esquema de direcciones por medio del cual cada usuario es identificado sin ambigüedad por **una Dirección Transmisor/Receptor** (O/R Address: Originator/Recipient Address). Conceptualmente es similar a una dirección postal tradicional.

Almacén del mensaje: Para operar como se menciono anteriormente, ambos, los MTAs y los UAs debe ser un sistema altamente confiables y disponible. Esto lo hace difícil para computadoras personales, las cuales son deseables como interfaz del usuario en el MHS, y que actúen como los UAs. Esto es por que las computadoras personales pueden ser apagadas o emplearse para otras actividades por largos periodos, entonces los MTAs no pueden entregar los mensajes a las computadoras personales que se usan como UAs. Para superar este problema, en la versión de 1988, se introdujo el concepto **Almacén de Mensajes** (MS: Message Store). El MS complementa la implantación de un UA, por ejemplo, una computadora personal dando mas seguridad, un mecanismo de almacenamiento disponible continuo para hacer las entregas de los mensajes a nombre de los UAs. El MS reemplaza el almacenamiento de menajes en los UAs. Los usuarios pueden obtener una cuenta, listas de los mensajes, buscar y borrar los mensajes contenidos en el MS.

Otros tipos de servicios de mensajes pueden participar en el MHS por medio de las **Unidades de Acceso** (AU: Access Units). Los estándares proporcionan los elementos necesarios para poder conectarse con otros servicios Telemáticos como

es el Telex y el Teletex. Un **Acceso de Entrega Física** (PDAU: Physical Delivery Access Unit) convierte un mensaje MHS a una forma física (copia dura) para poder entregar el mensaje con la dirección postal.

En resumen, el sistema completo se conoce como el **Ambiente de Manejo de Mensaje**.

4.3.1.2 Los principales componentes del MHS son el UA, MS y el MTA, y sus servicios principales son:

Servicios en la transferencia de mensajes (MTA)	
• Entrega a multidestinos	• Distribución a listas
• Reporte de entregas y no entregas	• Uso de directorio de nombres
• Control de acceso	• Redireccionamiento
• Poner sellos e información de la ruta	• Autentificación del origen
• Conversaciones satisfactorias	• Control de acceso seguro
• Control de un receptor alternativo	• Confiabilidad de los datos
• Posponer la entrega	• Puesta de sellos seguros para mensajes
• Mantener para la entrega	• Integridad de mensajes
• Mensajes de Prueba	• No rechazo
• Comprobación de entrega	

Mensajes interpersonales (UA)	
• Multi-parte, escritura en el cuerpo del mensaje	• Fecha de expiración
• Primaria, copia y recipientes de copia oculta	• Autentificación del usuario
• Notificación de los recibidos y no recibidos	• Sensibilidad
• Auto-reenvío y reenvío de mensajes	• Importancia
• Indicación del asunto del mensajes	• Copias parciales
• Referencia cruzada; En replica a la indicación	• Identificación del lenguaje

Almacén de mensajes (MS)	
• Borrado de mensajes	• sumario de mensajes
• Búsqueda de mensajes	• Alertas
• Listado de mensajes	• Auto - reenvío

Tabla 4.5 Principales componentes del MHS

4.3.1.3 Estructura del mensaje

Un mensaje dentro del MHS tiene definido una estructura que consiste de una **envoltura** y un **contenido** (muy similar a una carta de papel), figura 4.21. El contenido consiste de un encabezado y un cuerpo. El cuerpo puede tener múltiples partes de diferentes tipos de datos, por ejemplo, texto, imágenes, datos binarios. El encabezado contiene varios campos como, Para quien (To), De quien (From),

Copia para (cc), Criterios de confirmación y Asunto (Subject). Este es codificado por el UA y es entregado al MTA en un sobre. Para intercambiarlo dentro del MTS, el MTA entonces crea y codifica un sobre para transferirlo a otros MTAs para distribuirlo. El sobre es solo responsabilidad de los MTAs.

4.3.1.3.1 Manejo el mensaje

La razón por la presencia de un sobre separado y un encabezado, es que los MTAs necesitan modificar el sobre (post-marcandolo) con un avance de mensaje a través de los MTS. Los MTAs también adicionan información de la ruta que ha seguido el sobre hasta este MTA, esto, actúa como un sello de tiempo (timing stamp) el cual es usado para detectar fallas de enrutamiento de mensaje, por ejemplo, que el mensaje se quede en un ciclo. En conclusión, separar el sobre permite a los MTAs modificar la información de entrega sin necesidad de tocar el cuerpo del mensaje.

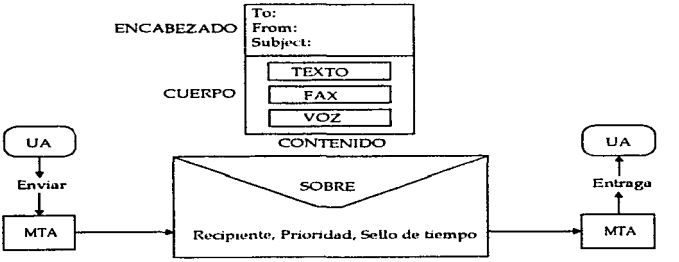


Figura 4.21 Estructura del mensaje MHS

4.3.1.3.2 Sobre

El sobre contiene un número de campos necesarios para localizar y entregar el mensaje a el o los recipiente(s). Cada sobre contiene un único identificador que es generado por el MTA original (MTS Identificador), y el nombre del remitente. Esto permite la entregar un reporte del mensaje.

4.3.1.3.3 Mensaje IPM

El mensaje de usuario IPM consiste de un encabezado y un cuerpo. El encabezado consiste de varios campos que especifican el remitente, el recipiente primario, la copia del recipiente. Otros campos del encabezado son: el asunto (subject), la fecha, la importancia del mensaje.

4.3.1.3.4 Uso del ASN.1

Los mensajes y protocolos del MHS son definidos usando el ASN.1, y codificados por medio del BER.

4.3.1.3.5 Protocolos del X.400

Los componentes y configuraciones funcionales definidos previamente proveen el modelo para diseñar los protocolos del MHS. Los protocolos MHS son conocidos como P1, P2, P3 y P7. La relación de estos protocolos con la Capa de Aplicación del Modelo OSI se muestra a continuación.

- **P1** El protocolo P1 es usado entre los MTAs para transferir los mensajes.
- **P2** Los procedimientos de P2 son usados entre los IPM UAs a través del MTS. En 1988 la versión de P2 se conoció como P22. Para el EDI ampliado, PEDI es usado entre los UAs.
- **P3** El protocolo P3 es usado entre un MTA y un UA, y entre un MTA y un MS.
- **P7** El protocolo P7 se usa entre un UA y su MS asociados.

4.3.1.4 Direccionamiento del MHS

4.3.1.4.1 Dominios del MTA

4.3.1.4.1.1 ADMD

En el esquema total de un MHS internacional, los MTAs son interconectados y organizados en dominios. Una colección de al menos un MTA, cero o mas UAs, cero o mas MSs, y cero o mas AUs manejados por una organización, constituyen un **Dominio de Control** (MD: Management Domain). Estos dominios existen en el nivel mas alto como un **Dominio de Control Administrativo** (ADMD: Administrative Management Domain). Debajo de este, los dominios existen en el nivel privado y son referidos como **Dominios de Control Privados** (PRMD: Private Management Domains). Los ADMD generalmente existen como "carriers" (un proveedor de portación o acarreador, por ejemplo: TELMEX o Avantel) o un servicio nacional que provee un servicio de mensajería para el público, teniendo

un papel muy importante en el MHS global para hacer conexiones internacionales, y así construyendo un backbone internacional.

4.3.1.4.1.2 PRMD

Los PRMD existen en el nivel corporativo. Los PRMD acceden el backbone internacional por medio de los ADMD. También pueden conectarse a otros backbones privados e internacionales PRMD independientemente de los ADMD.

El nombre del dominio[45] de control forma el nivel mas alto de la estructura jerárquica de direcciones O/R. Así, un usuario del MHS es direccionado usando la estructura de direcciones jerárquica de País-ADMD-PRMD-Nombre de la Organización-Nombre de la persona. Esta dirección debe ser única globalmente.

4.3.1.4.2 Direcciones I/O

Las direcciones I/O jerárquicas, son mostradas a continuación, es la base por medio del cual el sistema MHS opera. Cada usuario se le asigna una Dirección I/O sin ambigüedad que refleje la división de dominios en un país o dominio administrativo. Una Dirección I/O tiene los siguientes campos:

Nombre del País	De 1 a 2 caracteres del código ISO 3166 o un Código del País X.121 (3 dígitos).
Nombre del ADMD	Un nombre distintivo para un dominio administrativo seleccionado por el "carrier"
Nombre del PRMD	Un nombre distintivo para un dominio privado acordado entre el "carrier" y el PRMD.
Nombre de la Organización	El nombre de la compañía del usuario organización.
Nombre de la unidad Organización	Posibles nombres múltiples como son para de la departamentos, divisiones, y secciones - se requieren para identificar sin ambigüedad al usuario.
Nombre Personal	Apellido, iniciales, nombre, etc.
Atributos definidos por el dominio	Otro campo de nombre es necesario para un dominio en particular puede ser necesario para interconetarse con otro sistemas no X.400.

[45] Un domino es lógico no físico.

4.3.1.4.3 Uso del Directorio

En la versión de 1984 los estándares solamente operaban con las Direcciones I/O. Con la llegada del Directorio X.500, los estándares X.400 de 1988 ya tenían la opción de usar un directorio de nombres. Este directorio tiene un formato menos restringido (se omiten el ADMD y el PRMD) y su uso es mas amigable. Si un directorio de nombres es usado para especificar un receptor de un mensaje, el MTA busca en el Directorio la Dirección I/O correspondiente al usuario. El formato del nombre usado en X.400 1988 es un Nombre O/R que contiene un nombre de directorio o una Dirección I/O, incluso ambos.

4.3.1.5 Sistemas y estándares del X.400/MOTIS

Como se mencionó anteriormente, X.400, es la recomendación del CCITT, que define un sistema de intercambio de mensajes entre sistemas de almacenamiento y reenvío de mensajes. En términos de ISO, X.400 se conoce como MOTIS. Este sistema se basa en el modelo cliente-servidor.

X.400 es el nombre genérico para todo el conjunto de estándares. A continuación se explican brevemente todos ellos:

X.400 describe el modelo básico MHS de acuerdo con el Modelo OSI. X.400 describe en términos muy generales la forma en que un remitente interactúa con el sistema de agente de usuario (UA) para preparar, editar y recibir mensajes. También describe cómo interactúa el agente de usuario con la red de transferencia de mensajes (MT).

X.402 describe la arquitectura global de MHS y contiene ejemplos de posibles configuraciones físicas. Esta especificación contiene varias definiciones muy útiles, reglas de nombramientos y el direccionamiento.

X.403 proporciona directrices sobre la realización de pruebas de conformidad. Es un documento muy extenso y detallado que define los requisitos de conformidad, la metodología de pruebas, las estructuras de prueba, los temporizadores, las unidades de datos de protocolo, etc.

X.407 especifica convenciones que se utilizan en las tareas de procesamiento de información distribuida. Describiendo esas tareas de una forma abstracta.

X.408 proporciona recomendaciones para realizar conversiones de código y de forma, por ejemplo, la conversión entre el código ASCII y el juego de caracteres telefónicos S.61.

X.411 describe el servicio del nivel de transformación de mensajes (MTL). En esta recomendación se describe la forma en que el usuario de MTS transfiere mensajes con MTS mediante las definiciones de servicio y la sintaxis abstracta.

X.413 contiene las provisiones para el almacenamiento de mensajes (MS). Describe la forma en que MS actúa como intermediario entre el UA y el MTS.

X.419 Define los procedimientos para el acceso al MTS, al MS, y para el intercambio de mensajes entre MTA. Describe los contextos de aplicación con tres protocolos MHS, conocidos como P1, P2 y P3.

X.420 describe el servicio de **Mensajería Interpersonal** (IPM). Este servicio define la sintaxis y la semántica involucrada en la recepción y envío de tráfico interpersonal. Además, recomienda las operaciones para la transferencia de unidades de datos de protocolo a través del sistema.

X.435 mensajes EDI.

Un implantación real de los protocolos de X.400/MOTIS es el Servicio **de Manejo de Mensajeria** de Novell, **MHS** (Message Handling Service), el cual permite realizar las tareas de manejo de mensajes sobre redes de área local y extensa. MHS dispone de correo electrónico, sistemas de planificación para grupos de trabajo, intercambio electrónico de datos (EDI) y fax en red. MHS no es un sistema de correo en sentido estricto, realiza la manipulación del flujo de mensajes entre aplicaciones, de modo que es posible desarrollar aplicaciones que dialoguen unas con las otras mediante el intercambio de información, por ejemplo se puede hacer consultas a bases de datos a través de MHS. NetWare Global MHS es la última versión del sistema de manejo de mensajes, combinado con otros módulos opcionales de protocolos, permite la interoperatibilidad entre SMTP para redes TCP/IP, SNADS para AS/400 de IBM y redes de correo X.400 del CCITT e ISO.

4.3.2 Directorios X.500

4.3.2.1 Descripción de Directorio

4.3.2.1.1 Servicios del Directorio

4.3.2.1.1.1 Propósito

Los comités de estándares reconocieron que un servicio de directorio electrónico tenia que ser centralizado para tener éxito en cualquier sistema de comunicación global moderno, y la serie de **estándares X.500** son el resultado del trabajo de estos

comités. El objetivo es el de proveer una base de datos global lógica para servicio de directorio tanto publico como privado. La principal razón de establecer el servicio de directorios es el crecimiento del **Sistema de Manejo de Mensajes X.400** (MHS), pero los directorios apoyan o soportan una gran variedad de otras aplicaciones OSI y no OSI.

El Directorio es una colección de sistemas abiertos distribuidos que colaboran para tener acceso a una base de datos lógica de información sobre un conjunto de objetos reales. Los usuarios del Directorio, incluyendo tanto a personas como programas de computadoras, pueden leer o modificar la información, o parte de esta, siempre y cuando se tengan los permisos para hacerlo. El acceso al Directorio es de manera interactiva al soportando búsquedas hechas por personas y/o búsquedas automáticas hechas por las aplicaciones.

4.3.2.1.1.2 El nombramiento fácil para el usuario

En OSI, se utilizan los nombres lógicos se usan, por tanto el Directorio desempeña un número de funciones que resuelven los nombres lógicos a direcciones físicas de OSI. Un nombre lógico se diseña de manera que sea fácil de recibir y recordar por las personas, además de ser independiente de su ubicación; por ejemplo, con MHS, el nombre lógico de un receptor puede ser: el país, el nombre de la organización y nombre de la persona - pero aún se necesita convertir a una dirección de presentación que contenga una cadena de dígitos que es dependiente del tipo de red que se use. El Directorio es usado por la aplicación MHS para resolver este nombre cuando se envía el mensaje al receptor. También, cualquier otra aplicación de distribución de OSI requiere del uso de un directorio para la resolución de nombres.

Es común para la gente y otros objetos el ser conocido por varios nombres. Así el directorio debe de poder soportar alias, apodos o nombres alternos. El Directorio puede también manejar listas de distribución, es decir listas de los nombres de gentes u objetos que pertenezcan a grupos específicos.

4.3.2.1.1.3 Seguridad

Además de los servicios de seguridad que controlan el acceso a la información del Directorio mismo, el Directorio puede ser usado para soportar o dar apoyo a funciones de seguridad para otras aplicaciones. El Directorio puede retener o manejar una contraseña (password) para un usuario específico o llaves públicas certificadas para sistemas de encriptamiento, manteniendo los sistemas adecuadamente protegidos para no ser alterados. Estando en un directorio, la información tiene un punto de administración así la información indicada como segura puede ser accedida solo por los objetos (personas o programas) que tienen los permisos correspondientes.

4.3.2.1.1.4 Otras aplicaciones no especificadas por OSI

El Directorio no esta limitado a las redes de datos, este esta generalizado a fin de dar apoyo a una variedad de servicios de telecomunicaciones y tanto los servicios de las páginas blancas como las guías de teléfonos amarillas están esperando a ser una implantación comercial del Directorio.

4.3.2.1.2 Los estándares

Los estándares del Directorio son las recomendaciones del **X.500** al **X.521** del CCITT, que fueron publicadas en 1988. Los equivalentes ISO son el ISO 9594 parte 1 a la 8 que alcanzaron la condición de Estándares Internacionales (IS: International Standard) en 1991. Los estándares iniciales proveían un servicio básico, cabe mencionar que se están haciendo un gran número de extensiones.

4.3.2.1.3 Organización del Directorio

Un directorio global requiere de la cooperación de un número grande de administradores de redes y proveedores de servicios, cada uno de los cuales administra un rango de nombres y direcciones, a demás de que mantiene su propia base de datos separada. Para facilitar la operación uniforme de un directorio global, los estándares proveen los mecanismo para el intercambio de las bases de datos y los procedimientos para que sean accedidos por las aplicaciones de los usuarios o los usuarios mismos.

4.3.2.1.3.1 La organización funcional

Los estándares de X.500 identifican como los dos más importantes componentes funcionales para el Directorio, estos son el **Agente del Usuario del Directorio** (DUA: Directory User Agent) y el **Agente del Sistema del Directorio** (DSA: Directory System Agent). El DUA representa un usuario en el Directorio y provee el acceso a los DSAs que procesan las peticiones actuales o reales del Directorio. La información del Directorio puede estar distribuida en un conjunto de servidores DSAs que actúan en cooperación y proveen un servicio integrado llamado **Directorio distribuido**. Un DSA puede operar también como una base de datos única, en este caso se le conoce como una **Directorio centralizado**. Los estándares X.500 definen el DSA, sus puertos abstractos (interfaces), servicios, y los protocolos usados para acceder el DSA. El DUA es un componente abstracto que representa al que accesa al DSA(s) y servicios del directorio. Los estándares no definen las funcionalidades de una DUA, la cual se personaliza de acuerdo a las necesidades del usuario.

4.3.2.1.3.2 Dominios

El Directorio se organiza en un número de dominios administrativos interrelacionados, similar al concepto de dominio en X.400. Donde un dominio esta formado por uno o mas sistemas de bases de datos distribuidos bajo el control común de una organización pública o privada, y cada sistema tiene un fragmento de la base de datos global.

4.3.2.1.3.3 Propiedad

En la práctica, un carrier puede poseer el Directorio nacional (para permitir que sea un punto único para el acceso internacional para el servicio nacional), pero las compañías privadas pueden poseer y administrar su propio Directorio corporativo. En principio, los Directorios privados pueden estar vinculados como subordinados al Directorio nacional en una estructura jerárquica. Los controles de acceso permiten, el acceso a los usuarios al Directorio corporativo directamente o por medio del directorio jerárquico. El servicio dado a los usuarios es independiente de que si la petición para tener acceso a la información fue por acceso directo al Directorio o el acceso inició desde un sistema de Directorio superior o subordinado.

4.3.2.1.3.4 Repetición

Conceptualmente, la configuración más simple para la información del Directorio esta por cada DSA para tener un fragmento separado del Directorio global. Sin embargo, porque los usuarios que acceden están generalmente dispersos, y alguna forma de respaldo redundante se requiere comúnmente por la información, parte de la información del Directorio puede estar duplicada y estar interconectada, es así que algunos DSAs retienen copias de información que pertenecen a otros, esto se conoce como Directorios **shadowed** o **duplicados**. La duplicación puede optimizar el Directorio para localizar mas cerca de los usuarios copias de la información que es más frecuentemente accedida por ellos.

4.3.2.1.3.5 Necesidad de las autoridades

La información del Directorio por sí misma esta organizada en una estructura jerárquica, como se muestra en la figura 4.22. Las autoridades nombradas son responsables de asegurarse que los nombres destino estén localizados correctamente en cada nivel dentro de la jerarquía. Tal estructura se requiere para facilitar la administración total de Directorio y para la localización de nombres no ambiguos. A fin de participar en la red abierta global creciente, es esencial que cada persona y objeto direccionable en cualquier compañía u organización sea asignado o localizado con un nombre no ambiguo. Todas las organizaciones

deberían registrar sus nombres con las autoridades apropiadas de nombramiento de cada país (la autoridad de registro es comúnmente el miembro nacional ISO).

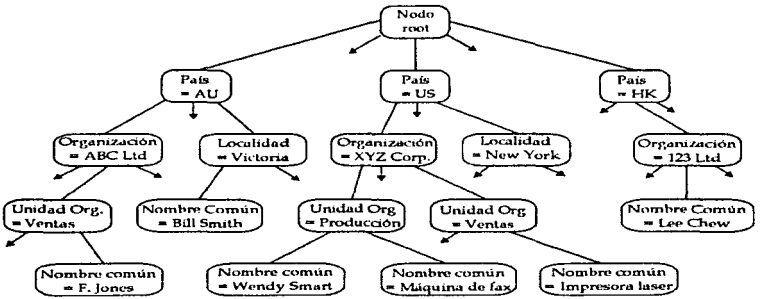


Figura 4.22 Estructura de nombres jerárquico X.500

4.3.2.2 Estructura del directorio

Los registros de información contenidos en el Directorio se refieren como la **Información Base del Directorio** (DIB: Directory Information Base) y están estructurados para formar un árbol invertido, referido como el **Árbol de Información del Directorio** (DIT: Directory Information Tree), figura 4.23. Los estándares del Directorio no están destinados para ser un modelo de una base de datos distribuida generalizada. En particular, el diseño del Directorio tiene tres suposiciones simplificadas que reflejan la naturaleza de las aplicaciones de telecomunicaciones que lo usará:

- Las consultas (es decir, leer desde el Directorio) serán mucho más frecuentes que las actualizaciones (escribir al Directorio).
- Las condiciones transitorias, en las que partes del DIB no son completamente consistentes, son tolerables (aunque en cortos periodos).
- Una arquitectura jerárquica es usada por el DIT.

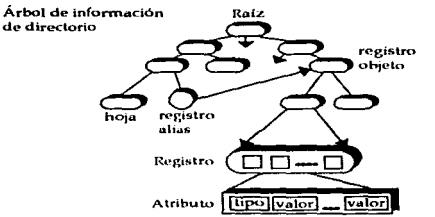


Figura 4.23 Estructura del árbol de información del Directorio X.500 (DIT) y sus registros.

4.3.2.2.1 Información Base del Directorio

4.3.2.2.1.1 Objeto

El directorio es construido con información acerca de **objetos**. El término **objeto** se usa para referirse al ejemplo real de algo, por ejemplo una persona, una computadora, un periférico, etc. Cada objeto pertenece a una **clase de objeto**, donde un identificador familiar comparte características comunes (por ejemplo la organización de la persona, la dirección de la persona, etc.).

4.3.2.2.1.2 Registro

El DIB esta compuesto de (Directorios) **registros**, que consisten de una colección de información de un objeto. El termino **registro** (entry) es usado para referirse a la información contenida en el Directorio sobre un ejemplo especifico de un objeto, como puede ser el nombre del empleado, el número telefónico y dirección. Cada objeto tiene un **registro del objeto** que es la colección primaria de la información sobre el objeto. Además del registro del objeto, puede haber uno o más registros de alias que den nombres alternos para dicho objeto.

4.3.2.2.1.3 DIT

Los registros del DIB se arreglan en forma de un árbol, conocido como **DIT**. Los vértices del DIT representan los registros, figura 4.23. Los registros más altos en el árbol (más cercano a la raíz o root) representan objetos como países u organizaciones, mientras que los registros más bajos en el árbol representan a las gentes o aplicaciones, etc.

4.3.2.2.1.4 Atributos

Cada registro se compone de atributos. Los registros tienen un conjunto de atributos definidos por un tipo de atributo y uno o más valores. La presencia y tipo de los atributos que componen un registro en particular son dependientes de la clase de objeto que el registro describe. Por ejemplo, una clase de objeto organización puede incluir los siguientes atributos:

- Nombre de la organización;
- Descripción y categoría del negocio;
- Ubicación, dirección postal;
- Teléfono, Fax y dirección ISDN etc.

La clase de objeto persona de la organización puede incluir los siguientes atributos:

- El nombre común (por ejemplo Ricardo Septién);
- Apellido;
- El nombre de la unidad de la organización (por ejemplo el nombre del departamento, división o sección);
- Titulo, descripción;
- Ubicación, dirección postal;
- Teléfono, fax y dirección ISDN etc.

La clase del registro de aplicación contiene:

- El nombre común (por ejemplo un calificador del registro de la aplicación);
- La dirección de presentación (por ejemplo la dirección del Punto de Acceso de Servicio de Presentación, PSAP: Presentation Service Access Point);
- Descripción, ubicación;
- Nombre de la unidad de organización y la organización;
- El contexto de aplicaciones soportadas.

Los estándares del Directorio definen un número de clases de objetos de uso general, como los nombrados arriba, y proveen la creación de nuevas clases de objetos a partir de las clases estándares. Por ejemplo, los estándares de X.400 MHS definen atributos adicionales (por ejemplo O/RName) y clases de objeto (por ejemplo el Agente de Usuario) para el uso del sistema de manejo de mensajes.

4.3.2.2.1.5 Valores alternativos

Cada atributo de un objeto puede tener múltiples valores almacenados debajo del registro del objeto en el Directorio; p. ej. puede haber varios números telefónicos disponibles para una organización o persona.

4.3.2.2.2 Nombres de Directorios

Cada registro tiene un **nombre distintivo** que es único y sin ambigüedad identifica el registro. Las propiedades del nombre distintivo se derivan de la estructura del árbol de la información, por ejemplo, el nombre de un Directorio consiste de un secuencia ordenada de nombres de los registros desde la raíz del árbol a un registro particular.

4.3.2.2.2.1 RDN

Dentro del DIT, cada registro tiene un **Nombre Distintivo Relativo** único (RDN: Relative Distinguished Name). Un RDN es un conjunto de valores para los atributos dados especialmente (los valores distintivos) a los registros. Frecuentemente, solo un valor del atributo se denomina como el RDN de un registro. Sin embargo, en algunas circunstancias, más de un atributo (por ejemplo atributos de Ubicación y Nombre común) pueden componer el RDN para un registro particular a fin de diferenciarlo entre dos objetos con nombres similares.

Como se muestra en la tabla 4.6, los RDNs de todos los registros con un registro superior inmediato particular, son distintos. Es responsabilidad de la autoridad pertinente el nombramiento para ese registro, para asegurar que sean adecuadamente asignados los valores distintivos de los atributos. La autoridad que da el nombramiento nunca deberá asignar más de una vez un mismo nombre a registros que tienen el mismo registro inmediato superior.

Nombre distintivo relativo		Nombre distintivo	Autoridad de registro
Raíz	{ }	{ }	-
País	C=UK	C=UK	ISO
Organización	O= Telecom	C= UK, O= Telecom	Autoridad registradora nacional
Unidad organizacional	OU= Ventas	C= UK, O= Telecom OU= Ventas	Corporativa

Tabla 4.6 Ejemplo de un nombre distintivo

El RDN para un registro es elegido cuando el registro es creado. Este puede ser alterado solo por usuarios con derechos apropiados de acceso.

4.3.2.2.2.2 Nombre Distintivo

El **nombre distintivo** de un objeto determinado se define como la secuencia de los RDNs de el registro que representa el objeto y todos sus registro superiores (en orden descendente). A causa de que hay una correspondencia de uno a uno entre los objetos y los registros de los objetos, el nombre distintivo de un objeto puede ser considerado para identificar el registro también.

El nombre distintivo comienza en nodo raíz y contiene los RDNs de todos los registros respectivos de cada rama y hoja.

4.3.2.2.2.3 Nombres alternativos

Además del RDN, el atributo de nombre para cada registro puede tener un número de valores alternos para admitir variaciones y abreviaturas comunes del idioma. Esto acomoda **nombres alternos**; por ejemplo el atributo de Nombre Común para una persona puede tener Ricardo Septién con el valor distintivo, y un nombre alternativo puede ser. Sr. Septién. Así, Ricardo Septién debe usarse en el RDN a fin de acceder el registro directamente (en una operación de leer). Si el nombre distintivo correcto para un registro no es conocido, entonces el usuario puede pedir al Directorio que localice cualquier registro que iguale ciertos atributos. Por ejemplo, una petición de búsqueda para registros con un atributo de Nombre Común que sea semejante a Sr. Septién también sería efectuada para localizar el registro para Ricardo Septién (los otros atributos, por ejemplo, Localización, puede también ser usado para la búsqueda).

4.3.2.2.2.4 Nombres de alias

Algunos de los registros del árbol son **registros de alias**, mientras que otros son registros de objetos. Un registro de alias no contiene información pero apunta hacia otro registro de objeto. Un alias o el nombre de un alias, para un objeto es un nombre que por lo menos en uno de sus RDNs esta en el registro de alias. Un nombre de alias provee la base para los nombres múltiples para los correspondientes objetos; por ejemplo un registro de alias es usado para redefinir objetos. El Directorio identifica y revalúa el alias para encontrar el registro correspondiente al registro de objeto. Los nombres de los alias permiten a los registros de los objetos que logren el efecto de tener nodos superiores múltiples. Así como el nombre distintivo de un objeto expresa su relación principal con alguna jerarquía de objetos, así un alias representa una jerarquía diferentes de objetos.

4.3.2.2.3 Operaciones de Directorios

La estructura jerárquica es la base por la cual los usuarios acceden la información del Directorio. Los usuarios pueden tener una información completa distintiva de accesos y nombres para el registro correspondiente. Alternativamente, los usuarios pueden tener uno o más atributos y pedirle al Directorio para que busque en la base de datos y proporcione información de cualquier registro semejante. Las operaciones que se desempeñan en el Directorio caen dentro de tres principales clasificaciones, es decir, de lectura, búsqueda y modificación. Dentro de estas clasificaciones están especificados los siguiente servicios:

- **Lectura**. Una petición de lectura apunta a un registro en particular, y causa que los valores de algunos o todos los atributos de un registro van a ser devueltos. El usuario debe especificar un nombre distintivo completo en la petición para referirse a un registro especifico. Donde solo algunos atributos serán devueltos, el usuario proveerá la lista de los tipos de atributos que le interesan.
- **Comparación**. Una petición de comparación apunta a un atributo en particular de un registro en particular. El usuario da un nombre distintivo y un valor propuesto para un atributo. La operación ocasiona que el Directorio verifique que el valor dado se igual al valor del atributo. El Directorio regresa una respuesta falsa o verdadera.
- **Abandono**. Una petición de abandono, se aplica a todas las peticiones de interrogación pendientes, informando al Directorio que el que origina la petición no se interesa más en la petición que fue hecha. El Directorio puede, por ejemplo, para el procedimiento de petición, y puede descartar cualquier resultado.
- **Listado**. Una petición de lista, ocasiona que el Directorio devuelva una lista de subordinados inmediatos de una registro particular en el DIT. El usuario debe proporcionar el nombre distintivo de un registro particular, y el Directorio regresa los nombres de los subordinados del registro (si existe).
- **Búsqueda**. Una petición de búsqueda ocasiona que el Directorio regrese información de todos los registros con parte segura del DIT que satisfaga alguna(s) condición(es). La petición de usuario incluye argumentos para identificar el alcance de la búsqueda en el DIT y las condiciones para el filtrado de los registros. La información devuelta de cada registro consiste en algunos o todos los atributos de ese registro, como es el de si se tiene derechos de lectura.
- **Agregar/remover un registro.** Una petición de agregar ocasiona la creación de un nuevo registro (por ejemplo un registro objeto, o un registro alias) para ser agregado al DIT. Una petición de remover un registro ocasiona que un registro se borrado del DIT.
- **Modificar registro**. Esta operación modifica los atributos de un registro especificado.

- **Modificar RDN.** Esta operación cambia el RDN de un registro.

4.3.2.2.3.1 El control de acceso

Los objetos dentro del Directorio pueden tener categorías para el control de acceso discreto para proteger los registros a accesos no autorizados y de sufrir modificaciones. El control de acceso se puede aplicar a un grupo de registros (una sub-rama), a un registro único, un atributo, a un registro o un valor de algún atributo. Las siguientes categorías de protección han sido definidas:

- Detección: Permite que el componente protegido pueda ser detectado (si existe) por el que accede.
- Comparación: Permite que el componente protegido pueda ser comparado por el que accede.
- Lectura: Permite que el componente protegido pueda ser recobrado (leído) por el que accede.
- Modificación: Permite que el componente protegido pueda ser actualizado por el que accede.
- Agregar/borrar: Permite que el componente protegido pueda ser creado, eliminado o modificado por el que accede.
- Nombramiento: Permite la modificación del RDN del subordinado del registro protegido por el que accede.

En general, el mecanismo de control de acceso verifica las categorías antes de operar sobre el componente protegido. El estándar, sin embargo, no especifica como el control de acceso se implementa y lo deja como medida local para el administrador del DSA.[46]

4.3.2.2.4 Esquema del Directorio

El Directorio impone un conjunto de reglas para asegurar que el DIT tenga consistencia frente a las excesivas modificaciones. Estas reglas son conocidas como **el esquema del directorio.** El esquema de Directorio es un conjunto de definiciones, limitaciones en lo que se refiere a la estructura fundamental del DIT, también los posibles caminos del registro son nombrados, la información que puede estar en un registro y los atributos usados para presentar esa información. Estas definiciones de esquema se aplican durante el acceso al Directorio para prevenir que los registros tengan tipos de atributos equivocados de atributos para sus clases de objetos, valores de atributos erróneos para el tipo de atributo, y los registros iguales tengan registros subordinados de clases equivocadas.

[46] Se debe de reconocer que la administración de tales aspectos requiere de un gran esfuerzo.

Formalmente, el esquema del directorio está comprendido de un conjunto de:

- **Definiciones de estructura**: Reglas que definen los nombres distintivos que los registros pueden tener y las maneras que pueden estar relacionados unos con otros mediante el DIT.
- **Definiciones de clases de objetos**: Las definiciones para el conjunto de atributos obligados y opcionales que deben y pueden estar presentes, respectivamente, en un registro de una clase determinada. La clases de objetos están definidas por un **Identificador de Objeto** (OID: Object Indetifier) y por una lista de los tipos de atributos que pueden ser opcionales u obligados.
- **Definiciones de tipos de atributos**: Las reglas que especifican el identificador del objeto por el cual el atributo es conocido, su sintaxis, y cuando tiene permitido tener varios valores.
- **Definiciones de la sintaxis de los atributos**: Las definiciones para cada atributo se hacen por medio del estándar ASN.1

La figura 4.24 resume las relaciones entre las definiciones del esquema y el DIT, los registros de directorios, atributos de un lado y valores de atributos del otro lado.

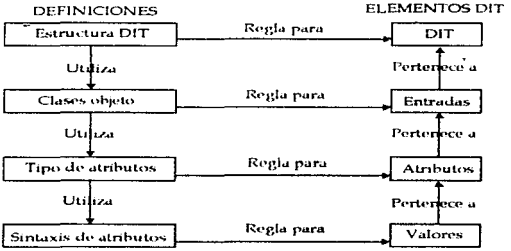


Figura 4.24 Esquema del Directorio

El esquema del directorio esta distribuido, como el DIB mismo, y puede variar entre los sistemas de directorios. Cada autoridad administrativa establece el esquema que aplicará para esas parte del DIB que administra.

El esquema de Directorio permite al sistema de Directorio, lo siguiente:

- Impedir la creación de registro subordinados de clases de objetos equivocados (por ejemplo, un país como un subordinado de una persona);
- Impedir la adición de un tipo de atributo para un registro de una clase de objeto inapropiado (por ejemplo, un número de serie a un registro de una persona); o
- Impedir que se pueda poner un valor a un atributo que no este definido.

4.3.2.3 El directorio distribuido

Los componentes funcionales principales del Directorio como se mencionó anteriormente, son el Agente de Usuario del Directorio (DUA: Directory User Agent) y el Agente de Sistema del Directorio (DSA: Directory System Agent), como se muestra en la Figura 4.25.

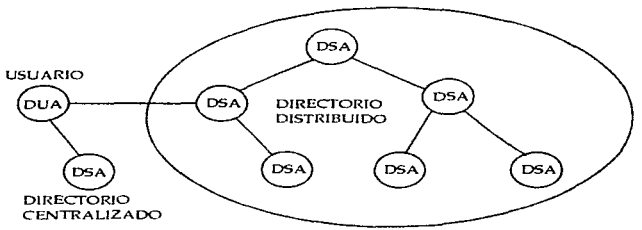


Figura 4.25 Componentes funcionales del Directorio estándar - Agente del Usuario del Directorio (DUA) y el Agente del Sistema del Directorio (DSA).

4.3.2.3.1 Componentes funcionales principales del Directorio

4.3.2.3.1.1 DUA

Cada usuario esta representado cuando accede el Directorio por **un Agente de Usuario del Directorio** (DUA), que es un proceso de la aplicación. Hay una relación de uno a uno entre el usuario y el correspondiente DUA. El DUA es el acceso del usuario para el Directorio y las operaciones de petición son pasadas entonces por el DUA al Directorio.

El Directorio puede ser accedido por un número de puntos por los DUAs. Para acceder al Directorio, el DUA se comunica con uno o más DSAs. El DUA y el DSA son componentes lógicos. En una configuración física, el DSA y el DUA pueden estar combinados o distribuidos, si están distribuidos se pueden asociar por medio protocolos inferiores del modelo OSI.

4.3.2.3.1.2 DSA

El DSA puede ser un componente único (llamado un Directorio **centralizado**) o estar conectado con otros DSAs (un Directorio **distribuido**). Cuando hay múltiples DSAs interconectados, la resolución de nombres puede realizarse por uno o mas DSAs. Un solo DSA, o grupo de DSAs puede referirse como un DMD (Directory Management Domain).

Cada DSA tiene una parte o fragmento del DIB. Un requerimiento importante del Directorio es que las respuestas que este regrese son independientes de la identidad y la ubicación del usuario. Además, el DUA no necesita conocer la estructura interna de los DSAs y su interconexión.

4.3.2.3.1.3 El contexto del nombramiento

Un DSA se responsabiliza de una parte del DIB total. La responsabilidad del espacio de nombres se refiere como el **contexto del nombramiento** del DSA. A fin de identificar la posición del DIB del inicio del contexto del nombramiento, al DSA se le da un prefijo del contexto. El prefijo del contexto se pone en el DSA que contiene el nodo raíz del directorio. El prefijo del contexto de los DSA subordinados corresponde al RDN de la entrada inicial del DSA.

4.3.2.3.1.4 Repetición

Las versiones iniciales de los estándares no proveían soporte a protocolos para la replica de datos, aunque es el objetivo de las propuestas adicionales. No obstante, los DSAs que usan las versiones originales de los estándares pueden usar replicas para acelerar el acceso, esto se lleva a cabo guardando una copia de la información que actualmente esta en otro DSA. En este caso, el control y actualización de las copias es una medida local (con el acuerdo del propietario de la información).

4.3.2.3.2 Interacciones de los DSA

El proceso de acceso al Directorio comienza con el DUA que establece una asociación con un DSA y pide una operación sobre el Directorio. Dependiendo de la ubicación de la información, tres modos de interacción de los DSA son definidos, llamados encadenados (chaining), multi-casting y referencia como se muestra en la figura 2.26 Los DSAs hacen uso del conocimiento sobre la ubicación

de los componentes o el DIB - tales conocimientos están en la forma de referencias con otros DSAs.

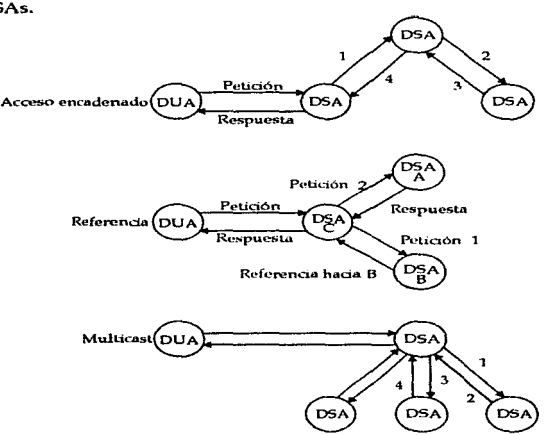


Figura 4.26 Interacciones del DSA - llamados encadenados (chaining), multi-casting y referencia.

4.3.2.3.2.1 Encadenamiento

El modo de encadenamiento de comunicación puede ser usado por un DSA para pasar una operación remota a otro DSA cuando el anterior tiene conocimiento específico sobre los contextos de nombramiento del posterior. El encadenamiento puede usarse para llamar a un DSA que esta arriba o abajo en la jerarquía de nombres.

4.3.2.3.2.2 Referencia

Una referencia es devuelta por un DSA en respuesta a una operación remota, por un DUA, o por otro DSA. La referencia puede constituir la respuesta completa, o simplemente parte de la respuesta. La referencia contiene la dirección de Presentación de otro DSA que tiene la información deseada o puede acceder esta.

Entonces, el DUA solicitante o DSA establece otra asociación con el DSA identificado por la referencia.

4.3.2.3.2.3 Multicast

El modo de comunicación multicast es usado por un DSA para pasar una operación remota idéntica, en paralelo o secuencialmente, a uno o más DSAs. El multicast es usado cuando el DSA original no conoce el nombre de contexto completo que tienen los otros DSAs. Normalmente uno de los DSAs será capaz de continuar la operación remota, y todas las demás regresarán el error de servicio "incapaz de procesar".

Los parámetros pueden ser colocados por el usuario para inhibir el encadenamiento y la referencia sobre las operaciones del DSA.

4.3.2.3.3 Los protocolos DAP y DSP

En la figura 4.27 se muestran al DUA y DSA como entidades separada en el modelo OSI. El **Protocolo de Acceso al Directorio** (DAP: Directory Access Protocol) opera entre el DUA y un DSA. *El* **Protocolo de Sistema del Directorio** (DSP: Directory System Protocol) opera entre los DSAs distribuidos.

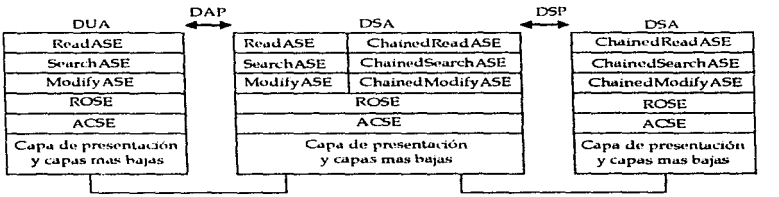


Figura 4.27 Protocolo de Acceso al Directorio (DAP) y el Protocolo del Sistema del Directorio (DSP)

Ambos el DAP y el DSP son los protocolos que proveen comunicación entre un par de procesos de aplicación. En el ambiente de OSI, esta se representa como la comunicación entre una par de **Entidades de Aplicación** (AE: Application entities) usando el servicio de capa de presentación. La función de una entidad de aplicación es proveer un conjunto de **Elementos de Servicios de Aplicación** (ASE: Application Service Element).

4.3.2.3.4 Arboles de Conocimiento

El DIB puede estar distribuido a través de múltiples DSAs, y en cada DSA se mantiene un fragmento del DIB.

Es un requerimiento del Directorio que para modos particulares de interacción con el usuario, la distribución del Directorio sea transparente, por medio de esto el usuario tiene el efecto que la totalidad del DIB aparece para estar dentro de cada DSA.

A fin de soportar los requerimientos de operación descritos anteriormente, es necesario que cada DSA que mantiene un fragmento del DIB sea capaz de identificar y opcionalmente interactúe con otros fragmentos de DIB mantenidos por otros DSAs.

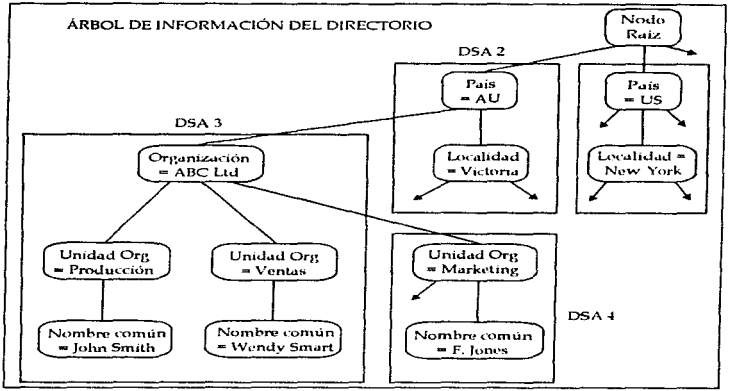
El conocimiento se define como la base para el mapeo de un nombre a su ubicación dentro de un fragmento del DIT. Conceptualmente los DSAs mantienen dos tipos de información:

- Información del directorio
- información del conocimiento

La información del directorio es la colección de los registros que comprende el nombre de contexto para que el administrador de un DSA tenga una autoridad administrativa.

La información de conocimiento abarca los nombres del contexto mantenidos por un DSA particular y denota como estos se adaptan en el DIT jerárquico total. La resolución distribuida de nombres, el proceso de ubicar el DSA que tiene la autoridad administrativa para un particular registro, dado el nombre de ese registro, se encuentra basándose en la información de conocimiento.

La figura 4.28 indica la estructura de un número de DSAs que se combinan para formar un hipotético DIB. El diagrama más inferior identifica la estructura del árbol de conocimiento dentro de DSA3.



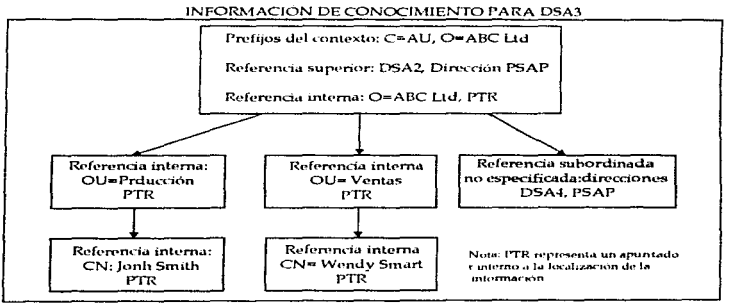


Figura 4.28 Información de conocimiento

4.3.2.4 Comportamiento operacional del DSA

Cada DSA esta compuesto con procedimientos capaces de completar con todas las operaciones del Directorio. En el caso de que un DSA sea centralizado, todas las operaciones son, de hecho, completamente efectuadas dentro de ese mismo DSA. En el caso que el DIB se distribuya a través de múltiples DSAs, la terminación de una operación típica se fragmenta, efectuándose una parte de la operación en cada DSAs que pueda colaborar.

Cada operación del Directorio puede hacerse en tres fases:

- La fase de resolución de nombres, se utiliza para ubicar el DSA que mantiene el registro sobre el cual se realizará una operación.
- La fase de evaluación, se desarrolla la operación por la cual se hizo la petición (.
- La fase de salida de resultados, es en la que los resultados de una operación especifica se devuelven a la solicitud del DUA. Si el modo de encadenamiento de interacción fue escogido, la fase de salida de resultados combina la información resultante de un número de DSAs.

4.3.2.5 Servicios de seguridad

4.3.2.5.1 Procedimiento de Autenticación de Contraseña

Un mecanismo para la implantación de una verificación simple de contraseña para los Agentes de Traslado de Mensaje (MTAs) usando el Directorio se ilustra en figure 4.29.

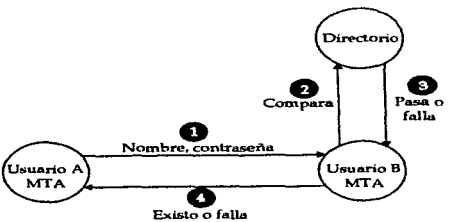


Figura 4.29 Autentificación usando verificación de contraseña simple.

1. El usuario original A envía su nombre distintivo y contraseña a un usuario receptor B.
2. B envía el aparente nombre distintivo y la contraseña de A, al Directorio en una operación de comparación, en el directorio se verifica la contraseña que se envía (desde B) con la que se mantiene en el directorio.
3. El Directorio le confirma a B si las credenciales de A son validas o no.
4. El éxito o fracaso de autentificación puede ser transmitida al usuario A.

La ventaja de este esquema es que el usuario A puede autentificarse para usar muchas aplicaciones diferentes sin contraseñas individuales que se tienen que registrar sobre cada sistema. El usuario A puede cambiar frecuentemente la contraseña en el Directorio centralizado sin necesidad de ser actualizado en varios sistemas diferentes.

4.3.2.5.2 Autentificación Fuerte

El estándar X.509 provee soporte para un esquema de control de llave pública asimétrica que puede ser usado por una variedad de servicios de seguridad. Esta es la base para los servicios de seguridad del X.400 (1988). El Directorio almacena copias certificadas de las llaves públicas de los usuarios que pueden ser usados en los sistemas de encriptamiento para proveer la autentificación, en datos confidenciales y los servicios de integridad de los datos.

4.3.2.6 Normas X.500

CCITT e ISO conjuntamente desarrollaron los estándares de Directorio (mostrados en el listado de la tabla 1.2). La versión de CCITT fue aprobada en 1988 y la versión de ISO en 1990.

CCITT	ISO	Titulo
X.500	9594-1	Introducción a los conceptos, modelos y servicios
X.501	9594-2	Modelos
X.509	9594-8	Marco de referencia de autentificación
X.511	9594-3	Definición de Servicios Abstractos
X.518	9594-4	Procedimientos para la Operación de Distribución
X.519	9594-5	Especificaciones del Protocolo
X.520	9594-6	Selección de tipos de atributos
X.521	9594-7	Selección de Clases de Objetos

Tabla 4.7 Estándares del Directorio

4.3.2.7 Conclusión

A causa de que el Directorio es potencialmente la base de almacenamiento y conocimiento para otras aplicaciones OSI (por ejemplo X.400 MHS, el sistema de control X.700, etc.), como atributos y clases de objetos se extienden a esos servicios, la definición de estos componentes deben ser adicionados al alcance del esquema del Directorio.

A largo plazo, la operación confiable del Directorio será el centro del éxito de otras aplicaciones. Cuando opere en un ambiente distribuido y se integre con otros estándares, el Directorio requerirá de sofisticados productos de administración y control para acomodar la complejidad inherente de los mecanismo y la creciente cantidad de información soporte global para las comunicaciones OSI.

4.3.3 Transferencia, Administración y Acceso de Archivos

4.3.3.1 Introducción

El manejo de archivos es uno de los principales servicios en cualquier red o sistema distribuido[47].

4.3.3.1.1 Servidores de archivos

Las principales características de un servidor de archivos son:

- La estructura de los archivos.
- Los atributos de los archivos.
- Las operaciones sobre los archivos.

El modelo más general de una **estructura de archivos** es la estructura de archivos jerárquico (que es la usada en FTAM), que tiene la forma de un árbol invertido. Cada nodo del árbol puede tener una etiqueta (casi siempre único), un registro de datos, ambos o ninguno. En la figura 4.30 se puede ver una archivo jerárquico.

[47] Existen cuatro principales sistemas de archivos distribuidos:
- Sistema de archivos en red (NFS: Network File System) de Sun Microsystem.
- Sistema de archivos Andrew (AFS: Andrew File System) de la Universidad de Carnegie Mellon
- Sistema de archivos distribuido (DFS: Distributed File System) de la OSF
- Acceso y manejo en la transferencia de archivos (FTAM: File Transfer Access and Management), implantado en entornos OSI

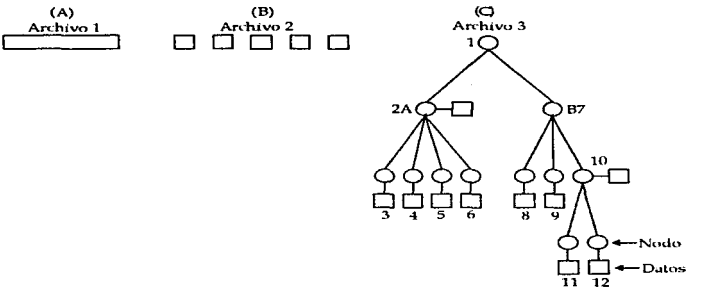


Figura 4.30 Archivos. A) No estructurado. B) Secuencia de registros c) Jerárquico.

Y generalmente se debe de tener un método de ordenamiento, que permita direccionar los nodos sin etiqueta mediante su posición y así poder ejecutar las operaciones de eliminación, reemplazo y transferencia de archivos completos. Si todos los nodos están etiquetados, se puede direccionar un nodo específico, indicando su ruta a partir de la raíz. También las etiquetas de los nodos sirven para direccionar subárboles completos.

Todos los archivos tienen **atributos** que los describen. Como mínimo, cada archivo debe tener un nombre o algún identificador y el tamaño que ocupa realmente.

Las **operaciones** sobre los archivos se puede aplicar a un archivo como un todo o a su contenido, es decir a los registros individuales.

4.3.3.2 Breve descripción de FTAM

El estándar OSI para la **Transferencia, Administración y Acceso de Archivos** (FTAM: File Transfer, Access and Management) permite a las aplicaciones acceder archivos de sistemas de archivos remotos. Los archivos pueden ser pasados como un todo entre procesos de aplicación de comunicación, o de otra manera los archivos remotos pueden ser accedidos para operaciones de lectura y escritura.

El estándar, FTAM (ISO 8571[48]) se encuentra dividido en cuatro partes:

Parte 1 Descripción general (esta sección)
Parte 2 Definición del Sistema de Almacenamiento Virtual
Parte 3 Definición del Servicio de Archivo
Parte 4 Especificación del Protocolo de Archivo[49]

4.3.3.2.1 Modelo FTAM

En la figura 4.31 se ilustra los principales componentes lógicos de FTAM en dos sistemas de comunicación de computo. FTAM esta definido en términos del dialogo que se tiene entre un **iniciador FTAM**, que soporta la aplicación del usuario, y un contestador que soporta el sistema de almacenamiento. El iniciador corresponde al cliente y el contestador al servidor. Cada actividad o acción sobre un archivo remoto es iniciado por el cliente. El servidor reacciona de manera pasiva para efectuar la acción pedida. El **sistema de almacenamiento virtual** es un modelo genérico de un conjunto de archivos. El sistema de archivos remoto puede ser tan simple como un disco flexible, una computadora personal o tan complejo como la raíz de un gran sistema de archivos de un mainframe o una base de datos. Para lograr la independencia de los vendedores, el sistema de almacenamiento virtual lleva a cabo el mapeo del modelo genérico de FTAM de un sistema de almacenamiento a un sistema de archivos real. Los detalles de la implantación de los datos fuente son de forma transparente a los usuarios del sistema de almacenamiento.

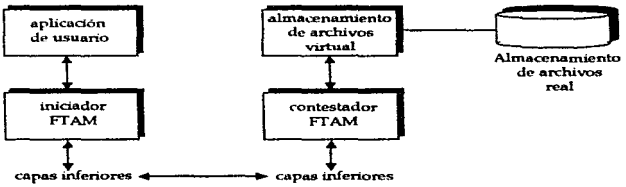


Figura 4.31 Modelo de FTAM

[48] No hay un equivalente de la CCITT.
[49] Se especifican las primitivas del protocolo FTAM, por lo que no se explicará a detalle en este trabajo. Para mayor información referirse a: Dickson Gary; Open System Interconnection; Prentice Hall 1992; pp 309-340.

Las aplicaciones de una computadora usan FTAM para acceder a los archivos sobre una computadora remota que a la vista de un usuario o aplicación tiene el aspecto de un recurso local. Las características de FTAM incluyen:

- Soporte para crear y destruir archivos (tanto secuenciales como jerárquicos);
- Transferencia de archivos completos (en ambas direcciones) entre la aplicación y el sistema de almacenamiento;
- Acceso a partes del archivo (por ejemplo leer o escribir campos individuales en una estructura de archivos);
- Soporte para una gran variedad de atributos para los archivos (por ejemplo, nombre del archivo, tamaño, fecha de creación, etc.); y,
- Manejo o control de archivos remotos (por ejemplo, crear o borrar archivos).

4.3.3.3 Definición del sistema de almacenamiento virtual

El uso de un modelo común (el modelo FTAM es común a todas las maquinas) para todo tipo archivos incluyendo bases de datos, puede proporcionar las fundamentos para la transferencia, acceso y administración de archivos entre diversos sistemas abiertos. Este modelo común es referido como **sistema de almacenamiento virtual**. Su objetivo es reducir la cantidad de detalles necesarios para la comunicación con archivos localizados en posiciones remotas en la red.

El sistema de almacenamiento virtual es una modelo abstracto de un sistema de almacenamiento real. Es decir, el sistema de almacenamiento virtual es un modelo de sistema de almacenamiento de archivos genérico (general) que puede ser entendido por diferentes sistemas abiertos (cuando un sistema abierto en particular lo utiliza (mapea), se convierte a un sistema de archivos real de ese sistema abierto). Es responsabilidad de cada sistema abierto el mapear las descripciones (esquema, atributos y operaciones de los archivos) del sistema de almacenamiento virtual dentro del sistema de manejo de archivos local real[50].

Todas las especificaciones de los protocolos y definiciones del FTAM se dan en términos de las características y datos del sistema de almacenamiento virtual y no en términos de un sistema de almacenamiento local real.

Termino	Definición
DATO	Cualquier representación, con algun significado es que se le puede asignar.
Información	La combinación de datos y el significado de este.
Archivo	Un conjunto de información referida a través de un nombre sin ambigüedad (claro) que tiene un conjunto de atributos comunes.
Sistema de almacenamiento	Una colección de archivos organizados, incluyendo sus atributos y nombres, que residen en un sistema abierto particular.

Tabla 4.8a Algunas definiciones de terminología del Sistema de Almacenamiento Virtual

[50] El uso de los datos depende de cada aplicación.

Termino	Definición
Sistema de almacenamiento virtual	Un modelo abstracto para describir archivos y sistemas de almacenamiento
MANEJO DEL SISTEMA DE ALMACENAMIENTO	La descripción y el manejo de la organización de los campos de información.
Objeto	Un archivo, un directorio de archivos o una referencia
Directorio de archivos	Un mecanismo para agrupar archivos, referencias y archivo-directorio en una estructura en forma de árbol lógico
Referencia	Un punto de referencia a otro objeto, ya sea un archivo o un directorio
Ruta	Una serie de nombres de objetos que identifican un objeto
ACCION A UN ARCHIVO	Un tipo de acción que se realiza sobre el contenido de un archivo
Transferir archivo	Una función que mueve un archivo entre sistemas abiertos
Acceder archivo	La inspección, modificación, o reemplazo de alguna parte del contenido de un archivo
Manejo de archivo	La creación y eliminación de archivos, y la inspección o manipulación de los atributos asociados con un archivo
ATRIBUTOS	Propiedades que identifican a un objeto
Atributos de archivo	El nombre, tamaño, fecha de creación, etc. de un archivo individual
Actividad de los atributos	Los atributos describen la actividad de uso de los servicios del archivo

Tabla 4.8b Alguna definiciones de terminología clave del Sistema de Almacenamiento Virtual

4.3.3.4 Definición de servicios de archivo

4.3.3.4.1 Protocolos para la administración de archivos

ISO está desarrollando diversos sistemas para la administración, el manejo de bases de datos y archivos de usuarios, pero el único sistema que esta disponible es el estándar de **Transferencia, Administración y Acceso de Archivos** (FTAM)

4.3.3.4.1.1 FTAM

FTAM está organizado basándose en el concepto de **atributo**, que describe las propiedades de un archivo. Actualmente se definen cuatro tipos de atributos:

- Grupo de kernel: Propiedades comunes a todos lo archivos.
- Grupo de almacenamiento: Propiedades de los archivos que se almacenan.
- Grupo de seguridad: Propiedades del control de acceso.
- Grupo privado: Propiedades más allá de FTAM.

El grupo de kernel, son las propiedades comunes a todos los archivos, por lo tanto, consta de un nombre de archivo, una descripción de la estructura de archivo

(secuencial o jerárquico), restricciones de operación (borrado, lectura, etc.), la localización del usuario del archivo y la identificación de las entidades de aplicación involucradas en el proceso de comunicación de FTAM.

El grupo de almacenamiento describe varias propiedades de un archivo, las propiedades son: información sobre las características de operación en curso del archivo o información sobre las últimas operaciones realizadas en el archivo. El grupo de almacenamiento incluye las siguientes propiedades:

- Fecha y hora de la última lectura, cambio o modificación de atributos.
- Identificación del creador, del último lector, del último modificador en el contenido como en atributos.
- Tamaño del archivo y disponibilidad.
- Identificación de la entidad a la que se le deben cargar los costos de almacenamiento y de actividades de acceso a los archivos.
- Descripcion de posibles bloqueos en el archivo.
- Identificación del usuario de FTAM originario.

El grupo de seguridad incluye los atributos de los criterios de permisos de acceso, procedimiento de cifrado y cualidades legales (marcas registradas, derecho de copia, etc.).

El grupo privado no esta definido en el estándar FTAM. Se utilizan con archivos con los que no se pueden definir atributos de almacenamiento de archivos virtuales.

El FTAM es una estructura jerárquica en forma de árbol. El árbol puede tener una sola raíz y varios nodos debajo de la raíz. Cada nodo tiene un identificador y un tipo de datos asociados al mismo. En un sistema de almacenamiento virtual, la noción convencional de **registros de datos** se denominan **unidades de datos** (DU), los nodos pueden tener o no unidades de datos asociadas. Las DU se relacionan entre sí mediante una estructura denominada **unidades de datos de acceso a archivos** (FADU). Las operaciones en los archivos se realizan sobre las FADU mediante los identificadores de FADU (o nombres). La FADU se identifica en forma de unidad de datos con tipo en el nivel de presentación. La DU es la unidad más pequeña a la que se puede acceder.

El FTAM puede tomar varias formas a la hora de acceder a un archivo o una parte del mismo. Por ejemplo, un archivo puede ser accedido partiendo de la raíz y viajando por los nodos en orden descendente. Otro ejemplo, es que las FADU se pueden acceder mediante señales de **siguiente, último, previo y comienzo.**

La forma en que esta ordenada y se recorre el árbol es la siguiente:

- Entrada al árbol por el nodo superior.
- Recorrido de los nodos comenzando por el superior, hacia abajo y hacia la izquierda.
- Moviéndose a la derecha cuando ya no quedan más caminos descendentes.
- Moviéndose hacia arriba si no se puede descender más.

Atributo	Tipo	Se fija cuando el archivo es creado	Puede cambiarlo el usuario	Mantenido por el servidor
Nombre del archivo	Cadena de caracteres	X	X	
Operaciones permitidas	Mapa de bits	X		
Control de acceso	Lista		X	
Número de cuenta	Entero	X	X	
Fecha y hora de creación del archivo	Hora	X		
Fecha y hora de última modificación del archivo	Hora	X		X
Fecha y hora de última lectura del archivo	Hora	X		X
Fecha y hora de última modificación del atributo	Hora	X		X
Propietario	Ident. de usuario	X		
Identidad del último modificador	Ident. de usuario	X		X
Identidad del último lector	Ident. de usuario	X		X
Identidad del último modificador del atributo	Ident. de usuario	X		X
Archivo disponible	Booleano	X	X	
Tipo de contenido	Ident. de objeto	X	X	
Clave de cifrado	Cadena de caracteres	X		
Tamaño	Entero	X		X
Tamaño máximo futuro	Entero	X	X	
Calificaciones legales	Cadena de caracteres	X	X	
Uso privado	Cadena de caracteres	X	X	

Tabla 4.9 Atributos de los archivos del almacén de archivo virtual OSI

Operación	Se aplica a todo el archivo	Se aplica al contenido	Mapa de bits	Descripción
Crear un archivo	X			Crear un archivo
Borrar un archivo	X		X	Destruye un archivo existente
Seleccionar un archivo	X			Tomar un archivo para el manejo de atributos
Des-seleccionar un archivo	X			Termina la selección en curso
Abrir un archivo	X			Abre un archivo para lectura o modificación
Cerrar un archivo	X			Cierra un archivo abierto
Leer un archivo	X		X	Lee un atributo del archivo
Cambiar un atributo	X		X	Modifica un atributo del archivo
Localizar		X		Localizar un archivo
Leer		X	X	Lee datos del archivo
Insertar		X	X	Insertar nuevos datos en el archivo
Reemplazar		X	X	Escribir encima de los datos existentes
Extender		X	X	
Borrar		X	X	Añade datos en algún registro Borrar un registro

Tabla 4.10 Posibles operaciones

4.3.3.5 Implantación del servidor

En el mundo de las conexiones en red, existen dos tipos de servidores de archivos, los orientados a conexión y sin conexión.

En el modelo correspondiente a un sistema sin conexión, se tiene un servidor sin estado. Para llevar a cabo el proceso de lectura o escritura de un archivo, el cliente envía una solicitud especificando el archivo, la posición del registro o etiqueta, así como la cantidad de datos que se van a transferir. Los archivos no tienen que ser abiertos o cerrados antes y después de ser utilizados. Cada una de las solicitudes está contenida por sí misma. Un ejemplo de este tipo de servidor sin estado, es el NFS del conjunto de protocolos TCP/IP.

A diferencia del anterior, el servidor orientado a conexión mantiene su estado interno. Cuando un archivo se abre, el servidor genera una entrada en una tabla para el archivo recientemente abierto. En general el índice de esta entrada se le devuelve al cliente para que lo utilice en solicitudes posteriores.

En la practica, los archivos se leen normalmente de manera secuencial, por lo que alguien tendrá que hacer un seguimiento de la posición en la que uno se encuentre dentro del archivo. En el modelo sin estado, el cliente es el que se encarga de mantener la posición del archivo y transmitirla junto con cada una de las solicitudes. Por otra parte, en el modelo con estado, el servidor es el que se encarga

de hacer el seguimiento de la posición dentro del archivo, de tal forma que el cliente solamente tiene que dar el índice de la tabla para identificar al archivo, y la cuenta de octetos.

Cada uno de los modelos tienen sus ventajas y desventajas. El principal atractivo del modelo del servidor sin estado es su gran robustez. Si llega a tener una caída y después se reactiva, no hay ninguna información de estado que se pueda perder, por lo que la única cosa que el cliente puede llegar a notar, es que se tiene un tiempo de respuesta más prolongado mientras que el servidor comienza a reactivarse. Sin embargo, la caída de un servidor con estado, hace que efectivamente se cierren todas las conexiones abiertas y descarga toda la responsabilidad del proceso de recuperación sobre el cliente.

FTAM es una norma del modelo OSI (es un sistema de archivos que cumple con GOSIP[51]), que proporciona servicios de transferencia de archivos entre sistemas cliente-servidor dentro de un entorno abierto, también ofrece acceso y administración de archivos sobre diversos sistemas.

Si quisiéramos comparar al FTAM con sus análogos en TCP/IP sería a los protocolos de Transferencia de Archivos (FTP) y al Sistema de Archivos en Red (NFS).

Los usuarios pueden manipular los archivos hasta el nivel de registro, que constituye la unidad de almacenamiento de archivos en FTAM, dispone de utilidades características de las bases de datos relaciónales[52], por ejemplo los usuarios pueden bloquear archivos completos o registros individuales.

FTAM como se dijo anteriormente es un sistema en el cual un servidor mantiene información orientada a la conexión, relativa al usuario y a la sesión, hasta que ésta se cancele, por tal motivo los archivos se transfieren entre los sistemas al establecer primeramente una sesión orientada a la conexión. El cliente FTAM establece el contacto con el servidor FTAM y pide una sesión. Una vez establecida la sesión tiene lugar la transferencia de archivos. FTAM utiliza el concepto de **almacenamiento virtual**, que proporciona una visión genérica de los mismos. De esta manera, el sistema de archivos FTAM oculta las diferencias entre sistemas de distintos fabricantes. FTAM especifica tipos de documentos tales como archivos binarios planos y archivos de texto, en los que cada línea finaliza con retorno de carro. Los datos se interpretan como registros y FTAM proporciona capacidades de almacenamiento virtual de archivos, que permiten el almacenamiento de estructuras de archivos orientados a registros.

---

[51] Es el conjunto de normas que propone el gobierno de los Estados Unidos, que cumplen con estándares OSI.

[52] A diferencia de NFS, este si puede manejar bases de datos de manera eficiente.

Las funciones típicas de FTAM son:

- Transferencia y recuperación de archivos desde servidores FTAM.
- Eliminación de archivos de servidores FTAM.
- Lectura de atributos de archivos en servidores FTAM.
- Listado, creación y borrado de directorios en servidores FTAM.

Por último, cabe decir que en la actualidad FTAM no se ha convertido en un sistema de transferencia de archivos muy utilizado entre sistemas de distintos fabricantes en el entorno de las redes locales, debido a que muchas realizaciones han fallado en su interoperabilidad. Pero en cambio, FTAM ha funcionado mejor como medio de transferencia de información de computadoras centrales a entornos distribuidos.

4.3.4 Manipulación y transferencia de trabajo (JTM)

En grandes organizaciones, los individuos tienen computadoras personales estaciones de trabajo en sus escritorios, los departamentos tienen minicomputadoras y la organización como un todo tiene una computadora central con mainframes, y supercomputadoras. De manera, frecuente ocurre que un individuo prepara algo de trabajo en su computadora personal que deberá correr en sobre un mainframe usando archivos localizados en la minicomputadora de su departamento, y que los resultados sean enviados a la computadora personal. La aplicación que maneja este tipo de entrada de trabajo remoto es referida como **Manipulación y Transferencia de Trabajo** (JMT: Job Transfer and Manipultion).

En un ambiente de procesamiento típico de datos, los usuarios y programadores someten "trabajos" a las computadoras. Estos trabajos son tareas (tal como recuperación de datos, actualización de archivos, etc.) para ser ejecutadas por las computadoras. En el pasado muchos trabajos fueron sometidos a códigos de tarjetas perforadas con un **Lenguaje de Control de Trabajos** (JLC: Jobs lenguaje Control). Ahora muchos trabajos son sometidos a una terminal para la ejecución de sentencias JLC previamente almacenados en disco. Las sentencias (generalmente llamado un procedimiento catalogado) son usados para invocar tareas deseadas.

JMT dirige las acciones de las computadoras por identificación de programas y archivos de datos que participan en el "trabajo"[53].

El propósito del estándar (ISO 8831 e ISO 8832) de manipulación y transferencia de trabajos (JTM), es permitir a los trabajos sometidos sobre cualquier sistema abierto

[53] El JCL también dirige la disposición de los programas, archivos, y trabajos de salida tal como reportes y listas.

correr sobre otro sistema abierto. En resumen esto requiere que el usuario especifique al sistema desde donde será hecho el trabajo[54]. La idea de JTM es:

a) Especificar los trabajos que serán ejecutados sobre un sistema,
b) controlar el movimiento de datos de los trabajos - relacionados entre los sistemas,
c) monitorear y manejar los procesos de la actividad.

JTM puede soportar los trabajos tradicionales "batch", además, puede soportar otros tipos de trabajos tal como procesamiento de transacciones, entrada de trabajos remotos (RJE) y acceso de bases de datos distribuidas.

4.3.4.1 Términos y conceptos JTM

Los servicios de JTM son proveídos por los **Elementos de Servicios de Aplicación** JTM (ASEs), protocolos ACSE (elemento de servicio de aplicación) y CCR (Compromiso, concurrencia y recuperación). Como se muestra en la figura 4.32 estos servicios combinados suplen al proveedor de servicio JTM. El estándar JTM describe como interactúa el proveedor de servicio con los usuarios JTM para soportar las operaciones JTM. Los usuarios JTM son representados por agencias. Estas agencias y los proveedores de servicios transfieren especificaciones de trabajo entre ellos para definir como se hará el trabajo. La especificación del trabajo contiene cada uno de los documentos del cual forma una unidad de interacción entre la agencia y el proveedor de servicio. JTM especifica con registros de control de transferencia como manejar el movimiento de los documentos al rededor de los sistemas. El tipo de documento que no concierne al JTM puede ser un programa o un procedimiento catalogado de JCL.

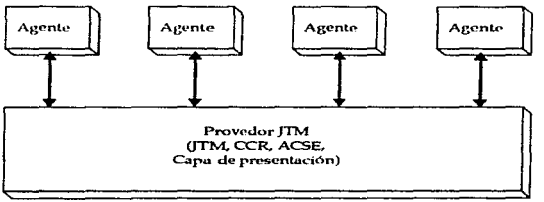


Figura 4.32 Vista funcional del Manipulación y Transferencia de Trabajos (JTM)

[54] Esto enfatiza que el JTM no se dirige a la estandarización de lenguajes de control de trabajos.

JTM también provee de servicios de monitoreo y reportes, los cuales son organizados alrededor de un monitor de trabajo OSI. Los reportes son enviados al monitor de trabajo que describe el estado en que se encuentra un trabajo OSI.

Tipos de agencias que son descritas en el estándar:

- Inicialización. Una agencia que causa que una especificación de trabajo será creada.

- Fuente. Una agencia que es un miembro de cualquier parte de un sistema abierto. Que es capaz de proveer documentos para la especificación de trabajo a la dirección del proveedor de servicio.

- Sink. Una agencia (también una parte de un sistema operativo) el cual recibe documentos que le pasa el proveedor de servicio.

- Ejecución. Una agencia la cual actúa inicialmente como un sink y mas tarde como una fuente como un resultado de documentos procesados tempranamente.

La especificación de trabajo de JTM puede especificar "further work" en otros sistemas abiertos. Por ejemplo, una lista de estados JCL puede invocar la ejecución de otro conjunto de estados JCL en otras computadoras. El trabajo total creado por las especificaciones de trabajo iniciales son llamadas una tarea OSI. La especificación del "further work" es llamada "proforma". La creación de una nueva especificación de trabajo de una "proforma" es llamada "spawning"

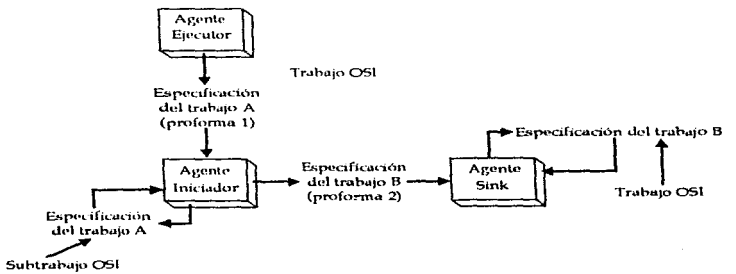


Figura 4.33Como pueden ocurrir Spawning y Proformas

La inicialización de agencia crea la especificación de trabajo inicial (Especificación de trabajo A) conteniendo de uno a "n" documentos y una proforma (proforma 1). Esta proforma es usada por una agencia de ejecución para crear una nueva especificación de trabajo (Especificación de trabajo B). La ejecución de la agencia también ejecuta parte de la tarea OSI (una subtarea OSI). El trabajo definido por la especificación de trabajo B es formado por una agencia sink como otra subtarea OSI.

4.3.4.2 Servicios Primitivos JTM

Los servicios primitivos son usados para invocar procedimientos JTM entre los usuario finales y el nivel de presentación.

4.3.4.3 Funciones de los parámetros primitivos.

Muchos de los parámetros primitivos son llamados parámetros de acción. Estos parámetros son usados para definir acciones específicas a los tipos de primitivas en las que son usadas. Documentos específicos, modificación de especificaciones de trabajos, transferencia controlada de trabajos y funciones de administración de control de reporte son establecidas en los parámetros de acción.

La mayoría de los otros parámetros son usados para autentificar e identificar los servicios de usuario y los documentos en el trabajo OSI.

4.3.4.4 Conclusiones

JTM hace uso del nivel de presentación ya que usa la petición de datos (P-DATA), recepción de datos y el control de información.

Usa el elemento de servicio de aplicación (ACSE)[55] y el de concurrencia y recuperación (CCR)[15] porque utiliza todas las peticiones, indicaciones, respuestas y confirmación de procedimientos JTM entre los usuario finales y el nivel de presentación.

La ventaja de la manipulación y transferencia de trabajos (JTM) es que puede proveer de servicios de monitoreo y reportes, a través de un monitor de trabajo OSI que describe el estado de un trabajo OSI.

---

[55] Para mayor referencia consultar el libro de Andrew S. Tanenbaum; Computer Networks, 2a edición; Prentice Hall; p. 532.

4.3.5 Terminal Virtual (VT)

Por alguna razón, la estandarización de terminales ha sido un completo fracaso, aproximadamente todas las terminales aceptan ciertas secuencias de caracteres, referidas como **secuencias de escape** (para el movimiento del cursor, entrada y salida de modo de video inverso, inserción y eliminación tanto de caracteres como de líneas, etc. Existen estándares como ANSI y otros para estas secuencias de escape, pero no todos las utilizan, ya que cada fabricante utiliza sus propias secuencias de escape (incompatibles con las de otros fabricantes).

El enfoque de OSI es resolver este tipo de problemas al definir una **terminal virtual** (VT), la cual es realmente una estructura de datos abstracta (modelo objeto) que representa el estado abstracto de la terminal real. Esta estructura de datos puede ser manipulada tanto por el teclado como por la computadora con el estado actual de la estructura de datos que esta siendo reflejada en pantalla. La computadora puede preguntar a la estructura abstracta por la entrada del teclado y puede cambiar la estructura abstracta de datos para causar que la salida aparezca en la pantalla.

La intención de la terminal virtual es definir el comportamiento de la terminal desde un punto establecido y desde sesiones de red. Idealmente, la definición del procedimiento es suficientemente flexible para permitir al usuario de la terminal cambiar el comportamiento de ésta fácilmente, proporcionando un medio para una terminal o aplicación de usuario y así poder acceder a una variedad de terminales y aplicaciones.

El concepto central de la terminal virtual es aislar las terminales y aplicaciones de cualquier otro tipo. De esta manera, las terminales diferentes pueden acceder a aplicaciones diferentes corriendo sobre sistemas diferentes.

La terminal virtual logra esta meta por medio de una terminal virtual de entidad que:

a) Simula una terminal real y
b) Negocia las características de operación de la terminal con otras terminales virtuales de entidad. Esto llega a ser la tarea para las VT al para resolver diferencias potenciales e incompatibilidades entre la terminal y la aplicación.

4.3.5.1 Modelando la terminal

Las terminales entran dentro de tres clases de broadcast: modo deslizante (scroll mode), modo de página, y modo de forma. El modo deslizante es el mas simple y el modo de forma el mas sofisticado. Para cada categoría , diferentes problemas son presentados y diferentes enfoques son necesarios.

Se examinan dos aproximaciones para la obtención de servicios de terminal virtual

- Modelo parámetro. Uso de códigos y parámetros para definir la terminal.

- Modelo objeto. Uso de objetos abstractos para modelar las características y funciones de la terminal

El modelo parámetro. Cuando las redes de paquetes basados en X.25 llegaron a existir en los años 70's, estas fueron reconocidas porque muchas terminales en operación fueron (y son) asíncronas, referidas como dispositivos de **modo deslizante** (scroll mode). Una terminal de **modo deslizante** tiene capacidades limitadas. Esta es llamada así porque cada carácter recibido es puesto sobre la pantalla creando líneas nuevas sobre la pantalla, las líneas viejas son desplazadas ascendentemente hasta que desaparecen de la pantalla.

Aún cuando este tipo de terminales son simples, ellas pueden divergir aún en como aceptar e interpretar los caracteres de control como un "line feed", tabulador horizontal, etc. Obviamente, se necesitó una interfaz[56] llamada "caja negra" (black box) que se insertaba entre la terminal y la red, este dispositivo se comunicaba con la terminal con el estándar RS-232 y hacia la red con un tipo de protocolo estándar. Este era referido generalmente como un **ensamblador/desensamblador de paquetes** (PAD: Packet Assembler/Disassembler).

Consecuentemente, CCITT definió interfaces PAD[57] estándares en sus recomendaciones X.3, X.28 y X.29 para las terminales asíncronas.

X.3 define los parámetros del PAD, X.28 la interface PAD de la terminal y el X.29 defina la interface computadora-PAD (DTE). El PAD no es exactamente una terminal virtual, el PAD es de hecho un **parámetro** manejador de terminal virtual. Este provee la conversión de protocolos para un dispositivo de usuario (DTE) para una red pública o privada, y complementariamente hace la conversión de protocolo en la recepción final de la red. Al hacerlo, este permite que diferentes tipos de terminales puedan comunicarse una con otra.

---

[56] Este tipo de terminales con modo deslizante no tiene ninguna capacidad de procesamiento, por tal motivo no se pueden comunicar con la red utilizando ningún tipo de protocolo estándar de red (a diferencia de una terminal con un CPU, puede ejecutar software de protocolos de red de manera interna).

[57] Mientras que el X.3 y estas asociaciones de estándares X.28 y X.29 hablan solamente de dispositivos asíncronos, muchos vendedores ofrecen otros servicios PAD que soportan protocolos síncronos de nivel de enlace de datos como BSC y SDLC, y también funciones de capas superiores.

El PAD orientado - asíncrono desempeña las funciones siguientes:

- Montaje de caracteres dentro de los paquetes
- Desmontaje del campo de datos de usuario a otro final.
- Manejo virtual de llamadas al inicio, limpieza de pantalla, reinicialización e interrupción
- Generación de señales de servicio de PAD a la terminal de usuario.
- Mecanismo para reenvió de paquetes (De paquetes muy grandes o que expiran en poco tiempo)
- Edición de comandos PAD
- Detección automática de rango de datos, código, paridad y características operacionales de uso de terminal.

El modelo objeto. Desarrollado por la ISO (International Standards Organization), este modelo usa objetos de datos abstractos para modelar funciones comunes y características encontradas en las terminales. La idea es que las funciones de la terminales se puedan describir en una notación abstracta para facilitar la interconexión de terminales y procesos de aplicaciones.

La idea básica de una terminal virtual de modelo objeto es la siguiente: cada terminal es descrita por una estructura (u objeto) y un perfil. Un perfil que puede ser parte de la estructura del dato. Un perfil es un conjunto de parámetros los cuales definen las características de la terminal. La estructura del dato no solamente describe el perfil de las terminales, pero define la operación de terminal especifica. El modelo objeto difiere del modelo parámetro en que la terminal de modelo objeto (o un dispositivo actúa como si fuera un agente) es considerado mucho más inteligente, quizá puede asumir perfiles diferentes.

Una terminal se comunica con una aplicación residente en un "host", ver figura 4.31. Cualquier entidad puede empezar la comunicación de procesos para informar a la otra con algunas señales preliminares. Luego las entidades pueden empezar un proceso de negociación para determinar que capacidades de terminal pueden ser soportadas. La terminal y el host operan mediante sus respectivas terminales virtuales donde ocurren mapeos locales. El vínculo del mapeo selecciona, usa las características y capacidades aceptables a la terminal, y la aplicación.

El proceso de negociación cambia tablas de control en cada una de la entidades de VT, ver figura 4.34. Estas tablas de control determinan como el contenido de la memoria de terminal será mapeada dentro de la pantalla de video. No obstante, a partir de que hay más memoria que puede ser localizada dentro de una pantalla a un mismo tiempo, el vinculo del proceso VT usa la tabla de control para determinar como mapear el contenido de la memoria de video conceptual dentro del video real de la pantalla.

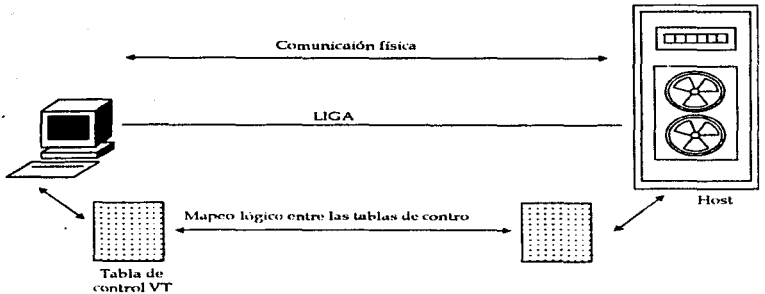


Figura 4.34 Ejemplo de un proceso JTM

El proceso de mapeo es llevado a cabo con el dispositivo objeto. Un dispositivo objeto existe por cada dispositivo real usado en la terminal (teclado, pantalla, impresora, etc.) Otro término usado para describir el video conceptual es el video objeto. Bajo el concepto VT, un video objeto es mapeado por un dispositivo objeto dentro de un video real.

Los estándares VT también usan un control objeto para definir los aspectos físicos del dispositivo, y otras actividades no relacionadas con la manipulación de texto.

Después de que la negociación es completada, las dos entidades podrían ser capaces de comunicarse con el mismo conjunto de servicios VT.

4.3.5.2 Especificaciones ISO (9040 y 9041)

Las especificaciones 9040 y 9041 describen un servicio de terminal virtual de clase básica y un protocolo respectivamente. Ellos describen como las entidades establecen y negocian una terminal virtual para obtener perfiles de servicio, transferencia de datos, control de acceso a las tablas de control de entidades, etc.

Los usuarios de terminales virtuales se comunican entre ellos mediante una área de comunicación conceptual (CCA). Esta área contiene el control de objetos y dispositivos objeto.

El CCA es compartido por los usuarios de terminales virtuales y la información es intercambiada por cualquier usuario VT actualizando y volviendo a poner el servicio disponible para otro usuario.

El control y objetos de dispositivos constan completamente del perfil de un ambiente de terminal virtual (VTE). El tercer tipo objeto es llamado un objeto de despliegue, el cual describe las imágenes de terminal virtual actual.

El objeto de despliegue es de uno, dos o tres arreglos dimensionales de elementos. Las dimensiones son llamadas X, Y y Z, y cada una es capaz de manejar un elemento gráfico "caja de caracteres". Este elemento:

a) Es vaciado: no se asigna nada a este,
b) contiene un atributo primario: un valor que selecciona un elemento gráfico específico;
c) contiene un atributo secundario: un valor el cual selecciona atributos para el objeto de despliegue, tales como el color, intensidad, brillo, fuente, etc.

Para definir un elemento gráfico se usa un conjunto de caracteres codificados de 7 bits (ISO 646) o bien un conjunto de 7 bits y 8 bits (ISO 2022).

4.3.5.3 Conclusiones

La terminal virtual simula una terminal real y resuelve grandes diferencias e incompatibilidades entre la terminal y la aplicación, logrando así una comunicación muy semejante a la que se tendría con la terminal real.

La terminal virtual puede ser modelada de dos maneras por **parámetro** el cual se refiere al modo texto usando códigos y parámetros para definir la terminal y usando **objetos** abstractos para modelar las características y funciones de la terminal.

Los estándares VT pueden definir los aspectos físicos del dispositivo, y otras actividades no solo relacionadas con la manipulación de texto, logrando con ello poder soportar gráficos, ya que el objeto de despliegue es de uno, dos o tres arreglos dimensionales de elementos. Y cada uno es capaz de manejar un elemento gráfico. Cada elemento del arreglo es direccionado por un indicador de despliegue y cada elemento es completamente independiente de otros elementos. Esta es la ventaja fundamental de los servicios de la terminal virtual de OSI con respecto a los del servicio telnet de TCP/IP.

4.4 Principales protocolos de redes IBM y Microsoft

IBM y Microsoft diseñaron los protocolos del **Sistema Básico de Entrada Salida en Red** (NetBIOS: Network Basic Input Output System) y la Interfaz Extendida de Usuario de NetBIOS (NetBEUI: NetBIOS Extended User Interface) para dar soporte a las comunicaciones en entornos de red de área local (de tamaño pequeño y mediano). En la figura 4.35 se muestra el entorno completo del protocolo.

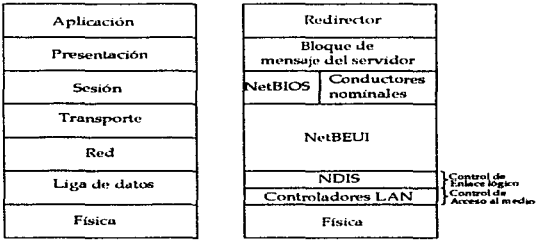


Figura 4.35 Entorno de los protocolos NetBIOS/NetBEUI

4.4.1 Definición de NDIS: Capa de Enlace de Datos

La **Especificación de la Interfaz del Controlador de Red** (NDIS: Network Device Interface Specification) es un conjunto de estándares para Microsoft, OS/2, DOS, entre otros programas que controlan las tarjetas adaptadoras para red.

Se diseño NDIS con el objetivo de proporcionar a los usuarios un acceso simultáneo a distintos protocolos de comunicación, esto se lleva a cabo de manera independiente de las tarjetas de la interfaz de red (NIC: Network Interface Card). En el diseño, los protocolos no necesitan conocer nada sobre la tarjeta de la interfaz. Es decir, no se necesita una interfaz especifica, sólo una interfaz genérica para los protocolos, como se muestra en la figura 4.36. Para utilizar una tarjeta NDIS, se instala la tarjeta y su controlador, se cargan todos los protocolos que se quieran usar y se unen con una orden llamada NETBIND.

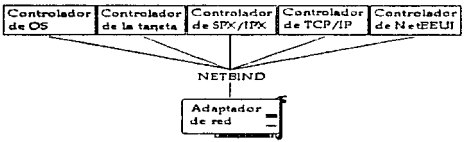


Figura 4.36 Interfaz NDIS

El propósito principal de NDIS es permitir la carga de múltiples pilas de protocolos en un servidor o estación de trabajo, así los usuarios pueden comunicarse con varios protocolos de comunicación de manera simultánea sin la necesidad de llevar a cabo alguna conmutación entre ellos.

La tarjeta adaptadora de red (NIC) es controlada por un programa llamado control de acceso al medio (MAC), el cuál es almacenado en la memoria ROM de la tarjeta de red. Este manejador, es un conjunto de instrucciones que llevan a cabo una seriación de los paquetes de red y los traslada entonces dentro de los espectros eléctricos necesarios para poder hacer la transferencia de datos de las tarjetas adaptadoras de red (Ethernet, token ring o FDDI) hacia el tipo de red correspondiente.

El estándar NDIS es implementado al nivel de la capa de enlace de datos del modelo de referencia OSI. Además, siguiendo las reglas de NDIS, los manejadores de MAC deben cumplir los estándares IEEE 802.3 o 802.5 que se establecen para Ethernet o token ring, respectivamente.

Los protocolos implementados sobre los sistemas operativos para redes de Microsoft, bajo NDIS utilizan manejadores de MAC para comunicarse con la tarjeta adaptadora de red. Los protocolos mismos son los programas o controladores de protocolos que implementan TCP/IP, IPX, XNS, NetBEUI, u otros protocolos de red. Los manejadores de los protocolos operan al mismo nivel de la capa de enlace de datos del modelo OSI (capa 2), pero están un paso arriba de los manejadores de MAC. Los manejadores de protocolo conforman las reglas y convenciones del IEEE 802.2.

En el pasado, las tarjetas adaptadoras de red eran típicamente controladas por un solo programa que contenía tanto al manejador de MAC como el manejador de protocolo. Este tipo de programas era denominado "manejador monolítico". El manejador monolítico consistía en programas rápidos que controlaban el viejo y lento hardware sobre las tarjetas adaptadoras de red antiguas. Conforme las redes llegaron a ser más complejas, y las demandas mayores, en muchas situaciones, los

diseñadores de las redes, deseaban correr múltiples protocolos sobre una sola tarjeta adaptadora de red.

NDIS rompe con el esquema y brinda una mayor flexibilidad y uniformidad a la implantación de manejadores de protocolo y MAC. NDIS a diferencia de los manejadores monolíticos, hace que el manejador de MAC y el manejador de protocolo sean independientes. Además de habilitar un protocolo común para ser utilizado sobre múltiples manejadores de MAC. En la práctica, esto habilita a Microsoft utilizar el manejador de protocolo TCP/IP o un manejador NetBEUI con la misma tarjeta adaptadora de red.

4.4.2 NetBEUI

NetBEUI es un protocolo tanto de nivel de transporte como de red del modelo de protocolo OSI (capas 3 y 4). Se integra con NetBIOS para ofrecer un sistema de comunicaciones eficiente en el entorno LAN de grupos de trabajo. NetBEUI proporciona los servicios de transporte que NetBIOS necesita.

NetBEUI es el protocolo más comúnmente utilizado por las redes Microsoft. Este, soporta las interfaces NetBIOS 1.0 y NetBIOS 3.0 para el uso de estaciones y servidores. NetBIOS provee tres servicios de comunicación primarios: manejo de nombre local, establecimiento de circuito virtual, y comunicación de tipo datagrama.

Los nombres locales son registrados con NetBIOS y proveen un significado para identificar los recursos de la red, usuarios, estaciones, dominios, nombres de computadora, o rutas relativas. El nombre local es utilizado para identificar que recursos son locales y cuales remotos a través de otros servicios de NetBIOS.

Circuitos Virtuales son enlaces de comunicación entre dos nombres de NetBIOS que proveen un modo eficaz de entrega de paquetes. Esto implica que el receptor deberá reconocer la recepción del paquete. Los circuitos virtuales son llamados "sesiones". Cuando una sesión es establecida, los permisos de acceso del usuario son validados por el nombre del servidor de recursos.

Comunicaciones tipo datagrama: este es el significado de transmitir paquetes de datos desde un nombre NetBIOS a otro, sin una garantía de entrega. El manejador de NetBIOS asume que el paquete de tipo datagrama es recibido por la estación destino. Si el paquete no fue recibido, este asume que el software de un diferente nivel más arriba reconocerá que un paquete especifico no fué recibido e iniciará una petición de retransmisión del paquete.

4.4.2.1 Bloques de Control de Red (NCBs)

Los **Bloques de Control de Red** (NCBs: Network Control Blocks) son la unidad básica de comunicación para NetBIOS y son segmentos de memoria asignados a tareas de NetBIOS. NCBs son puntos de transferencia común que habilitan la transferencia de datos y otra información entre, a, y desde las tareas de NetBIOS. La interface de programa de aplicación (API) de Microsoft contiene una descripción detallada de NCBs y su uso. La transferencia de datos alrededor de la red es primeramente ensamblada en bloques de mensajes del servidor (SMBs: Server Messages Blocks) y entonces llenados dentro NCBs para la transmisión actual.

Un aspecto importante de NetBEUI para los diseñadores de redes LAN es su falta de información de enrutamiento al nivel de protocolo de red. Microsoft evita este problema de ruteo en NetBEUI cuando utiliza puentes de encaminamiento fuente (source routing bridges). Después de qué la llamada es hecha a NetBEUI para encontrar un nombre sobre la red, el servidor destino regresa un mensaje de que el nombre es reconocido. Si la estación origen no recibe el mensaje de que el nombre fue reconocido por el servidor destino , NetBEUI lo intentará de nuevo durante un número especifico de veces. Cuando todos los reintentos han sido rechazados, el controlador de NetBEUI, fijará el bit más significativo en el campo de dirección fuente de el paquete y lo reenviará nuevamente. Un puente de ruteo fuente (source routing bridge) reconocerá el paquete como fuente de ruteo, y le adicionará el número de puente (bridge) como información adicional de ruteo, y adelanta el paquete al siguiente puente.

4.4.3 Entendiendo NetBIOS

El **Network Basic Input/Output System** (NetBIOS) es una interfaz de programación de aplicación (API) de alto nivel que fue diseñado para permitir a los programadores construir aplicaciones de red utilizando computadoras personales. NetBIOS fue introducido por IBM en 1984 y adoptado por Microsoft para utilizarse con sus productos de red MS-Net.

NetBIOS se diseño con la premisa de que las PCs en una LAN sólo necesitan comunicarse con otras PCs en la misma LAN.

NetBIOS no es realmente un protocolo; es una interface que provee aplicaciones de red con un conjunto de comandos para establecer sesiones de comunicación, envío y recepción de datos, además de un sistema de nombres de objetos de red. En perspectiva al modelo de referencia OSI, NetBIOS provee una interface a nivel de la capa de sesión. A este nivel NetBIOS provee una transferencia de datos orientada a conexión muy eficaz. Con solo un sistema de nombres para identificar las estaciones que pertenecen a la red. Adicionalmente, NetBIOS provee un

ineficaz servicio de datagrama sin conexión. NetBIOS no provee un servicio de enrutamiento. Sin embargo hace la construcción de interredes que son muy difíciles de realizar.

NetBIOS provee un conjunto de comandos para la asignación y manejo de los nombres de las estaciones sobre la red. En NetBIOS los nombres pueden ser únicos o un nombres de grupo. El anterior nombre es único a través de la red y no puede ser duplicado. Por otro lado un nombre de grupo puede ser utilizado por más de una estación en la red.

Cuando una aplicación desea establecer una conexión a un aplicación remota, esta utiliza el nombre de la estación remota para iniciar la llamada y entonces utiliza la sesión creada para intercambiar datos entre las aplicaciones.

Los comandos de NetBIOS pueden ser divididos cuidadosamente en cuatro categorías, dependiendo de que tipo de servicio proveen a la aplicación de red. Las cuatro categorías de NetBIOS son las siguientes:

- Comandos orientados a datagrama sin conexión.
- Comandos de sesión orientados a conexión.
- Comandos de administración de nombres
- Comandos de servicio general.

Los comandos orientados a datagrama sin conexión habilitan a una aplicación para poder enviar datagramas a estaciones individuales o por broadcast de datagramas hacia todas las estaciones . Utilizando los comandos de datagrama, De otra manera, una aplicación puede también recibir datagramas.

Los comandos de sesión orientados a conexión, habilitan a las aplicaciones para establecer y liberar sesiones de comunicación. Utilizando identificadores (ID's) de sesión, las aplicaciones pueden enviar y recibir mensajes a través de la sesión.

Los comandos de administración de nombres habilitan los nombres únicos y de grupo para su manejo y asignación. Estos nombres son utilizados por otros comandos de NetBIOS para identificar las estaciones sobre la red.

Los comandos de servicio general se utilizan para aquellas aplicaciones que desarrollan funciones que no están asociadas con el manejo de nombres ni comunicación de datos. Por ejemplo, una aplicación puede hacer una petición de información del estado en que se encuentra el adaptador.

4.4.4 Bloque de mensajes del servidor

Proporciona el lenguaje par a par y los formatos necesarios para que las computadoras se comuniquen unas con otras.

4.4.5 Redireccionador

Dirige las peticiones de red a los servidores de la red misma y las órdenes locales al sistema operativo local.

4.5 Principales protocolos de NetWare (Novell)

El conocimiento de los protocolos, representa los mecanismos que permiten a los sistemas de una red hablar unos con otros, es importante este conocimiento para poder entender las redes.

Los protocolos Netware son implementados en base a los mecanismos ODI, este provee la manera de usar los componentes de los protocolos de comunicación de una sistemática para construir la pila de protocolos de comunicación.

A continuación se muestran los protocolos Netware más importantes comparados con el modelo OSI. Ver figura 4.37.

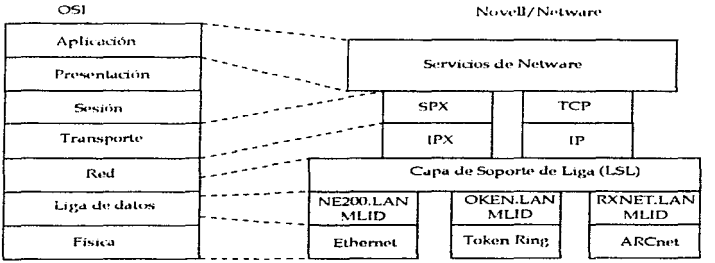


Figura 4.37 Interfaz de Datos Abiertos (ODI)

Se puede observar, que ODI opera en el nivel de enlace de datos mientras que SPX en la capa de transporte e IPX en la de red. Los protocolos mas importantes de Novell Netware son el IPX/SPX

4.5.1 Interfaz de Enlace de Datos Abierta (ODI)

La especificación de **Interfaz de Enlace de Datos Abierta** (ODI: Open Data Interface) describe el conjunto de interfaces y módulos de "software" utilizados para la comunicación desde los protocolos inferiores hasta los superiores.

ODI al igual que NDIS (microsoft), permite a los programas de red local funcionar simultáneamente con múltiples protocolos apilados de comunicación (IPX/SPX, TCP/IP básicamente) de manera independiente al del tipo de estructura de la capa física y las tarjetas de interface de red (NIC) y los detalles de los protocolos superiores.

Los componentes más importantes son:

- Manejador de interfaz de enlace múltiple (MLID: Multiple Link Interface Driver): El MLID es un programa de dispositivo escrito dentro de las especificaciones de ODI que maneja el envío y recepción de paquetes del nivel físico[58]

- Capa de Soporte de Enlace (LSL: Link Support Layer): El LSL es un módulo de software que implementa la interfaz entre "manejadores" (drivers) y las pilas de protocolos. Éste actúa esencialmente como una tarjeta de conmutación, direccionando los paquetes entre los "manejadores" y las pilas de protocolos correspondientes.

Cualquier "manejador" ODI puede comunicarse con cualquier otra pila del protocolo ODI mediante el LSL. El LSL maneja la comunicación entre IPX y los MLIDs. Cuando IPX tiene que transmitir un paquete, éste da el paquete al LSL, con el cual dirige el paquete al MLID apropiado.

4.5.2 Protocolo IPX: Capa de red

IPX es un estándar propietario desarrollado por Novell, derivado del **Protocolo Datagram Internet** (IDP) de Xerox.

El protocolo IPX (Internet Packet Exchange) es un protocolo de capa de red (capa 3 del modelo de referencia OSI), Este provee un servicio sin conexión de pocas conexiones (de datagrama). Este fue hecho para trabajar encima de todos los protocolos de enlace de datos existentes (control token, CSMA/CD y otros).

[58] Cada programa es único debido al "hardware" del adaptador (NIC) y al medio que utiliza, pero ODI elimina la necesidad de escribir cada programa por separado para cada uno de los protocolo de la pila.

El tamaño máximo de datos de un paquete IPX es 546 bytes (esto es sin restar los 8 bytes que utilizan las cabeceras del 802.2 LLC).

La longitud de una dirección física 802.IPX es 10 bytes. Estos 10 bytes de direcciones físicas consisten de los 4 bytes de la dirección de red IPX seguidos de los 6 bytes de la dirección de nodo IPX.

IPX es un protocolo que permite que los paquetes de información sean enviados sobre la red debido a que el IPX si soporta funciones de enrutamiento (a diferencia de su similar NetBEUI el cual no define funciones de enrutamiento en la capa de red). Estos paquetes pueden ser enviados de una máquina a otra o enviarse a todas las estaciones sobre la red (nodos) a través de la función de broadcast (broadcast). Un mensaje enviado por medio de la función de broadcast es usualmente limitado solamente a redes locales.

Otra tarea del protocolo IPX es la fragmentación, la cual se lleva a cabo cuando los paquetes tiene un tamaño muy grande y tienen que viajar a través de otra red donde el tamaño de su MTU es mas pequeña.

El formato de las direcciones IPX es el siguiente:

El campo de dirección de red

Nombre Tamaño (bytes)Descripción

Red2 bytes Dirección de red
Nodo6 bytes Dirección de nodo
Socket2 bytes Número de Socket

Para enviar los datos transportados por el paquete IPX a los procesos, se crea un número único que identifica a cada uno de estos, se trata entonces del número de Socket.

Los campos destino están formados por una dirección de nodo junto con un número de socket que identifican a que máquina y a que proceso va la información contenida en el paquete, de la misma manera los campos fuente identifican de que máquina y de que procesos vienen los paquetes.

Las direcciones destino de un paquete se usan para decidir si el paquete IPX deber ser enviado localmente o enviarse a un enrutador.

Como se mencionó anteriormente el protocolo IPX soporta funciones de enrutamiento, es decir, que el protocolo IPX enruta los paqueles a su destino no importando que no se encuentren sobre la misma subred. La manera como realiza esta tarea el IPX, es enviando un paquete de prueba de ruta, si un enrutador IPX

toma este mensaje entonces regresa una respuesta a la máquina que originó el mensaje, dicha respuesta contiene la dirección del enrutador IPX, finalmente el paquete IPX se envía por esta ruta. Los enrutadores IPX guardan tablas de enrutamiento que se refrescan cada minuto y contienen la información de enrutamiento de las otras subredes que están a su alcance.

Los sockets son dispositivos que permiten una decisión de nodo, si éste actúa sobre un paquete. Este permite correr múltiples programas sobre una PC que usa paquetes IPX. Esto significa, que un paquete de broadcast solamente será recibido por una máquina, si esta tiene un socket abierto para que el paquete este direccionado. Así los paquetes pueden ser ignorados por nodos que no son capaces de aceptarlos. Deberá tenerse especial cuidado para asegurar que dos programas no traten de enviar diferentes tipos de paquetes en el mismo socket.

Las redes IPX pueden soportar paquetes de redes IP (y subredes de cualquier clase), a través de encapsulamiento de datagramas IP dentro de datagramas IPX y asignación de números IP a los hosts sobre una red IPX, las aplicaciones basadas en IP son soportadas en estos hosts. De esta manera, la adición de una compuerta (Gateway) IP de encapsulamiento de paquetes IP dentro de datagramas 802.IPX permitiría a los hosts (hosts) sobre una red IPX comunicarse con la red Internet.

4.5.3 Protocolo SPX: Capa de transporte

El protocolo SPX (Sequenced Packet Exchange) es un protocolo de capa de transporte (encima del protocolo IPX) que provee servicios orientados a conexión.

El SPX es usado cuando se necesita una conexión de circuito virtual entre dos estaciones (emplea circuitos virtuales con identificadores específicos para permitir más de una sesión al mismo tiempo), ofreciendo una conexión orientada en la entrega de paquetes[59]. Este protocolo tiene el control de flujo y la secuencia, para asegurar que los paquetes lleguen en el orden correcto.

El SPX enlaza a IPX para proveer un mecanismo de entrega segura, que incluye una retransmisión en el caso de falla, usando un algoritmo de conteo de tiempo o temporizador (timing)[60] para decir cuando un paquete necesita ser retransmitido.

Como SPX es un protocolo orientado a conexión, guarda la secuencia de los paquetes, por lo tanto estos llegan en el orden correcto y de esta manera se evita que los datos sean duplicados.

---

[59] El SPX envía paquetes de control para establecer una conexión al igual que cuando la transmisión termina, además asegura que los nodos destino no se sobrecarguen con los datos que están llegando rápidamente.

[60] El temporizador es ajustado dinámicamente basado en un retardo de la transmisión de paquete.

CAPÍTULO 5
DISPOSITIVOS DE INTERCONEXIÓN DE REDES

5.1 Introducción

Varios eventos interesantes han tenido impacto en el trabajo del manejo de la red o diseño de esta en los últimos años. Primero, la proliferación de computadoras personales a incrementado el crecimiento del número de estaciones conectadas en una LAN. Segundo, el surgimiento de un gran número instituciones a forzado a los sistema a crecer. Tercero, en un desarrollo que tiene relación con los dos primeros, hay una necesidad para conectar redes en diferentes áreas geográficas. Este requerimiento adiciona otra variable para el diseño - la facilidad en la transmisión en Redes de Área Amplia (WAN).

En muchos casos las redes locales no son entidades aisladas. Una institución puede tener más de un tipo de red local en un sitio dado para satisfacer sus múltiples necesidades. Una Institución puede tener varias redes locales en varios sitios que necesitan ser interconectados para realizar un control centralizado o un intercambio distribuido de información.

Un conjunto de redes interconectadas desde el punto de vista de los usuarios puede parecer simplemente una conexión de red mas grande. Sin embargo, si cada una de las redes que constituyen la estructura retienen su identidad y mecanismos de comunicación especiales, los cuales son necesarios para comunicarse cruzando múltiples redes, entonces la configuración entera es frecuentemente referida como "interred" (internet) y cada una de las redes que la constituyen, como una subred.

Cada una de las subredes que constituyen una interred soporta comunicaciones entre los dispositivos unidos a esas subredes; estos dispositivos son referidos como "Sistemas Finales"[61] (ES). En adición, las subredes son conectadas por medio de dispositivos referidos en documentos ISO como "Sistemas Intermedios"[62] (IS). Los sistemas intermedios proveen una ruta de comunicaciones y desarrollan la transferencia necesaria y funciones de enrutamiento, de esta manera los datos pueden ser intercambiados entre dispositivos conectados a diferentes subredes en la interred.

[61] Sistema Final (ES, End System): Es un dispositivo conectado a una de las subredes de una interred que es usada para soportar aplicaciones o servicios de los usuarios finales.
[62] Sistema Intermedio (IS, Intermediate System): Es un dispositivo usado para conectar dos subredes y permite la comunicación entre sistemas finales conectadas a diferentes subredes.

A continuación se examinarán los dispositivos que permiten la interconexión de subredes y como se desempeñan respecto a los protocolos del modelo OSI.

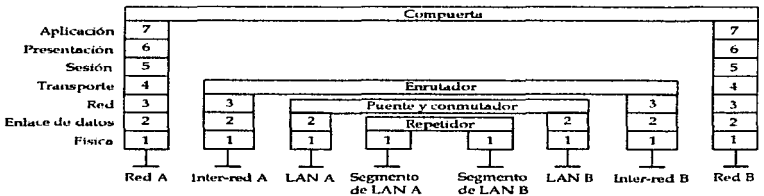


Figura 5.1 Nivel de funcionalidad de los dispositivos de interconexión de redes respecto al modelo de referencia OSI

5.1.1 Interconexión entre redes

Generalmente, las necesidad o las razones por las que se debe utilizar dispositivos para interconectar una LAN con otra, caen dentro de una de las tres categorías siguientes: para crecimiento, para tener mayor control o administración y requerimientos para conectarse a una red WAN.

A continuación se describirán las principales características de los dispositivos esenciales para la construcción e interconexión de las redes locales.

5.2 Repetidores

Un repetidor representa el tipo mas simple de dispositivo desde el punto de vista de diseño, operación y funcionalidad. Este dispositivo opera en la capa física del modelo OSI, regenerando la señal recibida de un segmento de red y retransmite la señal a otro segmento. En la figura 5.2 ilustra la operación del repetidor con respecto al modelo OSI.

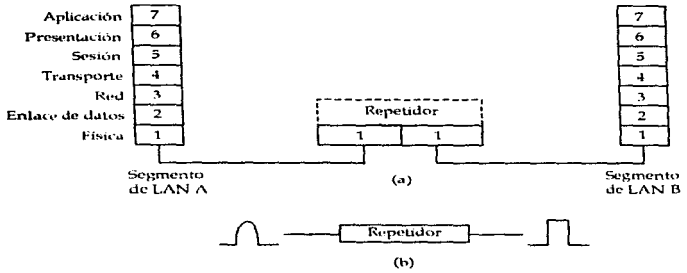


Figura 5.2 Repetidor:
a). Opera en la capa física del modelo OSI. b). Regenera la señal

5.2.1 Tipos de repetidores

Hay dos tipos básicos de repetidores. Un repetidor eléctrico simplemente recibe una señal eléctrica y entonces regenera la señal. Durante el proceso de la regeneración de una señal, una nueva señal es formada con las mismas características originales de la señal recibida. Este proceso se ilustra en la figura 1. Para transmitir una nueva señal, el repetidor quita cualquier atenuación y distorsión previa, permitiendo una excepción en la distancia permisible de transmisión. Aunque varios segmentos de la red pueden ser interconectados con el uso de repetidores para extender la cobertura de la red, hay limitaciones para la regeneración de la señal en una LAN. Por ejemplo, en una red Ethernet con cable coaxial de 50 ohms soporta una distancia máxima de 2.8 Km. y esta distancia no puede ser extendida mas allá por medio del uso de repetidores.

El segundo tipo de repetidor es comúnmente usado en dispositivos eléctrico-óptico. Este tipo de repetidor convierte una señal eléctrica en una señal óptica para transmitirse y desempeña la función contraria cuando revise una señal de luz. Al igual que un repetidor eléctrico, el repetidor eléctrico-óptico extiende la distancia que una señal puede llevarse sobre una red.

Un repetidor esta restringido para operar en la capa física del Modelo OSI, este trasmite un flujo de datos. Esto restringe el uso de un repetidor para unir redes idénticas o segmentos de la misma red. Por ejemplo, se puede usar un repetidor para conectar dos segmentos de redes Ethernet o dos segmentos de redes Token

Ring, pero no se pueden unir un segmento de red Ethernet con un segmento de red Token Ring.

5.2.2 Utilización de los repetidores

En la figura 5.3 ilustra dos ejemplos del uso de repetidores. En la parte superior de la figura 5.3 ilustra el uso de un repetidor para conectar dos segmentos de red local Ethernet tipo bus, cada segmento de red atiende a diferentes departamentos. En esta situación todos los mensajes de un segmento de red local son pasados a la otra, sin considerar su destino. El uso de repetidores de esta manera aumenta el trafico sobre los dos segmentos de red. Si se implementan sin considerar el flujo de trafico y los niveles de utilización sobre cada red, un problema de desempeño puede resultar cuando las redes separadas son interconectadas a través de repetidores.

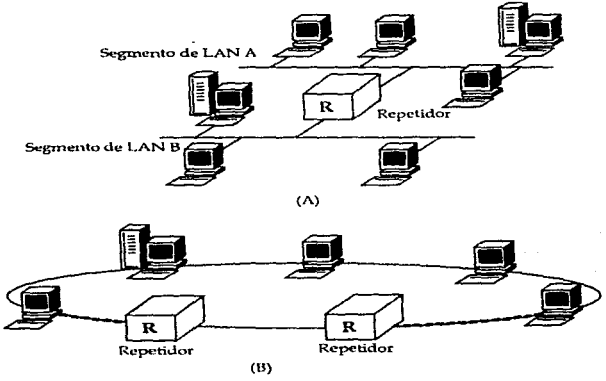


Figura 5.3 Uso de repetidores. Un repetidor puede ser usado para interconectar redes de área local y extender la distancia de transmisión de un LAN

En la parte inferior de la figura 5.3 un par de repetidores son usados para conectar dos unidades de acceso multi-estación (MSAUs: Multi-Station Access Units) usados para formar una red tipo Token Ring. En este ejemplo a diferencia de redes Ethernet, el repetidor simplemente permite la colocación de los MSAUs a distancias mas amplias y regenera las señales que fluyen sobre la red. El uso de los repetidores de esta manera no agrega mas tráfico a la red.

5.3 Puentes (Bridges)

En comparación con los repetidores que carecen de inteligencia y están restringidos a unir segmentos de un mismo tipo, los puentes (bridges) son dispositivos inteligentes que pueden conectar redes similares o distintas.

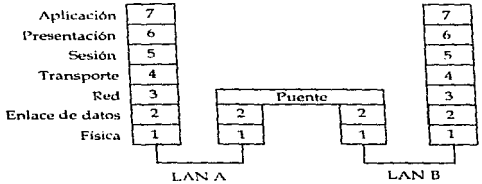


Figura 5.4 Un puente opera en la capa de enlace de datos del modelo de referencia OSI

5.3.1 Funciones de un puente

La función de los puentes es la de conectar dos redes separadas (segmentos de la red) para formar una sola red lógica de composición más compleja. La redes originalmente llegan a ser entonces segmentos de red que dan como resultado una red más compleja, la cuál funciona como si fuese un solo cable o un dominio de broadcast . El uso de puentes[63] resuelve algunas limitaciones que tienen las arquitecturas de los estándares IEEE para redes locales, como son:

1. Número limitado de estaciones que una sola red local conecta.
2. El Tamaño de área geográfica que abarca es limitado.
3. Cantidad de tráfico que soporta es limitado (causando cuellos de botella).

[63] Aun que los repetidores también conectan dos segmentos de red, los repetidores son utilizados para resolver las limitaciones eléctricas de la salida de los circuitos de la interface física de un segmento.

Cada una de los segmentos (redes) que un puente conecta no necesariamente deben ser del mismo tipo lo que con lleva varios factores que un puente debe resolver:

- Los diferentes tipos de redes LAN utilizan un formato de paquete diferente.
- Las redes o segmentos conectados no funcionan necesariamente a la misma velocidad, además de que cada norma IEEE permite varias tasas de transmisión.
- Además de que debe resolver los diferentes problemas posibles de los métodos de control de acceso al medio con las diferentes combinaciones de interconexión de las redes locales que el puente conecte.

		Segmento red local destino		
		802.3	802.4	802.5
Segmento red local	802.3	-	1,4	1,2,4,8
Fuente	802.4	1,5,9,8,10	9	1,2,3,8,9,10
	802.5	1,2,5,6,7,10	1,2,3,6,7	6,7

Acciones:
1. Llevar a cabo un reformateo de la trama y calcular el nuevo código de redundancia.
2. Invertir el orden de los bits.
3. Copiar la prioridad, sea o no sea significativa.
4. Generar una prioridad ficticia.
5. Desechar la prioridad.
6. Purgar el anillo (de alguna manera).
7. Poner los bits A y C (de manera inventada).
8. Preocuparse por la congestión (de una red LAN rápida a una red LAN lenta)
9. Preocuparse por qué el intercambio de testigo de ACK sea retardado o imposible.
10. Pánico si la trama resulta demasiado larga para la red LAN de destino.

Tabla 5.1 Trata de los problemas encontrados en dos redes tipo LAN (segmentos) conectadas a través de un puente.

Los puentes trabajan en el nivel de capa de enlace de datos (capa 2 del modelo de referencia OSI). Por lo que solo pueden ver las direcciones MAC de los paquetes. De esta manera aíslan el mecanismo de control de acceso al medio de los segmentos que el puente conecta. Con esto se puede decir que las colisiones de un segmento red Ethernet con CSMA/CD no se propagan mas allá del puente hacia la otro segmento de red y en el caso de un segmento token ring conectado por un puente, la señal token no cruza hacia el otro lado del puente.

Con un puente, solo los paquetes (frames) que tienen la dirección destino a un servidor sobre un segmento diferente serán redireccionados o retransmitidos a través del puente (trafico remoto). Los paquetes que tienen como dirección destino un servidor que se encuentra en el mismo segmento de red no son retransmitidos o redireccionados hacia otro segmento de la red. De esta manera el trafico local no sobrecarga otros segmentos de la red local lógica.

Con lo anterior se puede observar que los puentes son dispositivos que llevan a cabo una selección de los paquetes de datos que deben ser retransmitidos o redirigidos hacia el otro segmento que el puente conecta lo que ayuda a resolver problemas del tipo cuello de botella.

Para llevar a cabo la selección, los puentes examinan las direcciones MAC[84] origen y destino del encabezado de control del acceso al medio (MAC) dentro del paquete de datos transmitido. Todos los paquetes recibidos desde un segmento y que deberán ser redireccionados son almacenados y verificados de error antes de que sean repetidos hacia el otro segmento (repeated/forwarded). El almacenamiento de frames tiene ventajas y desventajas relativas a los repetidores.

Ventajas:

- Separación de cualquier restricción asociada con la función de interconexión significa que el número total de estaciones conectadas y el número de segmentos realizados en la red LAN pueden ser fácilmente incrementados. Esto es particularmente importante cuando se construyen amplias redes LAN distribuidas sobre amplias áreas geográficas.
- El almacenar los frames recibidos desde un segmento antes de retransmitirlos (forwarding) sobre otro segmento es una gran ventaja ya que significa que los dos segmentos interconectados pueden operar con diferentes protocolos de Control de Acceso al Medio. De esta manera el puente puede crear fácilmente una red LAN que sea una mezcla de diferentes tipos básicos de redes LAN y formar redes mas complejas.
- Los puentes desarrollan sus funciones de retransmisión (relaying) basadas solamente sobre subdirecciones MAC dentro de un frame con el efecto de que ellos sean transparentes a los protocolos utilizados por las capas superiores en la pila de protocolos. Esto significa que los puentes pueden ser utilizados con redes LAN que soportan diferentes pilas de protocolo en las capas superiores (NetBEUI, IPX/SPX TCP/IP, etc.).
- Los puentes permiten tener un mejor y sencillo manejo de administración de redes locales grandes además de que pueden ser monitoreadas por medio de la red misma. También pueden incorporarse mecanismos de acceso de control para improvisar seguridad en la red. Además de que la configuración operacional de la red puede ser modificada dinámicamente por medio de control de estado a través del manejo individual de los puertos del puente.
- Los puentes particionan una red LAN dentro de pequeños segmentos que improvisan sobre todo eficiencia y eficacia de toda la red total.

[84] Las direcciones MAC corresponden a las direcciones del nivel 2 (enlace de datos) del modelo OSI y representan la dirección física de la estación ya que es la dirección de la tarjeta de red (para mayor información referirse al estándar 802.1 referente al Sistema de direcciones del IEEE 802 en el capitulo 3 de este trabajo). La dirección MAC es única para cada estación, además de que cada puerto de un puente tiene también una dirección MAC.

Desventajas:

- Desde que un puente recibe y almacena todos los frames completamente antes de desarrollar la función de retransmisión (forwarding), esto introduce un retraso de tiempo correspondiente al almacenamiento y retransmisión comparado con los repetidores.
- No existe la realización de control de flujo en el nivel de la subcapa MAC y de aquí que los puentes puedan llegar a sobrecargarse durante períodos de mayor tráfico; esto es, un puente puede necesitar almacenar mas frames (previo a retransmitir los frames sobre cada segmento de salida) que pueden sobre pasar el espacio de memoria libre que el puente tiene disponible.
- Llevar a cabo la operación de conexión de segmentos con diferentes protocolos de subcapa MAC, significa que los contenidos de los frames recibidos deberán ser previamente modificados por el puente hacia los diferentes formatos de frame antes de ser retransmitidos. Además de tener la necesidad de llevar a cabo una nueva verificación de secuencia generada por cada puente.

5.3.2 Clases de puentes

Las redes locales pueden llegar a ser grandes en tamaño por el número de segmentos que se conectan a través de puentes, por lo que el organismo IEEE llevó a cabo un planteamiento para el diseño de puentes.

Los tres tipos de puentes mas utilizados son: los **puentes transparentes** también conocidos como **puentes de árbol expandido** (por el algoritmo spanning tree) el cual enlaza segmentos de tipo bus únicamente, los **puentes de encaminamiento fuente** (por el algoritmo source routing) que enlaza segmentos de tipo anillo, y los puentes **transparente de encaminamiento fuente**, que enlaza tanto segmentos tipo bus como anillo. La principal diferencia entre los dos primeros es el tipo de segmentos que enlazan y el algoritmo de encaminamiento que utilizan. Mientras que el tercero puede enlazar los dos tipos de segmentos a través de realizar una traducción de algoritmos.

Los puentes transparentes son aquellos que realizan todas las decisiones de ruteo, mientras que en los puentes encaminamiento fuente, las estaciones finales desarrollan la función de encontrar la mejor ruta (route-finding). Actualmente la norma 802.1D (algoritmo de árbol de expansión) es el estándar internacional relacionado a los puentes transparentes a diferencia del algoritmo source routing el cuál forma parte de el estándar para redes Token Ring 802.5 (el estándar de interconexión para segmentos token ring).

5.3.2.1 Puentes Transparentes (Transparent Bridges)

Un puente transparente actúa de manera que acepta y almacena todos los paquetes transmitidos a todos los segmentos de red a los cuales esta conectado (modo promiscuo). Cuando llega un paquete al puente, este debe decidir si lo desecha o lo redirige, debiendo saber hacia que segmento redirigirá el paquete. Esta decisión se toma a partir de la búsqueda de la dirección destino dentro de una tabla de direcciones que contiene el puente.

Cuando se conecta un puente por primera vez a una red, todas sus tablas se encuentran vacías. Por lo que el puente utiliza el algoritmo de inundación (flodding) y el algoritmo de aprendizaje hacia atrás como se explica a continuación: Como se mencionó anteriormente los puentes funcionan de manera promiscua, por lo que examinan todos los paquetes que se transmiten por los segmentos que conectan. Al ver la dirección de la estación origen y por que segmento entró el paquete, de esta forma actualiza su tabla de direcciones escribiendo que estación es accesible a través de que segmento. Para la dirección de la estación destino cada paquete de entrada se retransmite a todos los segmentos que conecta el puente con excepción del segmento por el que llegó.

Para permitir cambios en la topología de la red LAN[65], cada entrada en la tabla de direcciones tiene asociado una hora de llegada del paquete (aging timer), cada vez que llega un paquete procedente de una máquina que ya se encuentra en la tabla, su tiempo asociado a la dirección es actualizado (por lo que la hora asociada indica la ultima vez que se examinó un paquete de la estación en cuestión). Periódicamente un proceso llevado a cabo en el puente revisa las entradas en la tabla y elimina las entradas que tienen un tiempo mayor al tiempo de expiración. Este algoritmo hace notar que si una estación permanece callada durante algunos minutos, los paquetes que se le envíen tendrán que retransmitirse por medio de inundación hasta que vuelva a transmitir un paquete (frame).

El proceso de encaminamiento para un paquete de entrada en un puente depende del segmento donde se encuentren las estaciones transmisora y receptora, y se realiza de la siguiente manera:

- Si las direcciones de las estaciones origen y destino pertenecen al mismo segmento, el paquete es desechado por el puente.
- Si las direcciones de las estaciones origen y destino son de diferente segmento, retransmite el paquete hacia el segmento indicado por sus tablas.
- Si desconoce el segmento de salida, utiliza el método de inundación.

[65] La topología de la red LAN puede estar constantemente en cambio a medida que las estaciones y los puentes se activen, se desactiven o se muevan de un lugar a otro.

5.3.2.1.1 Algoritmo de árbol expandido (Spanning Tree Algorithm)

El **algoritmo de árbol expandido** (STA: spanning tree algorithm) fue desarrollado por DEC y adoptado como un estándar por el comité 802.1. El algoritmo de árbol expandido es un método de encaminamiento de redes múltiples donde mas de una ruta puede existir para conectar un segmento de la red con otro (ciclos o loops). Este algoritmo es utilizado para conectar segmentos con topología de bus.

En topologías simples es fácil garantizar la existencia de solo una ruta entre dos dispositivos. Pero como el número de conexiones incrementa o la interconexión de redes llega a ser más compleja, la probabilidad de que se creen múltiples rutas lógicas intencionales entre dispositivos (conocidos como ciclos activos "active loops") incrementan drásticamente.

Ciclos activos pueden ser un grave problema para redes basadas en puentes. Por que los ciclos activos producen innecesarios e indefinida duplicación de paquetes, ellos pueden causar exceso de tráfico que degrada todo el desempeño y hace que algunos protocolos simplemente paren de trabajar.

Para eliminar rutas redundantes e ineficientes (ciclos o loops activos) para redes que utilicen puentes transparentes el algoritmo de árbol expandido hace que los puentes se comuniquen entre sí y recubran la topología real por medio de un árbol de expansión que alcance todos los segmentos de la red LAN lógica.

Cabe mencionar que con un árbol expandido solo existe una trayectoria desde cada origen a su respectivo destino, se eliminan las rutas redundantes ineficaces.

Bajo el algoritmo de árbol expandido (STA), cada puente tiene un identificador que consiste de un campo de prioridad y una "dirección de la estación instalada por el fabricante".

Para formar el árbol, cada vez que transcurre un cierto tiempo, cada puente difunde su identidad y la lista de todos los demás puentes que reconoce están sobre los mismos segmentos que el puente en cuestión. En base a la información anterior, todos los puentes que forman la red lógica negocian entre si para determinar primeramente un puente raíz (bridge root). Este puente raíz es seleccionado con la base de tener el valor más alto de prioridad (si dos puentes tienen el mismo valor de prioridad, el que tenga el menor número de dirección de estación es seleccionado como el puente raíz). Mientras este proceso se realiza automáticamente, el administrador de la red puede fijar los resultados al dar a un puente el valor de mas alta prioridad.

Después de que el puente raíz ha sido seleccionado, cada puente restante determina cuál de sus puertos es el que tiene la ruta mas corta hacia el puente raíz, determinando a este puerto como puerto raíz (root port).

Después todos los puentes que forman la red lógica negocian entre si para determinar que ruta deberán tomar los datos y así formar el árbol de expansión.

Si más de un puente es unido a un mismo segmento, un solo puerto es seleccionado basándose en el que ofrezca el menor costo (el criterio es establecido por el administrador de red. El costo puede incluir elementos tales como velocidad de la línea y capacidad de almacenamiento (buffer capacity) etc .

Después de la designación de los puertos raíz y la negociación entre todos los puentes restantes se tiene como resultado el establecimiento de una ruta única entre cada uno de los segmentos y la raíz, por lo tanto a todos los demás segmentos. Aunque el árbol cubre todos los segmentos de la red LAN, no es necesario que todos los puentes participen en el árbol , esto con el objeto de evitar rutas redundantes ineficaces.

Una vez que todas las negociaciones han tomado lugar, cada puente establece a su puerto raíz en un estado de retransmisión para mover datos hacia el puente raíz. Otros puertos del puente son bloqueados para que de esta manera los paquetes no puedan viajar a través de ellos. El algoritmo de árbol expandido asegura que solo la ruta más eficiente sea disponible para cada puente.

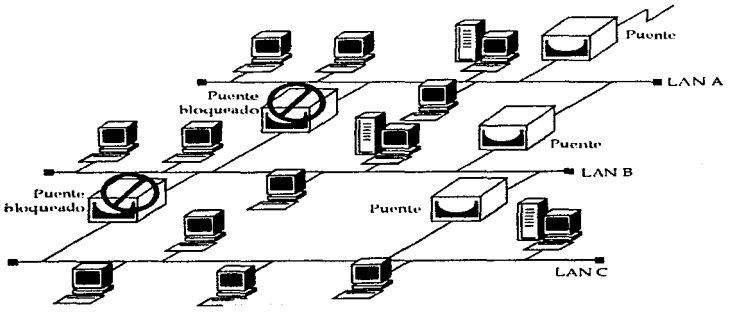


Figura 3.5 Ejemplo de puentes transparentes usando el método de árbol expandido

Los puertos que han sido bloqueado son puestos en modo de aprendizaje (learning mode), de esta manera pueden examinar el flujo de paquetes sobre la red y así actualizar su tabla de direcciones de la red.

Aun cuando el árbol de expansión haya sido establecido, el algoritmo continua funcionando para que de manera automática detecte los cambios de topología y de esta forma actualice el árbol. Es decir, si la ruta única llegara a fallar por cualquier razón (tal como falla en un cable), los puentes que participan en el STA automáticamente activan un puerto específico en estado bloqueado para que de esta manera se cree otra ruta y un nuevo árbol de expansión. El puerto anteriormente bloqueado entonces cambia a un modo de retransmisión y envía una notificación de su cambio a el puente raíz. El puente raíz se encarga de notificar a todos los puentes de la red para que actualicen sus bases de datos para que incluyan este nuevo puerto puente.

Para llevar a cabo los pasos anteriormente mencionados se requiere que los puentes intercambien información. Esta información es intercambiada en forma de **unidades de datos protocolo de puente** (BPDUs: bridge protocol data units). Un BPDU transmitido por un puente es direccionado hacia/y-recibido por todos los demás puentes sobre la misma red LAN. Cada BPDU contiene la siguiente información:

- El identificador de este puente y el puerto sobre el puente en cuestión.
- El identificador del puente, que el puente en cuestión considera para que sea puente raíz.
- El costo de ruta mínimo para este puente.

5.3.2.2 Puentes de encaminamiento fuente y el algoritmo de encaminamiento fuente (source routing 802.5)

Este método fue adoptado primeramente por IBM para conectar puentes a sus redes Token Ring. El algoritmo de **encaminamiento fuente** (source routing) en su forma elemental, supone que cada estación emisora de un paquete conoce si la estación receptora del paquete se encuentra localizada en el mismo segmento o en otro segmento de la red LAN.

Cuando el destino se encuentra en otro segmento, la estación emisora incluye en la cabecera del paquete la información de la ruta de encaminamiento que el paquete deberá seguir para llegar a la estación receptora.

Cada paquete que se transmita a otro segmento de la red incluye un campo de información de ruta (RI, route información), este campo esta presente siempre y

cuando el bit I/G de la dirección fuente tenga el valor de 1 (lo que indica a los puentes que se debe desarrollar un encaminamiento adicional).[66]

Los puentes de encaminamiento fuente solamente se interesan en aquellos paquetes que tienen el bit RII con valor de 1. Cada uno de estos paquetes es examinado por los puentes buscando en él, el número del segmento de red por el que llegó y si este número de segmento es seguido por su número de identificación de puente entonces el puente retransmite el paquete por el segmento de red cuyo número es el siguiente la información de encaminamiento.

En el diseño del algoritmo de encaminamiento fuente (source routing) esta implícito el hecho de que cada estación que conforma la red lógica conoce la ruta exacta de cada una de las otras máquinas que están conectadas. La manera en que cada máquina conoce estos destinos es: si una máquina desconoce la ruta del extremo receptor, esta máquina fuente emite un paquete de broadcast preguntando donde se encuentra el receptor. Todos los puentes copian este paquete de descubrimiento de tal manera que este paquete llega a todos los segmentos de la red lógica. Cuando regresa la respuesta, los puentes registran su identidad en el paquete, de tal manera que el emisor original puede ver con exactitud la ruta tomada y finalmente tomar la mejor opción. Una vez que una máquina ha descubierto un encaminamiento para un destino en particular, lo almacena en una memoria temporal, para que el proceso de descubrimiento no se tenga que llevar a cabo nuevamente. Este algoritmo de encaminamiento impone cierta carga administrativa a cada una de las estaciones por lo que el algoritmo no llega a ser completamente transparente.

Característica	Puente Transparente	Puente de encaminamiento fuente
Orientacion	Sin conexión	Orientado a conexión
Transparencia	Totalmente transparente	No transparente
Configuracion	Automático	Manual
Encaminamiento	Subóptimizado	Optimo
Localización	Aprendizaje hacia atrás	paquetes de descubrimiento o investigación
Fallos	Manejo por los puentes	Manejo por las estaciones
Complejidad	En los puentes	En las estaciones

Tabla 5.2 Comparación entre puentes transparentes y de encaminamiento fuente (source routing):

[66] El bit I/G también es llamado **bit indicador de información de ruta** (RII: routing information indicator). Los campos dentro de la cabecera del paquete que contienen la ruta de encaminamiento son llamados campos de **ruta designada** (RD: routing designator).

5.3.2.3 Puente Transparente de encaminamiento fuente (SRT) o traductor

Un puente transparente de encaminamiento fuente (SRT: source routing transparent) es eficaz para direccionar frames entre segmentos de bus y anillo.

Mientras el estándar de **puente transparente** es disponible sobre varios productos que soportan las normas IEEE 802.3 y 802.4, el estándar de puentes enrutamiento fuente es disponible para productos que soportan el estándar 802.5. Mientras que ambos productos tienen ventajas y desventajas, el problema principal con los dos es que son incompatibles. Es decir, no se puede llevar a cabo la interconexión de redes LAN's por medio de combinar puentes transparentes y puentes tipo encaminamiento fuente. Para este caso se ha desarrollado un nuevo estándar que ha sido desarrollado por el comité 802.5, referido así como una técnica de puenteo **transparente de encaminamiento fuente** (SRT: source routing transparent).

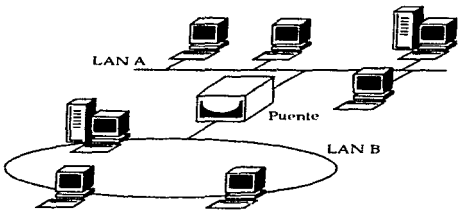


Figura 5.6 Operación de puente traductor. Un puente traductor conecta redes de área local que emplean diferentes protocolos en la capa de enlace de datos.

El principio de operación de un puente SRT es basado en el valor del bit RII en el campo de dirección fuente del encabezado MAC. Los valores de este bit indican si se desea llevar a cabo un encaminamiento por parte del puente o no. Cuando un puente transmisor fija el valor de 1 en el bit RII: indica que desea que se realice un encaminamiento. Si el bit RII es igual a 0 indica que no se debe realizar encaminamiento alguno. Esta característica del bit RII es debido a que este bit no es utilizado por estaciones que son soportadas por puentes transparentes. Como su nombre implica, la entrada del puente transparente, el manejo de encaminamiento es de manera transparente a la estación terminal. De esta manera el bit RII es siempre fijado en un valor de cero por una estación que no participa en el encaminamiento fuente.

Todos los paquetes (frames) que son transmitidos son examinados por el puente SRT. De esta manera si el bit RII tiene el valor 1, entonces el paquete (frame) es manejado por medio de la lógica de encaminamiento fuente; si el bit RII tiene un valor de 0, entonces el frame es manejado por lógica de puente transparente.

Para llevar a cabo la interconexión de redes LAN con topologías en bus y anillo se hace por medio de puentes STR. Para redes tipo bus se hace un puenteo transparente, para lo cuál el algoritmo de árbol expandido debe ser desarrollado entre todos los puentes. Para los segmentos de tipo anillo que utilizan algoritmo encaminamiento fuente, un algoritmo de árbol expandido también será desarrollado (dentro de la interconexión de topologías). Los requerimientos para la operación SRT es que el puente deberá permitir que estaciones de encaminamiento fuente y estaciones transparentes participen dentro del mismo algoritmo de árbol expandido.

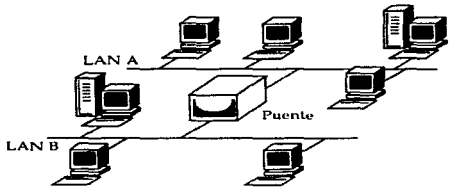
Con la observación anterior y partiendo de que el puente SRT incluye lógica de puenteo transparente, los puentes SRT pueden interoperar dentro de una estructura compuesta solo por puentes transparentes para crear un árbol expandido y llevar a cabo el algoritmo de árbol expandido. De esta manera, se puede tener una red LAN que mezcle puentes transparentes y puentes SRT. Sin embargo, una estructura compuesta por puentes que desarrollan encaminamiento fuente (802.5) no pueden ser incorporados dentro de tal configuración de interconexión de topologías, ya que son incapaces de pasar frames de tipo transparente o árbol expandido.

Cabe mencionar que con la proliferación de redes multiprotocolo y la necesidad de correr ambos tipos de aplicaciones de puenteo, es deseable considerar el uso de puentes SRT en cualquier nueva instalación Token Ring.

5.3.3 Resumen

Las funciones que realiza un puente se describen en la figura 5.7 y son resumidas a continuación:

- El puente lee todos los frames transmitidos en la red A
- Los frames con direcciones de destino sobre la red A se mantiene sobre la misma red
- Los frames con direcciones de destino sobre la red B son quitados de la red A y retransmitidos a la red B.
- El puente mantiene el trafico local, tanto de la red A como de la red B



(b)

Figura 5.7 Un puente conecta a dos redes de área local o segmentos de red en la capa de enlace de datos

5.3.3.1 Características

La funcionalidad de un puente se basa en las características incorporadas en el dispositivo. Se listan las 11 mejores características del puente que definen tanto la funcionalidad como el nivel de desempeño de un puente.

- Proporciona Filtrado y Reenvío
- Capacidad selectiva de Reenvío
- Soporta múltiple puertos
- Soporta interfaces para redes de área amplía
- Soporta varias interfaces de medios de transmisión para redes locales
- Operación transparente en la capa de enlace de datos
- Operaciones de traducción para unir redes distintas
- Operaciones de encapsulamiento para soportar el uso de redes de área amplia
- Se fabrican como adaptadores para computadoras y como dispositivos separados
- Auto-aprendizaje de enrutamiento, creación de tablas (en puentes transparentes)
- Encaminamiento fuente

Como nota final sobre la tecnología basada en puentes, es que esta es similar a, y muy frecuentemente confundida con la tecnología de conmutación. Donde la acción de conmutación se refiere usualmente a puenteo de alta velocidad. Pero cabe mencionar que existen importantes diferencias entre dispositivos de puenteo y dispositivos de conmutación.

5.4 Conmutadores (switch)

Un conmutador constituye un concepto relativamente nuevo, que aprovecha la topología en estrella y los diseños de concentradores para reducir la contención del canal sobre los segmentos de la red. Esto se efectúa a través de las técnicas de conmutación[67]. La tecnología de conmutación realiza una multi-segmentación de las redes locales. Esta tecnología opera en la capa 2 (capa de enlace de datos) del modelo de referencia OSI.

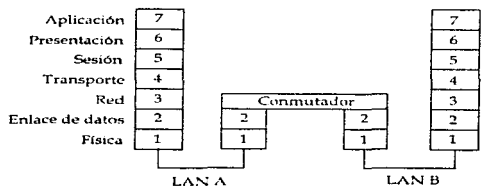


Figura 5.8 La tecnología de conmutación opera en la capa 2 del modelo de referencia OSI, capa de enlace

Si se estudia la conmutación con más detalle, en el caso hipotético de disponer de una red que se encuentra paralizada debido a un tráfico excesivo por el crecimiento del número de usuarios, es posible dividir la red en dos segmentos, con lo que se reduce la carga de tráfico de cada segmento a la mitad. Esta técnica asume que pueden mantenerse a todos los usuarios que habitualmente se comunican dentro del mismo segmento, reduciéndose de este modo la cantidad de tráfico que necesita atravesar el dispositivo de conexión de la red local. Si el tráfico continua siendo un problema, se podrá dividir la red en cuatro o seis segmentos, y así sucesivamente. Un conmutador realiza exactamente este tipo de segmentación, disponiendo de un cierto número de puertos. El conmutador manipula el tráfico entre las estaciones de trabajo de cada segmento, generándose así menor tráfico y contención por el canal de transferencia. Si una estación situada en un segmento necesita comunicarse con un servidor u estación de otro segmento, el dispositivo de conmutación actúa como puente y establece un circuito temporal entre los segmentos. Sin embargo, esta función de conmutación es superior a la efectuada por un puente normal, puesto que el retardo en el almacenamiento y reenvío se eliminan gracias al circuito directo entre los dispositivos.

[67] No se debe confundir con la conmutacion de puertos, la cuál consiste en una función de administración mediante la cual un administrador mueve una estación de trabajo de un segmento a otro a través de una aplicacion de administración.

Funcionalmente, los conmutadores son similares a los puentes pero hay que tener en cuenta que los conmutadores proveen un desempeño mucho mayor. Generalmente los conmutadores se diferencian de los puentes y enrutadores en los siguientes aspectos:

- Funcionamiento más simple.
- Agrega un mayor ancho de banda.
- Mucho menor tiempo de latencia (para conmutadores de arquitectura cut-through).

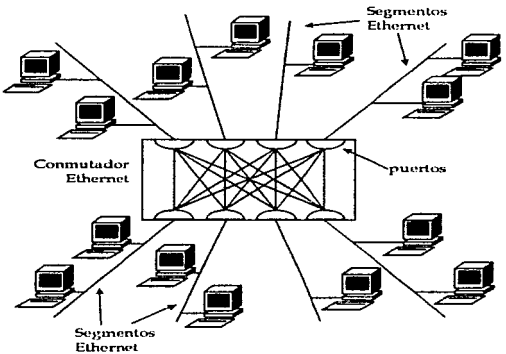


Figura 5.9 Ejemplo de una red ethernet conmutada

La primera diferencia de los conmutadores es el esquema de reenvío basado en hardware, opuesto al mecanismo de software usado en un puente y enrutador típicos, los conmutadores interconectan un gran número de puertos moviendo datos entre estos enteramente por lógica electrónica (microprocesadores y software no participan básicamente en el movimiento de datos). Los procedimientos de conmutación pueden ser encapsulados enteramente dentro de circuitos integrados de aplicaciones específicas (ASICs). Lo que permite una velocidad extremadamente alta de proceso de paquetes. Puentes y enrutadores, en contraste, generalmente usan procesadores de alto desempeño RISC para mover frames de datos. El movimiento de frames por microprocesador es mas caro, lento, requiere de mas grandes dispositivos y mas energía eléctrica. Además, los conmutadores pueden llevar a cabo una autoconfiguración (también se puede realizar una

configuración manual en el panel de control del conmutador o por medio de la red, pero solo es necesaria en características de configuración avanzadas, tal como operación Full dúplex o si se desean redes virtuales).

Segundo, los conmutadores como los puentes, fueron diseñados para dividir una red local extensa en pequeños segmentos, aislando el tráfico de cada segmento (tráfico local) de los otros, de esta manera se aprovecha mejor el ancho de banda mientras que permanece una completa conectividad de los segmentos. Sin embargo, los conmutadores típicos tienen un mayor número de puertos a diferencia de los puentes lo que permite la multi-segmentación, brindando varias rutas de datos independientes a través del dispositivo. Múltiples rutas de datos independientes son las que aumentan el rendimiento de los conmutadores a diferencia de los puentes.

5.4.1 Conmutadores estáticos y dinámicos

Algunos dispositivos referidos como conmutadores, no son conmutadores del todo. Los **conmutadores estáticos** no son más que un grupo de puertos conectados que conforman un mismo segmento (grupo). Todo el tráfico de cada uno de los puertos del grupo va a todos los demás puertos que conforman el grupo y no a los otros puertos de otros grupos. El mismo efecto puede ser llevado a cabo simplemente al conectar todos los miembros de un grupo a un simple concentrador.

Mientras en algunas circunstancias un conmutador estático puede ser usado completamente, los concentradores individuales son usualmente preferibles debido a la consideración de su precio y eficacia.

En contraste, los conmutadores dinámicos, llevan a cabo una operación de aprendizaje, donde este aprende sobre cuál puerto una estación es conectada cada vez que la estación transmite. Entonces, cada paquete recibido para esta estación es reenviado solo al puerto correcto, eliminando así tráfico incensario en el ancho de banda de otros puertos. Desde que la dirección de una estación es re-asimilada cada vez que la estación transmite, si las estaciones son cambiadas de localidad, el conmutador reconfigurará su tabla de reenvío inmediatamente. Con esto se preserva la completa conectividad.

5.4.2 Diferencias entre conmutadores de segmento y concentradores conmutados

La diferencia entre **conmutadores de segmento** (segment switches) y **concentradores conmutados** (switching hubs) es que un conmutador de segmentos puede manejar un segmento de red entero (múltiples estaciones) sobre cada uno de sus puertos, mientras que un concentrador conmutado puede

solamente manejar una sola estación por puerto (segmento dedicado). Idealmente, cada estación debería tener su propio puerto con un dedicado ancho de banda disponible. Sin embargo, actualmente esto no es la solución óptima. Concentradores conmutados son medidas excesivas para la mayoría de las aplicaciones. Un estación de trabajo típica pasa la mayoría de su tiempo esperando a que la entrada del usuario dejando al puerto dedicado del concentrador conmutado sin usar la mayoría del tiempo.

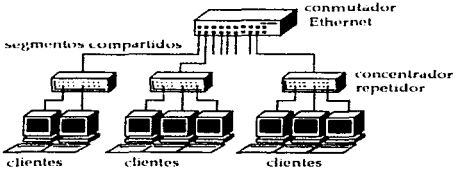


Figura 5.10 Conmutador de segmento

Desde que un conmutador de segmento puede tener varias estaciones sobre el mismo puerto, el hardware es usado mas eficientemente. Las estaciones que tienen bajos requerimientos de ancho de banda pueden compartir un puerto sobre el conmutador de segmentos, bajando así el costo de estación por punto. Las estaciones con un alto índice de uso, tales como servidores, pueden aún tener un puerto dedicado (segmento dedicado) sobre el conmutador de segmentos. Con conmutadores de segmento, el administrador de red tiene mas flexibilidad en acomodar anchos de banda entre estaciones, por lo anterior un conmutador de segmentos das una mejor solución costo-efectivo que un concentrador conmutado. Generalmente, los usuarios migran hacia segmentos dedicados de una sola estación como incrementa la demanda de ancho de banda de la estación misma.

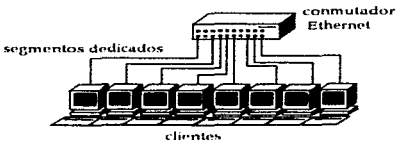


Figura 5.11 Concentrador conmutado ethernet

El utilizar conmutadores es particularmente atractivo por que el ancho de banda que estos soportan puede ser llevado a cabo sin la necesidad de tener que

reemplazar el equipo o cableado existente. Múltiples estaciones pueden ser conectadas a los puertos del conmutador en lugar de a los puentes o enrutadores. Proveyendo a los usuarios con las ventajas antes mencionadas.

Algunos conmutadores ofrecen un modo de direccionamiento seguro en el cual las direcciones de las estaciones asociadas con cada puerto puede ser introducido en una tabla. Esto previene a usuarios no autorizados a utilizar el conmutador. En los concentradores conmutados donde solo una estación puede ser conectada por puerto, el puerto puede ser deshabilitado si una estación no autorizada es detectada. Otras opciones que existen para los conmutadores son el soporte para SNMP que permite que el conmutador sea monitoreado y administrado por sistemas de administración SNMP tales como HP's Open View, Sunnet Manager y Novell's NMS.

5.4.3 Métodos de conmutación

5.4.3.1 Método Cut-through

Un conmutador **cut-through** provee una baja latencia por medio de bajos retrasos de envío entre todos los segmentos conectados. Un dispositivo **cut-through** empieza el envío de un frame a su destino antes de recibir el final del frame[68] (este procede a transmitir el frame hacia el puerto de salida destino después de que este ha recibido la dirección destino en el encabezado MAC del frame). La desventaja es que puede propagar errores desde un segmento de red a otro, ya que los errores solo pueden ser detectados al final de cada frame.[69]

La propagación de errores es particularmente concerniente con redes Ethernet, desde que la correcta operación del protocolo CSMA/CD genera frames corruptos y truncados (runts) a partir de las colisiones ocurridas durante la contención por el canal de transmisión.

En un conmutador **cut-through** propiamente diseñado, cuando un paquete esta siendo recibido es puesto en un almacenamiento para transmisión. Tan pronto como sea eliminada la posibilidad de que el frame se encuentre truncado (es decir, un runt)[70], el paquete está listo para la transmisión. Hay que hacer notar que como cualquier dispositivo Ethernet el conmutador esperará hasta que el segmento de salida este libre antes de que la transmisión tome lugar, si una colisión llegara a

[68] Esto puede mejorar la latencia de un paquete por un factor de hasta 20 veces sobre un dispositivo de almacenamiento-y-reenvío.
[69] Debido a que el campo de verificación CRC se encuentra al final del frame.
[70] Para garantizar que todos los runts son filtrados, un conmutador Ethernet deberá esperar hasta la recepción de 64 bytes (tamaño mínimo de un frame ethernet) antes de empezar la transmisión o reenvío. Si una red tiene paquetes con errores después de los primeros 64 bytes, el ancho de banda ensuciado por el reenvío del paquete incompleto es insignificante.

ocurrir el conmutador se mantendría en estado de espera y retransmitiría el paquete.

Desde que cada bit almacenado significa un retraso adicional de 8 microsegundos, 1500 bytes de paquete serían retrasados por 1200 microsegundos en un dispositivo de **almacenamiento-y-reenvío**, contra 60 microsegundos en un dispositivo *cut-through*. Esta diferencia en retraso es notable cuando se desarrollan largas transferencias de datos con protocolos que no están basados en tecnología de ventanas.

Sobre un propio funcionamiento de una red Ethernet, solo los frames los cuales no son validos son runts. Cualquier otro problema (tales como CRC o errores de alineación) son debidos a una mala configuración de red o el mal funcionamiento de un dispositivo.

5.4.3.2 Método de almacenamiento-y-reenvío (Store-and-forward)

Un dispositivo de **almacenamiento-y-reenvío** tiene que recibir un paquete completamente, antes de enviarlo al puerto destino. Este método impone una sanción de latencia pero puede verificar que el frame este correctamente disponible antes de su transmisión, evitando distribuir frames corrompidos o truncados. Todos los procesos necesarios toman lugar en el momento en que el paquete es recibido: Tan pronto como el paquete es completamente recibido y el CRC es verificado, este es enviado directamente a su destino.

Un procedimiento de almacenamiento-y-reenvío es necesario cuando un frame debe de ser movido desde un segmento de red de baja velocidad hacia un segmento con red de alta velocidad[71]. Esto es para asegurar que no existen huecos en el paquete.

Un conmutador de **almacenamiento-y-reenvío** puede aminorar teóricamente el retraso posible del procedimiento de **almacenamiento y reenvío**, sí lleva a cabo la tarea de identificar por donde va a mandar el paquete al mismo tiempo que lo esta recibiendo. Es decir, sobre poner o realizar de manera simultánea la recepción del paquete y el proceso de identificación de direccionamiento, lo que significa que el conmutador estará listo para empezar la transmisión de un frame, inmediatamente después de que el ultimo bit del frame sea recibido.

Por último, cabe mencionar que cuando el tráfico en la red se incrementa, los beneficios del modo de conmutación **cut-through** disminuyen. Por otro lado, con

[71] Un conmutador **cut-through** deberá cambiar a un procedimiento de almacenamiento-y-reenvío cuando se mueven frames entre segmentos de diferentes velocidades. La necesidad a futuro de mover frames entre red de diferentes velocidades, la necesidad de cambiar los procedimientos elimina la ventaja de retraso del procedimiento **cut-through**.

una baja utilización de la red, es decir, menor tráfico, hace que la probabilidad de dos o más paquetes lleguen al mismo puerto de salida simultáneamente sea relativamente pequeño. En cambio, cuando existe más tráfico sobre la red, la probabilidad de que dos o más paquetes lleguen simultáneamente al mismo puerto de salida asciende simplemente por que existen más paquetes. También, más tráfico significa que el puerto de salida estará ocupado por más tiempo, incrementando de nuevo la probabilidad de que un paquete encuentre ocupado el puerto de salida. Cuando un paquete encuentra un puerto de salida ocupado, este deberá ser almacenado hasta que el puerto de salida llegue a estar disponible para la transmisión. De esta manera incluso en un dispositivo con modo cut-through, cuando existe una carga de tráfico alta en la red, los paquetes necesitarán ser almacenados. Finalmente, Hay que tener en cuenta que las cargas de red típicas en un ambiente conmutado son relativamente altas.

Además, aún cuando **cut-through** puede ser usado, protocolos basados en ráfaga-de-paquetes (NCP de Novell, burst), o basados en tecnología de ventanas (TCP), reducen grandemente el significado de bajo retraso de conmutación, dando al método de almacenamiento-y-reenvío esencialmente el mismo nivel de rendimiento.

5.4.4 Latencia

La latencia es el tiempo que toma un conmutador para procesar un paquete. Esta es la cantidad de tiempo entre cuando un conmutador recibe una unidad de datos y cuando esa unidad de datos es reenviada fuera desde el conmutador. La latencia es medida de diferentes formas dependiendo del método utilizado por el conmutador. El método de almacenamiento-y-reenvío mide la latencia por LIFO , mientras que para cut-through es medido por FIFO.

LIFO significa último bit en entrar (Last In), primer bit en salir (First Out). Este es la longitud de tiempo que se toma desde el momento del ultimo bit de un frame es recibido en un puerto, hasta el momento del tiempo en el cual el primer bit del frame es enviado fuera a un puerto destino. Algunos conmutadores tienen una latencia muy cercana a la de los concentradores.

FIFO significa primer bit en entrar (First In), primer bit en salir (First Out). Este es la cantidad de tiempo que se toma desde el momento que el primer bit de un frame es recibido sobre un puerto hasta el punto del cual el primer bit es enviado fuera a un puerto destino.

Por que los métodos de medición de latencia difieren, es importante comparar la latencia para almacenamiento-y-reenvío a dispositivos almacenamiento-y-reenvío y latencia para *cut-through* a dispositivos *cut-through*.

El rendimiento es la velocidad de datos transferidos que un conmutador puede mantener sin perdida de paquetes. Mientras que la latencia mide el retraso de un solo frame, el rendimiento mide el número de paquetes, o frames por segundo sin perdida de paquetes perdidos. En un conmutador, el rendimiento es medido generalmente en paquetes por segundo (pps), pero también puede ser medido por frames por segundo (fps).

5.4.5 Arquitecturas de los conmutadores

Los conmutadores pueden estar basados en Circuitos Integrados de Aplicación Especificas (ASIC: Application Specific Integrated Circuit) o basados en procesador[72]. Los conmutadores basados en procesador están construidos con microprocesadores de estándares existentes realizando la conmutación por medio de software. Los conmutadores basados en ASIC son mas de una combinación de hardware y firmware con procedimientos de conmutación enteramente encapsulado dentro del ASIC. Los conmutadores ASIC son algunas veces preferidos sobre conmutadores basados en procesador, debido a que estos son mucho más rápidos.

Recientemente, los avances en la tecnología ASIC ha hecho que los conmutadores de redes locales sean una atractiva alternativa para los enrutadores y eventualmente para los concentradores.

Una de las principales diferencias entre conmutadores de redes locales se encuentra en la arquitectura del conmutador. Desde que más conmutadores en el mercado actual están basados en ASICs propietarios, es importante cuidar el diseño de este chip o conjunto de chips, y como estos integran el resto del conmutador, incluyendo las elecciones de las memorias de almacenamiento de entrada y salida. En el diseño del ASIC, el software deberá ser desarrollado, probado y entonces implantado en el chip ASIC. Una vez manufacturado, el conjunto de instrucciones no puede ser cambiado. De esta manera, el diseño de la ingeniería de conmutación es un factor crítico.

Los circuitos ASICs básicamente caen dentro de dos clases: ASICs largos, los cuales llevan el manejo de un gran número de puertos; o un arreglo de pequeños circuitos ASICs que manejan un pequeño número de puertos.

Idealmente, los conmutadores deberían implementar una arquitectura de matriz de puntos cruzados pura. Una matriz es básicamente un solo ASIC que lleva a cabo una malla con múltiples rutas de comunicación con cada puerto, teniendo una ruta dedicada para cada uno de los demás puertos del conmutador. Desafortunadamente, la arquitectura de matriz pura no se presta bien para la

[72]Los conmutadores que proveen servicios de capa de red generalmente son basados en procesadores RISC para manejar los servicios de software intensivo que provee el enrutamiento.

expansión, flexibilidad o conmutación de tecnología cruzada (por ejemplo, conmutación de 10 Base T a 100Base T). Una matriz de punto cruzado puro además requiere de mucha circuitería por lo que han realizado arquitecturas más complejas.

Existen tres arquitecturas de conmutadores comunes para redes locales: conmutador de barra cruzada con encolado de entrada (cross-bar with input queuing), conmutador de enrutamiento propio (self-routing) con memoria compartida y conmutador de bus de alta velocidad (high-speed bus) referidos también como **plano posterior** compartido (shared backplane).

5.4.5.1 Conmutadores cross-bar

Los conmutadores **cross-bar** son diseñados para optimizar conexiones punto a punto de enlaces seriales (pueden ser vistos de manera de calles que convergen en una sola intersección). En tráfico bajo, los datos no se necesitan almacenar en memoria antes de ser reenviados (cut-through). Sin embargo, los conmutadores *cross-bar* requieren memoria de almacenamiento (buffers) de entrada en cada puerto para almacenar datos si la intersección esta ocupada (bloqueado, blocking).

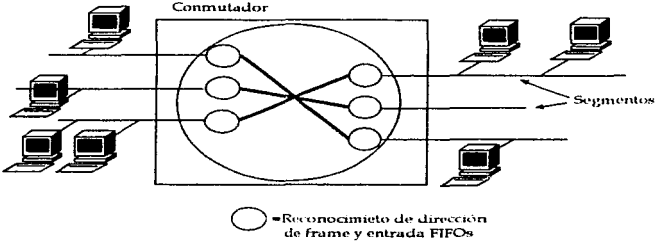


Figura 5.12 Conmutador de barra cruzada

Mientras que este es bajo en costo y fue el primero en el mercado, los conmutadores cross-bar son también simples y efectivos para el traslado de interfaces de baja velocidad (Ethernet y Token ring) a interfaces de alta velocidad (ATM y FDDI).

5.4.5.2 Conmutadores de memoria compartida

Los conmutadores de memoria compartida consolidan el almacenamiento de entrada dentro de una memoria global para uso común, el cual actúa como el **plano posterior** (backplane) del conmutador. Sin embargo, una arquitectura de memoria compartida no requiere un plano posterior para llevar datos desde un puerto a otro, lo cual hace que el conmutador de memoria compartida sea menos caro que los conmutadores de bus de alta velocidad. El almacenamiento de datos en memoria antes de que el conmutador pueda reenviarlos es llamado almacenamiento-y-reenvío e introduce un retraso

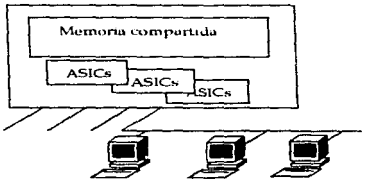


Figura 5.13 Arquitectura de conmutador de memoria compartida

5.4.5.3 Conmutadores de bus de alta velocidad o plano posterior compartido

Este conmutador conecta circuitos ASICs a un bus de datos de alta velocidad el cual sirve para conectar los puertos. Una vez que el dato es traducido a un formato común apropiado para la transmisión sobre el bus, el dato es llevado en el bus a su puerto destino. Desde que el bus puede manejar transmisiones completas desde cada puerto de manera simultánea hace que el conmutador de bus de alta velocidad sea frecuentemente considerado como un conmutador sin bloqueo (no-blocking) a partir de que el bus introduce rutas de datos sin problemas de cuello de botella.

Además de estos beneficios, el uso de la tecnología de ASIC es la que permite al conmutador dar un mayor desempeño que un puente tradicional dando una alta cantidad de manejo paquetes con un retardo extremadamente pequeño. Esto permite a un conmutador el manejo simultáneo de reenvío de paquetes a través de todos los puertos a la velocidad que el cable pueda brindar. Por ejemplo, una interfaz Ethernet puede soportar en teoría, un máximo de transmisión de 14880 pps de 64 octetos (tamaño mínimo). Esto significa que con un conmutador Ethernet de doce puertos y cables veloces, soporta seis conexiones simultáneas,

esto dada una salida de 89280 pps (6 conexiones x 14880 pps/conexión). El uso de la tecnología ASIC permite al conmutador entregar este desempeño sobre más puertos y a un costo más bajo por puerto que un puente tradicional.

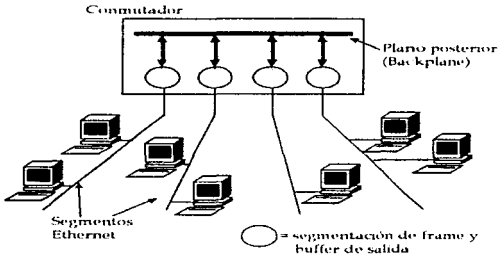


Figura 5.14 Arquitectura de bus de alta velocidad o arquitectura de plano posterior compartido de alta velocidad

5.4.6 Transmisiones Full Dúplex

Al usar transmisiones full dúplex, las senales viajan en ambas direcciones sobre una misma conexión, al mismo tiempo. Este tipo de transmisión bidireccional simultánea permite un aumento en la tasa de transmisión aumentando al doble.

Las comunicaciones full dúplex están disponibles solo para conexiones punto a punto. Es decir, full dúplex puede ser usado entre una estación de trabajo y un puerto del conmutador, entre dos puertos, o entre dos estaciones. Full dúplex no puede ser usado para compartir conexiones de puertos (como son repetidores o conexiones a puertos de hubs hacía múltiples estaciones de trabajo).

Dicho lo anterior, cabe mencionar que este tipo de conexiones son recomendadas para los enlaces del backbone de la red. No así para la conexiones hacia los clientes ya que las aplicaciones cliente/servidor básicamente transmiten trafico asimétrico de lectura/escritura, lo que tendría en consecuencia un desperdicio de recursos.

5.4.7 Control de flujo

Si, por ejemplo, el puerto de destino de un paquete recibido esta saturado, un conmutador convencional o puente no tiene elección y desecha el paquete. Esta situación se presenta frecuentemente en un ambiente donde se utilizan protocolos

basados en técnicas de ventana, tales como TCP. Si un conmutador notificara al emisor original que el paquete será desechado, el paquete podría ser retransmitido desde la memoria del hardware de la interfaz de red del emisor. Esto decrementa dramáticamente la carga sobre el protocolo de transporte de la estación. Pero de manera contraria, los conmutadores convencionales dependen del software de protocolo de la capa de transporte de la estación emisora para la detección de un paquete desechado, de esta manera, entonces se regenera y reencola el paquete. Otra forma de congestión ocurrirá cada vez que sean enviados más paquetes hacia un segmento particular que los que este puede manejar.

Para resolver la congestión, se tiene la necesidad de tener un control de flujo para cuando el conmutador es incapaz de liberar los datos dentro del medio de destino. Para llevar a cabo esto, los datos son entonces mantenidos en una memoria de almacenamiento hasta que estos puedan ser enviados hacia su destino. Si suficientes datos son almacenados y la memoria de almacenamiento se consume completamente, los frames serán desechados a partir de que no exista mas espacio en la memoria de almacenamiento para ellos. Algunos conmutadores intentan manejar la congestión al hacer que un segmento con carga pesada parezca tener numerosas colisiones, causando que todas las estaciones sobre los segmentos entren en un estado de espera en su envío de paquetes. Este método es llamado backpressure el cual ha sido diseñado primeramente para los conmutadores de segmento. Con backpressure, todos los nodos sobre un segmento son prevenidos de hablar durante el tiempo que el conmutador esta aplicando backpressure, y el tráfico no destinado para el conmutador es también detenido durante este tiempo.

El control de flujo es necesario, a partir de que los paquetes desechados tienen un grande impacto sobre el desempeño de la red (retrasos en el orden de segundos para cada paquete desechado) por lo que se deberá tener un gran cuidado para tratar de no desechar paquetes. En los puentes convencionales, enrutadores y conmutadores, el método usado para evitar el desecho de paquetes es el de tener grandes almacenes de memoria (buffers) para almacenar los paquetes que no pueden ser enviados.

Confiar en grandes almacenes de memoria (large buffers) para mejorar la sobrecarga de ancho de banda está sujeto a limitaciones adicionales. Grandes almacenes de memoria son simplemente recolectores máximizados. Si el segmento destino está muy congestionado para manejar el tráfico. Pequeños tamaños de ventana en los protocolos de la capa de transmisión (tales como IPX o TCP) pueden ayudar a reducir tales problemas; sin embargo, una red lo suficientemente larga puede agobiar aún los grandes almacenes de memoria y eventualmente desechar paquetes. Aún en las peores situaciones, excesivos almacenes de memoria también contribuirían a latencias en la red, esto es debido a que los paquetes de entrada deberán de esperar que los paquetes que están mas adelante en el almacen de memoria sean transmitidos dentro de sus respectivos segmentos. De esta manera grandes almacenes de memoria incrementan la latencia.

Un control de flujo más inteligente se puede efectuar, partiendo de que se ocupe un mecanismo de Detección de Colisión de Ethernet para permitir ver a las estaciones el tráfico que tiene cada una de las otras estaciones, esto a través del conmutador solamente cuando sea necesario. Cuando un segmento esta a su capacidad total, las transmisiones hacia ese segmento a través del conmutador se colisionarán, mientras que las transmisiones a los demás segmentos serán enviadas inmediatamente. Ya que utilizan el jamming para aquellos paquetes que son destinados a un puerto saturado y todo el demás tráfico de la red permanece sin ser afectado.

El jamming se puede llevar a cabo debido a que algunos conmutadores, debido a su extremadamente rápido tiempo de descodificación de dirección MAC, pueden determinar si un paquete destinado a un puerto ocupado ha llegado (de 1 a 4 microsegundos) después de que los 6 bytes de dirección de destino han sido recibidos por la MAC. Si esto pasa, puede transmitir un mensaje JAM hacia el segmento origen (jamming), interrumpiendo al emisor y causando ha este la retransmisión de los paquetes después de tener un tiempo de espera aleatorio. El tiempo de respuesta aquí es crítico, a partir de que el conmutador tiene que responder con una señal JAM casi instantáneamente para evitar atentar el retraso presupuestado por el dominio de colisión.

Otros conmutadores que ofrecen otro Control de flujo, utilizan un método inferior de control de flujo basado en el CSMA/CD. Este método es inferior partiendo del uso de este mecanismo, un dispositivo deberá constantemente transmitir sobre todos los segmentos conectados cada vez que un puerto de salida llega a estar saturado. Este efecto es indiscriminadamente lento para la red entera cuando se debe realizar un seguimiento paso a paso cada vez que un control de flujo es necesario.

5.4.8 Almacenamiento

Es primordial que un segmento conmutado deberá tener la capacidad de almacenar paquetes. Existen tres maneras básicas de que un paquete puede ser almacenado. En la entrada donde son recibidos, a la salida donde ellos serán transmitidos o en la **ruta** entre la entrada y la salida. El modo más efectivo es el tipo de almacenamiento de **ruta**. Ya que cuando un paquete es almacenado en la entrada solamente, puede ocurrir un problema cuando existen paquetes que necesitan ser entregados en dos puertos diferentes. Y cuando los paquetes son almacenados en la salida solamente, un problema ocurre cuando varios puertos tratan de enviar hacia un solo puerto.

El almacenamiento de ruta, evita ambos tipos de problemas al crear un par separado de almacenes de memoria entre cada par de puertos. Todos los paquetes

en cada almacén son provenientes del mismo puerto y van hacia el mismo puerto. El problema de bloqueo de entrada es evitado desde que para cada posible salida existe un almacén separado. También, desde que cada puerto tiene su propio almacén para cada puerto hacia otro, todos los puertos tienen igual acceso a todos los demás.

5.4.9 Port trunking

El **port trunking** es usado para permitir a varios puertos ser conectados conjuntamente y tratados como uno solo, es decir, un puerto de alta velocidad. Esto habilita a dos conmutadores ser interconectados por múltiples enlaces, con todos estos enlaces actuando como un solo enlace de alta velocidad. Por ejemplo, con port trunking, se puede llevar a cabo un enlace de dos conmutadores juntos con dos puertos 100VG. Esto deberá actuar como doblar el desempeño conmutador-a-conmutador comparado a la conexión de dos conmutadores con un solo puerto 100VG.

5.4.9.1 Problemas que pueden ocurrir

En varias redes, el mayor problema de cuello de botella es el tráfico de red manejado por un servidor. Considerando un conmutador de Ethernet que provee un canal privado de 10Mbps para cada estación unida a cada uno de sus puertos y en el cuál el servidor es unido a uno de los puertos del conmutador. Si "m" estaciones estuvieran accediendo al servidor simultáneamente, el servidor deberá manejar 10*m Mbps de datos. Si diez estaciones necesitan acceder el servidor a 10 Mbps, el servidor necesitará tener un manejo de 10*10 = 100 Mbps de datos. Un conmutador ordinario no puede proveer una solución a este problema. Por lo cual es necesario un conmutador que tenga puertos dedicados que puedan manejar 100Mbps de datos. Un ejemplo de estos conmutadores son los capaces de manejar un cierto número de sus puertos provean un canal privado de 10Mbps cada uno y otro número de puertos que provean canales a 100Mbps en los cuales los servidores pueden ser conectados. Teniendo en cuenta que los servidores deberán ser instalados con una tarjeta de red a 100Mbps. Por lo anterior se puede tener 12 conversaciones simultáneas entre canales de 10Mbps y un puerto a 100Mbps con lo que se agrega un ancho de banda de 220Mbps.

Basados en la idea anterior existen conmutadores que llevan a cabo el reenvío de trafico Ethernet a Ethernet rápido (Fast Ethernet), otros productos proveen conmutación Ethernet a FDDI, a ATM, o a otro sistema backbone propietario.

5.4.10 Redes locales virtuales (VLAN)

Las redes locales virtuales (VLANs) son una forma simple de creación de un dominio de broadcast virtual (virtual broadcast domain) dentro de un ambiente

conmutado independiente de la estructura física. Con VLANs, los administradores de red tienen la habilidad para definir un grupo de trabajo basado en una agrupación lógica de estaciones individuales en lugar de la infraestructura física de la red. El tráfico dentro de la red virtual es conmutada a velocidades del cable (wire speed) entre los miembros de la red virtual y el tráfico entre diferentes VLANs es enviado por medio de un enrutador.

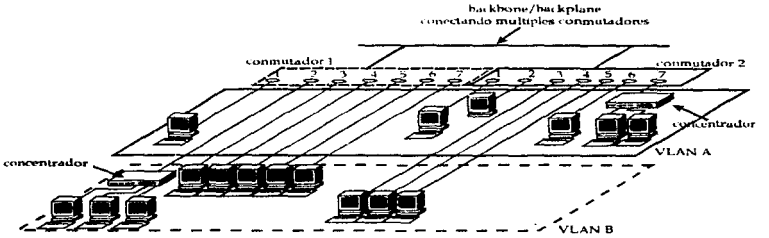


Figura 5.15 Redes Virtuales (VLANs) llevada a cabo por agrupación de puertos

Las redes locales virtuales representan una solución alternativa en lugar de enrutadores para dominios de broadcast . Partiendo de la base de que las VLANs permiten a los conmutadores también contener trafico de broadcast . Con la implantación de conmutadores en conjunción de las redes virtuales, cada segmento de red puede tener hasta un usuario, mientras que los dominios de broadcast (broadcast domain) pueden ser tan grandes y soportar hasta 1000 usuarios o tal vez más. Si son implementadas propiamente, las VLANs pueden seguir la pista de los movimientos de hacia nuevas locaciones de una estación sin necesidad de reconfiguración manual de direcciones IP. Por lo anterior, las VLANs pueden reducir significativamente el costo de administración de red, adicionar seguridad y control, y ayudar a los usuarios en una fácil transición desde redes locales con medios compartidos hacia arquitecturas de redes conmutadas.

La razón por la que un mayor número de organizaciones aún no hayan desarrollado VLANs, es por que los conmutadores de estas organizaciones no han sido desarrollados a una escala suficientemente grande para necesitar de redes locales virtuales dentro de estas, con lo que se espera que esta situación cambie próximamente.

Existen sin embargo, otras razones por las cuales no han sido implementadas en su mayoría por los usuarios:

- Las redes virtuales han sido, y son aún, sistemas propietarios, es decir, soluciones de un solo proveedor, por lo que son contrarias a los sistemas abiertos multiproveedor. Afortunadamente , existen solo pocos modelos básicos de redes virtuales, lo cual hace fácil agrupar mas productos dentro de las categorías de broadcast.
- Aun cuando varios analistas sugieren que el empleo de VLANs dan una mayor la posibilidad para emplear servidores centralizados, todavía se pueden ver grandes empresas con implantaciones de VLANs con dificultades en la habilitación completa de acceso de alto desempeño a servidores centralizados.

Las VLANs pueden ser vistas como un analogía a un grupo de estaciones finales, tal vez sobre múltiples segmentos de red local físicos, que no son restringidos por su localización física y pueden comunicarse como si estuviesen sobre una red local común. Para configurar las redes locales virtuales dentro de una red conmutada, un administrador utiliza una utilería de administración de VLANs para definir VLANs individuales y determinar cuales estaciones finales serán incluidas en cada una de las redes virtuales definidas.

La mejor diferencia entre los modelos de VLAN se encuentra en las reglas usadas para definir la asociación de la VLAN.

Las VLANs pueden ser definidas por diferentes criterios, incluyendo conmutación de puertos, direcciones de control de acceso al medio (MAC), direcciones de subredes, tipo de protocolos, tipos de aplicaciones e identificadores de VLAN especiales "etiqueta" (tag) para cada uno de los paquetes o frames. La mayoría de los proveedores ofrece solo uno o dos métodos de definición de VLAN en sus productos.
Como se vio anteriormente, existen diferentes maneras en las que se pueden asociar las redes virtuales para su definición. Dentro de este documento se dividieron las definiciones de VLAN dentro de 3 tipos generales:

- VLANs por agrupación de puertos (port grouping).
- VLANs por agrupación a nivel MAC (MAC-layer grouping).
- VLANs por agrupación a nivel de red (network-layer grouping).

5.4.10.1 VLANs por agrupación de puertos (port grouping)

Definiendo VLANs por agrupación de puertos (segmentos virtuales) es la manera más simple para crear redes locales virtuales dentro de una red. Esencialmente,

cada puerto sobre un conmutador constituye un segmento físico de la red local[7]. Definiendo una VLAN utilizando este método es simplemente cuestión de asociar un grupo de puertos del conmutador para formar un solo segmento virtual.

Algunos puertos del conmutador tienen múltiples estaciones finales conectados a ellos (mediante uno o más concentradores), mientras que otros tienen solo una estación. Todas las estaciones finales conectadas a los puertos asociados con una VLAN comparten un dominio de broadcast común (broadcast domain). La definición VLANs puramente por agrupación de puertos no permite a múltiples VLANs ser incluidas en el mismo segmento físico (o puerto del conmutador). Sin embargo, la primera limitación de definición de VLANs por puerto es que el administrador de las redes debe reconfigurar la asociación VLAN cuando un usuario es movido desde un puerto hacia otro, es decir, el movimiento de un usuario ha una diferente VLAN requiere la reconexión física hacia un concentrador sobre un puerto de conmutador diferente El tráfico entre segmentos virtuales o VLANs deberá pasar a través de un enrutador.

En las primeras implantaciones de VLANs se habían definido como asociación de VLAN por **grupos de puertos conmutados**. Además, en estas primeras implantaciones, las VLANs podían ser soportadas solamente sobre un mismo conmutador. En implantaciones de la segunda generación, las VLANs soportaban redes virtuales que se expandían sobre múltiples conmutadores.

La asociación por medio de agrupación de puertos conmutados sigue siendo el método más común de definir una VLAN, y su configuración es completamente directa. Su simplicidad hace que las VLANs de segmentos virtuales hace la forma más sencilla para diseñar y administrar. Un ejemplo de esta agrupación es demostrada en la figura 5.15.

5.4.10.2 VLANs por agrupación a nivel MAC (MAC-layer grouping)

Asociación de VLAN basada en direcciones de la capa MAC tiene un conjunto de ventajas y desventajas.

La agrupación por lista de direcciones MAC, es la agrupación en la cual las dirección MAC de cada estación final es declarada conjuntamente con la VLAN a la cual pertenece. Este método es altamente flexible y permite a diferentes estaciones sobre un mismo puerto del conmutador ser parte de diferentes VLANs.

---

[7] Los conmutadores de puertos son concentradores alambrados que proveen planos posteriores (backplanes) compuestos por múltiples segmentos. Cada uno de esos planos posteriores ofrece un ancho de banda compartido. Los concentradores de conmutación de puertos difieren de los concentradores tradicionales en que los puertos sobre el concentrador de conmutación pueden ser dinámicamente asociados con diferentes planos posteriores, los cuales pueden ser fácilmente llevados a cabo vía comandos de software. En esta arquitectura, un segmento de "plano posterior" iguala a un grupo de trabajo o VLANs.

Este sistema de agrupación también elimina la necesidad de mover a las estaciones hacia diferentes puertos del conmutador cuando estas deben cambiar de red virtual. De otra manera, le dan la habilidad a los administradores de red de mover una estación a diferentes locaciones físicas sobre la red y esta automáticamente mantiene su asociación con la VLAN. Esto es permisible partiendo de la base de que la dirección MAC es incluida dentro de la interface de red de las estaciones (NIC). Una VLAN definida por direcciones MAC puede ser pensada como una red virtual basada en usuarios

Una de las desventajas de la solución con VLANs basadas en direcciones MAC es el requerimiento de que todos los usuarios deberán inicialmente ser configurados para estar dentro de una VLAN mínima. Después de la configuración manual inicial, es posible un seguimiento automático de los usuarios, dependiendo de la solución del proveedor. Sin embargo , la desventaja de tener la configuración inicial de VLANs llega a ser clara en redes muy grandes con miles de usuarios, donde cada uno es explícitamente asignado a una VLAN particular. Las VLANs basadas en direcciones MAC que están implementadas en ambientes de medios compartidos correrán dentro de una serio degradación de desempeño como miembros de diferentes VLANs coexistan sobre un solo puerto del conmutador.

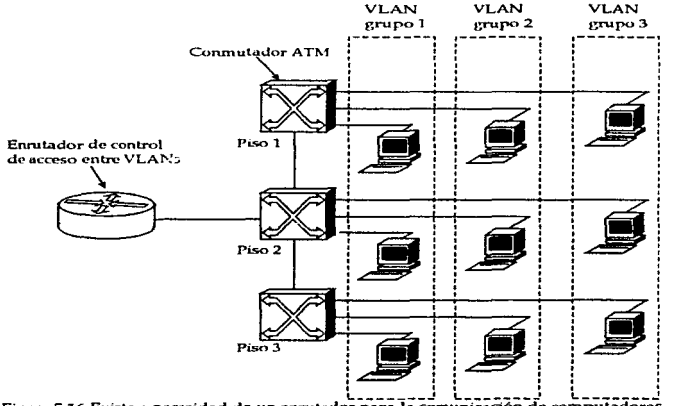


Figura 5.16 Existe a necesidad de un enrutador para la comunicación de computadoras pertenecientes a diferentes redes virtuales

Por último, cabe mencionar que al igual que las VLANs basadas en agrupación de puertos, las basadas en direcciones MAC deberán ser utilizadas en conjunción con enrutadores para proveer conectividad entre VLANs y el resto de la red.

5.4.10.3 VLANs por agrupación a nivel de red (network-layer grouping)

Las redes virtuales de nivel de capa de red, utilizan las direcciones del nivel de red del modelo de referencia OSI para poder implementar la red virtual. Por esta razón son frecuentemente llamadas "subredes virtuales". Cada estación final dentro de una red virtual dada es asignada con la misma dirección de subred. Los miembros de una subred particular son tratados como un grupo puenteado. Esto es, el tráfico es puenteado a nivel 2 dentro de la subred virtual. Pero aún se mantiene la necesidad de enrutar la conexión entre VLANs, es decir, se necesitará aún de un enrutador para establecerla conexión entre estaciones pertenecientes a diferentes redes virtuales.

Aunque estas redes virtuales son basadas en la información contenida de la capa de red, esto no constituye una función de **enrutamiento** y no deberá ser confundida con el enrutamiento de la capa de red.

Igual sin embargo, un conmutador inspecciona un paquete con dirección IP para determinar la asociación VLAN, no e lleva a cabo ningún calculo de enrutamiento, además de que no se emplea ningún protocolo RIP u OSPF, y los frames que atraviesan el conmutador son usualmente puenteados de acuerdo a la implantación del algoritmo de árbol expandido. Desde el punto de vista de un conmutador empleado en una VLAN basada en el nivel de la capa 3, la conectividad dentro de una VLAN dada es aún vista como un plano con topología de puente.

Teniendo en cuenta lo anterior se debe notar que varios proveedores están incorporando varias cantidades de capacidades de inteligencia del nivel 3 en sus conmutadores, habilitando funciones normalmente asociadas con el enrutamiento. Además los conmutadores con capacidades de capa 3 o **conmutadores multi-capas** frecuentemente tienen la función de envío de paquetes de enrutamiento construido dentro de un conjunto de chips ASIC, Sin embargo, un principal punto permanece: no importa donde esté localizado una estación en una solución VLAN, el enrutamiento es necesario para proveer la conectividad entre distintas VLANs. Con este método de agrupación de VLAN, los administradores de la red, pueden segmentar una gran red dentro de VLANs basadas en información del nivel de red contenida en cada paquete. Una red conmutada puede ser configurada para actuar como un enrutador de segmentos de red pero con una gran diferencia: múltiples estaciones pueden estar conectadas al mismo puerto del conmutador y ser miembros de diferentes VLANs. También, al estar basadas en la capa de red

son sensitivas a los protocolos de la capa de red que se ocupan en dicha red, diferentes VLANs pueden ser definidos para diferentes grupos de protocolos tales como IP, IPX y Apple Talk.

La principal desventaja de las subredes virtuales las cuales son dependientes de los protocolos, es que los conmutadores deben ser capaces de leer los diferentes formatos para cada uno de los protocolos utilizados sobre las VLANs. Sin embargo, la realización de subredes virtuales basadas en direcciones IP son las mas usuales de VLAN de capa de red.

Existen varias ventajas al definir VLANs en el nivel 3 o de red. Primero, este habilita el particionamiento por el tipo de protocolo. Segundo, los usuarios pueden mover físicamente de localidad sus estaciones sin necesidad de reconfigurar cada dirección de red de las estaciones. Tercero, definiendo VLANs al nivel 3 puede eliminar la necesidad para etiquetar el frame en orden para comunicar asociaciones VLAN entre conmutadores, reduciendo el transporte indirecto. Una desventaja de definir VLANs al nivel 3 puede ser el desempeño(contra VLANs de MAC o basadas en puertos). Ya que al inspeccionar las direcciones del nivel 3 en los paquetes, consume más tiempo que al buscar las direcciones en el nivel de direcciones MAC en los frames. Por esta razón , los conmutadores que ocupan información del nivel 3 para la definición de VLANs son generalmente mas lentos que aquellos que usan información del nivel 2. Además, las VLANs definidas en el nivel 3, tienen una particular dificultad al tratar con protocolos no enrutables tales como NetBEUI. Las Estaciones finales que corren protocolos no enrutables no pueden ser diferenciados y de esta manera no pueden ser definidos como parte de una VLAN de nivel de red.

La agrupación Multicast IP representa un aprovechamiento un poco diferente de la definición de red virtual, aun que el concepto fundamental de VLAN como dominio de broadcast aún es aplicado. Cuando un paquete es enviado vía multicast, este es enviado hacia una dirección que es una aproximación para un grupo definido explícitamente de direcciones IP que es establecido dinámicamente. Para cada estación se le da la oportunidad para unirse a un grupo multicast IP particular al responder afirmativamente a la notificación de broadcast, Las cual señalan la existencia de ese grupo. Todas las estaciones unidas en un grupo multicast pueden ser vistas como miembros de un misma red local virtual. Sin embargo, ellos son solo miembros de un grupo multicast particular durante un cierto período de tiempo. De esta manera, la naturaleza dinámica de VLANs definidas por grupos multicast IP habilitan un alto grado de flexibilidad y sensibilidad de aplicación. En adición, VLANs definidas por grupos multicast IP deberían intrínsecamente ser hábiles para extenderse sobre enrutadores y de esta manera conexiones con redes de área amplia (WANs).

	Conmutador de puertos	Conmutador de capa 2	Conmutador multicapas
Reconfiguracion por software	si	si	si
Aumentan el ancho de banda del grupo de trabajo	no	si	si
Conectividad entre VLANs	no	no	si
VLANs se pueden expandir sobre multiples conmutadores	no	no	si

Tabla 5.3 Algunas caracteristicas importantes de los conmutadores

NOTA: Mientras los tres tipos de asociación ofrecen alguna forma de redes virtuales, solo los conmutadores basados en el nivel de capa 3 o conmutadores multiprotocolos ofrecen completamente los beneficios del paradigma de redes locales virtuales.

Por ultimo, cabe mencionar que de acuerdo a la especificación para emulación de red local para ATM versión 0.1 (LANE : ATM LAN Emulation). Cuando ATM es implementado en una red local con medio compartido. Estas redes locales deberán ser definidas como redes locales virtuales (o emuladas) sobre la porción ATM de la red.

5.4.11 Desarrollos futuros

El diseño de concentradores se desplaza hacia el concepto de la conmutación. La tecnología de conmutación permite que el ancho de banda pueda ser escalada. Hoy en día, los productos de conmutación están disponibles para las tecnologías Ethernet, Fast Ethernet, Token ring, FDDI, y con la capacidad de realizar una actualización hacia la retransmisión de celdas ATM en el futuro. La tendencia consiste en proporcionar soporte multiprotocolo, puenteo, enrutamiento, conexión a redes de área amplia, funciones de administración y análisis de protocolos, todo ello en una misma unidad.

El ancho de banda generado por todos los componentes conectados al concentrador requerirá la tecnología de conmutación más rápida, proporcionada por ATM, que teóricamente puede realizar una distribución de gigabits por segundo. Es posible, que en cada puerto del concentrador, tenga un circuito dedicado a cualquier otro puerto a través de un conmutador ATM.

Las principales compañías de telecomunicaciones incorporan conmutación de ATM dentro de sus redes de larga distancia. El siguiente paso para las compañías que requieren conexiones entre redes locales sobre redes de área extensa consiste en instalar conmutadores ATM que pueden servir inicialmente como redes soporte para el entorno local y proporcionar enlaces de alta velocidad a redes locales

remotas. El paso posterior es la incorporación de ATM dentro de los concentradores intermedios y eventualmente de concentradores para grupos de trabajo y áreas de escritorio.

5.5 Enrutadores (Routers)

Los enrutadores operan al nivel de red del modelo OSI. El enrutamiento envuelve dos actividades básicas: determinación de los caminos de enrutamiento y la transportación de paquetes de información a través de una interconexión de redes. Los enrutadores se usan tanto en redes locales, como en redes de área amplia y cuando existen más de una ruta entre dos puntos finales de la red (caminos redundantes), además de proporcionar control de tráfico y filtrado de paquetes, como se muestra en la Figura 5.18.

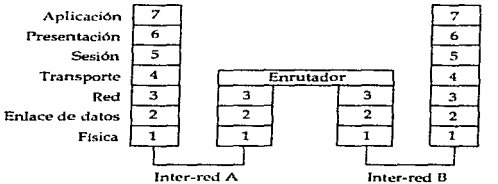


Figura 5.17 Función de un enrutador se desarrolla en la capa 3 o de red con respecto al modelo de referencia OSI

Como los puentes, los enrutadores proveen a los usuarios la unión de comunicación entre redes separadas físicamente y diferentes tecnologías como Ethernet, Token ring, y FDDI. A diferencia de los puentes, sin embargo, los enrutadores mantienen las identidades lógicas de cada uno de los segmentos de la red. De esta manera, una interconexión de redes basada en enrutadores consiste de varias y diferentes subredes lógicas, donde cada una de ellas es potencialmente un **dominio administrativo independiente**. De esta manera cada segmento[74] tiene una dirección de red local específica y por tanto se direcciona por separado. Así, los segmentos son más fáciles de manejar.

[74] Los enrutadores permiten segmentar redes, cada uno con diferentes dominios de difusión (broadcast).

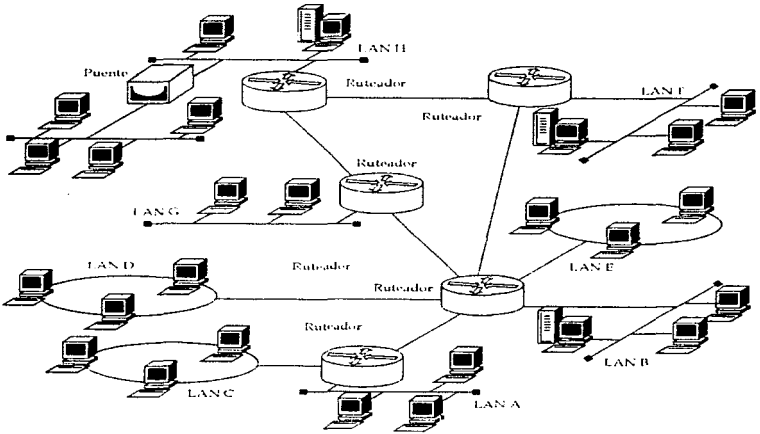


Figura 5.18 Ejemplo de la construcción de una interred usando enrutadores. Los enrutadores pueden ser utilizados para establecer redes complejas con cualquier tipo de tráfico, facilitando así el estado operacional y la utilización de diferentes rutas de red

Operando al nivel de la capa de red del modelo OSI, los enrutadores hacen decisiones más complejas que las realizadas por un puente o un conmutador. Para hacer estas decisiones ellos necesitan mas información, como datos sobre el costo de transmisión del paquete sobre ciertas rutas particulares. Esta información es contenida en una tabla de información conocida como tabla de enrutamiento.

La tabla de enrutamiento a diferencia de la encontrada en los puentes, es que incluye información sobre la ruta o rutas que cualquier paquete puede tomar a través de la red para llegar hasta su destino.

5.5.1 Funciones básicas de los enrutadores

Un enrutador examina la información de dirección de los paquetes y los envía hacia su destino a través de una ruta predeterminada. Los enrutadores mantienen tablas con información acerca de los enrutadores adyacentes y de las redes de área

local que hay dentro de la red. Cuando un enrutador recibe un paquete, consulta dichas tablas para ver si puede enviarlo directamente a su destino. En caso contrario, determina la posición de otro enrutador que puede hacerlo avanzar hacía su destino final.

La funcionalidad básica de los enrutadores es:

- Crear y mantener la tabla de enrutamiento; y
- Seleccionar el próximo salto del viaje para cada uno de los paquetes, basándose en la información con tenida en el paquete y la tabla de enrutamiento.

Las tablas de enrutamiento pueden ser creadas por enrutamiento estático o dinámico. Los primeros enrutadores no intercambiaban información acerca de las rutas de la red, en su lugar, enviaban habitualmente los paquetes a través de todos los caminos por medio del mecanismo de inundación, con esto se tenía el inconveniente de que algunos paquetes terminaban en un ciclo. Para evitar esto, se puede utilizar el **enrutamiento estático** [75], en el que algún administrador de la red es el responsable de programar las rutas manualmente para cada uno de los segmentos de cada una de las rutas posibles de la red. Un mejor método es el "enrutamiento dinámico", donde las tablas de enrutamiento son construidas automáticamente por el enrutador. En este caso, los enrutadores envían y recogen información usando paquetes especiales que contienen información orientada a las rutas. La información que reciben puede ser el número de saltos, los costos asociados a las rutas hacia el destino en la red o actualizaciones cuando un enrutador detecta un cambio en la red.

Para ayudar a mantener las tablas de enrutamiento, un enrutador difunde información cuando este detecta un cambio en la red. Tal información puede especificar la existencia de una nueva ruta a través de la red o que una ruta de servicio ha sido removida. La información difundida puede entrar en el rango de solo actualizar las tablas de enrutamiento, hasta impactar completamente toda la información de la tabla de enrutamiento.

El proceso de avance requiere la realización de un cierto mecanismo. Cuando el enrutador ha recibido la totalidad de un paquete, consulta la información de dirección en el encabezado del nivel de red del paquete y a continuación lo reenvía. Como consecuencia, el rendimiento se verá influenciado por las diferencias en los componentes del enrutador y en la arquitectura de este.

5.5.2 Enrutadores multiprotocolo

Los enrutadores pueden trabajar con un protocolo solamente, o bien con múltiples protocolos simultáneamente (como el IP o el IPX). Actualmente, el término "enrutador" usualmente significa enrutador multiprotocolo (un enrutador que

[75] El enrutamiento estático puede ser ventajoso en ambientes que requieran absoluta seguridad.

puede manejar múltiples protocolos). Un enrutador deberá tener el software apropiado para cada uno de los protocolos que este soporte, por que a diferencia de los puentes, los enrutadores son dispositivos "activos". Esto significa que pueden tomar varias decisiones para cada paquete. Por esta razón, los enrutadores a diferencia de los puentes, necesitan saber mas acerca de los protocolos.

Sin embargo, algunos protocolos (aquellos que no incluyen nivel de red) no pueden ser enrutables. Algunos ejemplos de protocolos no enrutables son el protocolo de conexión terminal de DEC "Transporte de Área Local" (LAT: DEC's Local Area Transport) y protocolos NetBIOS. Los protocolos no enrutables son puenteados generalmente, pero ellos pueden ser encapsulados dentro de un protocolo enrutable y de esta manera son trasladados a través de una interred.

Los enrutadores multiprotocolo dan lugar a esquemas de organización que posibilitan la conexión de los recursos de la red directamente a las propias plataformas soportadas por la red. En función de las capacidades del enrutador, un enrutador multiprotocolo puede ejecutar el software para el manejo de paquetes, de acuerdo con cada uno de los protocolos que soporta la red.

Los administradores pueden dirigir paulatinamente a los usuarios hacia los protocolos mas eficientes que soporte la compañía u organización, y una vez que todos los usuarios hayan realizado la transformación, deshabilitar los protocolos viejos y menos eficientes.

5.5.3 El procesamiento de paquetes realizado por los enrutadores

Cuando un enrutador recibe un paquete, comienza un procedimiento que lo desempaqueta y determina a donde se debe enviar. A continuación se dan los procedimientos que sigue el enrutador, cuando trabaja con un paquete:

1. Se comprueba si el paquete tiene un algún error, verificando el valor de código de paridad contenido en el paquete.

2. Se descarta la parte de la información del paquete que le añadieron los protocolos de nivel físico y de enlace de datos, como se muestra en la figura 5.19

3. Se evalúa la información que añadieron la computadora fuente y el protocolo de la capa de red.

La información del protocolo de nivel de red contiene la dirección destino del paquete, y en el caso de redes TCP/IP que utilizan algún algoritmo de **enrutamiento fuente** deben llevar una lista con información de los **saltos**

enrutador-a-enrutador que define la "mejor ruta" previamente determinada para cruzar la red.

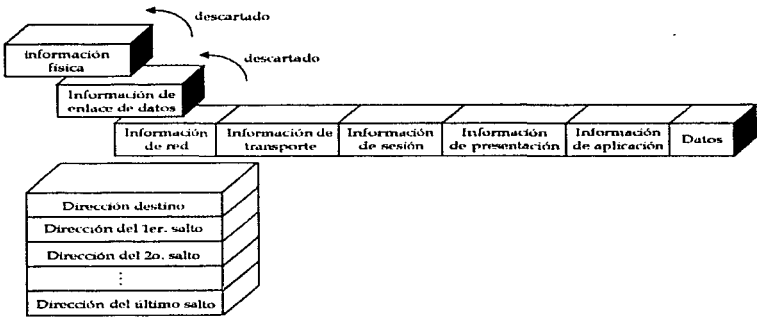


Figura 5.19 Procesamiento de paquetes realizado por los enrutadores

El enrutador puede realizar una de las siguientes opciones:

- El paquete podría estar dirigido al enrutador mismo, así que el enrutador evalúa cuál es la información sobrante en el paquete.
- Si un paquete tiene como destino la misma red origen, el enrutador simplemente lo envía de regreso.
- Si una lista de filtros está disponible, el enrutador compara la dirección del paquete con los valores de la lista y lo descarta si es necesario. Esto hace que un paquete pueda entrar o salir de la red. Esto se realiza en base a razones de seguridad como por ejemplo los llamados firewalls.
- Si el paquete contiene información procedente del enrutador fuente, en la que se contenga el nombre del próximo enrutador que está en la ruta hacia su destino, simplemente dirige el paquete hacia él.
- Si un enrutador no conoce la ruta, o no puede encontrar la dirección de destino del paquete en su tabla de caminos, descarta el paquete y puede devolver un mensaje de error a la fuente.

- Algunos paquetes (del tipo TCP/IP) contienen información acerca del número de saltos que han hecho en la red. Si un paquete sobrepasa un cierto número, el enrutador lo descarta ya que asume que está en un ciclo. Si es así, el enrutador podría devolver un mensaje de error a la fuente.

5.5.4 La elección del mejor camino

Naturalmente, la interconexión de redes presupone que debe tener una cierta tolerancia a las fallos. Por lo cuál se crean varias caminos entre los enrutadores, para que exista un camino redundante o de seguridad en el caso de que llegue a fallar un enlace. Algunas de estas rutas pueden usar una red de alta velocidad, como la Interfaz de Datos Distribuido por Fibra (FDDI), dentro del campus o del área metropolitana, o líneas digitales directas (T1) para redes de área extensa. Los enrutadores pueden enviar los datos por la mejor de estas rutas, en función del criterio de costo por usarlas (la más rápida, la más directa, la de menor precio o la que ha especificado un administrador). [76]

Los protocolos de enrutamiento eligen el menor camino a través de una red en base a criterios tales como el número de saltos entre los enrutadores de la red que tendría que hacer el paquete hasta alcanzar su destino. Además la mejor ruta debe evitar los caminos que cruzan segmentos de redes locales congestionados. Se puede dotar de prioridades a los paquetes. Por ejemplo, los paquetes con prioridad "alta" se enviarían a través de enlaces de comunicación digital de alta velocidad, y los de prioridad "baja", se enviarían a través de enlaces de telecomunicación de menor velocidad. El administrador de la red puede decidir cuáles son las mejores rutas de la red, o en algunos casos, hacen que sean los enrutadores los que elijan el mejor camino.

5.5.5 Algoritmos de enrutamiento

Cuando un paquete de datos viaja a través de la red y llega a un enrutador, este consulta en el paquete recibido, la dirección de destino del encabezado de nivel de red, enviándolo posteriormente a través de la ruta más adecuada. Este camino depende del protocolo de enrutamiento que se use.

El trabajo de los protocolos de la capa de red, es la proporcionar la información[77] que necesitan los enrutadores para crear los caminos óptimos a través de la malla

[76] Una red privada se forma con líneas alquiladas o de enlaces telefónicos y con enrutadores.
[77] La información necesaria para el enrutamiento provista por los protocolos de capa de red puede ser : solamente la dirección origen y destino del paquete, la ruta completa a través de la interred, o algún valor de prioridad que indique cuál es el camino que debe tomar el paquete dependiendo de los costos de la ruta.

de redes o interred. En función de esta información cada uno de los enrutadores hacen las decisiones necesarias de enrutamiento para determinar el mejor camino.

Esta determinación depende de varios factores, incluyendo :

- La medida de distancia, o "métrica de enrutamiento" en uso ;
- El núcleo del algoritmo implementado por el protocolo de alto nivel que está siendo usado; y
- La arquitectura de la red enrutada.

5.5.5.1 Métrica de enrutamiento para los algoritmos

En términos de distancia solamente, la mejor ruta a través de la red es la ruta más corta. Esto se puede ver suficientemente obvio hasta que se considera como se define el termino distancia.

En muchos casos la distancia geográfica entre dos puntos no es una buena manera de elegir la ruta a través de la red. Lo que nos hace pensar en otros factores como costos de economía o velocidades de las conexiones enlazadas.

Anteriormente los enrutadores usaban como "métrica de enrutamiento" al "número de saltos" para calcular la mejor ruta. Usando esta métrica, un enrutador resuelve la mejor ruta a través de la red basándose en el número de transmisiones enrutador-a-enrutador, o saltos, que requería cada una de las rutas. En esta métrica, la mejor ruta es definida como la ruta que requiere el menor número de saltos. Pero tomando en cuenta que esta métrica no hace referencia a otras variables como costos, velocidad de la línea, retrasos en la transmisión, precio de enlaces, etc. Para esto se han desarrollado métricas de enrutamiento mas completas.

Como se explicó anteriormente, dependiendo de la métrica de enrutamiento utilizada se determina como una ruta es preferible a otras. Varias métricas han sido utilizadas en los algoritmos de enrutamiento. Algunos algoritmos sofisticados de enrutamiento pueden basar la selección de la ruta sobre múltiples métricas, combinándolas de tal manera que resulten en una sola métrica. Todas de las siguientes métricas han sido utilizadas:

- Eficacia
- Retraso
- Ancho de Banda
- Carga
- MTU
- Costo de comunicación

Eficacia, en el contexto de algoritmos de enrutamiento, se refiere a la eficacia de cada uno de los enlaces. Algunos enlaces de red pueden fallar mas frecuentemente que otros. Una vez que llegan a fallar, algunos enlaces de red pueden ser reparados mas fácil y rápidamente que otros.

Retraso de enrutamiento se refiere a la longitud de tiempo requerido para mover un paquete desde su origen hasta su destino a través de la interred. El retraso depende de varios factores, incluyendo el ancho de banda de los enlaces intermedios, el encolamiento en los puertos de cada enrutador a lo largo del camino, congestionamiento de red sobre todos los enlaces de red intermedios y la distancia física para ser atravesada. Este punto es una conglomeración de diversas variables importantes, por lo que el retraso es una métrica comúnmente utilizada.

Ancho de banda se refiere a la capacidad de tráfico manejable disponible de un enlace. Aunque el ancho de banda es una tasa de máximo rendimiento alcanzable sobre un enlace, las rutas a través de enlaces con gran ancho de banda no necesariamente proveen las mejores rutas que las rutas con enlaces más lentos. Si, por ejemplo, un enlace rápido es mucho mas ocupado, el tiempo actual requerido para enviar un paquete hacia su destino puede ser mas grande a través del enlace con mayor ancho de banda.

Carga, se refiere al grado para los cuales un recurso de la red está ocupado (un enrutador por ejemplo). La carga puede ser calculada de diferentes maneras incluyendo la utilización del CPU y paquetes procesados por segundo (pps).

MTU (Unidad de Transferencia Máxima) se refiere la tamaño de paquete máximo que puede atravesar un enlace de red particular. Por ejemplo un enlace de red Ethernet puede manejar frames tan largos como 1.5 kilobytes, mientras que FDDI puede manejar frames de hasta 4Kb.

Costo de comunicación es otra importante métrica. Es el precio por enviar paquetes a través de líneas publicas o privadas[14].

5.5.5.2 Tipos de algoritmos de enrutamiento

Los algoritmos de enrutamiento pueden ser clasificados por tipo. Por ejemplo, los algoritmos pueden ser:

- Distribuidos o centralizados
- De una sola ruta o multirutas.
- Estación inteligente o enrutador inteligente
- Intra-dominio o Inter-dominio.
- Estáticos o dinámicos (Estado de enlace o vector de distancia).
- Plano o jerárquico.

Los algoritmos de enrutamiento pueden ser centralizados o distribuidos. Algoritmos centralizados calculan todos los caminos de enrutamiento en un dispositivo central. Este dispositivo es llamado frecuentemente un Centro de Control de Enrutamiento (RCC: Routing Control Center). El RCC periódicamente recolecta información de enrutamiento a partir de todos los enrutadores y distribuye tablas de enrutamiento óptimas hacia todos ellos.

Un enrutamiento centralizado tiene varias ventajas. Primero, releva a enrutadores individuales de la carga del cálculo de rutas. Segundo, este virtualmente asegura que todas las tablas de enrutamiento sean las mismas. Desafortunadamente, el enrutamiento centralizado también tiene desventajas serias. Si cualquier RCC fallara, la red entera se encontraría sin ayuda o debiendo a lo mejor confiar en tablas desactualizadas. Finalmente, dependiendo del tamaño y organización jerárquica de la interred, enrutadores cercanos al RCC pueden recibir información de actualización por adelantado de enrutadores distantes, creando así enrutamiento cíclicos (routing loops).

Los algoritmos distribuidos calculan los caminos de enrutamiento en cada enrutador individual. Cada enrutador periódicamente intercambia información de rutas con cada uno de sus vecinos. Los algoritmos distribuidos son más tolerantes a fallas que los algoritmos centralizados. Estos distribuyen actualizaciones sobre la red entera. Como el enrutamiento centralizado, estos pueden aún generar rutas en cíclicas. Con todo lo anterior, los algoritmos distribuidos son más comunes que los centralizados.

Algunos protocolos de enrutamiento sofisticados soportan múltiples rutas hacía el mismo destino. Estos algoritmos referidos como de rutas-múltiples permiten la multiplexaje de trafico sobre múltiples líneas; mientras que los protocolos de una sola ruta no lo permiten. Las ventajas de algoritmos multiruta son obvias; estos pueden proveer substancialmente un mejor rendimiento y redundancia.

Algunos algoritmos de enrutamiento asumen que la estación transmisora, determinará la ruta entera. Esto es usualmente referido como **enrutamiento fuente** (source routing). En sistemas de enrutamiento fuente, los enrutadores actúan como dispositivos de **almacenamiento-y-reenvío** (store-and-forwarding) solamente, e insignificantemente envían el paquete a la próxima parada o enrutador. En este tipo de esquema, las estaciones tienen el enrutamiento inteligente, esto se refiere como **estación-inteligente.**

Otros algoritmos asumen que la sistema terminal transmisor no sabe nada acerca de rutas. En estos algoritmos, los enrutadores determinan la ruta a través de la interred basándose sobre sus propios cálculos. A diferencia del anterior esquema, aquí, los enrutadores tienen el enrutamiento inteligente y son llamados **enrutador-inteligente.**

Existen esencialmente solo dos tipos de algoritmos sustentados bajo el enrutamiento dinámico. Estos son conocidos generalmente como **Algoritmos de Vector de Distancia** (DVAs: Distance Vector Algorithms) y **Algoritmos de Estado de Enlace** (LSAs: Link State Algorithms). Las diferencias entre los dos son importantes para el manejo de las redes. La principal diferencia entre **LSAs** y **DVAs** radica en la manera en que ellos resuelven las rutas disponibles a través de la red.

5.5.5.2.1 Protocolo de enrutamiento de vector distancia

Cuando usamos *Algoritmos de vector de distancia* (DVA también conocido como de Bellman-Ford), cada enrutador construye su propio "modelo" de la red y envía su modelo a todos sus enrutadores vecinos. Como los modelos son transferidos a través de la red, cada enrutador progresivamente incorpora esta información de segunda-mano dentro de su propia imagen de la red. Desafortunadamente, si uno de los enrutadores ha construido un modelo de red erróneo, todos los enrutadores heredan automáticamente este error.

Este tipo de protocolos enrutan los paquetes basándose principalmente en el número de saltos o en el costo hasta el destino. Esta información es la proporcionada los enrutadores vecinos.

Aquí, un enrutador con varios puertos, tiene asignado un costo asignado por el administrador de la red a cada uno de ellos, y su valor puede representar el costo real del uso de la línea o bien es un modo de indicar la preferencia de una línea en lugar de otra. El enrutador suma el costo de sus puertos al costo de sus vecinos, escogiendo el puerto que tenga un costo menor para llegar al destino. En caso de ser necesario, el enrutador vecino conectado al puerto habrá calculado las rutas adicionales a través de otros enrutadores.

La información acerca de las rutas y el tipo de la dirección del siguiente salto se almacena en tablas, y los enrutadores intercambian estas tablas aproximadamente cada 30 segundos. Inicialmente, cada red sabe a qué enrutador se conecta directamente. Cuando un enrutador recibe una tabla, compara las entradas de dicha tabla con la suya propia. A partir de esta información, actualiza su tabla incluyendo las nuevas rutas o borrando alguna de las existentes. La información de la tabla incluye:

- Número de red.
- Número de puerto.
- Costo.
- Dirección del siguiente salto.

Los protocolos más importantes de vector distancia son los siguientes:

- Protocolo de Información de Enrutamiento (RIP: Routing Información Protocol). Originalmente desarrollado para el Sistema de Redes Xerox (XNS: Xerox Network System) y posteriormente lo utilizó Novell NetWere y TCP/IP.
- Protocolo de Enrutamiento de Compuerta Interior (IGRP: Interior Gateway Routing Protocol). Desarrollado por Cisco.
- Protocolo de Mantenimiento de Tabla de Enrutamiento (RTMP: Routing Table Maintenance Protocol). Protocolo de Apple.

Cabe señalar que el mecanismo de "enrutamiento de vector distancia" no es adecuado para grandes redes que posean cientos de enrutadores, o para redes que se actualicen en forma constante.

5.5.5.2.2 Protocolo de enrutamiento de estado de enlace

Los Protocolos de Estado de Enlace (LSA: Link State Algorithm), a diferencia de los protocolos de vector de distancia (VDA), construyen un modelo de red basado en información mas confiable. Cada enrutador le dice al resto de la red que conexiones directas este tiene con su vecino(s). Los algoritmos LSAs son más confiables por que la información de enlace es transferida sin ser alterada entre los enrutadores; cada uno de los enrutadores construye su propio modelo. Usando esta información el enrutador puede decidir la ruta más corta.

El enrutamiento de "estado de enlace" requiere mayor poder de procesamiento que el de "vector distancia", pero proporciona un mayor control sobre el proceso de enrutamiento y se ajusta más rápidamente a los cambios. Los criterios de las rutas generadas se basan en: evitar las áreas congestionadas, la velocidad de las líneas, el costo debido al uso de la línea o en diversas prioridades.

Para el cálculo de las rutas se usa el algoritmo de Dijkstra, que se basa en lo siguiente:

- El número de enrutadores que debe atravesar el paquete para alcanzar su destino, éstos se denominan saltos. La mejor opción es la que contiene el menor número de saltos posible.
- La velocidad de las líneas de transmisión entre dos redes. Algunos enrutadores usan conexiones asíncronas lentas, mientras que otros emplean conexiones de alta velocidad.
- Los retrasos causados por la congestión de tráfico. Si una estación de trabajo está transmitiendo un archivo largo, el enrutador podría enviar paquetes a lo largo de distintas rutas para evitar la congestión por medio de balancear las cargas en las diferentes rutas.

- El costo de la ruta. Esta es una medida definida por un administrador (habitualmente en función del medio de transmisión).

El protocolo de enrutamiento de estado de enlace más común es el **Primera Ruta más Corta en Abrir** (OSPF: Open Shortest Path First) el cuál se utiliza para enrutar tráfico del tipo TCP/IP; otro similar es el **Enrutamiento entre Sistemas Intermedios** (IS-IS) del modelo de referencia OSI que además puede enrutar tanto tráfico IP como tráfico OSI.

Hasta recientes fechas, la mayoría de los protocolos de nivel superior habían sido basados en DVA y la implantación de las redes basadas en enrutadores eran implementadas con esquemas planos. Un ejemplo es el **Protocolo de Información de Enrutamiento** (RIP: Routing Information Protocol) miembro de los protocolos TCP/IP. En cambio, actualmente los nuevos protocolos son basados en algoritmos de estado de enlace. El protocolo **Primera Ruta más Corta en Abrir** (OSFP: Open Shortest Path First) es un protocolo basado en LSA en el conjunto de protocolos TCP/IP.

5.5.6 Arquitecturas basadas en enrutadores

Los enrutadores pueden soportar dos tipos de arquitecturas de red: en **plano** y **jerárquico**.

En una red en **plano**, no existe distinción entre diferentes partes de la red. Todos los segmentos se encuentran al mismo nivel, es decir, todos los enrutadores son puntos de todos los otros.

En un enrutamiento **jerárquico** usualmente se incluyen dos niveles. Los enrutadores ocupados en el nivel inferior son generalmente usados para comunicaciones dentro de ciertas **áreas definidas** de la red. Tales como varios segmentos internos de la red. Los enrutadores utilizados en el nivel mas alto, forman una área muy especial conocida como **área de backbone principal** (backbone-area). Los enrutadores de **área de backbone principal** transmiten paquetes entre enrutadores de la misma jerarquía y de jerarquías inferiores.

Los paquetes provenientes de enrutadores de jerarquía inferior, es decir, que no son del área de backbone principal, viajan hacia enrutadores del área backbone, donde estos viajan a través del área de backbone principal hasta que alcanzan el área definida de destino. A partir de este punto (área definida de destino), los paquetes viajan desde el último enrutador de **área de backbone principal** través de cero o más enrutadores de jerarquía inferior (no pertenecientes al área de backbone) hacia la estación final destino.

Aun que el **área de backbone principal** puede ser referido como **backbone principal** en una forma abreviada, existe una gran diferencia entre **área de backbone principal** y el término **backbone principal** de una red. El **área de backbone principal** es una construcción lógica que comprende solamente el manejo de comunicaciones entre enrutadores área-a-área, es decir, los de mayor jerarquía. Por tal motivo, **áreas de backbone** solamente existen en esquemas de red jerárquicos. De otra manera, el **backbone principal** físico de una red es, y puede existir en redes con arquitecturas de esquema plano o jerárquico.

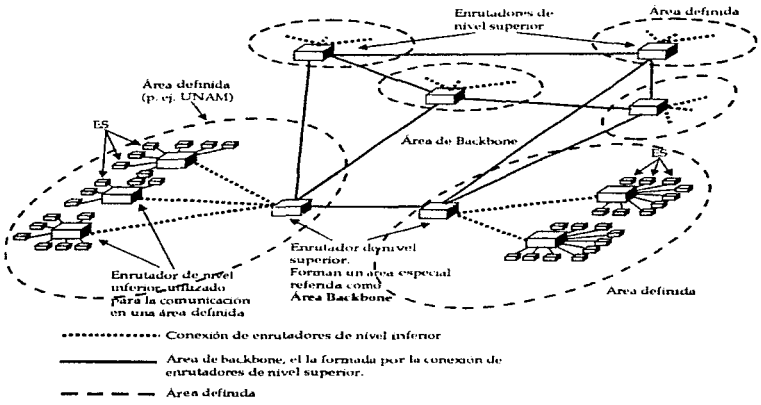


Figura 5.20 Ejemplo de enrutadores jerárquicos

Los sistemas de enrutamiento, frecuentemente designan grupos lógicos de nodos llamados dominios, sistemas autónomos o áreas. En sistemas jerárquicos, algunos enrutadores en un dominio pueden comunicarse con enrutadores de otros dominios (inter-dominio). Mientras otros solo pueden comunicarse con enrutadores dentro de su mismo dominio (intra-dominio). En redes muy largas, pueden existir diferentes niveles de jerarquía adicionales.

La principal ventaja de enrutamiento jerárquico es su habilidad para limitar las áreas en el intercambio de información de rutas cuando un cambio llega a ocurrir. Es decir, las rutas intra-dominio solo necesitan conocer acerca de otros enrutadores

dentro de su propio dominio, así sus algoritmos de enrutamiento pueden ser simplificados.

Las estructuras jerárquicas ofrecen otros beneficios, particularmente en grandes y complejas redes. Por ejemplo, rompiendo una gran red dentro de áreas que pueden ser controladas individualmente; con ello se puede ayudar a simplificar las tareas de administración de la red. Diferentes áreas pueden tener diferentes grados de accesibilidad y los segmentos de red pueden ser más fácilmente aislados, proveyendo un grado de seguridad deseado.

Tanto algoritmos de vector de distancia y de estado de enlace pueden ser usados para implementar arquitecturas jerárquicas. Sin embargo, el modelo compuesto por LSAa incluye información de la topología (los datos requeridos de la interconexión de segmentos de la red para crear las arquitecturas). En contraste, la información contenida en algoritmos DVAs los datos del modelo de red deben ser integrados manualmente en el orden para crear arquitecturas jerárquicas. De esta manera, el uso de un protocolo basado en LSA, facilita la creación de redes jerárquicas reduciendo considerablemente la cantidad de tiempo.

5.5.7 Las especificaciones de los enrutadores

Normalmente cuando una red es pequeña o está en un edificio solamente, se hace útil el uso de puentes. Esto puede facilitar el tráfico entre los distintos segmentos de una red local muy ocupada. Nótese a la derecha de la figura 5.21, que se han conectado varias subredes a través de puentes, y que el conjunto de las mismas está conectada al soporte FDDI mediante un enrutador.

Para la conexión de diferentes tipos de redes, como una Ethernet a una red FDDI o para hacer conexión a un enlace WAN, es más adecuado el uso de enrutadores. Si una red tiene protocolos múltiples, es necesario usar un enrutador multiprotocolo. Los enrutadores pueden distribuir la carga entre múltiples caminos (balanceo de cargas) simultáneamente. El balanceo de cargas puede superar la velocidad de transmisión para mensajes con alta prioridad y maximiza sobre todo la eficiencia de la red. Además proporcionan el control de las rutas que unen la compleja malla de enrutadores interconectados. También pueden reconfigurar una ruta si falla uno de sus enlaces.

Cuando se evalúan y se compran enrutadores, hay que cerciorarse de que todos los dispositivos de la interred usan los mismos métodos para el enrutamiento y trabajan con los mismo protocolos (algunos enrutadores utilizan técnicas de compresión de datos para el incremento del rendimiento de los paquetes). Para evitar problemas, se debe intentar usar siempre el mismo tipo de enrutador en todos los puntos. Aunque generalmente los métodos de enrutamiento están

estandarizados, un error al comprarlos podría causar problemas que se traducen en la degradación del resultado del enrutamiento.

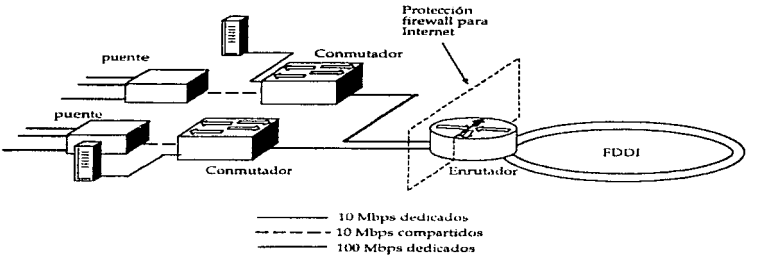


Figura 5.21 Enrutador que provee acceso a una red FDDI

Los sistemas de alta tecnología ofrecen facilidades de tolerancia a fallas, tales como, fuentes de alimentación redundantes y el reemplazamiento de los módulos al instante. Incluso llegando a ser difícil la configuración del enrutador, ya que se debe programar en el dispositivo facilidades como, protocolos múltiples, caminos redundantes, eficiencia y seguridad. Un buen programa de instalación puede facilitar esta tarea. Un ejemplo, es el enrutador multiprotocolo (MPR: Multiprotocol Router) de Novell simplifica en parte la configuración, ya que proporciona algunos de los parámetros válidos por defecto para las redes NetWare, tales como el tamaño de los paquetes, los temporizadores, etc.

Se pueden encontrar enrutadores con diversas características de complejidad. Encontrando dentro de los más complejos los concentradores (*hubs*) completamente cableados que integran en una solo dispositivo, los puertos, los puentes y los enrutadores de la red. Típicamente. incluyen 16 puertos con un soporte opcional para conexiones de área extensa, del tipo FDDI y T1. En el rango medio se encuentran unidades que tienen habitualmente pocos puertos, pero ofrecen esquemas centralizados de cableado y administración. Por último en el extremo bajo están los enrutadores autónomos, que deben emplazarse en varios sitios de la red.

Los enrutadores pueden clasificarse en locales y remotos. Los enrutadores locales tienen conexión para el equipo LAN, del tipo de segmentos Ethernet, Token Ring y FDDI. Un enrutador remoto tiene conexiones para redes de área extensa WAN tales como T1, X-25, Frame Relay, satélites, microondas y otros.

5.5.8 Entornos autónomos

Tanto en el enrutamiento referente a OSI como el de TCP/IP, se usa el concepto de **Sistema Autónomo** (AS: Autonomous System) o **Dominios Administrativos** (AD: Administrative Domain), que normalmente se conocen como dominios. Un dominio es una colección de estaciones y enrutadores que usan el mismo protocolo de enrutamiento y que son administrados por una autoridad solamente, figura 16. Por ejemplo, Internet es un conjunto de sistemas autónomos enlazados basados en TCP/IP, del que forman parte universidades, organizaciones gubernamentales y compañías.

Cada una de estas organizaciones tiene su propia red interna, unida a otras redes de Internet a través de enrutadores (aveces llamados pasarelas externas). TCP/IP tiene **Protocolos de Enrutamiento Interior** y **Protocolos de Enrutamiento Exterior**. Los protocolos OSI también usan el concepto de sistemas autónomos, pero el enrutamiento dentro del mismo dominio se llama enrutamiento **intra-dominio**.

La razón de la existencia de estos protocolos distintos, y la división de dominios, es que no es practico que los enrutadores sigan la pista de todos los sistemas de la red (esquema en plano). La información de enrutamiento se organiza en esta forma jerárquica, de modo que cada dispositivo enrutador sólo necesita almacenar la información necesaria para guiar a los paquetes hasta el siguiente enrutador de importancia.

5.5.8.1 Enrutamiento respecto a OSI

El entorno de Interconexión de Sistemas Abiertos (OSI) consiste en un dominio administrativo que incluye sistemas finales (ES) que son dispositivos de no enrutamiento (computadoras de usuarios o anfitriones) y Sistemas Intermedios (IS) dispositivos de enrutamiento. Un dominio administrativo usa generalmente los mismos protocolos y es controlado por la misma autoridad. Todo el enrutamiento dentro del dominio se conoce como enrutamiento **intra-dominio**. Todo el que se produce fuera de éste para la conexión con otros dominios, se denomina enrutamiento **inter-dominio**.

Todos los sistemas finales en un dominio de enrutamiento particular (referido como área en terminología OSI) tienen un acceso completo a todos los otros sistemas finales en el mismo dominio. El enrutamiento *inter-dominio*, involucra conexiones con entornos en los que no se poseen permisos, y en consecuencia los administradores podrían optar por la selección manual de rutas en lugar de delegar esta tarea a un protocolo de enrutamiento que construyera los caminos entre los dominios de manera automática.

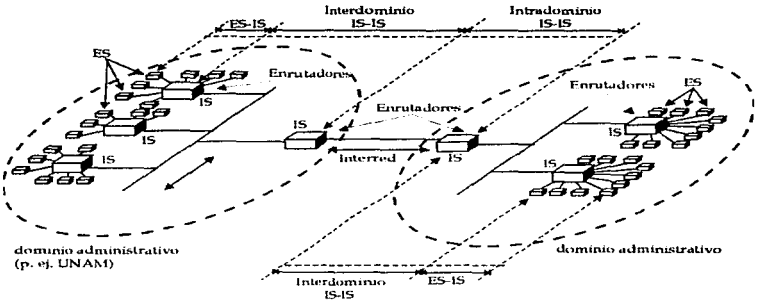


Figura 5.22 Entornos autónomos en el modelo de referencia OSI

Como se ilustra en la figura 4, la arquitectura OSI de enrutamiento es jerárquica y consta de varios protocolos de enrutamiento, incluyendo entre estos :

- **ISO 9542 Protocolo de Enrutamiento entre Sistema Final y Sistema Intermedio** (ES-IS: End System to Intermediate System) para usarse con CLNP (Coneccionless Network Protocolo). Este protocolo describe como los sistemas finales ESs se comunican con sistemas intermedios en un ambiente sin conexión. Los sistemas finales (ESs) dentro de un departamento o grupo de trabajo son aquellos que se comunican con otros a través de la red. Los sistemas intermedios (ISs) se conectan a dicha red para formar los dominios de enrutamiento.
- **ISO 10589 Protocolo de Enrutamiento entre Sistemas Intermedios de Intra-dominio** (IS-IS: Intermediate System to Intermediate System intra-domain routing protocol) Este protocolo describe como los enrutadores o sistemas intermedios se conectan con otros enrutadores en el mismo dominio administrativo, dando lugar a una conexión *intra-dominio*.
- **IDRP Protocolo de Enrutamiento entre Sistemas Intermedios inter-dominio** (IDRP:IS-IS Inter-domain routing protocol). Este protocolo describe como los enrutadores se comunican con otros enrutadores de diferentes dominios. El dominio administrativo se enlaza a otro dominio administrativo, con lo que se forma una interred.

Los protocolos ES-IS e IS-IS se usan para intercambiar información de enrutamiento entre sistemas y así llevar a cabo el intercambio de información . No se debe confundir con los protocolos OSI de distribución de datos llamados **Servicio de Red No Orientado a la Conexión** (CLNS: Connectionless Network Service) y **Servicio de Red Orientado a la Conexión** (CONS: Connection Oriented Network Services). CLNS es un servicio de datagramas que opera al nivel de red y que puede compararse al Protocolo Internet (IP) o al Intercambio de Paquetes entre Redes (IPX) de NetWare. CONS proporciona servicios de sesiones (orientados a conexión) y trabaja al nivel de la capa de transporte, el cual puede compararse con el Protocolo de Control de Transmisión (TCP) de Internet o al Intercambio Secuencial de Paquetes (SPX) de NetWare.

Estos tres protocolos forman una estructura de enrutamiento jerárquico. La información fluye desde un sistema final (ES) a sistemas intermedios (ISs) utilizando ISO 9542. Los ISs intercambian información con otros ISs en el mismo dominio usando ISO 10589, y con sistemas intermedios (ISs) en diferentes dominios usando IDRP.

5.5.8.1.1 ISO 9542 Protocolo de enrutamiento entre Sistema Final y Sistema Intermedio (ES-IS)

Este protocolo es de descubrimiento de vecinos, usado por los sistemas terminales para encontrar la dirección de otros nodos de la misma red. Este protocolo solo se emplea entre sistemas terminales y enrutadores. Hay que señalar que el sistema terminal (ES) sólo ve un "salto" hasta cualquier sistema con el que necesite comunicarse. Para enviar un mensaje a un ES de otro dominio de enrutamiento, el ES transmisor envía paquetes a su sistema intermedio (IS) local y es este IS local el que luego se ocupa de todo el enrutamiento en las áreas interiores y exteriores al dominio.

La tarea del sistema terminal (ES) en el acuerdo ES-IS es bastante simple. Sólo necesita seguir la pista de las direcciones de red de los sistemas con los que puede comunicarse directamente. Esto incluye a los otros ESs de la misma red, o al sistema intermedio enrutador (IS) que le permite enviar mensajes a otros sistemas.

5.5.8.1.2 ISO 10589 Protocolo de enrutamiento entre Sistemas Intermedios (IS-IS) del mismo dominio

Este protocolo es basado en algoritmo de estados de enlace, opera únicamente dentro de un dominio administrativo. A este nivel de la jerarquía OSI, la ocupación primordial es el intercambio de información de enrutamiento y la construcción de las tablas, las que indican cuales son las mejores rutas a través de

la red. Es posible designar a un solo enrutador para que difunda la información de enrutamiento.

El protocolo IS-IS define una área, que es un conjunto de redes físicas y los dispositivos conectados a ellos. Los enrutadores que interconectan redes dentro de una área se denominan enrutadores de nivel 1. Los que interconectan un área con otras son los enrutadores de nivel 2. Un **dominio de enrutamiento** es una conexión de áreas conectadas mediante enrutadores de nivel 2 que trabajan como si formaran una sola unidad administrativa. El enrutamiento tiene lugar como sigue:

1. Un sistema final (ES) envía un paquete a cualquiera de los enrutadores de nivel 1 de su área, de entre los que estén directamente conectados a él.

2. El enrutador determina dónde está situada la dirección de destino y reenvía el paquete a través de la mejor ruta.

3. Si la dirección está en otra área, el enrutador de nivel 1 envía el paquete al enrutador de nivel 2 más cercano.

4. El enrutador de nivel 2 podría a su vez enviar el paquete a otro enrutador de nivel 2, y así sucesivamente, hasta que el paquete alcance su área de destino.

5. Finalmente, un enrutador de nivel 1 del área de destino se ocupará de que el paquete llegue al sistema final.

Por último, este protocolo puede operar en una variedad de subredes, incluyendo redes locales de broadcast (broadcast LANs), redes de área amplia (WANs) y enlaces punto-a-punto.

5.5.8.1.3 Enrutamiento entre Sistemas Intermedios (IS-IS) entre dominios

En el nivel de inter-dominio de la jerarquía OSI, el enrutamiento IS-IS facilita la comunicación entre dos dominios administrativos independientes. Una característica interesante de este nivel, es que no se emplea de forma habitual la configuración de enrutamiento automático, ni la selección automática de la mejor ruta, debido a problemas potenciales de seguridad entre los dos dominios conectados. Además de que también existen consideraciones de costos, como quién paga el enlace, además de autorizaciones, como la admisión a usuarios desconocidos. Usualmente, en estos entornos tampoco se recomienda la conmutación automática de caminos. Lo normal es que los administradores de la red los programen manualmente.

El **Protocolo de Enrutamiento Entre Dominios** (IDRP: Inter Domain Routing Protocol) es un protocolo OSI de enrutamiento basado en algoritmo de estados de enlace (LSA) que enruta paquetes no orientados a la conexión en el entorno entre dominios. Es similar al *Protocolo de Compuerta de Frontera* (BGP: Border Gateway Protocol) de TCP/IP, y se adapta bien a los cambios en la topología, tales como líneas con fallas o conexiones reconfiguradas.

El protocolo IDRP se diseño principalmente para interredes, con lo que se tiene que reducir para que se pueda ocupar del enrutamiento dentro de una red. Este protocolo utiliza caminos seguros y estables entre los nodos terminales de los dominios que conecta. Se puede añadir soporte para IP, con lo que se podría enrutar tanto IP como CLNP (Connectionless Network Protocol: Protocolo de red no orientado a la conexión) en los inter-dominios con un mismo protocolo referido como "dual IS-IS".

5.5.8.2 Enrutamiento respecto a TCP/IP

La arquitectura de enrutamiento de Internet (TCP/IP) es similar a la arquitectura de Interconexión de Sistemas Abiertos (OSI). Existe también una jerarquía de sistemas formada por subredes a las que se conectan las estaciones. Estas subredes se acoplan a los enrutadores, que son los que las conectan a las otras subredes dentro del sistema autónomo. Un **sistema autónomo** (también llamado sistema interior o dominio) es una colección de subredes y enrutadores que, generalmente usan los mismos protocolos de enrutamiento y están bajo el mismo control administrativo. A continuación se mencionan los protocolos más comunes dentro del esquema TCP/IP tanto para compuerta interior como de compuerta exterior.

Los *Protocolos de* **Compuerta Interior** como el **Protocolo de Información de Enrutamiento** (RIP: Routing Información Protocol) y la **Primera Ruta más Corta en Abrir** (OSPF: Open Shortest Path First) se usan para intercambiar información de enrutamiento dentro de un dominio. El OSPF es un protocolo de enrutamiento interior, muy similar al protocolo IS-IS del modelo OSI.

En los límites de los dominios se encuentran los enrutadores de frontera, que conectan un dominio con otro. Estos enrutadores emplean el **Protocolo de Enrutamiento Exterior** (EGP) para intercambiar la información de enrutamiento. El **Protocolo de Compuerta Exterior** (EGP: Exterior Gateway Protocol) proporciona un medio para que dos enrutadores vecinos situados en los límites de sus respectivos dominios, intercambien mensajes de información. Existe una alternativa al EGP que es el **Protocolo de Compuerta de Frontera** (BGP: Border Gateway Protocol) y que aporta algunas mejoras como la posibilidad de especificar **enrutamiento basado en políticas** (Policy-Base routing).

5.5.8.2.1 Protocolos de compuerta interior

Los **protocolos de compuerta interior** son los que se utilizan para el intercambio de información de enrutamiento en el interior de los dominios. Los más habituales son:

5.5.8.2.1.1 Protocolo de Resolución de Dirección (ARP: Address Resolution Protocol)

ARP es el protocolo de descubrimiento de vecinos en el esquema de redes TCP/IP. Actúa de forma similar al Enrutamiento entre Sistemas Final y Sistema Intermedio (ES-IS, End System to Intermediate System) de OSI. Tanto los enrutadores como las estaciones, usan ARP para anunciarse a ellos mismos con otros sistemas vecinos. Es decir, un enrutador emite paquetes que contienen una dirección IP, la computadora o el dispositivo conectado a la red que posea esa dirección, devuelve su dirección MAC. La información recolectada por el enrutador se sitúa en las tablas de enrutamiento para futuros usos y de esta manera mantener sus tablas. Un protocolo similar, llamado **ARP Inverso** (RARP: Reverse Address Resolution Protocol), realiza la tarea opuesta, obtiene la dirección IP a partir de una dirección MAC dada.

5.5.8.2.1.2 Protocolo de Información de Enrutamiento (RIP: Routing Information Protocol)

Este protocolo es basado en algoritmos de vector distancia (DVA) para el cálculo de los caminos de enrutamiento intra-dominio. Se produce un intercambio de tablas de enrutamiento RIP aproximadamente cada 30 segundos, y los enrutadores reconstruyen sus tablas basándose en esa nueva información. El protocolo RIP fue diseñado para redes razonablemente homogéneas pequeñas o moderadas de tamaño. Sin embargo, en redes más grandes o interredes de trabajo mas complicadas, RIP ha tenido varias desventajas. Primero, RIP tiene un límite de contador de saltos de hasta 16. Segundo, el protocolo no puede escoger rutas basadas en parámetros de tiempo real, tales como, retraso o carga. Por lo anterior, puede ocurrir que un enrutador se retrase durante la reconstrucción de sus tablas si esta conectado con un enlace WAN de bajo rendimiento. Además, el intercambio de la tabla de enrutamiento puede añadir mucha sobrecarga a la red, lo que provocará una mayor congestión y un mayor retraso en las actualizaciones de las tablas. Si una ruta falla, el restablecimiento de una nueva ruta se puede ver retrasada por el tiempo necesario para reconstruir las nuevas tablas de enrutamiento.

5.5.8.2.1.3 Primera Ruta más Corta en Abrir (OSPF: Open Shortes Path First)

OSPF es un algoritmo de enrutamiento basado en algoritmos de estado de enlace para enrutamiento intra-dominio y es derivado del **Protocolo Interior de Enrutamiento entre Sistemas Intermedios** (IS-IS del mismo dominio) de OSI. Las tablas de enrutamiento OSPF sólo se actualizan cuando es necesario y sólo con la información significativa.

Características adicionales del OSPF incluyen costos iguales de enrutamiento multi-ruta y enrutamiento basado en peticiones de tipo de servicio (TOS) de capas superiores. Soporta enrutamiento basado en TOS para aquellos protocolos de capas superiores que pueden especificar particulares tipos de servicio. Por ejemplo, una aplicación puede especificar que ciertos datos tienen la prioridad de urgentes. Si OSPF tiene enlaces de alta prioridad disponibles, estos pueden ser usados para transportar los datagramas urgentes.

OSPF soporta una o más tipos de métricas, si solo una métrica es utilizada, esta será considerada como arbitraria y no podrá soportar TOS. Si más de una métrica es usada, TOS es soportada opcionalmente a través del uso de métricas separadas.

5.5.8.2.2 Protocolo de compuerta exterior (EGP: Exterior Gateway Protocol)

El **Protocolo de Compuerta Exterior** fue el primer protocolo inter-dominio usado por Internet. Utilizado para la comunicación entre los enrutadores principales de Internet. Es decir, proporciona un camino para que enrutadores próximos, situados en los límites de sus respectivos dominios, intercambien mensajes e información. Así, los enrutadores intercambian información acerca de sí mismos. Cada dominio tiene al menos un enrutador susceptible de convertirse en un enrutador EGP. Estos enrutadores principales de Internet, forman el backbone de enrutamiento.

Cada EGP intercambia información de enrutamiento con los enrutadores interiores de su dominio, mediante un **Protocolo de Compuerta Interior** (IGP), de tal modo que se conoce la dirección de los sistemas terminales de ese dominio local. Las enrutadores EGPs se conectan con los enrutadores EGPs de otros dominios e intercambian información acerca de los sistemas terminales de sus respectivos dominios. Con esta información, los enrutadores pueden determinar el mejor camino para enviar la información a otros sistemas exteriores a su dominio.

Las principales funciones de los enrutadores EGP son las siguientes:

- Realizar el procedimiento de conexión entre vecinos, para lo cual se conectan los enrutadores exteriores y deciden intercambiar información.
- Verificar periódicamente a los enrutadores vecinos, mediante el envío de un mensaje y la espera de la respuesta. Este proceso se realiza para cerciorarse de que todavía está disponible el enrutador exterior.
- Intercambiar periódicamente información de enrutamiento.

Las rutinas del protocolo EGP de un enrutador pueden realizar un escrutinio entre los enrutadores vecinos para obtener información actualizada. Habitualmente se mantienen dos tablas, una con los caminos interiores realizada a partir de los **protocolos interiores** o intra-dominio del tipo de RIP u OSPF, y otra con los caminos exteriores, obtenida con EGP. Sin embargo, EGP tiene fallos que el **Protocolo de Compuerta de Frontera** (BGP: Gateway Protocol) trata de resolver. Esto es consecuencia de que el protocolo EGP se diseño cuando TCP/IP constaba de un solo sistema de cableado principal (backbone), es decir, un esquema en **plano**. Por tanto, es ineficiente para la red con múltiples redes interconectadas (o backbones) de hoy en día.

Finalmente, los enrutadores EGP tienen prefijadas unas tablas estáticas de enrutamiento, que definen explícitamente cuáles de los enrutadores se pueden conectar. Esto evita bucles y proporciona seguridad, pero hace más difícil modificar el tamaño de la red.

5.5.8.2.3 Protocolos de "Enrutamiento Basados en Políticas" entre dominios

Dentro de las funciones de enrutamiento avanzadas se han propuesto varios nuevos protocolos de enrutamiento entre dominios, para que se usen entre redes. A medida que el número de redes crece, deja de ser fácil adaptar los protocolos exteriores existentes para que trabajen con este mayor número.

El **enrutamiento basado en políticas** provee a los administradores de red a habilidad de especificar fuentes adicionales de información para las tablas de enrutamiento y modelo de la red. Estas fuentes pueden incluir información derivadas desde el estado operacional de la red o información que por medio estático, el administrador de la red configura. Tales políticas pueden ser definidas sobre bases enrutador-a-enrutador. Enrutamiento basado en políticas es frecuentemente utilizado como un significado de proveer seguridad a la red.

Los nuevos protocolos que implementan el **enrutamiento basado en políticas** son más adaptables que el protocolo EGP. El "enrutamiento basado en políticas"[78] da a los administradores un mayor control sobre la red, además permiten dar prioridad al tráfico, la implantación de medidas de seguridad y el cobro de los servicios. Algunos ejemplos de este tipo protocolos es el Protocolo de Compuerta de Frontera (BGP) y el Protocolo de Enrutamiento Entre Dominios (IDRP).

5.5.8.2.3.1 Protocolo de Compuerta de Frontera (BGP: Border Gateway Protocol)

El **Protocolo de compuerta de frontera** se implementó como una solución provisional. BGP es un protocolo de enrutamiento inter-dominio creado para el uso de enrutadores del backbone de Internet. A diferencia de EGP, BGP fue diseñado para detectar enrutamientos cíclicos y para utilizar una métrica de tal manera que un enrutamiento más inteligente pueda ser realizado.

Aun que BGP es un protocolo inter-dominio, BGP puede ser usado dentro y entre dominios. Dos vecinos de comunicación BGP entre dominios deberá residir sobre el misma red física. Los mensajes de actualización de BGP son enviados sobre el mecanismo de transmisión confiable TCP. La métrica de BGP es un número de unidad arbitraria especificando el "grado de preferencia" de una ruta particular. Estas métricas son generalmente asignadas por el administrador de la red a través de archivos de configuración.

Este proporciona algunas de las ventajas del enrutamiento basado en políticas, pero no resuelve los problemas implícitos al cambio de tamaño. También añade algunos atributos a las rutas, en el tipo de costo o la seguridad de un camino. Además, el protocolo BGP reduce el ancho de banda requerido para el intercambio de la información de enrutamiento, ya que esta información se envía incrementalmente, en lugar de enviar la totalidad de la base de datos.

5.5.8.2.3.2 Protocolo de Enrutamiento Mediante Políticas Entre Dominios (IDPR: Inter Domain Policy Routing)

El IDPR entre dominios es un protocolo basado en algoritmos de estado de enlace que implementa el enrutamiento fuente y el enrutamiento basado en políticas entre dos dominios. El enrutamiento fuente aporta algunas ventajas sumamente prácticas, dado que los paquetes soportan en sí mismos la información acerca de la ruta. Inicialmente, es necesario descubrir el camino adecuado, pero a continuación dicho camino se sitúa simplemente en la cabecera de los paquetes.

---

[78] En la actualidad, el enrutamiento entre políticas es un requisito en Internet.

	RIP	IGRP	OSFP	ISO IS-IS ISO ES-IS	EGP	BGP
Estático vs Dinámico	D	D	D	D	D	D
Distribuido vs Centralizado	D	D	D	D	D	D
Singular vs Multiruta	S	M	M	ES-IS=S IS-IS=M	M	S
Plano vs Jerárquico	P	P	J	ES-IS=P IS-IS=J	P	P
Fuente vs Enrutador inteligente	E	E	E	E	E	E
Intra vs Inter-Dominio	Intra	Intra	Intra	ES-IS=intra IS-IS=ambos	Inter	Inter
Estado de Enlace vs Vector de Distancia	DV	DV	EE	ES-IS=no IS-IS=EE	no	no
Años de especificación inicial	10	6	2	5	9	2
Factores de métrica considerados	contador de saltos, retraso, ancho de banda, carga, MTU	Costo, Núm. de unidad de confiabilidad opcional, servicioTOS.	arbitrario	ES-IS=- IS-IS= numero de unidades arbitrario	núm. de unidades arbitrario	arbitrario

Arbitrario: es un número de unidad arbitraria especificado por el grado de preferencia de una ruta particular. Estas métricas son generalmente asignadas por un administrador de red a través de un archivo de configuración. El grado de preferencia puede estar basado sobre cualquier número de criterios, incluyendo inclusión de dominios (las rutas con menor inclusión de dominios son mejores), tipos de enlace (el enlace es estable? rápido? eficaz ?) y otros factores.

Tabla 5.4 Resumen de características de los protocolos de enrutamiento

5.5.8.3 Resumen

Protocolos interiores o intra-domino

- Protocolo de resolución de direcciones de TCP/IP (ARP Address Resolution Protocol) es de reconocimiento de vecinos.
- Protocolo de información de enrutamiento (RIP: Routing Información Protocol) es un protocolo basado en vector distancia de TCP/IP.
- Primero Ruta más Corta en Abrir (OSPF) es un protocolo de enrutamiento basado en algoritmo de estado de enlace, OSPF es el protocolo de enrutamiento interior habitual en TCP/IP, aunque también se utiliza el IS-IS del modelo OSI. Cabe mencionar que es mejor que el protocolo RIP.

- Sistema Final a Sistemas Intermedio (ES-IS) es un protocolo OSI, que facilita a los sistemas finales encontrar los enrutadores u otros sistemas finales del mismo dominio.
- Enrutamiento entre Sistemas Intermedios del mismo dominio (IS-IS) es un protocolo OSI que enruta paquetes entre dos enrutadores en el interior de un dominio. Es un protocolo basado en estado de enlace.

Protocolos exteriores o inter-dominios

En los límites de los dominios autónomos existen ciertos enrutadores intercambiando información unos con otros mediante los protocolos exteriores. En la terminología de Internet se conocen como Protocolos de Compuerta Exterior (EGP: Exterior Gateway Protocol).

- Protocolo de Compuerta Exterior (EGP), es el protocolo original de TCP/IP.
- Protocolo de Compuerta de Frontera (BGP), actualmente esta reemplazando al protocolo EGP.
- Protocolo de Enrutamiento Intermedio (IDRP), es un protocolo estándar al modelo OSI.

Características	Puente	Enrutador
Protocolos o algoritmos de enrutamiento	Normalmente no	Si
Transparencia de protocolos	Si	Solo con ruteadores de protocolos independientes
Uso de direcciones de red	No	Si
Modo de operación promiscuo	Si	No
Decisión de reenvío	Elemental	Puede ser complejo
Multiples trayectorias de transmisión	Limitado	Alto
Control de enrutamiento	Limitado	Alto
Control de flujo	No	Si
Fragmentación de frames	No	Si
Tasa de procesamiento de paquetes	Alto	Moderado
Costo	Menos caro	Mas caro

Tabla 5.5 Comparación entre puentes y enrutadores

5.5.9 Trabajo conjunto de conmutadores y enrutadores

Como se explicó anteriormente en este capítulo, un conmutador es un dispositivo de propósito especial específicamente diseñado para la resolución de problemas de desempeño de direccionamiento de redes locales que van desde anchos de banda pequeños y cuellos de botella de redes. Los conmutadores resuelven estos problemas al proveer un ancho de banda agregado, un rendimiento alto de

transmisión de paquetes y una baja latencia a un bajo precio por puerto. Estos dispositivos no han sido diseñados con el objetivo principal de proveer un control íntimo sobre la red. Los conmutadores deben ser vistos como proveedores de ancho de banda y no como proveedores de fuentes de seguridad, redundancia, control o administración de red. Los conmutadores resuelven estos problemas al segmentar un dominio de colisión de red local dentro de pequeños dominios de colisión más pequeños. Esta segmentación reduce o casi elimina la contención de estaciones por el acceso al medio y provee a cada estación con un gran ancho de banda compartido de red local.

Por otro lado, un enrutador es un dispositivo de propósito general diseñado para desarrollar las siguientes funciones principalmente:

- Segmenta la red dentro de dominios de broadcast individuales.
- Suple un envío inteligente de paquetes.
- Provee un acceso costo-efectivo hacia un red de área amplia (WAN).
- Soporta rutas de red redundantes.

A diferencia un conmutador, el cual es específicamente diseñado para agregar capacidades de ancho de banda, los enrutadores son diseñados para proveer seguridad, políticas y administración de red.

Una de las funciones primarias de un enrutador es la de proveer un aislamiento de tráfico para ayudar al diagnóstico de problemas. Ya que cada uno de los puertos de un enrutador es una subred separada, el tráfico de broadcast no cruza el enrutador. La definición de frontera de red hace mas fácil para un administrador de una red proveer redundancia y aislamiento de problemas resultado de varias causas. Los enrutadores mantiene estos eventos locales en el área en la cuál ellos ocurrieron. Los enrutadores son los únicos dispositivos que pueden proveer un acceso económico a redes de área amplia (WAN). Otro importante beneficio de los enrutadores es su habilidad para soportar topologías de malla de redes que proveen rutas redundantes y ciclos activos. En adición, los enrutadores pueden desarrollar un balanceo de cargas a través de las diferentes caminos y hacer un mejor uso del ancho de banda disponible. A diferencia de los conmutadores y puentes , los cuales requieren de una topología libre de rutas redundantes o ciclos.

Los enrutadores tienen otras importantes capacidades, dentro de estas se incluyen:

- Proveer seguridad a través del uso de sofisticados filtros de paquetes tanto en ambientes de redes de área amplia como en redes locales.
- Permite la creación de diseño de redes jerárquicas.
- Una integración flexible de diferentes tecnologías de enlace de datos, tales como, Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

5.5.9.1 Diferencias entre segmentación con conmutadores y enrutadores

Probablemente un área de gran confusión acerca de los conmutadores y los enrutadores es su habilidad de segmentar una red. Partiendo de que los conmutadores y los enrutadores operan en diferentes niveles del modelo OSI cada dispositivo puede desarrollar un tipo de segmentación único diseñado para beneficiar a diferentes necesidades de aplicación.

Como se mencionó anteriormente, un conmutador es un dispositivo de propósito especial llevando a cabo la segmentación de una red local, con el objetivo de proveer un ancho de banda adicional. Un enrutador es un dispositivo de propósito general diseñado para segmentar un red con los objetivos de limitar el tráfico de broadcast (broadcast traffic) y proveer seguridad, control y redundancia entre dominios de broadcast individuales.

Para propósitos de esta discusión, una red local es definido como un repetidor de dominio de colisión. Un conmutador es diseñado para segmentar el dominio de colisión de una red local dentro de varios dominios de colisión más pequeños. Esto puede resultar como en agrandar el desempeño de la red por que la segmentación en el nivel de la capa 2 reduce el número de estaciones compitiendo por el acceso al medio.

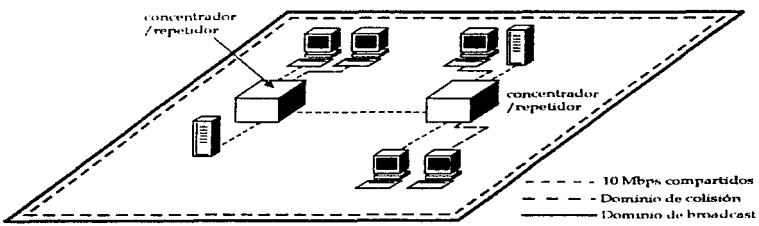


Figura 5.23 Grupo de trabajo antes de la instalación de un dispositivo inteligente de red para llevar a cabo alguna segmentación

La figura 5.24, ilustra como un conmutador segmenta un gran dominio de colisión dentro de pequeños dominios de colisión. Cada dominio de colisión representa un ancho de banda de 10Mbps.Antes de instalar el conmutador, todas las estaciones en el dominio de colisión de red local compartían 10Mbps de ancho de banda.

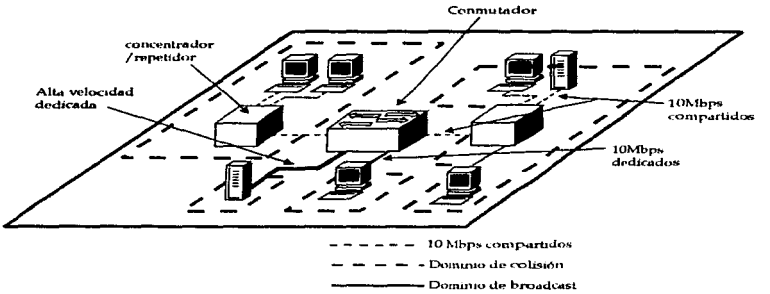


Figura 5.24 Se demuestra como se lleva a cabo la segmentación de un grupo de trabajo por medio de un conmutador

La instalación del conmutador incrementa el desempeño al proveer a los usuarios con un ancho de banda agregado de 60 Mbps.

Es importante hacer notar que los dominios de colisión individuales son aún miembros del mismo dominio de broadcast . Esto significa que el tráfico de broadcast generado en un dominio de colisión es aún enviado a todos los otros dominios de colisión, asegurando que todas las estaciones en la red puedan aún comunicarse unas con otras.

5.5.9.2 Subredes segmentadas por enrutadores

Una subred es un dominio de broadcast puenteado o conmutado compuesto de dominios de colisión individuales. Un enrutador es diseñado para interconectar y definir los niveles de los dominios de broadcast (broadcast domains).

La figura 5 demuestra un gran dominios de broadcast que ha sido segmentado por conmutadores dentro de pequeños dominios de colisión. En este ambiente conmutado, el tráfico de broadcast originado en un dominio de colisión es enviado a todos los otros dominios de colisión.

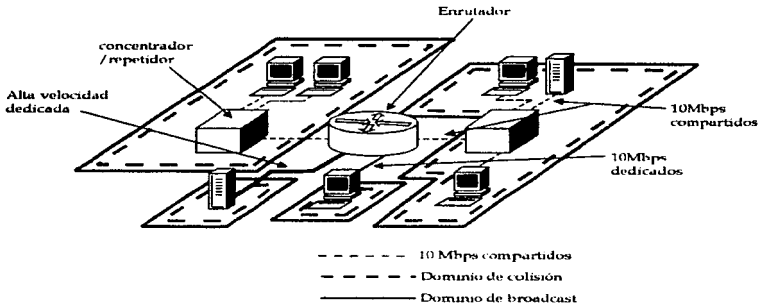


Figura 5.25 Se demuestra un grupo de trabajo segmentado por medio de un enrutador

En la figura 6 ilustra la misma red después de que ha sido segmentada por un enrutador dentro de dos diferentes dominios de broadcast . En un ambiente enrutado, el tráfico de broadcast generado dentro de cada dominio de broadcast no fluye cruzando el enrutador dentro de otro dominio de broadcast . Como un resultado, la cantidad de tráfico experimentado por una interred como un todo es reducido.

Después de entender las diferentes maneras que los enrutadores y conmutadores segmentan una red. Puede existir la confusión del por que un enrutador que opera al nivel de la capa 3 puede también desarrollar funciones de nivel de la capa 2 de un conmutador. La segmentación de capa 3 no solo crea dominios de broadcast separados, también crea un dominio individuales de colisión para cada una de las interfaces del enrutador. Esto significa que un conmutador o un enrutador pueden ser empleados para segmentar una red local y proveer ancho de banda adicional. A partir de esta observación, queda saber cual es la mejor elección para el diseño actual de las redes.

Si las aplicaciones requieren soporte de rutas redundantes, envío inteligente de paquetes o acceso a redes de área amplia, un enrutador deberá ser seleccionado. Si la aplicación requiere solamente de incremento de ancho de banda para facilitar el tráfico de cuello de botella, un conmutador es probablemente la mejor elección. El costo para un nivel de desempeño dado es el mejor diferencia en la decisión para instalar un enrutador o un conmutador en un ambiente de grupo. Los diseñadores de redes deben determinar la existencia de otros requerimientos, tales como

redundancia, seguridad o la necesidad de limitar el tráfico de broadcast . Que son las justificaciones para hacer un gasto extra y utilizar un enrutador dentro de un ambiente de grupos de trabajo.

La tendencia actual es conjuntar el empleo mutuo de estos dos dispositivos. En lugar de escoger entre conmutadores, puentes y enrutadores, los diseñadores de redes deberán entender como llevar a cabo la combinación de estas tecnologías y construir una red de alto desempeño y que sea escalable. Siguiendo la filosofía "conmutar donde se pueda y enrutar donde se deba".

Por lo anterior, se puede decir que , la conmutación y en enrutamiento son tecnologías complementarias que permiten a las redes escalar a tamaños mas allá que los que se pueden desarrollar usando solamente una tecnología. Los conmutadores pueden ser integrados fácilmente dentro de redes con enrutadores ya existentes como reemplazos para la base instalada de repetidores, concentradores, y puentes. Cuando ATM sea eventualmente implementada en el backbone, el enrutamiento será una tecnología requerida para la comunicación entre redes locales virtuales (VLANs). Aun que la tecnología de conmutación es aún el principal punto hacia el futuro, el enrutamiento continuará siendo una tecnología importante tanto como las aplicaciones de escritorio se encuentren basadas en protocolos de red local que permitan direccionamiento, tales como IP, IPX y AppleTalk.

5.5.9.3 Diseño de ambientes de un backbone colapsado

Durante varios años, las organizaciones han estado desarrollando estructuras de arquitecturas de "backbone colapsado" en los centros de información. En un ambiente de "backbone colapsado", grandes cantidades de datos son transferidos cruzando el plano posterior de un dispositivo de "backbone colapsado".

El aprovechamiento del **backbone colapsado** tiene un número de beneficios cuando es comparado a las arquitecturas tradicionales de **backbone distribuido** (distribuited backbone) que este complementa. Un diseño de **backbone colapsado** de complejidad centralizada, incrementa el desempeño, reduce los costos y soporta el modelo de grupo de servidores (server farm). Sin embargo, este aprovechamiento tiene sus limitaciones. Desde que el dispositivo de **backbone colapsado** puede llegar a ser un potencial problema de cuello de botella y posiblemente es un solo punto de falla (para reparar esto se recomienda tener un dispositivo redundante contra fallos).

El dispositivo que desempeña la función de **backbone colapsado** puede ser un conmutador de alto desempeño o un enrutador. Dependiendo de si la función primaria del **sistema de principal** es puramente de desempeño, la selección idónea es un conmutador. Si el objetivo es desempeño y seguridad se debe

seleccionar un enrutador. Un enrutador es más complejo y mas caro que un conmutador.

Los **backbones** son una parte esencial de la infraestructura de comunicación que deberá ser protegida contra fallos. En la actualidad se utilizan tanto conmutadores como enrutadores trabajando conjuntamente en un diseño que completamente el "backbone".

5.6 Brouters

Actualmente los ambientes de interconexión de redes remotos o sitos centralizados, existe un lugar tanto para enrutadores como para puentes. Puentes y enrutadores son frecuentemente usados conjuntamente para ayudar a simplificar las conexiones que de otra manera serían complejas. Esta relación complementaria es reflejada actualmente en dispositivos puente/enrutador referidos comúnmente como **brouters**. Estos dispositivos combinan las dos tecnologías, enrutan ciertos protocolos mientras puentean otros.

Un **brouter** puede ser considerado como un dispositivo híbrido, presentando una combinación de las capacidades del puente y del enrutador simultáneamente.

5.6.1 Modo de operación de los brouters

Cuando un brouter recibe un frame este lo examina y determina si es destinado para otra red. Si es así, este verifica el protocolo del frame para determinar si es soportado por la Capa de Red (que soporta las funciones del enrutador). Si es soportado, el brouter enruta el frame de manera similar como lo hace un enrutador. De otra manera, si el frame no es soportado por el protocolo de red, el brouter manejará el frame usando la capa de enlace de datos como si fuese un puente.

Cabe mencionar que un dispositivo enrutador ignora simplemente un frame que no soporte el protocolo de red, mientras que el brouter lleva a cabo una función de puente para dicho frame. Por lo tanto, en comparación al enrutador, el brouter provee una capa adicional de conectividad entre redes, aunque la conectividad tenga lugar en una capa menor del modelo de referencia OSI.

5.6.2 Utilización de los brouters

La principal ventaja del uso de los brouters es que se obtiene la habilidad de tecnologías tanto de puente como de enrutador. La capacidad de desempeñar estas dos funciones habilita al brouter para remplazar el uso separado del puente y del enrutador en algunas aplicaciones de interconexión de redes. Por ejemplo, considere el uso de un puente y un enrutador separados en la figura 5.27 (parte

superior). En este ejemplo, el puente da la capacidad para interconectar dos redes relativamente cerca, mientras que el enrutador da la capacidad para interconectarse con redes distantes. Se puede reemplazar el puente y el enrutador por un brouter obteniéndose el mismo nivel de funcionalidad, esto se muestra en la figura 5.27 (parte inferior). Aun así, con la utilización del brouter se puede introducir retardos que afectan el desempeño de la red.

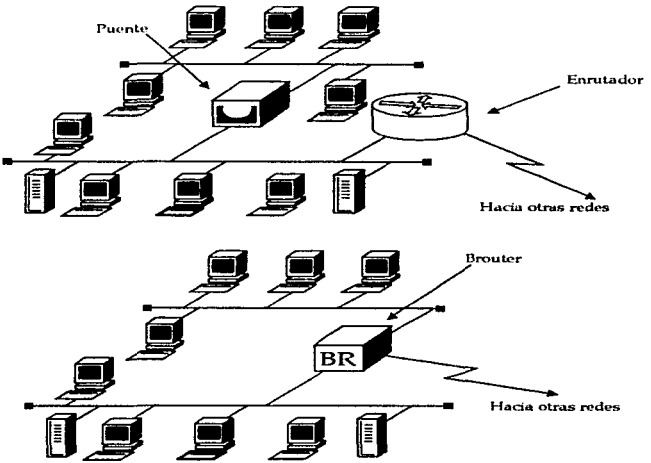


Figura 5.26 Reemplazo de un brouter en lugar de un enrutador y un puente por separado. brouter es un dispositivo híbrido que representa una tecnología nueva de puente y enrutador. Es decir, un brouter es un dispositivo que envía paquetes entre redes en el nivel de red y en el nivel de enlace de datos

5.7 Compuertas (Gateway)

El termino de **compuerta** (gateway) fue adoptado originalmente para referirse a un dispositivo que proporcionará una trayectoria de comunicación entre dos redes locales y una computadora mainframe desde la capa física hasta la Capa de Aplicación. En la figura 5.28 se ilustra la operación de una compuerta con respecto al Modelo de Referencia OSI. Desde su descripción de operación original, el termino "compuerta" ha sido usado mas libremente para describir una gama de productos que van desde puentes que simplemente conectan dos redes locales hasta convertidores de protocolos que proveen un acceso asíncrono dial-up a una red SNA de IBM.

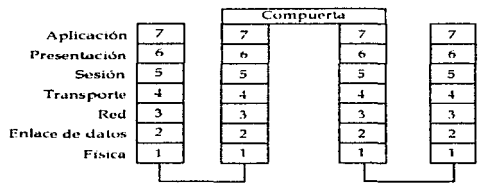


Figura 5.27 Operación de una compuerta con respecto al modelo de referencia OSI

5.7.1 Definición de compuerta

Para el propósito de este trabajo se usara el termino **compuerta** como destino originalmente, para describir dispositivos que desempeñan la conversión de protocolos a través de las siete capas del Modelo de Referencia OSI. Así, una compuerta desempeña todas las tareas de un enrutador así como también la conversión de protocolos.

5.7.2 Operación de una compuerta

Las compuertas son protocolos específicos para su función, generalmente usados para proveer acceso a mainframes. Algunos vendedores fabrican compuertas multiprotocolos. Tales productos se fabrican normalmente como tarjetas adaptadoras que contienen procesadores (procesos) separados que se instalan en alguna unidad de una computadora personal o dispositivo especialmente diseñado por el fabricante. Cuando se usa con el software apropiado del vendedor, este tipo de compuerta es realmente una compuerta N-in-1, donde N se

refiere al número de conversión de protocolos y conexiones separadas que puede manejar la compuerta.

En la figura 5.29 se ilustra el uso de una compuerta multiprotocolo para unir estaciones de trabajo de una red local a un mainframe IBM por medio de una enlace SDLC y por medio de una conexión frame relay a una red de paquetes conmutados. Una vez conectada a la red de paquetes conmutados, el tráfico de la red local puede ser enrutada.

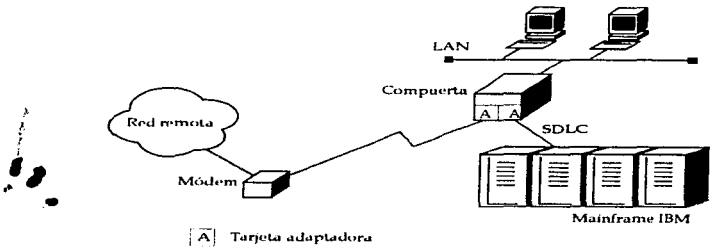


Figura 5.28 Operación de una compuerta multiprotocolos. El cuál puede ser usado para proveer facilidad de acceso a estaciones de una red LAN hacia múltiples esquemas computacionales

Las compuertas se diseñan para ser usadas principalmente para conectar redes LAN-a-WAN y no para la comunicación entre redes locales únicamente. Debido a las sofisticadas funciones que realiza una compuerta este es mas lento que un enrutador. Además, a consecuencia del gran número opciones para los protocolos que pueden ser considerados cuando se configura una compuerta, su instalación es considerablemente mas difícil que la instalación de un enrutador.

5.8 Concentradores (Hubs)

Tanto las redes Ethernet como Token Ring usan concentradores o hubs. En una red Token Ring, el concentrador se refiere a una Unidad de Acceso Multi-estación (MSAU: Multistation Access Unit). La conexión de las estaciones de trabajo al MSAU forman una estrella, con los MSAUs interconectados forman un anillo. En una red Ethernet 10BASE-T, las estaciones de trabajo conectadas al concentrador en forma de estrella. Los concentradores son conectados uno con otro, formando un bus.

Ethernet como Token Ring utilizan una instalación estándar de cableado entre las estaciones de trabajo y el concentrador, como es el cable de par trenzado. Puesto que las estaciones de trabajo son conectadas a un punto único, la administración de redes basada en concentradores son usualmente simples y de menor precio, permitiendo desde un punto central realizar la configuración y reconfiguración, monitoreo y administración de la red. Este tipo de productos proveen a los usua.ios la habilidad para construir redes de área local, desde redes con un pequeño número de nodos hasta redes con varios protocolos y varios cientos de nodos que pueden ser monitoreados, modificados y analizados desde un punto solamente.

Hay varios tipos de concentradores, por lo que en este documento solo se trataran los más importantes.

5.8.1 Tipos de concentradores

Los concentradores se caracterizan principalmente por ser del tipo pasivo o del tipo activos, estos se explican a continuación.

5.8.1.1 Concentradores pasivos

Este tipo Tiene pocos puertos para la conexión de estaciones de trabajo en una configuración tipo estrella, no llevan a cabo ninguna amplificación de señal. Es un panel de distribución que no requiere una conexión eléctrica alguna.

5.8.1.2 Concentradores activos

Generalmente contienen un mayor número de puertos que los concentradores pasivos, además de que regeneran las señales y requieren de una conexión eléctrica. Estos se utilizan como repetidores. La detección de colisiones se maneja por las tarjetas de interfaz de red de cada uno de los sistemas terminales.

Los concentradores se conectan con otros, generalmente, en una forma jerárquica comúnmente referida como en cascada, como se muestra en la figura 5.30, este tipo de configuraciones se utilizan en un **sistema de cableado estructurado** (EIA/TIA 568). Generalmente se utiliza cable de par trenzado. Los concentradores hacen posible la existencia del cableado estructurado y proporcionan de esta manera los siguientes beneficios:

- Los cambios en una red serán fáciles de realizar si se cuenta con un sistema de cableado estructurado construido a partir de concentradores.
- Se podrá expandir en una forma más ordenada y sencilla.
- Los concentradores se pueden utilizar con varias tecnologías, como Ethernet, FDDI, Token Ring y tener conexiones a redes de área amplia.

- **Los concentradores tienen utilidades para la tolerancia a fallas.**

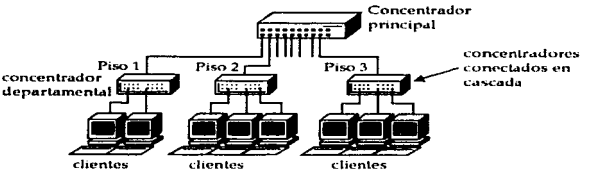


Figura 5.29 Ejemplificación de concentradores jerárquicos o conectados en cascada

Una desventaja que existe cuando se utiliza cable de par trenzado de cobre es la limitación de la distancia. Los concentradores reducen en cierta manera el problema, debido a que actúan como dispositivos repetidores. Por ejemplo, en una red Ethernet 10Base-T, una estación puede encontrarse al final de una configuración serie hasta con cuatro concentradores intermedios (en cascada).

La topología de las redes que utilizan concentradores es una configuración en estrella, esto tiene una gran ventaja y es que cada cable conecta una estación única y la desconexión o falla de una de estas líneas no afecta a toda la red, por esta misma razón se hace más fácil la detección de fallas.

5.8.2 Evolución de los concentradores

En las redes Ethernet originales se utilizaba cable coaxial, que tenía varias desventajas, como la pérdida de conectores, las interferencias producidas por fuentes externas, las conexiones a tierra, los cables excesivamente inflexibles o una simple falla en la conexión de un cable a un conector en forma de T. El problema era localizar de forma precisa la falla. Los concentradores se diseñaron para resolver en gran parte estos problemas.

Los concentradores han evolucionado a través de varias generaciones. Actualmente son los principales componentes de los sistemas de cableado estructurado. Un concentrador puede actuar como el centro de **backbone principal** de una compañía. Los concentradores se conocen a menudo como dispositivos de **soporte colapsado**.

Los concentradores llegaron a ser populares en el entorno de escritorio con el crecimiento de la configuración en estrella de Ethernet 10Base-T. Los administradores expandieron sus redes mediante la compra de concentradores adicionales y los enlazaron mediante cables de conexión. Después se crearon cajas

que disponían de ranuras de expansión, en los que se podían situar 10, 12 o más conectores RJ-45 sobre un módulo de expansión que se puede conectar a cada una de dichas ranuras. El resultado produjo potencia y redujo el costo del componente.

El concentrador utiliza una arquitectura de bus especial que le permite servir de soporte a redes como Ethernet, FDDI, ATM, Token Ring, etc.

Proporcionan facilidades de administración que pueden utilizarse desde una estación de trabajo, normalmente con aplicaciones gráficas, que muestran planos de la red completa y permiten ampliar segmentos individuales para la visualización de estadísticas o la obtención de información de auditoría.

5.8.2.1 Concentradores de la primera generación

Los primeros concentradores consistían en simples repetidores que daban soporte a un medio único de transmisión. La configuración de cableado que se utilizaba era apropiado para una red local departamental o para un grupo de trabajo de alrededor de 20 usuarios. No había soporte para protocolos de administración como SNMP.

En el mercado actual, todavía existen concentradores de repetición de la primera generación, debido a que existen numerosas redes locales pequeñas.

5.8.2.2 Concentradores de la segunda generación

Los concentradores de la segunda generación se denominan **concentradores inteligentes** (*smart hubs*), pues incorporan utilidades de administración. Estos concentradores añaden la capacidad de soporte a distintos tipos de medios y pueden realizar acciones de puenteo entre éstos. También incluyen utilidades de recopilación de estadísticas sobre los módulos de los concentradores y sobre los puertos de los mismos. Las utilidades de administración basados en protocolos SNMP comienzan a aparecer en los concentradores de la segunda generación.

Otra característica de estos concentradores es el **plano posterior** (backplane) con diferentes buses que dan soporte a distintos tipos de arquitecturas, como Ethernet, Anillo, etc. La disposición de los buses es de uno por cada tipo de red, o de un bus multicanal que soporte de cada tipo de red. Este **plano posterior** (backplane) se encuentra administrado habitualmente por un procesador RISC de altas prestaciones.

Otra utilidad que aparece con estos concentradores es la capacidad de creación de segmentos lógicos de red local dentro de un solo concentrador. Esta utilidad permite a los administradores, situados en una consola de administración remota,

dividir una red local en segmentos más pequeños, por motivos de organización y rendimiento.

5.8.2.3 Concentradores de la tercera generación

Los concentradores de la tercera generación consisten en concentradores corporativos, que dan soporte a todas las necesidades de cableado e interconexión de una organización. Disponen de utilidades inteligentes, planos posteriores de alta velocidad, y son altamente modulares, aceptando un número de módulos interconectables entre sí, además de la inclusión de conexiones de área extensa y gestión avanzada.

Tienen utilidades de administración avanzadas para la supervisión y la realización de informes sobre las condiciones de trabajo de la red completa. La fiabilidad es también una utilidad importante por lo existen numerosas utilidades redundantes de protección contra los fallos de los componentes, como fuentes de alimentación eléctrica y enlaces para bus y área extensa. Muchos de los concentradores más recientes utilizan planos posteriores de conmutación de celdas ATM, que trabajan en el rango de transmisión de gigabits.

En particular los concentradores de la tercera generación disponen de utilidades que dan soporte a sistemas de cableado estructurado construido con cables de par trenzado de grado de datos. Algunas de sus utilidades se mencionan a continuación:

- Planos posteriores (backplanes) segmentados que dan soporte a Ethernet, FDDI, ATM, etc.
- Soporte a redes de alta velocidad que proporcionan utilidades de interconexión.
- Capacidad de conmutación para micro-segmentar la red en redes locales dedicadas a cada estación.
- Circuitos dedicados entre nodos finales, con objeto de aceptar altos volúmenes de tráfico o bien tráfico sensible al tiempo.
- Utilidades de administración distribuida construida dentro de cada módulo con objeto de mejorar las prestaciones bajo condiciones de carga pesadas.

5.8.3 Clasificación de los concentradores

Es posible clasificar a los concentradores en tres grupos principales. Estos grupos se definen básicamente atendiendo a la configuración del cableado estructurado. Las tres categorías son el **concentrador para un grupo de trabajo**, el **concentrador intermedio** y el **concentrador corporativo**.

5.8.3.1 Concentradores para grupos de trabajo

Un concentrador para un grupo de trabajo conecta un grupo de máquinas dentro de su entorno inmediato. Dentro de una misma organización pueden existir distintos grupos de trabajo.

5.8.3.2 Concentradores intermedios

Un concentrador intermedio se encuentra generalmente en el armario de distribución localizado en cada edificio. Los cables se ramifican desde éste hasta los concentradores para grupos de trabajo. El concentrador intermedio puede disponer de un enlace directo de fibra óptica al concentrador corporativo.

5.8.3.3 Concentradores corporativos

Un concentrador corporativo representa el punto de conexión central para todos los sistemas finales conectados a los concentradores para grupos de trabajo. Los concentradores corporativos forman por sí mismos el soporte de la red o proporcionan la conectividad a ésta. Dentro de un concentrador corporativo pueden situarse módulos de administración avanzada.

Como se mencionó anteriormente, se puede comenzar con concentradores para grupos de trabajo, conectar éstos a través de concentradores intermedios y posteriormente, conectar estos últimos mediante una red soporte como FDDI, o bien utilizar un concentrador corporativo, que permitirá una mejor administración.

Los concentradores corporativos deben diseñarse para cumplir requisitos críticos, fundamentales para una completa organización, y ser compatibles con nuevas tecnologías como ATM. Algunas de sus características se enumeran a continuación:

- Integración de diversos componentes de red en un lugar único.
- Alta fiabilidad, posibilitada por utilidades redundantes tolerantes a fallas.
- Un punto de conexión centralizado para los concentradores departamentales o para grupos de trabajo.
- Conexiones de alta velocidad capaces de aceptar el resultado de alto rendimiento generados por super servidores con multiprocesamiento (pueden montar módulos especiales para servidores dentro del concentrador).
- Capacidad de reconfiguración dinámica de la red desde una consola de administración.
- Capacidad de conexión a los puertos desde la consola de administración.

- Utilidades de administración avanzada, tales como detección y diagnóstico de fallos, componentes de intercambio y expansión modular, con objeto de mejorar la administración y ahorro de costos.

5.8.4 Componentes y características de los concentradores

Las características que se explican a continuación, se encuentran fundamentalmente en concentradores corporativos, los cuales proporciona funciones de puenteo, enrutamiento y administración entre otros

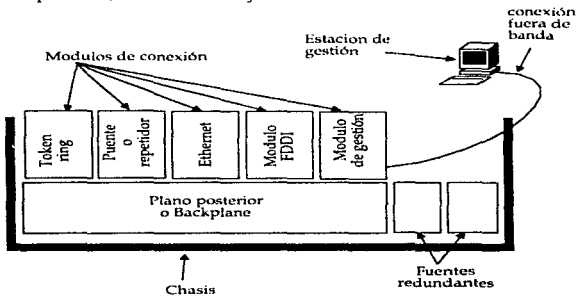


Figura 5.30 Componentes de un concentrador

5.8.4.1 Armazón y plano posterior

El armazón es la caja que rodea y cubre los componentes del concentrador. Su diseño y distribución determina el número de módulos de expansión y de otro tipos de componentes que se puede situar en el concentrador. Será necesario tener la posibilidad de instalación de dos fuentes de alimentación para el control de fallas.

El **plano posterior** (backplane) es a un concentrador lo que la tarjeta madre (mother board) a una computadora. El plano posterior proporciona el bus o los puntos de conexión para los módulos de expansión, de modo que será necesario asegurarse de que dispone del número suficiente de ranuras como para permitir una expansión futura. Algunos concentradores proporcionan extensiones al plano posterior dentro de otros armazones a través de conexiones de alta velocidad. Los tipos de buses que se manejan son los siguientes:

- **Bus estándar:** es un bus tipo EISA o MCA, como el utilizado en las computadoras personales. Cada módulo conectado al bus debe utilizar una interrupción para obtener acceso al mismo. Esta técnica es normalmente inadecuada en redes corporativas.
- **Bus múltiple:** El plano posterior dispone de numerosos buses, cada uno de los cuales se encuentra dedicado a transportar un tipo especial de tráfico. Un concentrador típico con bus múltiple dispondrá de un bus Ethernet, un bus para una red en anillo con testigo y un bus FDDI.
- **Bus segmentado:** En este diseño, el bus se divide en segmentos unidos mediante conectores comunes. Los módulos se conectan a los conectores, y tienen la capacidad de conexión con otros módulos sobre el mismo bus, formando segmentos lógicos de una LAN. Cualquier puerto o módulo pueden llegar a ser parte de un segmento de red personalizado bajo el control del administrador de la red a través de la consola de administración, asumiéndose que dichos puertos son del mismo tipo de LAN.
- **Bus de multiplexaje:** Un bus único se divide en múltiples buses lógicos mediante técnicas de multiplexaje. Cada bus es un canal dentro del flujo con multiplexaje. Esta técnica proporciona muchos de los beneficios del bus segmentado.

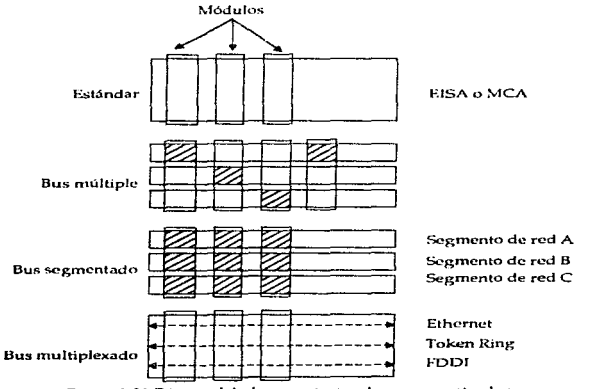


Figura 3.31 Diseño del plano posterior de un concentrador

La segmentación es una consecuencia de los concentradores. Un segmento es un conjunto de estaciones que comparten el mismo número de red y se transfieren paquetes. Los puentes son necesarios para conectar un segmento a otro. Los segmentos que poseen un gran número de estaciones de trabajo pueden saturarse debido al tráfico, por lo que es una buena idea dividir las redes en múltiples segmentos. Cada segmento debería agrupar a los usuarios que comparten los mismos recursos y pertenecen a los mismos departamentos o grupos de trabajo. Sin embargo, la escasez de canales dentro de un plano posterior limitará el número de los segmentos que se pueden configurar. La mayoría de los concentradores disponen típicamente de tres canales Ethernet y dos para una red en anillo con testigo, lo que significa que se estará limitado a tres o dos segmentos respectivamente. Para superar esta limitación, algunos proveedores proporcionan conmutadores que permiten subdividir un canal en múltiples segmentos. Alternativamente, los **concentradores de conmutación de puertos** proporcionan otra solución. Hay que tener en cuenta que los puentes entre segmentos pueden añadir muchos gastos.

5.8.5 Utilidades de conmutación de puertos

La **conmutación de puertos** es una utilidad relativamente nueva en los concentradores, que proporciona una forma de reconfigurar rápidamente las conexiones a las estaciones de trabajo, cuando, por ejemplo, un usuario cambia de departamento. Consideremos lo que ocurre cuando una compañía se reorganiza, o es totalmente orientada a grupos. Cada usuario necesita unirse a un departamento o grupo de trabajo distinto, y cada estación de trabajo debe conectarse al segmento apropiado para poder acceder a los recursos ubicados allí. El administrador necesita una forma rápida de unión de todos esos usuarios, sin importar su ubicación física, dentro de un único segmento, de modo que pueden compartir fácilmente el tráfico de la red local. Cuando el grupo de trabajo se separa, las estaciones de trabajo pueden reconfigurarse dentro de otros segmentos.

Según el modelo antiguo, los módulos de concentración a los que las estaciones de trabajo se conectaban definían segmentos de red local. Los módulos se encontraban cableados para repetir las señales únicamente entre los puertos conectados. Para mover a un usuario a un nuevo segmento LAN, había que mover físicamente el cable desde un módulo repetidor a otro. Además, si uno de los módulos repetidores disponía de diez puertos, pero un departamento o grupo de trabajo únicamente disponía de cinco estaciones de trabajo, cinco de dichos puertos permanecían sin utilizar mientras que otro módulo podría no disponer del número suficiente de puertos.

Según el modelo actual, los módulos se conectan a un ***plano posterior multisegmentado* a alta velocidad**, como se muestra en la figura 5.33. Cada puerto dispone generalmente de su propia conexión al plano posterior, en lugar de un

segmento cableado dentro del propio módulo. Los administradores configuran los segmentos en una estación de trabajo mediante la selección de los puertos que se desea que formen parte de un segmento o grupo. Estos segmentos o grupos se conectan lógicamente y no físicamente. Hay que tener en cuenta que, en la figura, los puertos se dispersan formando distintos segmentos de red local. El punto más importante es que el plano posterior compartido hace posible la creación de segmentos que extienden los módulos multipuerto.

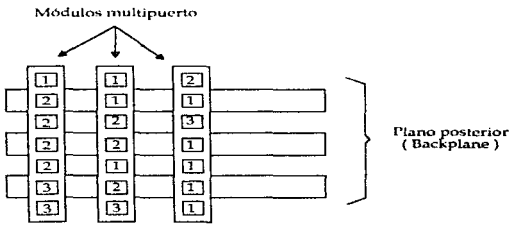


Figura 5.32 Plano posterior multisegmento

Esta capacidad de creación de **redes locales virtuales** sirve de soporte a grupos temporales con sus miembros situados en distintas ubicaciones físicas. Según esta estrategia, no existen puertos desperdiciados. Cada puerto se conecta al plano posterior, donde puede configurarse dentro de cualquier segmento de la red local. Una limitación de la tecnología en uso es que no se puede unir distintos tipos de redes, tales como Ethernet y redes en anillo con testigo, dentro del mismo segmento. Para ello, se hará necesario un puente.

NOTA: No se debe confundir la conmutación de puertos con los concentradores de conmutación. La conmutación de puertos es una utilidad de administración utilizada para configurar las estaciones de trabajo en segmentos lógicos. Los concentradores de conmutación disponen de bancos de puertos y proporcionan una forma de establecer conexiones dedicadas entre dos puertos cualesquiera.

El número de segmentos que pueden crearse depende del concentrador y del diseño de su plano posterior. Algunos proveedores únicamente dan soporte a unos pocos segmentos en el plano posterior, mientras que otros dan soporte a un número superior a cien. Se debe tener en mente que podría existir la tendencia de creación de muchos segmentos pequeños, lo que puede plantear un problema de puenteo. Si los usuarios de un segmento necesita acceder a los usuarios o recursos de otros segmentos, se necesitan funciones de puenteo para conectar todos los

segmentos. El número de puentes requeridos podría, eventualmente, producir daños sobre el sistema y exigir demasiado presupuesto.

La conmutación de puertos se presenta también como un problema en los protocolos de interconexión tales como IP, en el cual las estaciones de trabajo utilizan la dirección de red en el nivel de capa de red para realizar la comunicación. Si una estación se mueve de un segmento lógico a otro, la dirección de red deberá actualizarse manualmente.

5.8.6 Utilidades que proporcionan fiabilidad

Existe una necesidad creciente de proporcionar este tipo de utilidades en los concentradores, debido a que elementos tales como unidades de concentración, puentes, enrutadores, componentes de administración e incluso servidores, están localizados en un lugar solamente. Para aplicaciones críticas no es extraño crear concentradores redundantes. Si se produce el fallo de un concentrador, el otro lo reemplazará inmediatamente. Algunas de las utilidades redundantes de los concentradores se describen a continuación:

- **Redundancia de alimentación eléctrica:** La mayoría de los concentradores disponen de una fuente de alimentación que comparte la carga de energía eléctrica que se precisa, o bien que se activa si se produce un fallo en la alimentación.
- **Módulos de intercambio:** Esta utilidad permite cambiar un módulo sin desactivar la unidad completa.
- **Administración:** Las utilidades de administración incorporan normalmente administración remota y soporte al protocolo SNMP.
- **Configuración sencilla:** Cuando las estaciones de trabajo o los usuarios cambian de grupo de trabajo, debe ser sencillo reconfigurar la estación para adaptarse a la nueva configuración. Esta acción puede realizarse mediante software ubicado en algunos sistemas.

5.8.7 Utilidades de seguridad

Los concentradores pueden proporcionar un nivel de seguridad imposible de conseguir mediante los antiguos métodos de conexión. Por ejemplo, las utilidades de conmutación de puertos pueden controlar las enlaces de comunicación entre los puertos e impedir la conexión de un usuario desde otra estación o la interconexión a otra red. El filtrado se posibilita a través de la dirección MAC, mediante métodos similares al filtrado realizado por los puentes.

5.8.8 Escalabilidad por Módulos

Los módulos consisten en dispositivos individuales que se conectan al plano posterior del concentrador para proporcionar conexiones a las estaciones de trabajo, así como puenteo, enrutamiento y funciones de administración. A continuación se proporciona una lista de los tipos de módulos más comunes. Existe una cierta cooperación entre los distintos fabricantes de concentradores y, en algunos casos, un fabricante puede producir módulos especializados acoplables a los concentradores suministrados por otros fabricantes.

- Existen módulos redundantes que proporcionan alimentación eléctrica, con utilidades de intercambio que permiten reemplazar a las unidades defectuosas.
- Se encuentran disponibles módulos Ethernet que dan soporte a conexiones coaxiales, de par trenzado y fibra óptica, hacia estaciones de trabajo Ethernet mediante 10Base-T u otras topologías de red.
- Están disponibles módulos para redes Token Ring, que admiten de 12 a 24 puertos y varios tipos de cable de cobre de par trenzado blindado o sin blindar, así como cable de fibra óptica.
- Existen módulos FDDI sobre los que se apoyan redes de soporte corporativo o estaciones de trabajo de altas prestaciones.
- Los módulos que realizan puenteo o enrutamiento se encuentran disponibles para la interconexión de redes internas al concentrador sobre las que transmitan distintos protocolos, como SPX/IPX de Novell, TCP/IP, entre otros.
- Se encuentran disponibles módulos de administración que aceptan la norma SNMP o nuevas normas como CMIP.
- Existen dispositivos en forma de módulos que realizan una supervisión de los protocolos, como el analizador de protocolos LANterm de Cabletron para Novell, acoplado a los concentradores inteligentes NMAC.

Los módulos deberían disponer de indicadores luminosos que pudieran dar a los administradores alguna idea del estado de cada puerto con un simple vistazo. Por ejemplo, una luz roja indica mal funcionamiento de un puerto.

5.8.9 Utilidades de administración

Las utilidades de administración son importantes. La mayoría de los concentradores disponen de sus propios microprocesadores que pueden ejecutar programas para realizar un seguimiento de los paquetes de datos y errores producidos, almacenando esta información en una base de información de administración (MIB: Management Information Base). Un programa de administración ejecutado en una estación de trabajo con tareas de administración recoge la información de la MIB periódicamente y le da un formato adecuado para su presentación al administrador. La información es útil para orientar el seguimiento, en problemas genéricos, problemas de congestión puntuales y para

evitar problemas potenciales futuros. La alarma puede alertar a los administradores cuando llega a ciertos valores de umbral establecidos por ellos mismos. Por ejemplo, las alertas pueden avisar a un administrador que el tráfico de la red excede un determinado nivel, de modo que así podría emprender acciones correctivas, como segmentar la red o mover un usuario que genera un alto nivel de tráfico a un segmento dedicado

La mayoría de los fabricantes acepta el Protocolo Básico de Administración de Red (SNMP). SNMP se ejecuta sobre TCP/IP, utilizándolo para obtener información de la estación de trabajo MIB y transportarla hasta la computadora de administración. Si se han alcanzado los niveles de umbral, SNMP utilizara TCP/IP para enviar mensajes de aviso (alarmas) a la computadora de administración. Otros esquemas de administración es una norma de la ISO referida como Protocolo Genérico de Información de Administración (CMIP) y el NetVIEW de IBM.

Los concentradores se administran normalmente a través de aplicaciones gráficas que permiten a los administradores controlar cada dispositivo y nodo de la red desde una sencilla estación de administración. El software de administración se basa normalmente en UNIX, aunque también existen paquetes disponibles en Windows y OS/2. Las utilidades de administración de un controlador pueden proporcionar los servicios siguientes:

- Desconexión automática de los nodos que originan problemas y que perturban el funcionamiento de la red.
- Aislamiento de los puerto con propósitos de pruebas. Por ejemplo, un nodo podría encontrarse enviando un número excesivo de paquetes hacia el exterior. Puede aislarse dicho nodo para realizar un diagnóstico.
- Conexión y desconexión de las estaciones de trabajo, en función del día de la semana.
- Algunos fabricantes de concentradores proporcionan herramientas de análisis de protocolos y módulos acoplables en el interior del concentrador.
- Administración remota de los componentes de la red.

Una vez recogida la información, es necesario realizar la administración. El software de administración puede proporcionar un cierto número de utilidades que realizan una clasificación de los datos y muestran información útil de forma tabulada o gráfica. Las interfaces gráficas de usuario permiten realizar una ampliación de segmentos específicos de la red y mostrar información sobre los nodos, puentes o enrutadores en dichos lugares. También se pueden añadir o mover usuarios. El software de administración proporciona además, una forma de recoger información sobre la red durante un período específico de tiempo para su análisis posterior, o puede observarse un registro histórico de información para la comparación con la información actual. El análisis podrá ayudar a justificar la necesidad de nuevos componentes o módulos de expansión.

CAPÍTULO 6
TECNOLOGÍAS DE REDES DE ALTA VELOCIDAD

La utilización de servidores cada vez más poderosos, aunado con una tendencia de crecimiento, dan como resultado, un gran número de usuarios y más tráfico de red por servidor, llevando de esta manera a que las redes actuales alcancen rápidamente sus niveles de saturación. Además, el surgimiento de nuevas aplicaciones que demandan mas capacidad en el ancho de banda y cuidado en los requerimientos de transmisión (menor latencia, menor cantidad de errores etc.), Ha hecho que los administradores de red tengan la necesidad de planear una actualización de sus redes, ver figura 6.1.

Muchas opciones de red de alta velocidad están disponibles o llegaran a estarlo para satisfacer las necesidades de los diferentes tipos de usuarios. Estas nuevas tecnologías de redes rápidas, están redefiniendo los ambientes de las redes locales, ofreciendo una velocidad de transmisión de al menos 100Mbps. El problema que los administradores enfrentan es saber cual tecnología es la que satisface mejor sus necesidades y como poder migrar hacia esta sin un cambio drástico de los dispositivos de su red actual.

En este capítulo, se trata de explicar de manera concisa, las tecnologías que en este momento tienen un mayor auge en la tendencia de las redes locales (LAN) y redes de área amplia (WAN) tratando de ayudar a la comprensión de estas, para que de esta manera se pueda tomar una mejor decisión sobre una tecnología de red.

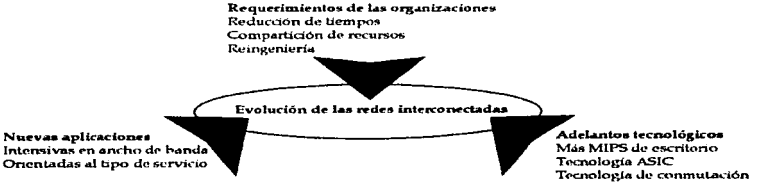


Figura 6.1 Nuevo paradigma de las redes.

6.1 REDES DE ÁREA LOCAL (LAN)

6.1.1 Tecnologías de Conmutación de redes LAN

Fundamentalmente las redes actuales (Ethernet y Token Ring) están basadas en el concepto de ancho de banda compartido, es decir , el ancho de banda se comparte entre los usuarios conectados a la red. Por otro lado se empezó con un modo no estructurado de adición de usuarios, por lo tanto, los usuarios se empezaron a conectar según fuera necesario y sin tomar en cuenta el crecimiento de usuarios y las consecuencias de congestionamiento que se tendrían. En la mayoría de los casos son redes Ethernet basados en cable coaxial con cada estación conectada directamente al cable, por tal motivo muchos dispositivos fueron conectados a estas y en algunos casos sin notificación al administrador de la red. De esta manera cada dispositivo conectado al segmento de red tomaba su turno dentro de la contienda por ancho de banda para poder transmitir en el bus Ethernet o por el turno de obtener la señal (token) en el caso de un anillo Token Ring.

Existen principalmente tres desventajas en este tipo de redes: los cables usados fueron inseguros, caros y la detección de fallas no es sencilla (por no poder tener una configuración de topología de estrella).

Este esquema de ancho de banda compartido fue muy efectivo cuando las redes locales consistían de un pequeño número de dispositivos[79] que necesitan transferir sus archivos e imprimir sus documentos. Actualmente las redes han crecido en complejidad y tamaño (a cientos de dispositivos). La conmutación de redes locales es una tecnología de interconexión que le da un nuevo respiro a las redes locales con ancho de banda compartido como Ethernet y Token Ring. Esto se lleva a cabo al poder dividir toda la red compartida en pequeños segmentos de red con un ancho de banda compartido dedicado a cada segmento. Al realizar esto, efectivamente se reduce el número de dispositivos de red sobre cada segmento de ancho de banda compartido; brindando mas ancho de banda agregado a la red entera y poder aislar el tráfico en segmentos específicos.

6.1.1.1 Relación entre los puentes y los conmutadores

El término puenteo se refiere a una tecnología en la cual un dispositivo (referido como puente) conecta dos o mas segmentos de red LAN. Un puente transmite datagramas de un segmento a su destino en otro segmento. Cuando un puente es conectado por primera vez en una red, este empieza a operar examinando la dirección MAC (dirección de control de acceso al medio) del datagrama que fluye a través de él, y de esta manera construye una tabla de destinos conocidos.

[79] Las redes LAN tradicionales fueron diseñadas para proveer recursos compartidos entre un número relativamente bajo de usuarios, generalmente de hasta 50.

Si el puente conoce que la dirección destino de ese datagrama se encuentra en el mismo segmento del que provino, el puente desecha el datagrama por que no tiene la necesidad de retransmitirlo. Si el puente conoce que la dirección destino se encuentra en otro segmento, el puente retransmite el datagrama sobre ese segmento solamente. Si el puente no conoce el segmento destino del datagrama, el puente retransmite el datagrama sobre todos los segmentos excepto el segmento origen, esto se lleva acabo por medio de una técnica llamada inundación (flooding), es decir, por broadcast[80]. Por lo tanto, se puede decir que el principal beneficio del puenteo, es que limita el tráfico a ciertos segmentos de la red.

De manera similar a los puentes, los conmutadores conectan varios segmentos de redes LAN, utilizando una tabla de direcciones MAC para determinar el segmento destino de un datagrama y así reducir el trafico en los demás segmentos. Pero de otra manera los conmutadores operan a velocidades mucho mayores que los puentes y enrutadores, debido a que los conmutadores de redes LAN mueven los datos principalmente por medio de hardware (circuitos ASICs: Application Specific Integrated Circuit) en lugar de software (procesadores RISC). De esta manera, son mucho mas rápidos y proveen un mayor rendimiento a un menor costo. La mayoría de los conmutadores, soportan tanto tecnologías de velocidades bajas como Ethernet o Token Ring, así como tecnologías de alto rendimiento como 100BaseT, FDDI y ATM. Esta habilidad de los conmutadores de soportar varias tecnologías inmediatamente incrementa el rendimiento de la red sin la necesidad de una actualización masiva de infraestructura de la red, además de que algunos conmutadores pueden soportar nuevas funcionalidades, tales como las redes virtuales (VLANs), que brindan una configuración flexible al administrador de red, al permitirle distribuir los grupos de trabajo de una manera lógica y no estar sujeto a la localización física de las estaciones.

Por tal motivo, se dice que la conmutación es una tecnología que ayuda a aliviar los problemas de congestión en redes actuales como Ethernet, Token Ring y FDDI, al reducir el tráfico e incrementar el ancho de banda. Estos conmutadores (referidos como conmutadores de redes LAN), están diseñados para trabajar con infraestructura de cable existente, de manera tal, que pueden ser instalados con un mínimo de cambio en las redes existentes. Frecuentemente reemplazan a los concentradores compartidos.

[80] Este tipo de dispositivo trabaja bien en redes pequeñas, partiendo del punto de vista de que la broadcast es normalmente un muy pequeño porcentaje del tráfico total. Pero en cambio, en redes de gran tamaño, el número de dispositivos conectados llega a ser lo suficientemente grande, que al realizar una función de broadcast puede llegar a sobrecargar dicha red hasta el punto de sufrir un colapso.

6.1.1.2 Redes Token Ring conmutadas

En principio, La transmisión en las redes Token Ring se basa en una señal referida como señal token, la cuál es pasada alrededor de las estaciones conectadas al anillo. Cuando una estación tiene posesión de la señal token, esta tiene permitido transmitir, mientras que las demás estaciones del anillo deberán esperar por la señal token, aun cuando no exista actualmente una transmisión sobre el anillo.

Las redes pequeñas (anillos con un menor número de usuarios) tienen menores retrasos en el paso de la señal token. Sin embargo, grandes redes, aún garantizan que cada estación eventualmente, tendrá acceso a la señal token en una modalidad round robin. La segmentación de un gran anillo por medio de un conmutador reduce el número de usuarios por anillo, reduciendo así la congestión y el retraso entre oportunidades de las estaciones de tener la señal token. Además, los conmutadores de redes Token Ring brindan una mejor tolerancia a fallas en la red. Aunque cabe mencionar que estos beneficios no son tan notables para los usuarios finales como los son para las redes Ethernet conmutadas.

6.1.1.3 Redes Ethernet conmutadas

Por otra parte, las redes Ethernet son el tipo más común de red local actualmente, la cual tiene un máximo de ancho de banda de 10 Mbps. La red Ethernet tradicional es una tecnología half dúplex. Donde cada dispositivo ethernet verifica la red para ver si no existe transmisión de datos sobre el medio[81], si no hay, puede empezar a transmitir sus datos, si no, espera un tiempo para volver a verificar y poder transmitirlos. En el caso de que dos estaciones comiencen su transmisión al mismo tiempo, da como resultado una colisión. Cuando una colisión ocurre, los dispositivos entran en un estado pasivo durante un tiempo aleatorio para realizar un nuevo intento posteriormente. Como cada vez mas anfitriones son conectados a estas redes compartidas, los anfitriones deberán esperar con mas frecuencia para poder empezar a transmitir, igualmente, ocurrirán mas colisiones (debido a que mas anfitriones trataran de transmitir al mismo tiempo).

Actualmente el rendimiento de las redes Ethernet tradicionales se ven mas afectadas, debido a que los usuarios ejecutan software con mas funciones intensivas de red, tales como aplicaciones cliente/servidor, lo cuál causa que el anfitrión transmita datos mas frecuentemente y durante periodos largos de tiempo.

Es por esto que un conmutador de red LAN Ethernet brinda un mayor ancho de banda, al separar la red en varios dominios de colisión con un menor número de estaciones y reenviar el trafico de una manera selectiva hacia el segmento

[81] Mientras un dispositivo envía sus datos, todos los demás dispositivos de la red LAN están obligados a esperar para transmitir, por lo tanto solo una transmisión es permitida a la vez.

apropiado[82]. Otra ventaja, es que su desempeño no requiere de grandes cambios del sistema de cableado, adaptadores de red ni de reconfiguración de software en las estaciones.

De esta manera, en lugar de compartir la capacidad limitada de ancho de banda (10Mbps) de Ethernet entre muchas computadoras, cada estación o cada pequeño grupo de estaciones, puede tener un segmento de 10 Mbps dedicados conectados a un conmutador de alta capacidad.

6.1.1.3.1 Tipos de redes Ethernet conmutadas

Es importante realizar un examen minucioso de los requerimientos de ancho de banda de cada uno de los usuarios y de esta manera poder balancear el número de usuarios por segmento, ya que se tienen diferentes necesidades por usuario o por grupo de usuarios. Existen dos opciones de incrementar el desempeño del grupo de trabajo en Ethernet, dependiendo del tipo de segmento Ethernet conmutado, los cuales pueden ser:

- Ethernet conmutado compartido (múltiples estaciones)

Un grupo de trabajo actualmente consiste de uno o más repetidores, de ancho de banda de 10Mbps compartidos. Todos los usuarios y servidores locales en el grupo, compiten por estos 10 Mbps de ancho de banda. Al adicionar un conmutador Ethernet y conectar el repetidor(es) de 10Mbps a los puertos del conmutador, cada segmento (cada puerto del conmutador) tiene 10 Mbps, incrementando el ancho de banda efectivo disponible a los usuarios (debido a que son pocos los usuarios que compiten por el ancho de banda en cada segmento)

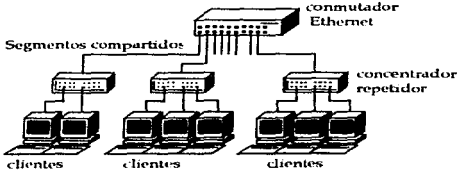


Figura 6.2 Ethernet conmutado compartido (múltiples estaciones)

[82] Cada segmento de red Ethernet es conectado a un puerto del conmutador LAN, de esta manera se crean dominios de colisión aislados. De esta manera al dividir a los usuarios en diferentes dominios de colisión se puede reducir el numero de colisiones en cada segmento y por tanto, el desempeño aumenta.

- Ethernet conmutado dedicado (una sola estación)

En este esquema, referido como segmento Ethernet dedicado, se conecta cada dispositivo final a un puerto del conmutador, de esta manera se dedica 10Mbps de ancho de banda a cada dispositivo final.

Esta solución es especialmente deseable para los diferentes servidores de la red o para clientes que requieran altos anchos de banda para sus necesidades. Aunque, pensando a futuro, los usuarios se deben migrar hacia segmentos Ethernet conmutados dedicados dependiendo del ancho de banda que vayan necesitando.

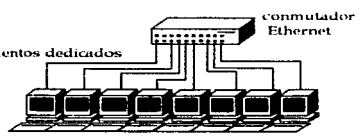


Figura 6.3 Ethernet conmutado dedicado (una sola estación)

6.1.1.4 Otras funciones disponibles en algunos dispositivos de conmutación

Redes Virtuales

Las redes Virtuales referidas como VLANs (Virtual LAN), son grupos de usuarios que son definidos basándose en su función lógica[83] en lugar de su locación física. De esta manera, las redes virtuales ayudan al desempeño y facilitan la administración de las redes en ambientes grandes de redes conmutadas. Por lo tanto, se puede decir, que una red LAN virtual (VLAN) es un grupo de anfitriones o dispositivos de red que forman un solo dominio de puenteo.

En conclusión, los conmutadores son ideales para ayudar al desempeño de las redes actuales (Ethernet y Token Ring) al poder expandir las capacidades del ancho existente. Además de que preservan la protección de inversión al no requerir de grandes cambios en las redes actuales para poder realizar sus funciones. Mientras que por otro lado, cabe mencionar que los conmutadores de redes LAN son tecnologías propietarias que trabajan del mismo modo.

[83] El criterio para poder agruparlos por su función lógica puede ser que los usuarios utilicen un protocolo en común o son parte del mismo departamento etc.

6.1.2 Interfaz de Datos Distribuidos por Fibra (FDDI)

6.1.2.1 Historia de FDDI

En 1982, un subcomité del Grupo de Trabajo Técnico X3T9 del Instituto Nacional Americano de Estándares (ANSI), estuvo encargado del desarrollo de un estándar de redes de datos de alta velocidad. El estándar propuesto comenzó inicialmente como una Interfaz de Datos Distribuidos Localmente (LDDI: Locally Distributed Data Interface). Está, estuvo pensada inicialmente como un sistema de banda ancha (broadband) con un alcance de un kilómetro y siete nodos conectados. Pero muy rápido se dieron cuenta que este no seria útil para el tipo de redes en que lo planeaban utilizar. En 1986, ANSI había revisado el documento original y publicó una propuesta que finalmente sería el FDDI que se conoce actualmente.

La arquitectura FDDI constituye un excelente medio para construir redes de campus o backbone, como se muestra en la figura 6.3. Los segmentos de redes de área local se conectan al backbone, al igual que las computadoras centrales y otros dispositivos.

Mientras que las redes pequeñas que constan de un número escaso de segmentos de LAN probablemente obtendrán mas beneficios mediante un backbone Ethernet de cable coaxial. Las redes mas extensas, que poseen numerosos segmentos LAN, generadoras de una cantidad importante de trafico debido a las estaciones de trabajo de altas especificaciones, la transferencia de archivos gráficos u otro tipo de trafico, se beneficiarían mas con FDDI.

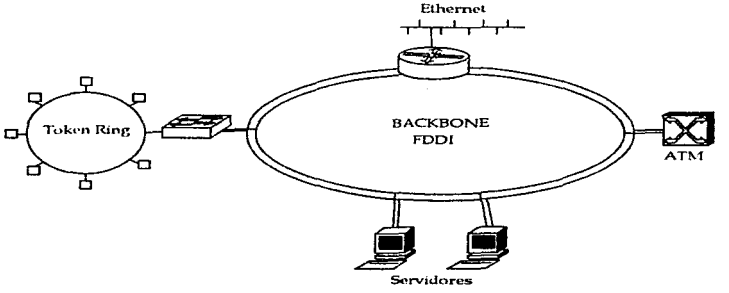


Figura 6.4 FDDI constituye un excelente medio para construir redes de campus o backbone

6.1.2.2 Modo de operación de FDDI

La arquitectura FDDI especifica una topología que tiene dos anillos de fibra óptica independientes y de rotación inversa, que proporciona una velocidad global de 200 Mbps, es decir, 100 Mbps para cada uno de los canales, figura 6.4. Los dispositivos, que se encuentran conectados tanto al anillo primario como al secundario, tienen la clasificación A. Mientras que los dispositivos tipo B se encuentran unidos a un solo anillo. Lo interesante de la especificación FDDI, es que permite designar con la clasificación A, a las estaciones críticas que necesiten apoyo adicional y canales de mayor velocidad. Las estaciones, de menor importancia, pueden dejarse como estaciones de Clase B, a un menor costo.

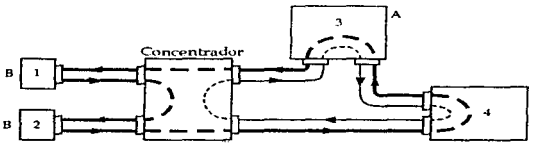


Figura 6.5 FDDI usa una topología con dos anillos de fibra independientes y de rotación inversa.

Las estaciones conectadas directamente a FDDI disponen de una conexión punto a punto con las estaciones adyacentes. En la configuración de anillo doble se utiliza un canal para la transmisión mientras el otro permanece como de seguridad. Algunas estaciones, las denominadas estaciones de acoplamiento doble (DAS: dual-attached station) se conectan a los dos anillos, figura 6.5. De otro modo, las estaciones de acoplamiento único (SAS: single-attached station), figura 6.6, se conectan a través de un concentrador, figura 6.7, el cuál proporciona las conexiones oportunas a muchas SASs. Una de las ventajas de esta configuración es que una estación SAS que falle no puede interrumpir el funcionamiento del anillo. Además, la mayoría de las SASs son estaciones de trabajo de usuario que se apagan de manera frecuente, por tal motivo, si se realizara su conexión de una forma directa, podría interrumpir el funcionamiento del anillo.

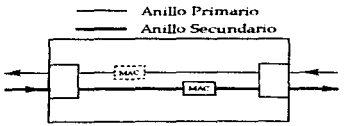


Figura 6.6 Estación de acoplamiento doble. (DAS: dual-attached station)

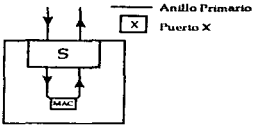


Figura 6.7 Estaciones de acoplamiento único (SAS: single-attached station)

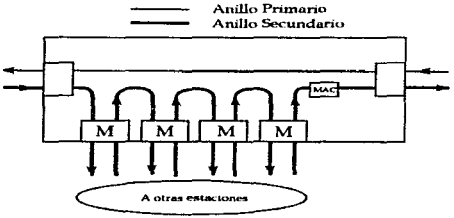


Figura 6.8 Concentrador FDDI.

Los concentradores permiten conectar estaciones y reconfigurar el sistema. También se encargan de aislar los nodos problemáticos mediante el punto de concentración. FDDI no exige necesariamente que todos los canales sean de fibra óptica. El concentrador puede incluir una interfaz en el que el usuario instalara fibra óptica para una parte de la red, y par trenzado o coaxial para otra parte de la red.

FDDI establece un esquema de sincronización de red muy particular. El mejor código que puede emplearse en una red es aquel que proporciona cambios de señal frecuentemente. Estas variaciones permiten ajustar constantemente el receptor con los datos recibidos, garantizando de esta forma una perfecta sincronización entre el nodo emisor y el receptor. Por ejemplo, el código Manchester que utiliza el estándar 802.5 (Token Ring) solo tiene una eficiencia del 50%[84]. En otras palabras, el código Manchester requiere un ancho de banda del doble de grande que el de la transmisión.

[84] Ya que cada bit exige dos transmisiones de estado en la línea (es decir, dos baudios). Si se usa el código Manchester, una transmisión a 100 Mbps exigirá un ancho de banda de 200 Mbps (200 Mhz).

Es por esto que ANSI, considero que una velocidad de 200 Mhz tendría repercusiones en el costo de las interfaces y los dispositivos de temporización. Debido a esto, ideo el código llamado 4bits/5bits, ver tabla 6.1, en el que se usa un código de cuatro bits para crear otro de cinco bits. Es decir, por cada cuatro bits que envía el transmisor, FDDI crea cinco. Estos cinco bits proporcionan la autosincronización buscada. De este modo, FDDI con una velocidad de 100 Mbps, solo exige un ancho de banda de 125 Mhz.

DATOS DE USUARIO		CÓDIGO 4Bits/5Bits	
Binario	Hexadecimal	Código	Símbolo
0000	0	11110	0
0001	1	01001	1
0010	2	10100	2
0011	3	10101	3
0100	4	01010	4
0101	5	01011	5
0110	6	01110	6
0111	7	01111	7
1000	8	10010	8
1001	9	10011	9
1010	A	10110	A
1011	B	10111	B
1100	C	11010	C
1101	D	11011	D
1110	E	11100	E
1111	F	11101	F

Tabla 6.1 Estructura del código 4bits/5bits

La ventaja de esta configuración es que ahorra ancho de banda, pero su desventaja es la perdida de la autosincronización presente en la codificación tipo Manchester. Para compensar esta perdida, se utiliza un largo preámbulo con objeto de sincronizar el receptor con el reloj del transmisor. Además, se requiere que todos los relojes sean estables, por lo menos en un 0.005%. Con esta estabilidad, se puede enviar tramas de hasta 4500 octetos, sin peligro de que el reloj del receptor pierda la sincronía con respecto al flujo de datos.

Los protocolos FDDI básicos han sido modelados sobre la base de los protocolos 802.5. El cual trabaja de la siguiente manera, para que una estación transmita datos, primero deberá capturar el testigo (token); después transmite una trama y la quita cuando regresa de nuevo. Una de las diferencias entre la FDDI y el 802.5, es que la estación en el 802.5 no puede generar un testigo nuevo, hasta después de que su trama haya recorrido por completo la trayectoria y regresa de nuevo al lugar inicial. En el caso de FDDI, que potencialmente puede tener conectados 1000 estaciones y hasta 200 kilómetros de fibra óptica, se debe tener en cuenta la cantidad de tiempo perdido que se tendría que esperar para que la trama recorra

el anillo completo, este tiempo podría ser bastante significativo. Por esta razón se decidió permitir que una estación inserte un testigo nuevo en el anillo, tan pronto como esta termine de transmitir sus tramas. Por tanto, en un anillo muy grande, varias tramas podrían encontrarse en circulación al mismo tiempo dentro del anillo.

Al igual que muchas otras redes locales, la red FDDI emplea un método de temporización del testigo. Donde cada nodo mide el tiempo que tarda el testigo en regresar a él (este es referido como Tiempo de Rotación del Testigo, TRT), y lo compara con el Tiempo Previsto de Llegada (PTT). Si el testigo regresa antes de lo estimado según el PTT, ello indica, casi con seguridad, que la red no esta congestionada. El nodo queda autorizado para enviar todo el flujo de datos que necesite, siempre que no supere el tiempo marcado por PTT. Si, por el contrario, el testigo llega después del plazo PTT, lo mas probable es que la red este bastante congestionada, por lo que el nodo solo deberá transmitir el trafico de alta prioridad, dejando al de baja prioridad para otro momento en que la red este menos congestionada.

Hasta este momento, conviene destacar dos aspectos de este protocolo. En primer lugar, como ya hemos comentado, una vez capturado el testigo (señal token), se colocan los datos en el anillo y se vuelve a insertar la señal testigo posteriormente. Sin embargo, cuando una estación captura el testigo, el anillo permanece inactivo durante un breve periodo de tiempo, mientras se prepara el paquete. Esto proporciona al ETD y a la unidad de interfaz con el anillo algo mas de tiempo para estructurar el paquete y hacerlo pasar por la interfaz. Esta relativa sencillez baja el precio de las interfaces. En segundo lugar, como el testigo se envía inmediatamente después del paquete, cualquier otra estación que se encuentre después en la línea podrá adquirir también el testigo, si el tiempo de rotación del testigo y su tiempo previsto de llegada entran dentro de los límites especificados por los parámetros. Este esquema permite aprovechar mucho mejor las redes grandes, en las que el intervalo de latencia necesario para recorrer todo el anillo sea muy largo. En tercer lugar, el anillo FDDI permite establecer de cierta manera prioridades, jugando con los parámetros TRT y PTT.

6.1.2.3 Relación entre FDDI y OSI

La relación entre FDDI y el Modelo de Interconexión de Sistemas Abiertos (OSI), se muestra en la figura 6.8. El nivel superior de FDDI encaja en el subnivel de acceso al medio (MAC: Media Access Control) del nivel de enlace de datos. Por encima se encuentra el nivel de Control Enlace Lógico IEEE 802.2 (LLC: Logical Link Control), que puede actuar como un puente y transferir los paquetes entre las redes Token Ring y Ethernet representadas en dicha figura. Los paquetes destinados a una estación de trabajo local se envían a los protocolos de niveles superiores en vez de reenviarlos.

La norma de gestión de estaciones (SMT: Station Management) mostrada en la figura, gestiona la configuración e inicialización de la estación y del anillo, la inserción y extracción de la estación y la información de diagnóstico.

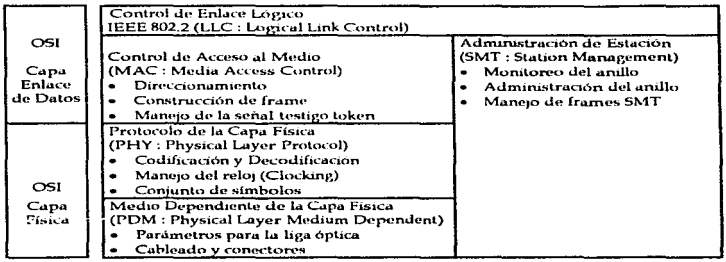


Figura 6.9 Relación entre OSI y FDDI

6.1.2.4 Estándares de FDDI

Los procedimientos, métodos o sistemas son definidos por un conjunto de estándares creados para FDDI por el grupo de trabajo ANSI X3T9.5. Cuando son adoptados por ANSI, los estándares de FDDI son enviados a la organización de estandarización ISO. De esta manera, FDDI es comprendida por cuatro áreas funcionales principalmente, y estas son:

6.1.2.4.1 Las cuatro subcapas principales de FDDI

En este trabajo las cuatro subcapas principales de FDDI serán estudiadas por separado para mostrar sus responsabilidades:

1) Medio dependiente de la capa física (PMD: Physical Media Dependent)
2) Protocolo de la capa física (PHY: Physical Layer Protocol)
3) Control del acceso al medio (MAC: Media Access Control)
4) Administración de estación (SMT: Station Management)

PDM: El primer componente de las cuatro subcapas con que consta el estándar de FDDI es el PDM. La subcapa PMD de FDDI corresponde a la Capa 1, la Capa Física, del modelo OSI. Por lo tanto, PDM especifica las señales ópticas y la forma de las ondas sobre el cable de fibra óptica, además de la instalación de éste (incluyendo los conectores). Esta especificación da una distancia máxima de 2Km

entre estaciones FDDI, con un cable de fibra óptica[85] de un mínimo de 500 Mhz, además, pueden ser utilizados LEDs transmisores de 1300 nm (nanómetros). La atenuación máxima del anillo FDDI es de 11 decibeles (dB) entre terminal y terminal, esta es típicamente referida como 2.5 dB por km. ANSI aprobó la subcapa PMD del estándar FDDI en 1988.

También existe una subcapa PMD que utiliza fibra óptica monomodo referida como SMF-PMD. Esta es similar a la PMD, pero esta especifica la utilización de fibra óptica monomodo y un láser para la transmisión/detección. De esta manera, se puede cubrir una distancia de 60km en lugar de 2km entre estaciones. Esto fue desarrollado debido a las necesidades en las que se tenía que extender una red mas de 2km.

PHY: La subcapa PHY de FDDI corresponde a la mitad superior de la Capa 1 (la Capa Física) del Modelo OSI. La función principal de la subcapa PHY es la de codificar y decodificar las señales y del reloj. Como se mencionó anteriormente, FDDI utiliza un esquema de decodificación llamado 4 bytes/5 bytes dando eficiencia del 80% sobre una señal de reloj de 125 Mhz. También provee una función de reloj distribuida a FDDI. Además, de especificar en esta subcapa el tamaño máximo del frame de 4500 de FDDI. La subcapa de PHY del estándar FDDI fue aprobado por ANSI en 1998. El proyecto de mejora de la subcapa PHY referida como el PHY-2, fue aprobado por ANSI en 1990 y se encuentra actualmente bajo en desarrollo.

MAC: La subcapa tres del estándar FDDI es la MAC. Esta subcapa corresponde a la mitad mas baja de la Capa 2 (Capa de Enlace de Datos), del Modelo OSI. Las funciones de la subcapa MAC son la de planear y transferir datos dentro y fuera del anillo FDDI. También es manejado por la subcapa MAC la construcción de los paquetes, reconocimiento de las direcciones de las estaciones, la señal testigo (token passing), y la generación y verificación de la Secuencia de Verificación del Frame (FCS: Frame Check Sequences). La subcapa MAC fue aprobada por ANSI en 1986. El proyecto de mejora de la subcapa MAC referida como MAC-2, fue aprobado en 1990 por ANSI y actualmente esta en desarrollo.

SMT: La subcapa cuatro de FDDI es el SMT. Las funciones principales del SMT son la configuración inicial del anillo FDDI, monitoreo del bit de error y el wrapback. SMT cubre las subcapas PDM, PHY y MAC. SMT incluye la Administración de la Conexión (CMT: Connection Management), la Administración o Manejo del Anillo (RMT: Ring Management) y funciones y servicios basados en frames. La parte de SMT del estándar FDDI se llevo mas tiempo para ser aprobado y fue el mas debatido del estándar FDDI. Finalmente, fué aprobado en el año 1993.

---

[85] Cable de 62.5/125 μm (micron), y al menos cable de 50/125 μm serán reconocidos por las especificaciones PDM.

6.1.2.5 Topología y Capacidad de FDDI

Los dos anillos paralelos que conforman a FDDI son llamados anillos primario (anillo A) y secundario (anillo B). La ruta o trayectoria de la red FDDI, ruta A, es usada en operaciones normales. La ruta o trayectoria secundaria de la red FDDI referida como ruta B, es usada para redundancia, y no es usado en operaciones normales. La ruta B es una ruta de respaldo y solo es usada cuando hay problemas en la ruta primaria. Todo el trafico de la red FDDI es cambiado del anillo A al anillo B automáticamente cuando ocurre algún problema.

El estándar de FDDI especifica la distancia máxima y el máximo numero de estaciones. Pudiendo soportar arriba de 500 estaciones conectadas directamente a un anillo FDDI. Aun que cabe notar, que la cifra de 500 no significa el numero total de unidades individuales que pueden acceder a una red FDDI; esto se refiere solo a las estaciones conectadas directamente a un anillo. Es decir, una estación FDDI puede ser un concentrador, puente, brouter, enrutador o una estación final que conectan a cualquier numero de unidades individuales conectadas a esta. Esto significa que el numero máximo de estaciones individuales no esta limitado por el ancho de banda.

Utilizando cable multimodo de 50/125 se puede cubrir una menor distancia. Por otro lado, al utilizar, cable de fibra óptica monomodo de 9 µm se puede extender la distancia entre estaciones FDDI por arriba de los 60 km dependiendo del equipo usado, pero la distancia del anillo sigue siendo de hasta 100 kilómetros. Es por esta razón, que el anillo FDDI deberá ser segmentado en anillos por medio de compuertas (gateways), enrutadores, puentes, para superar el límite de los 100 km.

Cable de fibra

Como se explico en el capitulo 3, existen dos tipos de fibra óptica[86], monomodo y multimodo. El primero, propaga la transmisión de una frecuencia de luz única, mientras que el segundo, propaga varias frecuencias.

El tipo mínimo de cable de fibra óptica que puede utilizarse es el de 62.5/125 micras de tipo multimodo. El cable multimodo puede utilizarse si la especificación FDDI lo consiente. Estas especificaciones se encuentran disponibles a través de cualquier fabricante de FDDI. Aunque, algunos prefieren cables de un gran ancho de banda (tipo monomodo), anticipándose a los requerimientos futuros.

El cable de fibra óptica fue caro en sus orígenes. Sin embargo, la competencia ha reducido los precios considerablemente, con lo que representa la mejor elección para tecnologías futuras.

[86] Hay que tener en cuenta que la versión FDDI con cable de par trenzado de cobre se ha normalizado recientemente y es referida comúnmente como CDDI.

Clases de equipos FDDI

Hay dos tipos básicos de estaciones FDDI: de unión simple y de unión doble. Las cuatro clasificaciones de estas estaciones son: 1) estación de unión simple (SAS: single attached station); 2) estación de unión doble (DAS: dual attached station); 3) concentrador de unión simple (SAC: single attached concentrator); 4) concentrador de unión doble (DAC: dual attached concentrator). Las estaciones FDDI clase A (DAS y DAC) usan tanto el anillo primario como el secundario debido a su habilidad para reconfigurar el anillo secundario sin interrumpir al usuario, si el anillo primario o alguna estación falla. El anillo secundario trabaja igual que el anillo primario, pero en dirección opuesta.

Las estaciones FDDI clase B (SAS y SAC) solo pueden ser usadas en el anillo primario como un método de conexión a un costo mas bajo para estaciones de trabajo que no son tan criticas. No se ofrece una conexión redundante con este método. Típicamente, un DAC es usado para conectar varias estaciones SAS clase B. Un concentrador mas inteligente, se usa para conectar estaciones FDDI al anillo dual. Y de esta forma, varios SASs son colocados atrás de un concentrador.

Protección contra fallas

La arquitectura FDDI provee de una conmutación de derivación o desvío opcional en cada nodo para poderse recuperar de una falla de un nodo o un canal. En la figura 6.9 se muestra una posible reconfiguración en el caso de pérdida de uno o varios canales (la figura presenta el caso de pérdida del canal entre los dispositivos tres y cuatro). FDDI se reconfigura cambiando los lazos de los dispositivos tres y cuatro. Como puede apreciarse en la figura, de esta manera, la red permanece intacta. La reconfiguración de los lazos interno y externo de los dispositivos tres y cuatro consigue que todos los dispositivos sigan teniendo acceso a la red.

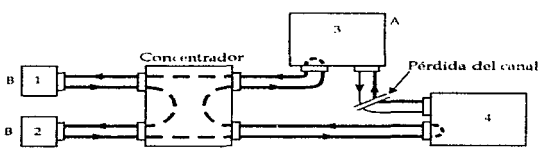


Figura 6.10 Reconfiguración de un sistema FDDI

Si una estación o nodo llegase a fallar, FDDI estipula que se debe poder puentear el nodo. Lo que se realiza, es que un espejo redirige la luz hacia una vía alterna. por ejemplo, en la figura 6-13, si el dispositivo 4 se daña, las señales se podrían dirigir fuera del dispositivo utilizando los mismos canales.

Método de acceso de FDDI

FDDI utiliza un método de acceso de paso de testigo (Token passing). Este método esta basado en pasar una trama referida como señal de testigo de estación a estación en un solo sentido (estaciones adyacentes) a través de la red; si una estación necesita transmitir datos captura el testigo. En este momento al ser poseedor de la señal testigo, la estación transmite los datos y sitúa la señal testigo de vuelta en el anillo al finalizar. Se debe utilizar un mecanismo de regulación para evitar que una estación mantenga el testigo durante demasiado tiempo. Para acomodarse a aquellas estaciones que generen un alto volumen de trafico, el administrador de la red puede dar prioridad a dichas estaciones, generalmente concediéndoles un periodo mayor de tiempo de transmisión antes de liberar el testigo. Se debe tener en cuenta las siguientes características:

- Las estaciones directamente conectadas a FDDI trabajan como repetidores. Reciben los paquetes de un vecino y los envía hacia el otro, siguiendo el sentido correcto. Cuando un nodo detecta su dirección en un paquete, lo copia en su memoria.
- Pueden existir múltiples tramas en la red. Esto es, si una estación devuelve el testigo mientras que sus tramas enviadas todavía se encuentran en transito, las otras estaciones pueden comenzar a transmitir.
- Existe un mecanismo de gestión denominado gestión de la estación, que capacita a los administradores del sistema a gestionar y realizar una supervisión de las redes FDDI, los nodos aislados que producen fallos y el trafico en ruta.

Tipos de FDDI

Hasta el momento, este trabajo se ha concentrado en la norma FDDI original, que se encuentra perfectamente establecida. Por otro lado, las nuevas aplicaciones de multimedia y vídeo en tiempo real presentan requisitos especiales de transmisión, basados en su naturaleza sensible al tiempo. Los retrasos en la distribución de paquetes en transmisiones de vídeo en tiempo real pueden hacer que su presentación ante el usuario tenga un aspecto discontinuo o entrecortado. Cuando se retrasan algunos paquetes y otros llegan a tiempo, los paquetes con retraso simplemente se eliminan. La naturaleza de paso de testigo de FDDI y la estructura variable de sus tramas no ofrece el flujo uniforme de datos requeridos por el vídeo en movimiento. Estos problemas se resuelven de diferentes formas, según se discute a continuación. FDDI dispone de tres modos de transmisión. Los dos primeros, asíncrono y síncrono, ya aparecen en la norma FDDI original, mientras que el tercero, basado en circuitos, puede proporcionar circuitos dedicados. Este ultimo modo, se encuentra disponible en la nueva norma FDDI-II[87].

[87] La norma FDDI-II requiere la instalación de nuevas tarjetas de adaptación (NICs: Network Interface Card).

SERVICIOS ASÍNCRONOS: El modo de anillo asíncrono se basa en el uso de un testigo. Cualquier estación puede acceder a la red mediante la captura del testigo. Este modo implica que no se establece priorización sobre algún tipo de tráfico, lo que perjudica al transito sensible al tiempo. Un método de resolución de los problemas de distribución de tráfico de vídeo en movimiento y multimedia en las redes FDDI existentes consiste en almacenar los paquetes recibidos hasta completar el conjunto y ordenarlos, y entonces exhibir el vídeo. Sin embargo, esto origina un retraso inaceptable en videoconferencias interactivas, en la cual las personas establecen conversaciones, aunque si es aceptable si se trata de una simple visualización de una secuencia almacenada de vídeo.

SERVICIOS SÍNCRONOS: El modo de anillo síncrono con testigo permite realizar una priorización de tráfico sensible al tiempo, de modo que los paquetes lleguen dentro de unos márgenes de tiempo. Las tarjetas FDDI que ofrecen capacidad síncrona conceden a los gestores de la red la posibilidad de reservar parte del ancho de banda para el tráfico sensible al tiempo. Mientras que las estaciones de trabajo asíncronas contienden por el resto. Las capacidades síncronas deben añadirse a través de actualizaciones de software en la mayoría de tarjetas FDDI existentes. El comité de ANSI trabaja actualmente en una nueva norma, de modo que esta utilidad estará disponible como opción estándar.

SERVICIO BASADO EN CIRCUITOS: El modo basado en circuito (únicamente en FDDI-II) puede crear una línea de comunicación dedicada entre dos estaciones de trabajo con un ancho de banda garantizado. Los servicios basados en circuitos en FDDI-II se proveen mediante la asignación de intervalos de tiempo regulares y repetidos durante la transmisión con objeto de crear un canal de comunicación dedicado entre dos estaciones. Este método se denomina transmisión isócrona.

Función	FDDI
Protocolo principal	Token Passing
Formato del frame	Token Passing
Medio de transmisión	Cable de fibra óptica
Topología	Anillos dobles de rotación inversa independientes
Velocidad de los datos	100 Mbps
Distancia máxima	100 Km
Administración de las estaciones	Descentralizado
Tolerancia a fallas por la ruptura del cable	Reconfigurable
Tolerancia a fallas causado por una estación	Reconfigurable
Clocking (tiempo de reloj)	En cada nodo
Liberar el token	Inmediatamente
Codificación/Decodificación	4 bytes/5 bytes
Eficiencia	80 %
No. máximo de nodos	500
Máxima distancia entre nodos	2 km entre estaciones activas
Velocidad del reloj	125 Mhz

Tabla 6.2 Principales características técnicas de FDDI

6.1.2.6 FDDI-II

La arquitectura FDDI-II no es una alternativa o competidor de FDDI sino una extensión o mejora de este. En 1984 el comité X3T9.5 de ANSI fue el encargado para desarrollar un estándar de redes de alta velocidad para datos, voz y vídeo. Esta llego a ser el FDDI-II. FDDI-II describe el estándar para Control de Anillo Híbrido (HRC: Hybrid Ring Control) que especifica una versión compatible con FDDI. Esto añade la capacidad para el servicio de conmutación de circuitos a los servicios de paquetes básicos de FDDI, para crear una red local de servicios integrados de alta velocidad.

FDDI-II es considerado como un superconjunto del estándar ANSI FDDI. FDDI-II es compatible hacia abajo con FDDI a partir, de que FDDI-II puede interpretar la parte de datos de FDDI. FDDI no es compatible hacia arriba con FDDI-II por que FDDI no puede interpretar la parte de voz y vídeo de FDDI-II. Los servicios básicos de FDDI pueden estar disponibles desde una estación FDDI-II, pero cualquier estación sobre el anillo FDDI-II deberá soportar el Control de Anillo Híbrido (HRC) antes de que el anillo pueda desempeñar las funciones esperadas de FDDI-II.

La norma FDDI-II se ha diseñado para redes que necesitan transportar vídeo en tiempo real u otro tipo de información que no puede tolerar retrasos de tiempo. La arquitectura, requiere que todos los nodos de la red utilicen FDDI-II; de otro modo, la red se convierte en una FDDI. Por tal motivo, las estaciones FDDI existentes deben conectarse a su propio tipo redes.

FDDI-II utiliza técnicas de multiplexaje que divide el ancho de banda en circuitos dedicados, de esta forma puede garantizar la distribución del trafico multimedia. Puede crear hasta 16 circuitos separados que trabajan dentro de unos márgenes de velocidad establecidos entre 6.144 Mbps hasta 99.072 Mbps cada uno. La razón de esta variación reside en que el ancho de banda se configura según las necesidades de las estaciones. Cada uno de estos canales pueden subdividirse posteriormente para producir un total de 96 circuitos separados a 64 Kbps.

Estos canales pueden servir de soporte a trafico asíncrono e isócrono. Los intervalos regulares de tiempo se asignan al anillo para la transmisión de los datos. Las estaciones que gozan de prioridad utilizan el numero de intervalos que necesitan para distribuir sus datos dentro de márgenes de tiempo. Si estos intervalos no se utilizan por estas estaciones, inmediatamente son asignados a otras.

FDDI-II es frecuentemente de manera errónea representada como mas rápida que FDDI. En la actualidad, FDDI-II opera a la misma velocidad que FDDI con las mismas limitaciones y especificaciones físicas, pero esta debe ser considerada como una FDDI *mejorada*. FDDI-II tiene la capacidad de HRC que le permite el manejo adecuado de tráfico de voz y video debido a una latencia reducida y demoras pronosticables. Sin HRC, FDDI no puede predecir el tiempo y no podrá llevar voz. Además para el video comprimido para FDDI fue una cuestión muy complicada debido a la implantación de la parte síncrona de la especificación del protocolo de FDDI.

Además de la capacidad del conmutación de paquetes que soporta el protocolo de FDDI, FDDI incluye la capacidad de conmutación de circuitos. Este modo de conmutación de circuitos provee soporte para determinar el tiempo usado para la transmisión de vídeo, voz, entre otros.

El anillo FDDI-II solo opera en el modo en el que fue inicializado, es decir, Básico o Híbrido. El tamaño del frame en el modo híbrido no esta limitado a 4500 bytes como es para el modo Básico.

La distancia máxima entre estaciones FDDI es de 2 kilómetros.
Red basada en fibra óptica multimodo de 62.5/125 µm.
Una circunferencia total de 100 kilómetros del anillo FDDI.
500 estaciones conectadas directamente al anillo FDDI como máximo
El estándar ANSI esta diseñado por el comité X3T9.5.
Puede ser inicializado en modo híbrido o modo básico.
Se tiene una baja en la tasa de error (un error cada 10^{-9} bits).
Conmutación de derivación óptica opcional para un máximo rendimiento
Latencia reducida.
Una velocidad de 100 Mbps con una reloj de red que corre a 125 Mbps
Tamaño del paquete variable con un máximo de 4500 bytes.
Capacidad de transmisión de voz y video.

Tabla 6.3 Estándares de FDDI-II

6.1.2.6.1 Esbozo del Control del Anillo Híbrido de FDDI-II

FDDI-II integra un nuevo documento, el Control de Anillo Híbrido (HRC: Hybrid Ring Control) , a los cuatro documentos existentes que definen el estándar FDDI. HRC es la principal diferencia entre FDDI-II y FDDI. HRC es la subcapa mas baja de la capa de liga de datos, tomando su lugar entre la subcapa MAC y la PHY. El HRC es utilizado para la creación de redes FDDI-II describiendo un modo híbrido de operación que incluye la transmisión de paquetes utilizados en FDDI y otros esquemas de red. El documento HRC también describe un modo de transporte isócrono, utilizado por las redes públicas conmutadas.

El HRC esta compuesto de los protocolos Multiplexor Híbrido (H-MUX: Hybrid Multiplexor) y el Control de Acceso al Medio Isócrono (I-MAC: Isochronous Media Access Control). El H-MUX integra paquetes de datos isócronos en ciclos que se transmiten y reciben del medio utilizando los servicios de la capa Física (capa 1 del modelo de referencia OSI). El I-MAC provee canales de transmisión separados para la transferencia de información isócrona de los usuarios. El formato, los contadores, los ciclos de sincronización y de operación, además de las interfaces H-MUX y I-MAC están definidos por el estándar de subcapa HRC. Los nodos que tienen entidades H-MUX son referidos como nodos FDDI II.

El anillo HRC puede operar hasta 100Mbps, a velocidades incrementales de 6.144 Mbps.

Los canales de transmisión de FDDI-II pueden operar a diferentes tasas pero nunca pueden excederse de 6.144 Mbps. Los canales de banda amplia pueden estar combinados por niveles más altos para formar canales con velocidades por encima de los 6.144 Mbps, sin embargo, esta no es una función del HRC.

El protocolo de FDDI-II soporta dinámicamente particiones de anchos de banda entre los servicios de paquetes y circuitos que permiten ambos modos de operación, conmutación de paquetes y conmutación de circuitos. La asignación del ancho de banda es realizada con 8 Kbps gradualmente hasta llegar a los 6.144 Mbps. La interoperabilidad entre FDDI y FDDI-II solo se puede llevar a cabo en el modo básico, es decir, únicamente para manejo de datos.

Hay dos modos de operación de una estación de FDDI-II, estos son, modo básico e hibrido. FDDI-II provee el modelo de operación hídrido en donde la operación de timed-token y la conmutación de circuitos son soportados en el mismo medio. Existen dos tipos de trafico en el modo híbrido: conmutación de circuitos y conmutación de paquetes[88].

La arquitectura FDDI-II soporta servicios de datos isócronos, en una estructura especial de frame referida como un ciclo. La especificación HRC opera para ajustar la longitud de los ciclos a un múltiplo de 125 microsegundos, consistente con el reloj de datos públicos de 8 Mhz.

6.1.2.6.2 Especificaciones del SMT para FDDI-II

El proyecto propuesto para un nuevo estándar X3, referido como Administración de Estación para Servicios Comunes de Control del Anillo Híbrido de FDDI (FDDI SMT-2-CS: Station Management for FDDI Hybrid Ring Control Common Services), fue propuesto en el año 1992.

[88] El estándar FDDI como originalmente estaba concebido (es decir, sin la especificación HRC) y su servicio asociado de datos isócronos, solo soportaba la conmutación de paquetes de datos.

Las nuevas capacidades de Administración de Estación (SMT-2) son requeridas para la operación y administración de nodos y redes FDDI-II. El estándar se construyó sobre el actual SMT (Administración de Estación). El estándar SMT-2 completo esta conformado por tres documentos, estos son: Servicios Comunes de Administración de Estación para FDDI-II (SMT-2-CS), Servicios de paquetes de Administración de Estación para FDDI-II (SMT-2-PS) y los Servicios Isócronos de Administración de Estación para FDDI-II (SMT-2-IS).

6.1.2.6.3 Aplicaciones sobre FDDI-II

La razón por la cual los usuarios se dirigirán a la implantación de FDDI-II será la habilidad de este para llevar tanto tráfico de voz, vídeo, datos al mismo tiempo. Muchas aplicaciones futuras necesitaran la gran cantidad de ancho de banda suministrada por FDDI-II. Estas, incluirán aplicaciones como fax a color, hypertexto, imágenes medicas, imágenes para teléfono y la transferencia de bases de datos grandes. Las comunicaciones de multimedia interactivas se espera que sean una de las aplicaciones principales para migrar hacia FDDI-II.

6.1.2.7 CDDI Interfaz de Datos Distribuidos por Cobre FDDI/UTP

Una tecnología de cableado alternativo que cumple con la norma FDDI, consiste en la utilización de cable de cobre de par trenzado no blindado (UTP: Unshielded Twisted Pair). El cuál fue propuesto originalmente por IBM, DEC, Cabletron Systems, Crescendo Comunications entre otros. La norma TP-PMD (Twisted-Pair - Physical Medium Dependent) de ANSI define una red FDDI que trabaja con cable de par trenzado sin blindar de Categoría 5 o cable de par trenzado blindado Tipo 1 de IBM (STP: Shielded Twisted Pair). La especificación CDDI, tiene las características de FDDI, exceptuando una diferencia en cuanto a la longitud que puede cubrir el cable. El cable UTP admite hasta 100 metros entre los nodos, mientras que la fibra óptica admite 2 kilómetros entre ellos.

El cable UTP de Categoría 5 es adecuado para la comunicación de datos de alta velocidad (100 Mbps) sobre distancias cortas, en una configuración similar a la topología en estrella utilizada en Ethernet 10Baset-T. El cable de Categoría 5 forma parte de la especificación de cableado estructurado EIA/TIA 568[89]. La transmisión de información de alta velocidad es posible llevarla a cabo adaptando la especificación de 100 Mbps al cable de par trenzado. [90]

Por lo anterior, las instalaciones de Ethernet 10Base-T con cable UTP de categoría 5 están preparadas para migrar a CDDI. Se debe tener presente que FDDI y 10BaseT

[89] Para mayor información, referirse al capitulo 3 "conceptos y estándares de redes de área local".
[90] Un ejemplo de esta adaptación, es el mantener el trenzado del cable par trenzado hasta las derivaciones de las placas en la pared del área de trabajo y bloques de comunicación.

presentan distintas configuraciones de cableado (aunque ambas admiten las conexiones de las estaciones de trabajo a los concentradores, sin embargo, FDDI también acepta conexiones de estaciones de trabajo entre sí, adoptando una configuración que forma un anillo doble). Las estaciones de trabajo se conectan mediante una configuración en forma de estrella desde un concentrador[91], lo que puede proporcionar una conexión a un anillo de fibra óptica FDDI.

Como nota final, los backbone que enlazan las redes de área local distantes seguirán utilizando FDDI, es decir, se encontraran basados en fibra óptica. Y el sistema de cableado intraedificios puede ser llevado a cabo por medio de la especificación CDDI. Sin embargo, con la presencia de CDDI, el precio de las tarjetas FDDI serán más barato. Por esta razón, los administradores deben evaluar cuidadosamente los productos y precios existentes en el mercado.

6.1.2.7 FDDI conmutado

Descripción

Por varios años, FDDI a 100 Mbps ha sido utilizada para compartir el medio de comunicación, siendo el más utilizado durante varios años como el backbone de redes. De hecho, hasta muy recientemente, era el único backbone de alta velocidad disponible. Sin embargo, como las redes LANs conectadas al backbone cada vez son más grandes y más rápidas, un número creciente de corporaciones se han dado cuenta que 100 Mbps de ancho de banda compartido no es suficiente para sus necesidades actuales y futuras. Según la tendencia de la industria, la tecnología que resolverá esta situación es la tecnología de transferencia de celdas ATM. Pero como se vera más adelante, la interoperabilidad entre proveedores, es una característica que deben cumplir los conmutadores ATM, lo cual todavía se encuentra en desarrollo. De tal manera, que las organizaciones que no pueden esperar para agregar mas ancho de banda a sus redes, vuelven hacia los conmutadores FDDI para mejorar la capacidad de su backbone en sus redes.

Tal vez el inconveniente de comprar conmutadores FDDI actualmente, es que significa invertir en una tecnología vieja. Si los administradores de redes corporativas buscan una manera para aumentar la capacidad de su backbone congestionado, deberán entender todo acerca de FDDI conmutado. Ya que los primeros usuarios de los conmutadores FDDI informan que en la mayoría de los casos los conmutadores aumentan el desempeño del backbone FDDI en por lo menos el 50%.

[91] El cable que procede de los concentradores debe proporcionar un cruzado específicamente de los pares 1 y 2 formando así una configuración llamada de crossover en algún punto, este se puede efectuar en el trayecto que hay desde el concentrador al panel de conexión (recordando que panel de conexión organiza el trayecto del cable que se dirige hacia las estaciones de trabajo a través de los muros del edificio).

Todos los conmutadores FDDI tienen dos cosas en común. El primero de estos, es que mejoran dramáticamente el desempeño de los medios compartidos de la redes FDDI dividiendo estos, en segmentos de redes conmutadas dedicados, Figura 6.10. Segundo, y a diferencia de los conmutadores Ethernet, los conmutadores FDDI son caros. Esto implica que la mayor parte de los conmutadores FDDI se deben emplear como backbone (que es donde se puede amortizar el gasto a través de todos los nodos de la red) más que en grupos de trabajo que proveen conectividad a las estaciones de trabajo. Por otro lado, utilizar conmutador para segmentar un anillo FDDI es más barato que la alternativa tradicional de instalar un enrutador.

Los conmutadores FDDI están basados en los estándares establecidos de FDDI, por lo cual pueden interconectarse con los productos FDDI normales (incluyendo adaptadores, concentradores, enrutadores y analizadores de redes) que son vendidos por más de 100 fabricantes. Las corporaciones que tienen actualmente anillos FDDI pueden aumentar el desempeño de su backbone fácilmente y sin necesidad de hacer cambios a su hardware de interconexión de FDDI instalado, simplemente uniendo sus equipos FDDI al conmutador FDDI[92].

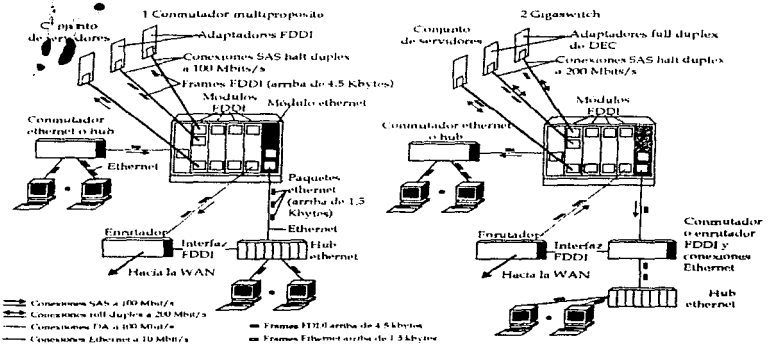


Figura 6.11 FDDI conmutado

[92] Cabe hacer notar que instalar un backbone con FDDI conmutado es un mas fácil que instalar un backbone ATM, en una red que tenga ya instalado FDDI.

6.1.3 FAST ETHERNET (100BaseT)

6.1.3.1 Historia

En julio de 1993, un grupo de compañías de intercomunicación de redes se unió para formar la alianza de Fast Ethernet también conocida como 100Base-T. La característica principal, fue el desarrollo de la especificación 802.3u del IEEE. La cual fue aprobada en junio de 1995. Los objetivos principales de la alianza son: mantener el protocolo de control de acceso al medio CSMA/CD; soportar los esquemas de cableado utilizados por Ethernet a 10 Mbps, además de asegurar que la tecnología Fast Ethernet no requiera de cambios a los protocolos de las capas superiores y software que ocupan las estaciones de trabajo de la red. Por lo anterior se puede decir que Fast Ethernet preserva la estructura principal del Ethernet a 10 Mbps.

6.1.3.2 Capa de enlace de datos

Una de las características principales de Fast Ethernet es que mantiene el protocolo de transmisión de Ethernet CSMA/CD. Sin embargo 100base T reduce en un factor de 10 el tiempo de duración en el que un bit es transmitido sobre el canal de Ethernet; de esta manera, se lleva la velocidad del paquete desde 10 Mbps a 100 Mbps. Los datos pueden moverse entre Ethernet y Fast Ethernet sin ningún requerimiento de traducción de protocolos. ya que Fast Ethernet mantiene sin cambio las características de la función de control de error, formato y la longitud del paquete utilizados por el sistema Ethernet a 10 Mbps.

6.1.3.3 Capa física

6.1.3.3.1 Tipos de medio para Fast Ethernet

Fast Ethernet mantiene los medios utilizados por Ethernet original, como son: par trenzado sin blindar (UTP), par trenzado blindado (STP), y Fibra óptica. Por lo que Fast Ethernet especifica 3 subcapas físicas separadas para cada tipo de medio :

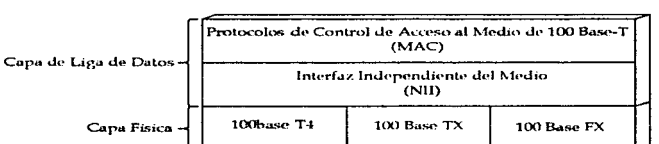


Figura 6.12 Subcapas de Fast Ethernet

Cabe mencionar, que los estándares utilizados por Fast Ethernet son:

100Base-TX y 100Base-FX han sido adoptados de los estándares del medio físico primeramente desarrollados por ANSI para la Interface de Datos Distribuidos por Fibra (FDDI, ANSI estándar X3T9.5) y CDDI. Esto combina la escalabilidad Ethernet MAC con los mismos circuitos PHY y transceivers desarrollados para FDDI y CDDI. Los estándares TX y FX son también conocidos como 100Base-X.

Por otro lado, el estándar T4 es una nueva tecnología de señalización propuesta para hacer posible la utilización de cable par trenzado de baja calidad (cable par trenzado categoría 3, 4 para grado de voz) y de esta manera transmitir las señales de Ethernet a 100 Mbps.

La flexibilidad de estas especificaciones permite implementar 100Base-T sobre una infraestructura de cableado utilizada por el sistema Ethernet 10BaseT.

100BaseT4	cuatro pares de alambre UTP de categoría 3, 4 y 5 para voz o grado de datos (half dúplex)
100BaseTX	dos pares de alambre UTP o STP categoría 5 para datos.(Half o Full dúplex)
100BaseFX	dos fibras de 62.5/125-micrones multimodo de Fibra óptica (Half o Full dúplex[2])

Tabla 6.4 Principales tipos de Fast Ethernet

6.1.3.3.2 Esquemas de señal en la capa física

Cada subnivel físico utiliza un esquema de señal que es apropiado según el tipo de medio que utiliza:100Base-T4 utiliza tres pares de alambres para la transmisión de 100 Mbps y el cuarto par para la detección de colisiones. Este método baja la señal de 100BaseT4 a 33Mbps por par, haciendo posible de esta forma transmitir 100Mbps a través del cable UTP de categoría 3, 4 y 5.

100Base-TX utiliza un par de alambres para la transmisión (con una frecuencia de operación de 125 Mhz al 80 por ciento de su eficiencia para permitir una codificación 4B5B) y otro par para la detección de colisión y recepción.

100Base-FX utiliza dos fibras ópticas, la primera para la transmisión y la segunda para la detección de colisión además de la recepción.

En 100base-TX y 100base-FX, los canales de la señal física son basados en el estándar ANSI X3T9.5 para FDDI. 100baseTX utiliza el esquema de codificación de línea MLT-3, el cuál es una especificación para FDDI sobre cable UTP categoría 5. Actualmente MLT-3 también es utilizado como esquema de señal para ATM sobre cable UTP categoría 5.

6.1.3.3.3 Topología para Fast Ethernet

En primer lugar, se debe mencionar que en Fast Ethernet los segmentos son definidos como "segmentos de enlace" para cumplir las especificaciones de Ethernet. Un segmento de enlace se define como un medio punto-a-punto que conecta a dos y solo dos MDI's.[93]

De esta manera, la topología física soportada para los segmentos de enlace de todos los diferentes tipos de medio que maneja 100Base-T es la topología en estrella o backbone colapsado. De esta forma se hace una división de múltiples dominios de colisión[94]. El diámetro de cada dominio de colisión depende del medio y tipo de concentrador repetidor utilizado dentro del dominio de colisión.

El enlace se lleva a cabo de la siguiente manera, se conecta una interfaz Ethernet en la estación de una de las terminaciones del segmento de enlace, y en la otra terminación del segmento es conectada al concentrador. De esta forma un conjunto de segmentos de enlace son conectados a un concentrador central por medio del cual son comunicados.

Componentes para la conexión de 100Mbps

La figura 6.12 muestra los componentes definidos en el estándar IEEE para la unión de un medio de sistema a 100Mbps.

- Dispositivo de capa física (PHY).
- Interfase independiente del medio (MII: Medium Independent Interface).
- Equipo Terminal de Datos o Computadora (DTE: Data Terminal Equipment, or Computers).
- Medio Físico (Physical Medium): puede ser cualquiera de los tres tipos de medios para interconexión de 100Mbps, explicados anteriormente. Se puede realizar la conexión al medio físico con la "Interface Dependiente del Medio " o MDI. En el sistema 100Base-T, el MDI es un conector de 8 pines para cable par trenzado o un conector para fibra óptica.

---

[93] La construcción de una pequeña red con un segmento puede consistir de dos computadoras una al final de cada lado del segmento de enlace.
Una instalación mas compleja utiliza puertos de concentradores repetidores, o concentradores de conmutación de paquetes, para proveer un largo número de segmentos de enlace. De esta manera se pueden unir varios segmentos de enlace con sus computadoras asociadas como puertos existan en el concentrador y todas las computadoras se comunican por medio del concentrador
[94] Cada puerto de un puente, enrutador o conmutador inicializa un dominio de colisión.

- Dispositivo de capa física PHY (Physical Layer Device). Este dispositivo desarrolla la misma función que la realizada por un transceiver en el sistema de 10 Mbps. Este consta de un conjunto de circuitos integrados dentro del puerto Ethernet o de un dispositivo de red (de esta manera invisible al usuario) o puede ser una pequeña caja equipada con un cable MII, como el transceiver externo y el cable de transceiver utilizados en el sistema Ethernet 10Base-T.

- Interface Independiente del Medio (MII: Medium Independent Interface). El MII es un conjunto circuitos electrónicos opcional que provee una forma de unir la función de control de acceso al medio de Ethernet en el dispositivo de red con el Dispositivo de Capa Física (PHY) que envía las señales dentro del medio de la red. Un MII puede opcionalmente soportar operaciones de 10 Mbps y 100 Mbps, permitiendo conectar dispositivos de red en segmentos de medios de 10Base-T o 100Base-T de una manera adecuada. El MII convierte la señal de la línea recibida desde varios segmentos de diferentes tipos de medio por el transceiver (PHY) en señales de formato digital que son de esta manera provistas a los chips de Ethernet dentro del dispositivo. Es decir, el MII opcional (el conector hembra de 40 pines asociado y el cable MII), hacen posible conectar un dispositivo de red a cualquiera de los varios tipos de medio soportados, previendo de esta manera una máxima flexibilidad.

- El MII puede ser unido a un transceiver externo a través de un conector MII de 40 pines y un pequeño cable MII. El pequeño cable MII utilizado con transceivers externos de 100 Mbps es especificado como un cable de 40 pines con plug final de 40 pines, equipado con el jack macho. El cable puede ser de una longitud máxima de 0.5 metros. También es posible para los transceivers externos unirse directamente a el conector MII sobre el dispositivo sin intervención del cable, si el diseño del transceiver lo permite. (dibujo en cisco.7 apéndice).

- Equipo Terminal de Datos (DTE: Data Terminal Equipment) o terminal El dispositivo de red.es definido como equipo terminal de datos en el estándar IEEE. Cada DTE conectado a Ethernet es equipado con una interfaz Ethernet. La interfaz Ethernet provee una conexión al sistema de medio de Ethernet y contiene los componentes electrónicos y el software necesario para desarrollar las funciones de control de acceso al medio requeridas para enviar los paquetes sobre el canal Ethernet.

Conexión de un DTE

Para realizar la conexión de una estación (DTE) se debe tener una interface Ethernet, la cual recibe y envía paquetes de datos de Ethernet de las computadoras conectadas a la red. La interface es conectada al medio utilizando un conjunto de equipo que puede incluir un conector de cable MII y un PHY (transceiver) con su MDI asociado (jack RJ45 de par trenzado o conector de fibra óptica). La interface o puerto repetidor puede ser también diseñada para incluir los componentes electrónicos del PHY internamente a la estación, en este caso en la parte exterior únicamente se observará el conector del medio físico que soporta. Cada tipo de medio soportado por Fast Ethernet tiene su propio PHY y MDI, diseñado específicamente para trabajar sobre el tipo de medio utilizado.

Distancias del sistema de cableado

Las especificaciones para 100Base-TX y 100Base-T4 permiten un segmento de enlace de hasta 100 metros. mientras que 100Base-FX permite un segmento de enlace de hasta 412 metros aproximadamente. Sin embargo, una versión 100Base-FX full-dúplex no estandarizada puede ser utilizada principalmente para la interconexión de edificios y concentradores cubriendo una distancia de 2 kilómetros[95].

Diferentes tipos de medio pueden ser conectados por medio de un repetidor. Por lo que, el 100baseT define dos clases de repetidor: Clase I y Clase II[96]. Fast Ethernet es implementada en una topología en estrella, haciendo notar que el diámetro de la red es proporcionalmente mas pequeño que Ethernet a 10 Mbps .

Un repetidor Clase I permite tener largos tiempos de retraso, y opera por traducción de las líneas de señal sobre un puerto de entrada de forma digital, y retraduce las líneas de señal cuando son enviadas hacia afuera a través los puertos de salida.

Esto hace posible la repetición de señales entre segmentos de medios que utilizan diferentes esquemas de señal, tales como 100BASE-TX/FX y 100base-T4, permitiendo que los diferentes tipos de segmentos sean conectados dentro de un concentrador repetidor (repeter hub). El proceso de traducción en los repetidores Clase I se utiliza para subir un número de bits de tiempo , De esta manera solo un repetidor Clase I puede ser utilizado en un dominio de colisión dado, cuando la máxima longitud de cableado es utilizada.

---

[95] El IEEE actualmente se encuentra trabajando en una versión estándar para full-dúplex. Pero en este momento las soluciones 100Base-FX full-dúplex son propietarias.

[96] El estándar de Fast Ethernet requiere que los repetidores sean etiquetados con numero romano centrado dentro de un círculo para hacer referencia a repetidores de clase I o de clase II.

Una red 100Base-T que utiliza concentradores Clase I no permite mas que un repetidor entre dos dispositivos nodos finales. Si más de un Concentrador Clase I es instalado sobre la red, entonces un puente (bridge), enrutador o conmutador deberá ser requerido entre cada uno de los concentradores.

Un repetidor Clase II esta restringido a pequeños retrasos de tiempo, e inmediatamente repite la señal de entrada hacia los puertos de salida sin un proceso de traslación. Para llevar a cabo los pequeños retrazos de tiempo, los repetidores de Clase II solo llevan a cabo conexiones entre tipos de segmento que utilizan la misma técnica de señal. Tales como 100BASE-TX y 100BASE-FX. De esta manera, un máximo de dos repetidores Clase II pueden ser interconectados sin la necesidad de otro dispositivo dentro de un dominio de colisión dado, cuando la máxima longitud de cable es utilizada.

Los tipos de segmentos con diferente técnica de señal (100BASE-TX/FX y 100BASE-T4) generalmente no pueden ser conectados por medio de un concentrador repetidor Clase II.

Como se mencionó anteriormente, Fast Ethernet es implantada en una topología en estrella, donde el diámetro de la red es proporcionalmente menor que Ethernet 10 Mbps dando un incremento de 10 veces en la velocidad del paquete, y dependiendo de las necesidades de un dominio de colisión, se puede incluir un repetidor Clase I o dos repetidores Clase II.

En las siguientes tablas 6.5, se describen las relaciones de distancia y los repetidores Clase I y Clase II.

MODELO	Cobre	Cobre y T4 y FX	Fibra óptica TX y FX	Fibra óptica
DTE-DTE (sin repetidor)	100	no existe	no existe	412
1 repetidor Clase I	200	231	261 [a]	272
1 repetidores Clase II	200	no existe [b]	309 [a]	320
2 repetidores Clase II	205	no existe [b]	216.2 [c]	228

a. asume 100 metros de enlace de cobre y un enlace restante de fibra óptica.
b. No aplicable T4 y FX no puede ser enlazado con un repetidor Clase II por la técnica de señal que utilizan.
c. asume 105 metros de enlace de cobre y un enlace de fibra.

Tabla 6.5 Relaciones de distancia y los repetidores Clase I y Clase II.

Opciones de subcapa física	Especificación de cable	Longitud (metros)
100BaseTX	categoría :	
	UTP 5, dos pares	100 half/full dúplex
	STP tipo 1 y 2, dos pares	100 half/full dúplex
100BaseT4	Categorías UTP 3, 4 y 5, cuatro pares	100 half/full duplex
100BaseFX	62.5/125 multimode fiber, dos ramas	412 half/duplex 2000 full/duplo

Tabla 6.6 Opciones de subcapa física

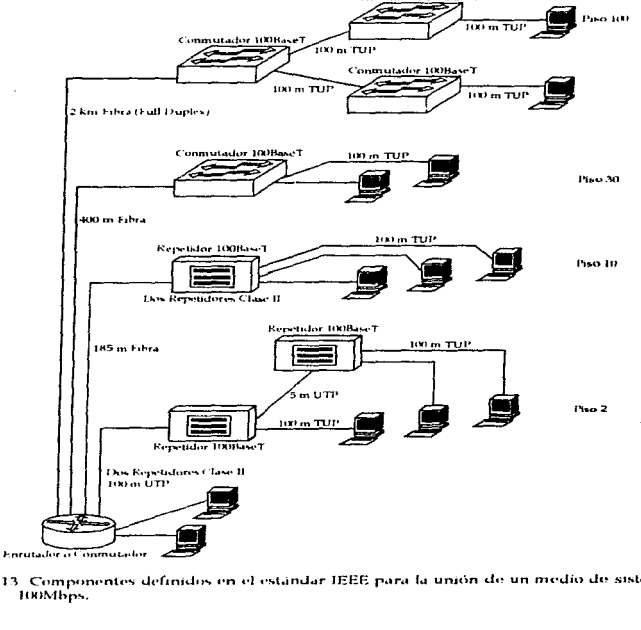


Figura 6.13 Componentes definidos en el estándar IEEE para la unión de un medio de sistema a 100Mbps.

6.1.3.4 Características opcionales para Fast Ethernet

6.1.3.4.1 Auto Negociación

La función de Auto-Negociación es una parte opcional del estándar Fast Ethernet que describe un proceso de configuración automático para los dispositivos en las terminaciones de un enlace. Esto hace posible el modo para intercambio de información entre los dispositivos sobre un segmento de enlace según sean sus capacidades (10/100 Mbps), y de esta manera desarrollar el mejor modo de operación sobre el enlace.

El protocolo de Auto-Negociación, además incluye una verificación automática para otras capacidades, por ejemplo, si un concentrador es capaz de soportar modo de operación full-dúplex sobre alguno o todos los puertos. Esto sirve de manera que, las interfaces conectadas al concentrador que también soporten modo de operación full-dúplex pueden entonces configurarse para utilizar el modo full-dúplex en interacción con el concentrador.

Pulso de enlace rápido (FLP)

La Auto-Negociación se desarrolla utilizando señales de Pulso de Enlace Rápido (Fast link Pulse) FLP[97]. Las señales FLP son generadas automáticamente al encender la interfaz o pueden ser seleccionadas manualmente a través del administrador de la interface del dispositivo que soporta la función de Auto-Negociación.

Las señales Pulso de Enlace Rápida fueron diseñadas de manera que puedan coexistir con las señales NLP(Normal Link Pulse), de esta manera un dispositivo de 10BASE-T que utiliza señales NLP puede continuar la detección propia de la integridad del enlace aún cuando sea conectado junto con un concentrador que soporta Auto-Negociación y por lo tanto envía señales FLP. Como la señal original de pulso de enlace de 10Base-T, las señales FLP se llevan a cabo durante los tiempos ociosos sobre el enlace de la red, de esta manera no se interfiere con el tráfico normal. Ambas señales FLP y NLP son especificadas únicamente para medios del tipo cable par trenzado sin blindar (UTP)[98].

---

[97]FLP (Fast Link Pulse). Esta señal es una versión modificada de la senal Pulso de Liga Normal NLP (Normal Link Pulse), utilizada para verificar la integridad del enlace como fué definido en las especificaciones del original Ethernet 10Base-T.

[98]Esto significa que los dispositivos y puertos repetidores enlazados sobre segmentos de fibra óptica no pueden participar en la Auto-Negociación.

Las señales FLP son empleadas para enviar información acerca de las capacidades del dispositivo, así, el protocolo de Auto-Negociación define reglas para la configuración de los dispositivos basándose en esta información. De esta manera un dispositivo conectado a un concentrador donde ambos soportan Auto-Negociación pueden de forma automática negociar y configurarse por si mismos para utilizar el modo de operación óptimo de más alto desempeño común para los dos dispositivos.

La Auto-Negociación es una característica opcional, y de esta manera, el protocolo de Auto-Negociación es diseñado para trabajar con interfaces 100Base-T que no soportan tanto las señales FLP como la Auto-Negociación, así como también con las interfaces 10Base-T. El sistema de Auto-Negociación incluye una interface de manejo opcional que permite deshabilitar la Auto-Negociación, o forzar de manera manual que el proceso de Auto-Negociación se lleve a cabo. Asimismo se puede utilizar la interface de manejo para seleccionar manualmente un modo de operación específico para un determinado enlace del concentrador.

La definición de Auto-Negociación también provee una función de detección paralela que permite el reconocimiento de las capas físicas half-full dúplex 10Base-T, half-full dúplex 100Base-TX y 100Base-T4 (aún si uno de los dispositivos conectados no ofrece capacidades e Auto-Negociación).

Enlaces Ethernet Full Dúplex

El protocolo de Auto-Negociación se provee para un amplio rango de segmentos Ethernet del tipo par trenzado, también como enlaces Ethernet Full-dúplex. Ethernet Full-dúplex es una variante de la tecnología Ethernet que actualmente esta siendo estandarizada por el IEEE. En la ausencia de un estándar oficial, se puede decir que las reglas para la longitud de un enlace Full-dúplex puede variar dependiendo del vendedor (ya que esta tecnología es propietaria).

El modo de operación Full-dúplex requiere que cada terminación de un enlace, solo se conecte a un solo dispositivo (ej. una estación a un puerto del conmutador concentrador).

Partiendo de la observación de que solo existen dos dispositivos en ambos extremos de un enlace en modo Full-dúplex, no se intenta crear canales de Ethernet compartidos o capaces de soportar múltiples dispositivos en el enlace ya que este segmento es dedicado[99]. De esta manera se puede decir que un dispositivo final del enlace de Ethernet en modo Full-dúplex no tiene que escuchar otras transmisiones o colisiones al momento de enviar datos. Es por esta razón, que no es necesario adicionar el sistema original de control de acceso al medio de Ethernet referido como CSMA/CD.

[99]un ejemplo de enlaces compartidos son como el enlace de bus con cable coaxial

Por lo tanto, si no se necesita utilizar el mecanismo de control de acceso al medio para compartir el canal de señal con múltiples estaciones, un dispositivo final del enlace de Ethernet de modo Full-dúplex no tiene que escuchar otras transmisiones o colisiones al momento de enviar datos.

La operación Full-dúplex es bastante simple comparada con el Ethernet normal, ya que los dispositivos finales de un enlace Ethernet de modo Full-dúplex pueden enviar y recibir datos simultáneamente sobre el enlace. Una ventaja de este aprovechamiento es que el enlace Full-dúplex puede teóricamente proveer dos veces el ancho de banda proporcionado por el Ethernet normal en modo half-dúplex.

Los esquemas de señal 10BASE-T, 100BASE-TX, y 100BASE-FX pueden soportar las operaciones de modo Full-dúplex, a partir de que estas, tienen rutas de transmisión y recepción de señal que pueden estar simultáneamente activas. Otra de las ventajas que ofrece, es que los enlaces de fibra óptica en modo Full-dúplex pueden ser mucho mas largos que las especificaciones permitidas por un segmento normal de 100BASE-FX. Esto es por que la falta de cualquier requerimiento para adicionar tiempo de viaje redondo (round trip timing) del dominio de colisión permite a la fibra óptica ser tan larga como lo permita el presupuesto de perdida óptico. Por esta razón, una versión de un enlace de fibra óptico en modo Full-dúplex de 100Mbps puede generalmente proveer una longitud de segmento de alrededor de 2 kilómetros.

Prioridades de Auto-Negociación

Cuando dos dispositivos que soportan el protocolo de Auto-Negociación con múltiples capacidades son conectados conjuntamente, estos encuentran su modo de operación de más alto desempeño basado en una tabla de prioridades. Esta tabla del protocolo de Auto-Negociación contiene un conjunto de prioridades en los cuales los dispositivos que conforman el enlace seleccionan su más alto conjunto de habilidades común.

Las prioridades están listadas en la tabla desde el más alto a el más bajo. El modo de operación Full-dúplex da la más alta prioridad que el Ethernet original (half dúplex), partiendo de que el sistema full-dúplex puede enviar mas datos que un enlace en operación half-dúplex a la misma velocidad. De esta manera si los dispositivos terminales de un enlace pueden soportar la operación full-dúplex, y si ellos también soportan Auto-Negociación de esta capacidad, entonces ellos automáticamente se autoconfigurarán para el modo de full-dúplex de alto desempeño.

La tabla 6.7, demuestra que si los dos dispositivos terminales de un enlace pueden soportar, por ejemplo 10Base-T y 100Base-TX según lo requieran, entonces el protocolo de Auto-Negociación conectará ambos dispositivos terminales del enlace en modo 100BASE-TX en lugar de 10Base-T.

A:	100Base-TX Full Duplex
B:	100Base-T4
C:	100Base-TX
D:	10Base-T Full Duplex
E:	10Base-T

Tabla 6.7 Nivel de conexión para Auto Negociación

Ejemplos de Auto-Negociación

Los siguientes ejemplos ayudaran a ilustrar algunos aspectos de la operación de un enlace de cable par trenzado con o sin Auto-Negociación.

- Una de las terminaciones del enlace no soporta la Auto-Negociación.
- Operación en modo de alto desempeño.
- Puertos de concentrador conmutador.
- La Auto-Negociación y el tipo e cable.

Una de las terminaciones del enlace no soporta la Auto-Negociación.

Si el protocolo de Auto-Negociación solo es soportado por un dispositivo final del enlace, el diseño del proceso de Auto-Negociación puede detectar en que (and respond correctly using)condiciones se encuentra un dispositivo y responde correctamente, utilizando un mecanismo llamado Detección Paralela (Parallel detection). Por ejemplo, si una interface Ethernet de velocidad-dual 10/100 con Auto-Negociación es conectado a un concentrador con modo 10Base-T que no soporta el protocolo de Auto-Negociación, la interface generará señales FLP, pero solo recibirá señales NLP del concentrador de 10Base-T. El protocolo de Auto-Negociación en la interface detectará la presencia de señales NLP (pulsos de enlace normal) y automaticamente habilitará la interface en modo 10Base-T.

De manera similar, cuando un concentrador que soporta el protocolo de Auto-Negociación con múltiples capacidades en sus puertos, es conectado a una interface que solo soporta 100Base-Tx y no es equipado con Auto-Negociación, el protocolo de Auto-Negociación configurará el puerto del concentrador para operar en modo 100Base-TX. La Detección paralela trabaja para 100Base-T tan bien como para dispositivos 100BaseTX y 100Base-T4 sin Auto-Negociación. La detección Paralela para 100Base-TX/T4 checa las señales de enlace que son recibidas por el Monitor de Enlace (Monitor Link), las características son especificadas para un modo dado. Si la Detección Paralela determina que un modo de monitor de enlace

es satisfactorio para el enlace de recepción, el concentrador habilita el enlace con ese modo.

Operación en modo de alto desempeño

En algún momento dado, cuando un concentrador de 10Base-T es reemplazado por un concentrador repetidor 100Base-T, entonces la interface de velocidad-dual recibirá señales FLP cuando el concentrador se encienda, de esta forma, el protocolo de Auto-Negociación resultará operando a 100Mbps en ambos dispositivos (en la interface y el puerto del concentrador). La conmutación de 10 Mbps a 100Mbps ocurrirá sin intervención manual.

La Auto-Negociación asegura que todos los dispositivos conectados a el concentrador, operen a un común denominador más alto. Desde que un repetidor concentrador es utilizado para crear un canal de señal compartida para todos los dispositivos conectados a los puertos del repetidor. Este canal de señal compartida deberá operar no mas rápido que el dispositivo más lento conectado a el repetidor concentrador.

Si un concentrador repetidor tiene uno de sus puertos conectado a un dispositivo que solo soporta 10Base-T, con el resto de los puertos conectados a dispositivos de 100Base-T, entonces el concentrador negociará una velocidad de 10 Mbps para todos los puertos, desde que es el común denominador mas alto para todos los puertos. Cuando cada dispositivo conectado al concentrador repetidor sea capaz de operar a 100 Mbps, entonces el concentrador negociará 100 Mbps para todos los puertos.

Si no existe una tecnología común manejable, detectada en ambas terminaciones de un enlace, entonces el protocolo de Auto-Negociación no realizará la conexión, y el puerto se configurará en condición o estado de apagado. Por ejemplo, si un dispositivo en modo 100Base-T4 es conectado a un puerto sobre un conmutador en modo 100Base-TX, como no puede llevar a cabo una transferencia de datos, no se establecerá conexión sobre ese enlace.

Puertos de Concentrador Conmutador

A diferencia a un concentrador repetidor, en el cuál todos los puertos deben operar a la misma velocidad, un concentrador conmutador provee puertos que operan de manera independiente. Un concentrador con puertos con conmutación puede soportar 10 Mbps de operación en un puerto, y 100Mbps de operación en otro puerto del mismo concentrador.

Dejando considerar el caso de un puerto de conmutación sobre el concentrador central es conectado a un segmento que conecta a un concentrador repetidor. ambos concentradores son equipados con Auto-Negociación. El concentrador repetidor en turno, conecta a varias computadoras. En este caso, los dos concentradores deberán utilizar el protocolo de Auto-Negociación sobre el enlace que los conecta y deberán negociar el común denominador mas alto de las capacidades que pueden ser soportados por los enlaces.

Si cualquier computadora conectada a el concentrador repetidor es equipada con un interface que solo soporta 10Base-T entonces el concentrador repetidor operará todos los puertos en modo 10Base-T, y también negociará un operación 10Base-T con el puerto conmutador del concentrador central. Mas tarde cuando todas las máquinas concentrador repetidor sean capaces de operar en modo 100Base-TX, por ejemplo, el repetidor concentrador repetidor negociará a enlace a 100Base-TX con el concentrador conmutador central.

La Auto-Negociación y el tipo e cable

El sistema de Auto-Negociación es diseñado para que un enlace no llegue a ser operacional hasta que se igualen las capacidades existentes en cada terminación del enlace. Sin embargo, el protocolo de Auto-Negociación no es capaz de examinar el cable utilizado en el enlace.

Mientras que la Auto-Negociación es una característica de comodidad que permite seleccionar un modo de alto desempeño de forma automática, aún se requiere que el tipo de cable utilizado sea el correcto y sea empleado para que el modo de más alto desempeño, pueda ser seleccionado sobre el enlace. Los dispositivos que soportan Auto-Negociación proveen además capacidades de control o manejo que permiten al administrador de red seleccionar un modo para cierto enlace dado. Al utilizar la administración o manejo de la interface se puede asegurar que un cierto enlace no lleve a cabo una negociación de un modo de operación que excede las capacidades del cable utilizado para este enlace.

El estándar IEEE 802.3 provee dos modelos de verificación de configuración de múltiples segmentos Ethernet banda base a 100Mbps.

El primer modelo es llamado Sistema de Transmisión Modelo 1, y consiste de un conjunto de configuraciones simplificadas que pueden ser aplicadas a sistemas Ethernet a 100 Mbps. El segundo modelo, Sistema de Transmisión Modelo 2 provee un conjunto de cálculos que se utilizan para verificar topologías mas complejas de Ethernet a 100Mbps.

6.1.4 100VG-AnyLAN

6.1.4.1 Introducción

En junio de 1995 la grupo IEEE certificó la especificación 100VG-AnyLAN[100] con el estándar 802.12. El protocolo 100VG-AnyLAN referido también como Protocolo de Prioridad por Demanda (DPP: Demand Priority Protocol), es un estándar de red de área local (LAN) que busca proveer una alta velocidad a redes LAN de medio compartido, tratando de mantener el sistema de cableado existente de las redes actuales [101].

Aunque 100VG-AnyLAN tiene varias similitudes con el protocolo 802.3 (Ethernet a 10 Mbps), este, emplea un acceso de datos y métodos de señalización que difieren drásticamente tanto del Ethernet convencional (Ethernet 10Mbps) así como también de Fast Ethernet (100BaseT, IEEE 802.3u). Esto es debido a que en lugar de utilizar el protocolo de acceso al medio conocido como CSMA/CD, el 100VG-AnyLAN utiliza un protocolo de acceso de datos conocido como Acceso de Prioridad por Demanda (DPA: Demand Priotity Access). Este método difiere del CSMA/CD principalmente en dos características:

- La transferencia de datos es controlada por el concentrador en lugar del adaptador de cada una de las estaciones.

- Las colisiones son eliminadas por que a cada nodo se le garantiza un turno de envío de datos

Teóricamente, este protocolo determinístico incrementa el ancho de banda disponible, al eliminar las colisiones y retransmisiones. Además de que tiene la habilidad de reconocer dos niveles de prioridad de petición de transmisión (prioridad normal y alta)

Las redes 100VG-AnyLAN no llevan a cabo una contención por el medio de transmisión, por lo tanto, no tienen colisiones, siendo capaz de esta manera de manejar mas cantidad de tráfico.

---

[100] El nombre 100VG-AnyLAN se refiere primeramente, a una tecnología de 100Mbps, VG es por el tipo de cable utilizado, es decir UTP de grado de voz (VG:Voice Grade) y por último el AnyLAN hace referencia a que puede manejar los formatos de frame de redes Ethernet y Token Ring (AnyLAN: Cualquier LAN).

[101] Necesitando solamente una pequeña reconfiguración de la red.

6.1.4.2 Topología

Las reglas de diseño aceptadas para las redes 100VG-AnyLAN son un conjunto de las soportadas por Ethernet y Token Ring. Esto significa que cualquier topología Ethernet o Token Ring compuesta con tipo de medio par trenzado y fibra óptica puede ser duplicada utilizando componentes 100VG-AnyLAN, sin cambiar de manera drástica la topología o diseño de la red.

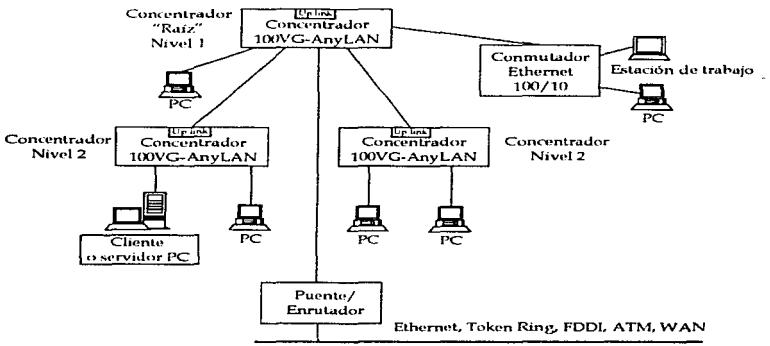


Figura 6.14 Topología de 100VG-AnyLAN

De hecho, la principal capacidad de 100VG-AnyLAN es su influencia de la topología física en estrella que utiliza. Tomando ventaja de esta topología, 100VG-AnyLAN utiliza la inteligencia de un concentrador para el mejor uso del manejo de la red, además del control de la red. El esquema de inteligencia central implementa una técnica de conmutación llamada "prioridad pot demanda" (demand priority). Este método lleva a cabo un arbitraje de las peticiones de los nodos conectados para tener acceso a la red, construyendo de esta manera un control de flujo de manera natural que permite a 100VG-AnyLAN minimizar la latencia de la red, maximizar el rendimiento y habilitar el soporte para las aplicaciones sensibles al tiempo, tales como multimedia.

6.1.4.3 Estructura de una red 100VG-AnyLAN

Como se mencionó anteriormente, la topología de una red 100VG-AnyLAN debe ser una estrella física (con apariencia de árbol), sin ciclos ni ramas. La pieza central de esta topología es un concentrador central o repetidor, referido comúnmente como concentrador raíz o concentrador de nivel 1, con un enlace conectado a cada uno de los nodos creando así la topología de estrella Algunos otros componentes de la estructura de 100VG-AnyLAN son conmutadores, puentes y enrutadores.

El concentrador es un controlador central inteligente que administra el acceso a la red (control de tráfico), a través de efectuar continuamente una rápida exploración de petición de cada uno de los puertos de red. Esta rápida exploración es comúnmente llamada round robin. Cada concentrador de menor nivel mantienen a su vez, sus propias tablas de direcciones por puerto, es decir, contiene las direcciones de las estaciones conectadas en cada uno de sus puertos.

El estándar 100VG-AnyLAN puede soportar formatos de frame de los estándares Ethernet 802.3 y Token Ring 802.5. Pero no simultáneamente, por tal motivo, todos los concentradores localizados en el mismo segmento de red deberán ser configurados para manejar el mismo formato de frame[102].

Características de los concentradores

Cada concentrador incluye un puerto **up-link** y "n" número de puertos **down-link** como se demuestra en la fig3 (hp). El puerto **up-link** funciona como un puerto nodo pero es reservado para conectar dicho concentrador hacia un concentrador de nivel superior. Los "n" puertos **down-link** son usados para conectar nodos (ya sea estaciones finales o concentradores de nivel inferior.

El número máximo de niveles de concentradores en cascada soportado en una red 100VG-AnyLAN es de 5.[103]

Sin embargo, cada nivel de concentradores, acorta la máxima distancia permisible entre un concentrador raíz y un nodo final, a un kilómetro.

Como una nota final, no se debe tener más de siete puentes o conmutadores entre dos nodos de la red. Esto es debido al protocolo de árbol expandido (802.1d), no una limitación del estándar 100VG-AnyLAN.

---

[102] Un puente puede ser usado para conectar segmentos de red 100VG-AnyLAN que utilizan diferentes tipos de formatos (Ethernet o Token Ring). Un enrutador puede ser usado para conectar una red 100VG-AnyLAN a redes FDDI, ATM o una conexión a WAN.

[103] Es aconsejable para tener un mejor desempeño de la red que se mantenga un máximo de 3 niveles de concentradores en cascada. Ya que este es el máximo número permitido en la especificación 802.3 Ethernet.

Modos de operación de los puertos

Cada puerto del concentrador puede ser configurado para operar en modo **normal** o modo **monitor** (o modo promiscuo). Los puertos configurados para operar en modo normal, se le envían solamente los paquetes que tienen la dirección del dispositivo que ellos conectan. De manera contraria, a los puertos configurados en modo **monitor** se les envían todos los paquetes que el concentrador recibe. De esta manera, el protocolo 100VG-AnyLAN brinda mas de seguridad que el estándar 802.3, debido a que el concentrador solamente transmite los paquetes hacia el puerto que conecta al dispositivo que tiene la dirección destino indicada en el paquete (modo normal). Esto reduce la oportunidad de un monitoreo de transmisiones no autorizado.

6.1.4.4 Capa física

Las reglas de cableado para 100VG-AnyLAN son muy similares a Ethernet 10BaseT, sin embargo existen algunas diferencias importantes.100VG-AnyLAN opera sobre los siguientes tipos de medios : 4 pares de cable UTP categoría 3, 4 y 5, sobre 2 pares de cable STP y sobre fibra óptica monomodo o multimodo. Con lo que se obtiene un diez por ciento de incremento en el ancho de banda sobre redes tipo Ethernet, y un seis por ciento de incremento sobre redes de alta velocidad de tipo Token Ring existentes, usando la misma infraestructura de cableado.

Cable par trenzado sin blindar:
Para transmitir datos sobre UTP, 100VG-AnyLAN utiliza una tecnología llamada **Quartet Coding**. Usando este aprovechamiento, la transmisión de los datos son dirigidos en paralelo a través de cada par de los cuatro pares de cable UTP. Sobre cada par, un eficiente esquema de codificación llamado **5B6B** NRZ es usado para transmitir dos bits de información por ciclo. De esta manera, el Quartet Coding permite la transmisión de 100 Mbps de datos cruzando cuatro pares de cable UTP mientras mantiene frecuencias de señal individual no mayor a 15Mhz. Este aprovechamiento permite a 100VG-AnyLAN operar sobre el sistema de cableado existente con cable categoría 3, 4 o 5 sin necesidad de cambiar los conectores, conectores cruzados y las distancias del cableado.

Cable par trenzado blindado STP:
Cuando la transmisión de datos sobre cable par trenzado sin blindar, 100VG-AnyLAN transmite los datos en dos flujos paralelos. Este aprovechamiento utiliza mayores frecuencias que las utilizadas sobre UTP.

Medio Fibra óptica:
Varias redes Ethernet y Token Ring toman ventaja de las características de distancia y aislamiento eléctrico que ofrece la fibra óptica, particularmente en los esquemas de backbone entre edificios, campus o en ambientes con un nivel alto de

interferencia o ruido u otros ambientes especiales. 100VG-AnyLAN soporta enlaces de fibra óptica multimodo de hasta 2 kilómetros entre los dispositivos.

El enlace que conecta al concentrador y a un nodo puede ser constituido por:

4 pares	UTP categoría 3,4 y 5
2 pares	UTP categoría 5
2 pares	STP tipo 1
2 ramas	fibra óptica

Tabla 6.8 Tipos de cables soportados por 100VG-AnyLAN

Dependiendo del tipo de cable y su categoría, existen varios límites de distancia La máxima longitud del cable desde el concentrador a cada uno de los nodos es de 100 metros de cable UTP categoría 3 y 4, 200 metros de cable UTP categoría 5 y STP, y de 2000metros para cable de fibra óptica[104]. Al poder tolerar una amplia variedad de cables, la especificación 803.12 permite preservar la infraestructura de cableado de la mayoría de las redes actuales. Sin embargo, se debe tener en cuenta, que 100VG-AnyLAN requiere cuatro pares de alambre para cable UTP categoría 3.

Aunque existen restricciones para la topología como son

- No debe haber existencia de ciclos
- El cable plano es prohibido (cable UTP de 25 pares) para los nodos en modo monitor (modo promiscuo)[105].
- se debe tener un número máximo de 1024 nodos sobre un segmento.

En la siguiente tabla se muestran las máximas distancias permitidas entre un concentrador raíz y un nodo final:

Tipo de medio	Número de concentradores entre el concentrador raíz y un nodo final	Número de niveles en red	Distancia máxima recomendada entre el concentrador raíz y un nodo final
Categoría 3	1	2	100 m
Categoría 3	2	3	75 m
Categoría 3	3	4	50 m
Categoría 3	4	5	25 m
Categoría 5	1	2	200 m
Categoría 5	2	3	150 m
Categoría 5	3	4	100 m
Categoría 5	4	5	50 m
Fibra óptica	1	2	4 km
Fibra óptica	2	3	3 km
Fibra óptica	3	4	2 km

Tabla 6.9 Distancias soportadas por 100VG-AnyLAN

[104] Tere Parnell; Guide to building high-speed networks; McGraw Hill 1996; p. 121.
[105] Esto es debido a que se puede tener un problema grave de señal crosstalk, retransmisiones y un desempeño ineficaz.

6.1.4.5 Funciones de la capa de control de acceso al medio (MAC)

Las funciones de la subcapa de control de acceso al medio de 100VG-AnyLAN incluye el protocolo de control de **Prioridad por Demanda** (Demand Priority), la **preparación de enlace** (link trainig) y la **preparación de frame** MAC.

6.1.4.5.1 Prioridad por demanda

El protocolo de Prioridad por Demanda es un método de control de Acceso al Medio (MAC) en el cuál los nodos emiten una petición (o demanda) hacia el concentrador al que se conectan para enviar un paquete sobre la red. Cada petición es etiquetada con una prioridad **normal** (nivel para paquetes de datos normales) o una petición de prioridad **alta** (nivel para paquetes que soportan aplicaciones de multimedia con tiempo crítico). A las peticiones con prioridad alta se les garantiza acceso a la red antes que las peticiones con prioridad normal, proveyendo un método que garantiza un servicio apropiado para aplicaciones sensibles al tiempo. El proceso de etiquetación[106] de prioridad normal y prioridad alta es complementada por un software de aplicación de niveles superiores y es pasado a la subcapa MAC como parte de información del paquete. En el método de Prioridad por Demanda, los paquetes de datos son dirigidos a su puerto destino únicamente[107]. A partir de que ningún otra estación sobre la red ve el paquete de datos, esta técnica de conmutación de paquetes, brinda un nivel de privacidad de enlace o seguridad que no es provista actualmente por otras tecnologías de red (como Ethernet, Token Ring o FDDI).

¿Como trabaja el esquema de acceso de Prioridad por Demanda? Como se ilustra en la figura anterior, el nivel 1 o concentrador raíz continuamente explora las peticiones de los nodos, usando un procedimiento de arbitraje llamado "round robin". La exploración "round robin" permite al concentrador determinar cuales nodos, si existe alguno, tienen petición para el envío de paquetes y con que modo de prioridad. En un ciclo de exploración "round robin" se permite a cada nodo enviar un paquete sobre la red. Los concentradores conectados como nodos (de nivel inferior), también completan un ciclo de exploración "round robin", y expiden una petición a el concentrador raíz o concentrador superior. Un solo puerto puede solamente enviar un paquete (por si otros nodos tienen peticiones pendientes). Un concentrador de nivel inferior con "n" nodos conectados será capaz de enviar "n" paquetes cuando este concentrador sea seleccionado durante el proceso "round-robin" (si es que no existen otras peticiones de alta prioridad pendientes).

---

[106] El nivel de prioridad puede ser establecido por estación o por una aplicación de software (aun que todavía no existen aplicaciones que tomen ventaja de esta característica que ofrece 100VG-AnyLAN).

[107] Excepto para casos de diagnóstico de la red, los administradores de red pueden activar puerto (s) del conmutador de forma individual para llevar a cabo un monitoreo de todo el tráfico que pasa a través del concentrador.

Cada concentrador mantiene una lista separada para peticiones de prioridad normal y otra para peticiones de prioridad alta. Las peticiones de prioridad normal son servidas en orden de puerto hasta que una petición de alta prioridad es recibida. Después de completar la transmisión del paquete actualmente en progreso, el concentrador servirá las peticiones de alta prioridad. Todas los paquetes de alta prioridad serán servidos antes que el concentrador regrese al servicio de la lista de prioridad normal. Para garantizar el acceso para peticiones de prioridad normal durante un exceso de tráfico de alta prioridad, el concentrador continuamente monitorea los tiempos de petición-a-envío de cada nodo. Si el retraso excede un máximo de tiempo establecido (generalmente de 300 ms), el concentrador automáticamente promueve la petición normal a una tabla de servicio de alta prioridad

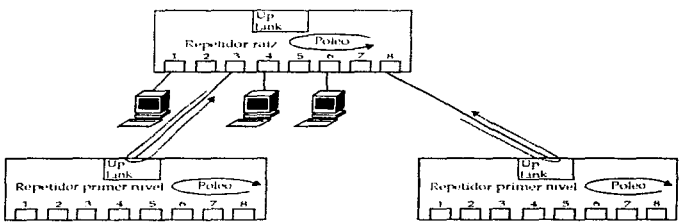


Figura 6.15 Un ejemplo de un ciclo de exploración round-robin. Primero considerando que todos los puertos tienen peticiones de prioridad normal pendientes y que la secuencia round-robin esta en el concentrador raíz o de nivel 1, puerto 1, en tiempo t=0. La orden de servicio de paquete deberá ser1-1 (nivel 1 - puerto 1), 2-1 (nivel 2 -puerto1),2-3, 2-n, 1-3 y 1-n. Si el nodo 1-1, 2-3 y 1-3 expiden peticiones de prioridad alta en t=0, el orden de servicio de paquete deberá ser 1-1, 2-3, 1-3, 2-1, 2-n y 1-n.

6.1.4.5.2 Preparación de enlace (Link Training)

La preparación de enlace, es un procedimiento de inicialización de enlace, que como su nombre lo indica, prepara al concentrador y la circuitería del nodo para la recepción y transmisión de datos, además de que verifica la operación de la conexión entre el concentrador y el nodo conectado.

Durante la preparación de enlace, el concentrador y el nodo, intercambian una serie de paquetes de verificación especial. Este procedimiento provee una verificación funcional del cable (para verificar que el cable esta correctamente

alambrado y que los datos puedan ser completamente transferidos hacia/desde el concentrador y el nodo.

La función de preparación de enlace también permite al concentrador aprender de manera automática acerca de los dispositivos nodo conectados en cada uno de los puertos. Los paquetes recibidos por un concentrador desde el nodo durante la función de preparación, contienen información como: el tipo de dispositivo (concentrador, puente, enrutador, etc), modo de operación (normal o monitor), y la dirección de la estación del dispositivo conectado a ese puerto. El procedimiento de preparación de enlace se inicia por el nodo, cuando el concentrador y el nodo son encendidos por primera vez, o cuando el nodo es por primera vez conectado al concentrador. El nodo o el concentrador pueden también invocar a un procedimiento de preparación de enlace cuando ciertas condiciones de error se han detectado.

6.1.4.5.3 Preparación de frame MAC

El procedimiento de preparación de frame MAC es realizado, después de recibir el paquete desde la subcapa de Control de Enlace Lógico (LLC). La subcapa MAC adiciona la dirección de origen y cualquier bit requerido para llenar el campo de datos. Una secuencia de verificación de frame (FCS: Frame Check Sequence) es entonces calculada y agregada al final del paquete. El FCS será utilizado por el concentrador receptor y el nodo para determinar si el paquete ha sido recibido sin errores.

6.1.4.5.4 Latencia determinística

Partiendo de la observación de que los dispositivos no transmiten sus paquetes hasta que ellos reciben un reconocimiento desde el concentrador, las redes de prioridad por demanda tienen un control de flujo que evita la colisión de paquetes y permite tener prioridades en el tráfico de la red.

Al evitar la colisión de paquetes, el método de prioridad por demanda, elimina el elevado consumo por las colisiones e incrementa substancialmente el rendimiento utilizable por la red, de esta manera, el método simplifica la operación de la red y mejora ciertas características de la red como por ejemplo, la latencia. El esquema de arbitraje "round robin" del método de prioridad por demanda es completamente determinístico, la latencia máxima o retraso de la red, observado por un paquete de información es de igual forma determinístico.

Comparado con las redes Token Ring, el esquema "round robin" utilizado por los concentradores de prioridad por demanda colapsa el proceso de Token-passing dentro de la operación del concentrador mismo. Eliminando así, retrasos de la rotación del token y reduciendo la latencia para las estaciones sobre una red

ociosa. En adición, el método de prioridad de demanda relaja el límite del número de estaciones en un solo anillo o subred. A diferencia de un ambiente Token Ring tradicional, la latencia experimentada por las estaciones individuales sobre una red de prioridad por demanda, no es afectada por el número de estaciones ociosas conectada, a dicha red.

6.1.4.5.5 Garantía de ancho de banda

La habilidad de garantizar un continuo e ininterrumpido ancho de banda es uno de los requerimientos críticos de red para un eficiente soporte de las aplicaciones sensibles al tiempo. Por medio de la priorización del tráfico de red y tomando ventaja del control de flujo que ofrece el método, 100VG-AnyLAN es capaz de garantizar el ancho de banda para aplicaciones específicas a pesar de otro tráfico existente en la red.

6.1.4.5.6 Esquema de transmisión de un paquete de datos

La transmisión de paquetes de datos consiste de una serie de secuencias donde el lado de envío, es decir, el nodo de transferencia hace una petición de envío y por otro lado es reconocida por el puerto del concentrador al que se conecta dicha estación transmisora. Como se puede observar, la secuencia de envío de transmisión de un paquete de datos es a través de una petición del nodo terminal y controlado por el concentrador. Esto se explica de manera mas detallada a continuación:

1. Si un nodo terminal, tiene un paquete de datos listo para enviarse, este transmite una petición de control con prioridad normal o una de prioridad alta hacia el concentrador local del nivel. De otra manera, si no tiene datos para transmitir, el nodo terminal transmite una señal de control inactiva (idle_Up control signal).
2. El concentrador explora todos los puertos locales para determinar cuales nodos terminales piden petición de enviar un paquete y con que etiqueta de prioridad es la petición.
3. El concentrador selecciona el próximo nodo terminal con petición de prioridad alta pendiente. Los puertos son seleccionados en base al orden de puertos. Si no hay peticiones de prioridad alta pendientes, entonces el próximo puerto de prioridad normal es seleccionado (selección en base al orden de puerto y el nivel). Esta selección causa al puerto seleccionado a recibir la señal de Concesión (the Grant signal). La transmisión del paquete empieza una vez que el nodo terminal detecta la señal de Concesión .
4. El repetidor entonces envía la señal de arribo a todos los otros nodos finales, alertando a estos la posibilidad de un paquete de llegada. El concentrador decodifica la dirección de destino del frame transmitido como éste esta siendo recibido.

5. Cuando un nodo terminal recibe la señal de control de "Arribo", este se prepara para recibir un paquete al parar la transmisión de petición y escucha el medio para el paquete de datos.
6. Una vez que el concentrador ha decodificado la dirección destino, el paquete es entregado a la dirección del nodo terminal o nodos terminales y a cualquier nodo en modo monitor (promiscuo). Aquellos nodos que no reciben el paquete de datos, reciben la señal "baja inactiva" (Idle_down signal) proveniente del concentrador.
7. Cuando el nodo o nodos terminales reciben el paquete de datos, ellos regresan a su estado anterior a la recepción del paquete de datos, enviando una señal de inactivo (Idle_Up) o haciendo una petición para enviar el paquete de datos.

Este proceso es utilizado por el Protocolo por Prioridad de Demanda permitiendo a cada uno de los nodos terminales la transmisión de paquetes de datos hacia otros nodos.

6.1.4.6 Compatibilidad de 100VG-AnyLAN

100VG-AnyLAN es igualmente eficaz para proveer una actualización tanto de Ethernet como de Token Ring a partir de que maneja frames tanto Ethernet y Token Ring. Ya que la operación del protocolos de prioridad por demanda es relativamente independiente del formato de frame especifico, la Prioridad por demanda puede transmitir frames Token Ring como frames Ethernet. Cuando 100V es utilizado para actualizar porciones de una red Ethernet 10BaseT existente, un puente de igualación de velocidad (puente traslacional) es todo lo necesario para conectar las subredes 10BaseT y 100VG-AnyLAN. El puente almacena los paquetes de alta velocidad como estos van entrando a la red de baja velocidad. A partir de que el mismo frame Ethernet puede ser usado sobre ambos tipos de subred, no es necesario un proceso de traducción.

De una forma similar, cuando porciones de red Token Ring existentes son actualizadas a 100VG-AnyLAN un puente de igualación de velocidades (puente translacional) es todo lo necesario para conectar las dos subredes. El mismo formato de frame Token Ring puede ser usado para las redes Token Ring y 100VG-AnyLAN. Las verdaderas capacidades de integración de 100VG-AnyLAN son mejor demostradas cuando 100VG-AnyLAN es usado para actualizar un ambiente mixto de redes Token Ring y Ethernet. Las subredes Token Ring y Ethernet pueden ser actualizadas a 100VG-AnyLAN individualmente compartiendo una infraestructura de hardware común. Estaciones individuales pueden continuar operando utilizando su formato de frame original, mientras transmiten información a 100 Mbps. Los servidores y otros recursos pueden ser configurados para aceptar y responder a paquetes tanto en formato Ethernet como Token Ring, o un enrutador puede ser usado para trasladar frames Ethernet y Token Ring para la comunicación entre dos subredes independientes.

6.1.5 Modo de Transferencia Asíncrono (ATM)

6.1.5.1 Introducción

ATM (Asynchronous Transfer Mode) es un protocolo de conmutación de celdas orientado a conexión en modo full dúplex; el cual designa un ancho de banda a cada estación por medio de multiplexión por división de tiempo asíncrono (multiplexión estadística)[108] para el control de flujo de información sobre la red. ATM actualmente opera en un rango de ancho de banda que va desde 25Mbps a 622Mbps. Siendo la primera tecnología capaz de soportar de manera simultánea diferentes tipos de tráfico (voz, video y datos).

Entre sus principales características se encuentran:

- Excelente escalabilidad.
- Designación de ancho de banda en base a demanda.
- Habilidad para manejar todo el rango de tráfico de red (voz, datos, imagen, video, graficación y multimedia).
- Adaptabilidad de ambientes LAN con WAN.
- Ausencia de mecanismos de recuperación a nivel de capa de enlace en nodos intermedios.
- Tecnología de conmutación basada en hardware.
- Uso de múltiples capas de aplicación (AALs).

Todas estas características hacen que ATM sea una tecnología ampliamente aceptada por las empresas de comunicación por lo cual es vista como la tecnología de transporte de la siguiente generación.

6.1.5.2 Historia de ATM

ATM tuvo sus inicios como parte del estándar de Red Digital de Servicios Integrados de Banda ancha (B-ISDN: Broadband-Integrated Services Digital Network) desarrollado en 1988 por el Comité Consultivo Internacional para Telefonía y Telegrafía (CCITT) actualmente ITU. B-ISDN es una actualización de ISDN de banda estrecha N-ISDN: Narrow-ISDN), la cual define redes públicas de telecomunicaciones digitales.

En 1991 se formó el Forum ATM, el cuál se hizo para expedir los convenios industriales sobre las interfaces ATM. Por lo tanto, el Forum ATM se dirige en el establecimiento de estándares para la industria de ATM.

[108] Para mayor información referirse al Anexo B.

La tecnología cell relay referida comúnmente como ATM es una evolución a partir de los conceptos de **Frame relay** y la **conmutación de circuitos multi tasa**[109] o **multi velocidad** (multirate circuit switching).

La conmutación de circuitos multi-tasa designa canales con tasa de transmisión fija, cell relay de igual manera permite la definición por medio de canales virtuales[110] pero a diferencia del anterior, los designa con una tasa de transferencia dinámica (con la característica de tener un tamaño pequeño de celda, cell relay permite tener además una tasa de transmisión constante (CBR)).

Del concepto frame relay, cell relay toma el esquema de no llevar a cabo ningún control de errores dentro de los nodos intermedios, permitiendo la recuperación de estos a través de los protocolos de las capas superiores en los sistemas finales. Es decir, el nivel ATM no realiza ninguna retransmisión y no existe ningún reconocimiento de que las celdas han sido recibidas. El servicio de entrega eficaz puede ser implementado como una función de las capas superiores por encima del nivel de la capa ATM (en los nodos finales), donde el reconocimiento de recepción de datos y la retransmisión de los datos erróneos puede ser realizada por los requerimientos de conexión de entrega eficaz (entonces un protocolo de nivel de transporte como el TCP (capa 4 del modelo OSI) es requerido encima de la capa ATM para que sea garantizada la entrega).

Cabe hacer notar que a diferencia del tamaño de frame variable en Frame relay, cell relay tiene como unidad de transmisión un tamaño fijo de celda de 53 bytes que reduce el retraso de transmisión y de almacenamiento[111]. Es debido a estas características que se pueden llegar a alcanzar altas velocidades de transmisión.

---

[109] Este es un alcance del enfoque del multiplexaje por división de tiempo (TDM) utilizado inicialmente en la conmutación de circuitos. En la conmutación de circuitos una estación debe operar a una tasa de datos fija la cual debe ser usada sin tomar en cuenta la aplicación. Una estación es conectada a la red por medio de un solo canal físico el cual acarrea múltiples canales, cada uno con una tasa de datos fija (canales B de 64 Kbps). El trafico sobre cada canal puede ser conmutado de manera independiente a través de la red hacia varios destinos. Este tipo es utilizado en ISDN. De esta manera el usuario tiene un número de tasas de datos a elegir, pero estas son fijas de manera que una tasa de bit variable (VBR) es difícil de llevar a cabo de forma eficiente.

[110] Un canal virtual esta compuesto por dos conceptos: la idea de enlace virtual y una conexión virtual.
Obviamente los sistemas de usuario final son separados por mas de un enlace virtual en la mayoría de los casos. En estas instancias, la concatenación de varios enlaces virtuales es referido como conexión virtual. Una conexión guía todas la celdas a lo largo de la misma ruta sobre la red ATM, y cada conexión consiste de una serie de enlaces, donde todos y cada uno tienen un número de identificación consistente. Este número identificador solo tiene significado local en el área del enlace que cruza entre dos nodos.

[111] Se debe especificar que no existe espacio entre celdas. Y en momentos cuando la red esta ociosa o sin tráfico, celdas sin asignación son transportadas.

6.1.5.3 Modelo de referencia de protocolos ATM

El protocolo de referencia ATM basado en estándares desarrollados por el ITU. El modelo de referencia de protocolos para ATM esta dividido en tres niveles :

Servicios y Aplicaciones
Capa de Adaptación ATM (AAL) (ATM Adaptation Layer)
Capa ATM
Capa Física

Tabla 6.10 Modelo de referencia de ATM

Los cuales son divididos a su vez en diferentes subniveles:

Capa/Subcapa	Función
Capa de adaptación ATM	Convergencia
Subcapa de segmentación y reensamblado	Segmentación y reensamblado
Capa ATM	Control de flujo genérico generación/extracción de encabezado Translación de VPI/VCI de la celda Multiplexión y demultiplexión de la celda
Capa Física Capa de Convergencia de transmisión	Cell-rate decoupling Generación/verificación de encabezado HEC Delineación de celda
Capa de medio físico	regulación del tiempo de bit medio físico

Tabla 6.11 Modelo ATM más a detalle

En la siguiente se muestra la relación del Modelo de Referencia OSI con el Modelo de Referencia ATM

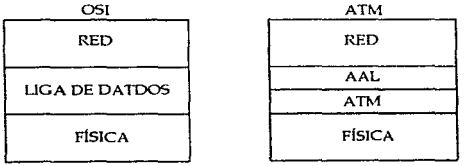


Figura 6. 16 Relación de ATM y OSI

6.1.5.3.1 Capa física

El aspecto más importante del nivel físico de ATM es que no define ningún tipo de medio específico. Soporta muchos tipos de medios, inclusive aquellos existentes y utilizados en otros sistemas de comunicaciones. Varias especificaciones de interoperabilidad aún se encuentran bajo desarrollo. Los expertos industriales, ratifican a la **red óptica sincrona** (SONET: Synchronous Optical Network)[112] como el medio de transporte físico para ATM tanto para aplicaciones WAN como LAN. Se recomienda también FDDI (100 Mbps), canal de fibra (155Mbps), OC3 SONET (155Mbps) y T3 (45 Mbps) como la interfaz física para ATM[113].

Capa física de	UNI privadas	
Formato del Frame	Tasa de bit	Medio
Flujo de celdas*	25.6Mbps	UTP
STS-1	51.84 Mbps	UTP3
FDDI	100Mbps 125Mbaud	MMF
STS-3c, SMT-1	155.52 Mbps	UTP5
STS-3c STM-1	155.52 Mbps	SMF, MMF, coaxial
Flujo de Celdas	155.52 Mbps	MMF,STP
STS-3c, SMT-1*	155.52 Mbps	UTP3
STS-12, SMT-4	622.08 Mbps	SMF,MMF

Capa física de	UNI publicas	
DS1	1.544 Mbps	Par trenzado
DS3	44.736 Mbps	Coaxial
STS-3c, SMT-1	155.52 Mbps	SMF
E1*	2.048 Mbps	Par trenzado, coaxial
E3*	34.368 Mbps	Coaxial
J2	6.312 Mbps	Coaxial
n x T1*	n x 1.544 Mbps	Par trenzado

*	Bajo desarrollo
DS	Servicio digital
MMF	Fibra Multi-Modo
SMF	Fibra Mono-Modo
STP	Par trenzado blindado
STM	Modo de Transporte Sincrono
STS	Sistema de transporte Sincrono
UTP	Par trenzado sin blindar

Tabla 6.12 Sumario de especificaciones físicas para ATM:

[112] SONET es un esquema de transporte de capa física soportado internacionalmente (referido en Europa como SHD) desarrollado a principio de los anos 80s. La interface WAN a 155Mbps para proveedores de redes publicas estará basado sobre SONET.
[113] Actualmente la mayoría de las compañías proveen de enlaces T3 a sus redes ATM.

6.1.5.3.2 La capa ATM

La capa ATM es la responsable de transportar la información a través de la red. ATM utiliza conexiones virtuales para la información de transporte. Las conexiones son consideradas virtuales por que aun que los usuarios pueden conectarse fin-a-fin, las conexiones solo se realizan cuando las celdas necesitan ser enviadas. Cabe mencionar que la conexión no es dedicada para uso exclusivo de una sola conversación (aun que a vista del usuario así parece).

6.1.5.3.3 Capa de adaptación ATM (AAL)

La Capa de Adaptación ATM (AAL: ATM Adaptation Layer) como su nombre lo indica es la responsable de desarrollar el mapeo necesario entre la capa ATM y los protocolos de capas superiores[114]. Es decir, esta capa es donde ATM encapsula el trafico de las aplicaciones superiores del usuario dentro del formato de ATM.

Actualmente AAL esta dividida en dos subcapas, **subcapa de convergencia** (CS: Convergence Sublayer) y la **subcapa de segmentación y reensamblado** (SAR: segmentation and reassembly).

Como se puede observar, la red ATM es independiente del tipo de tráfico que esta lleva, esto es debido a que ATM no conoce la estructura de la información que acarrea y no lleva a cabo ningún proceso de reconocimiento de esta; además de que la red ATM es de cierta forma independiente del tiempo, es decir, no existe relación entre la coordinación del tiempo de la aplicación origen y el tiempo de reloj de la red.

Todas estas características de independencia de la información que puede acarrear, deben ser construidas dentro del límite de la red ATM, por lo que caen dentro del área de la capa AAL las especificaciones de Calidad de Servicio (QoS: Quality of Service) ofrecidas por la red ATM. El AAL debe además resolver los problemas de flujo de datos para la aplicación y la variación del retraso de celda.

6.1.5.3.3.1 Subcapa de convergencia (CS)

La subcapa de convergencia permite la transmisión del trafico de voz, video y datos a través de la misma fabrica de conmutación. Este interpreta los datos de entrada desde una aplicación de capa superior y la prepara para ser procesada por la subcapa de segmentación y reensamblado[115].

---

[114] Esta tarea es usualmente llevada a cabo en los equipos terminales o en adaptadores terminales (TA: terminal adaptors)

[115] La subcapa CS es subdividida a su vez en CS Parte Común (CPCS: Common Part CS) y CS Servicio Específico (SSCS: Service Specific CS). El primero CPCS, convierte los datos de las capas superiores en una forma mas manejable para la segmentación dentro de pequeños componentes en

El CS desarrolla las tareas de proceso de variación del retraso de celdas, sincronización de fin-a-fin y manejo de celdas perdidas o mal insertadas. Obviamente, las operaciones y funciones desarrolladas por la subcapa de convergencia varían dependiendo del tipo y formato de los datos de entrada.

6.1.5.3.3.2 Subcapa de segmentación y reensamblado (SAR)

Como parte del nivel AAL, a la subcapa SAR le concierne la segmentación de la información de las capas superiores dentro un tamaño manejable para el campo de información de una celda ATM. Antes de que una aplicación transmita datos sobre la red ATM, la subcapa SAR realiza la **segmentación** de los datos del usuario dentro de las celdas, ocupando 48 bytes (payload) de una celda ATM. Una vez que las celdas ATM alcanzan su destino, la subcapa SAR destino **reensambla** las celdas en datos para los protocolos de las capas superiores y los transmite hacia el destino local apropiado.

6.1.5.3.4 Clases de Calidad de Servicio ATM (QoS: Quality of Service)

Como se mencionó anteriormente ATM puede transportar cualquier tipo de trafico, por lo que este debe ser identificado como tal y de esta manera preservar los parámetros de calidad de servicio (QoS) que requieren cada uno de ellos por separado. Esto surge a partir de que en ATM no existen canales físicos[116] distintivos para cada uno de los servicios por separado, debido a esto, todo tipo de tráfico puede tomar lugar dentro de una misma conexión lógica. Esta conexión lógica esta basada dentro de una estructura identificada por dos partes que son: el canal virtual (VCI) y la ruta virtual (VPI).

Para mantener los parámetros de garantía de comunicación y la calidad de servicio requerido por la información que es transportada por ATM, el Forum ATM ha definido cuatro clases de servicio en la capa de adaptación ATM (AAL) referidos como Calidad de Servicio (QoS).

Clase A : AAL 1
Clase B : AAL 2
Clase C y D: AAL 3
Clase C y D: AAL 5

---

la subcapa SAR. El segundo SSCS, puede no ser requerido, ya que solo mapea los datos desde la interface AAL hacia el CPCS, dependiendo de la aplicación en las capas superiores

[116] No existen canales para video o canales para voz, todos van a través de una conexión lógica.

6.1.5.3.4.1 Clase A

Clase A también referido como Tasa de Bit Constante (CBR: Constant Bit Rate), provee un canal virtual de transmisión con ancho de banda fijo. El CBR es utilizado primeramente por el trafico caracterizado por un flujo continuo de bits a una tasa regular, con un ancho de banda que es altamente sensible al retraso e intolerante a la perdida de celdas tal como video en tiempo real y tráfico de voz.

6.1.5.3.4.2 Clase B y C

Tasa de Bit Variable (VBR: Variable Bit Rate), el cuál tiene una naturaleza de ráfaga (bursty) y puede ser caracterizado por aplicaciones de voz o vídeo que utilizan compresión. La clase B es trafico VBR de Tiempo Real (RT-VBR), donde el retraso de fin-a-fin es critico, tal como video conferencia iteractiva. La Clase C es trafico en tiempo no-real (NRT-VBR), donde el retraso no es tan critico, tal como video playback, preparación de cintas y mensajes de video correo.

6.1.5.3.4.3 Clase D

El trafico tipo D es dividido en dos clases: Tasa de Bit Disponible (ABR: Available Bit Rate) y Tasa de Bit Sin Especificar (UBR: Inspecified Bit Rate). Estas clases son para trafico de red LAN con características de ráfaga y aquellos datos que pueden ser más tolerantes al retraso y perdida de celdas. UBR es un servicio de mejor esfuerzo que no especifica tasa de bit o parámetros de trafico y no tienen garantía de calidad de servicio. Originalmente proyectado como una manera para hacer uso del exceso de ancho de banda existente, UBR puede ser sometido a tener celdas perdidas y desecho de todos los paquetes. ABR de la misma manera es un servicio de mejor esfuerzo, pero difiere de UBR en que es un servicio de administración, basado en la tasa de celdas mínimo (MCR: minimum cell rate) y con una perdida de celdas. Por último, cabe señalar que ninguna garantía de variación de retraso esta actualmente prevista tanto para los servicios UBR como para ABR.

Clase	A	B	C	D
Sincronización de tiempo entre el origen y el destino	requerido	requerido	no requerido	no requerido
tasa de bit	Constante	variable	variable	variable
modo de conexión	orientado a conexión	orientado a conexión	orientado a conexión	sin conexión
Ejemplo de servicios	Voz y video a una tasa constante de bits	Audio y video comprimido	Transferencia de datos orientada a conexión	transferencia de datos sin conexión.

Tabla 6.13 Clases de servicio en la capa de adaptación ATM (AAL)

Clase de Servicio	Ancho de Banda garantizado	Variación de retraso garantizado	Rendimiento garantizado	Regeneración garantizada
CBR	Sí	Sí	Sí	No
VBR	Sí	Sí	Sí	No
UBR	No	No	No	No
ABR	Sí	No	Sí	Sí

Tabla 6.14 Clases de Servicios

En una red ATM, cada momento que una aplicación necesite establecer una conexión entre dos usuarios, este deberá negociar un contrato de tráfico que especifica la clase de servicio de la conexión. Las clases de servicio ATM cubren un rango de parámetros de servicio y garantías de QoS. Las garantías de servicio pueden definir niveles mínimos de ancho de banda disponible, límites superiores del retraso de las celdas y celdas perdidas[117]. Por esta razón es que ATM entrega importantes ventajas sobre las tecnologías de redes de área local (LAN) y de área amplia (WAN) existentes. Con la promesa de un ancho de banda escalable y los parámetros de calidad de servicio (QoS: Quality of Service) requeridos de forma garantizada, lo cuál, es lo que facilita el desarrollo de nuevas clases de aplicaciones tales como multimedia y videoconferencias.

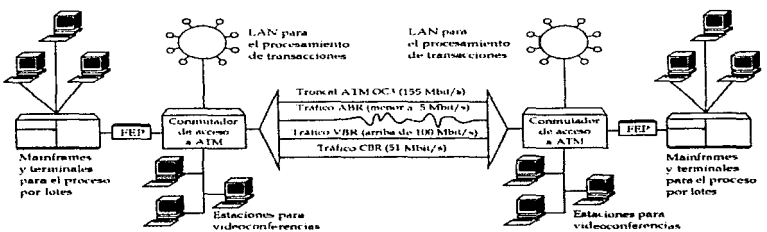


Figura 6.17 Uso del ancho de banda que garantiza la calidad del servicio en ATM.

6.1.5.3.5 Topología de una red ATM

ATM es formada por una topología de malla de conmutadores. Esto lleva a la conclusión, de que cualquier punto en la red puede ser alcanzado desde cualquier otro punto vía múltiples rutas que envuelven conexiones independientes entre conmutadores. Además, como limitación tiene únicamente las características de atenuación del medio utilizado.

[117] Para mayor información: Stephen Saunders; High Speed LANs; McGraw Hill 1996; pp 123-134.

Como se explico anteriormente, la independencia del tipo de medio es un principio de ATM. Varias capas físicas son especificadas, desde 25Mbps, incluyendo otras como 100Mbps a 155Mbps hasta llegar a 622Mbps. ATM a 155Mbps incluye soporte para categoría 3, 4, 5 UTP, tipo-1 STP, cable fibra óptica (fibra multimodo y monomodo para redes LAN).

Los conmutadores de la malla son generalmente dispositivos multipuertos que realizan la conmutación de las celdas. Este conjunto de conmutadores ATM son interconectados por enlaces ATM punto-a-punto o interfaces. Los conmutadores ATM soportan dos tipos de interfaces: Interface de Red-Usuario (UNI: User Network Interface) y Interface Red-a-Red (NNI: Network Node Interface).

La interface UNI (User Network Interface) es la que interconecta los sistemas finales ATM (hosts, enrutadores, etc.) a un conmutador ATM[118], mientras que la interface NNI puede ser definida de forma imprecisa como una interface que conecta a dos conmutadores ATM. Por otro lado, de manera mas precisa, una NNI es cualquier enlace físico o lógico que cruza entre dos conmutadores ATM intercambiando el protocolo NNI.

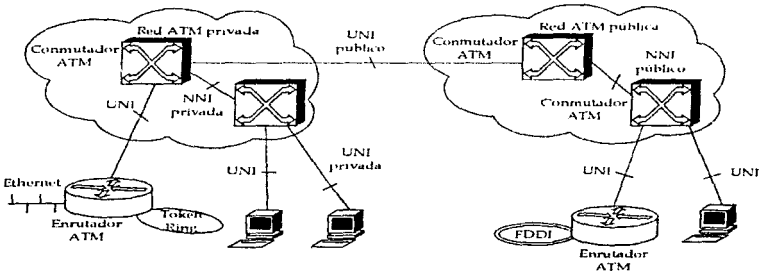


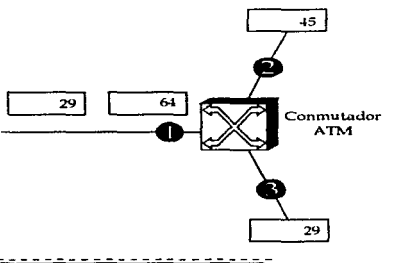
Figura 6.18 Operaciones de un conmutador ATM

[118] ATM no tiene una analogía de enlace físico redundante provisto por FDDI, con su conexión de estaciones de manera dual (dual attached stations). De manera que cualquier sistema final que requiera una conexión redundante a una red ATM, deberá soportar dos UNIS separadas (donde una tendrá que trabajar en modo de espera (standby)).

6.1.5.3.6 Celdas pequeñas, Rutas virtuales, Circuitos Virtuales

Las redes ATM son por naturaleza orientadas a conexión. Esto significa que un circuito virtual se necesita establecer previo a cualquier transferencia de datos. Los circuitos virtuales de ATM son compuestos de dos tipos: rutas virtuales (virtual paths) identificados por el identificador de ruta virtual (VPI) y canales virtuales (VC, identificado por la combinación de un VPI y un identificador de canal virtual (VCI). Por lo tanto, una ruta virtual es un grupo (manojo de) de canales virtuales.

Entrada Puerto	VPI/VCI	Salida Puerto	VPI/VCI
1	29	2	45
2	45	1	29
1	64	3	29
3	29	1	64



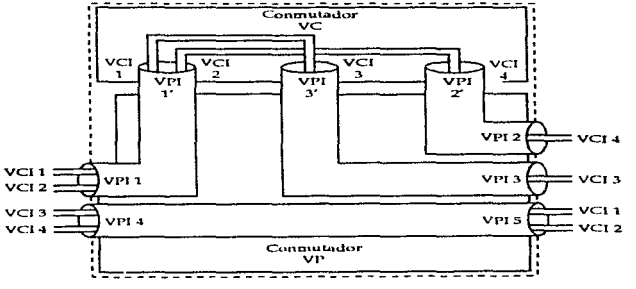


Figura 6.19 Circuito virtual y conmutación de rutas virtuales

Mientras que el multiplexaje estadístico es generalmente bueno para aplicaciones de datos (que tienen requerimientos relajados para la entrega estable de información) este no es completamente usado para la transferencia de voz y vídeo. El problema con el multiplexaje estadístico es que los frames de datos son de tamaño variable[119].Por lo que se tiene una variación en el tiempo de arribo y que lo hace poco utilizable para trafico de voz y de vídeo. ATM resuelve este problema al dividir la información no importando su tipo dentro de pequeñas celdas o bloques de longitud fija[120]. Una celda ATM es de 53 bytes de longitud (5 bytes de encabezado de información y 48 bytes de datos referidos como payload). En una red ATM, la información debe ser introducida en formato de celda, o ser convertida a celdas por medio de una función referida como **adaptación.** Como se mencionó anteriormente, una red ATM consiste de una serie de conmutadores ATM conectados por troncales ATM. Los conmutadores en el nivel que se conectan los usuarios, proveen la función de adaptación para crear celdas. Otros conmutadores en el corazón de la red mueven las celdas por todos lados, compartiendo las troncales y conduciéndolas hacia su destino. En el conmutador destino, se realiza la función de adaptación inversa, recreando el flujo original de datos a partir de las celdas, y pasa este flujo hacia el dispositivo destino.

El formato de datos en celdas le permite a las redes ATM combinar múltiples flujos de información eficientemente, además de permitir también, la prioritización de tráfico critico (voz y vídeo). Esto se realiza de la siguiente manera: Dos fuentes de información entran a la red ATM, una fuente es de tráfico crítico (voz o vídeo) y otra es menos crítica (datos). Ambas fuentes son primero divididas en celdas. Aun si la red empieza a transportar el flujo de datos (menos críticos), este puede intercalar las celdas de tráfico mas crítico en cualquier limite de celda, dejando el resto del tráfico de datos esperar un poco mas para su transmisión. Esto mantiene al mínimo el retraso experimentado por el trafico más critico, dejando a ATM acarrear información de todos los tipos.

Aún con el intercalado de celdas y la prioritización de celdas, pueden existir situaciones en donde las redes ATM desarrollen congestionamiento. Para mantener al mínimo el retraso generado en este tipo de situaciones, ATM es capaz de desechar celdas para disminuir el congestionamiento. La estrategia exacta seleccionada para el desecho de celdas es algo que depende del equipo del vendedor, pero generalmente es basado en los parámetros de prioridad en la calidad de servicio ofrecido, y por el tipo de tráfico.

---

[119] Si alguna información importante y pequeña se encuentra detrás de una información sin importancia y grande, la información importante será retrasada en su paso a través de la red mientras la información larga y menos importante es transferida.

[120] La flexibilidad inherente en la estructura de la celda ATM, le permite igualar las velocidades entre la de transmisión y la velocidad en que son generadas por la fuente.

6.1.5.3.7 Los conmutadores[121]

El dispositivo de conmutación es el componente mas importante en las redes ATM. Puede utilizarse como un concentrador o de otra manera puede servir como un dispositivo de comunicación de área extensa, que transmite celdas ATM entre redes LAN remotas.

La operación básica de un conmutador ATM es simple: una celda proveniente de un enlace sobre un valor conocido de VCI/VPI; busca el valor de conexión en una tabla de translación local para determinar el puerto de conexión de salida y el nuevo valor VPI/VCI de la conexión sobre ese enlace; y entonces retransmite la celda sobre ese enlace con los identificadores de conexión apropiados.

La operación de transmisión de un conmutador es simple, ya que las tablas de translación son previamente establecidas por medio mecanismos externos antes de que se lleve a cabo alguna transmisión. La manera en la cual las tablas son establecidas determina los dos tipos fundamentales de conexión ATM: Conexión virtual permanente (PVC) y Conexión Virtual Conmutada (SVC).

6.1.5.4 Protocolos ATM para redes LAN

6.1.5.4.1 Protocolo de Interface de Red para Usuario (UNI)

El UNI define la interoperabilidad entre el equipo del usuario y el puerto de conmutación ATM. El protocolo UNI de ATM provee múltiples clases de servicios y reservación de ancho de banda establecido durante la llamada de una conexión virtual conmutada. Una UNI publica define la interface entre una red ATM de servicio público y el usuario, usualmente soporta una interface SONET o DS3. Una UNI privada, de otra manera, define una interface entre un usuario final y un conmutador ATM privado, y ambos deben tener una interfaz de cable de cobre o de fibra óptica.

6.1.5.4.2 Interconectividad ATM con protocolos existentes

Un suceso principal por definir en ATM, será la habilidad de éste para permitir la interoperabilidad entre la base de tecnologías ya instaladas actualmente de redes WAN y redes LAN (Ethernet, Token Ring, FDDI), así como la interacción con la pila de protocolos de las capas superiores.

[121] Para mayor información referirse al Anexo 6.B.

Siendo ATM un protocolo punto-a-punto orientado a conexión, no es fácil llevar a cabo dicha integración a la forma de trabajar de las redes LAN heredadas[122], ya que los protocolos de transporte actuales tales como TCP/IP, IPX y NetBEUI son orientados a la no conexión por tal motivo no comprenden el sistema de direccionamiento de ATM (VPI y VCI), además de que las aplicaciones actuales aún no tienen forma de notificar los parámetros de calidad de servicio que requieren o del ancho de banda necesario para ser enviados.

Existen diferentes formas posibles en las que ATM puede ser realizado dentro de una arquitectura de interconexión de redes para las aplicaciones actuales y futuras, estas formas pueden clasificarse en dos:

La primera forma, es la de emular la operación de los protocolos de red LAN actuales a través de utilizar equipo ATM. De esta forma, las aplicaciones actuales deberán continuar ejecutándose como antes, y ATM deberá adaptarse de manera que tendrá que aumentar sus protocolos actuales con otros nuevos diseñados específicamente para aplicaciones multimedia.

La segunda forma, es conectar los servicios ATM directamente a las Interfaces de Programas de Aplicación (API: application program interface) utilizados por las aplicaciones actuales, Al utilizar nuevas Interfaces de Programas de Aplicación para las nuevas aplicaciones, y emular el conjunto de protocolos actuales para las aplicaciones existentes, se evita el uso completamente de los protocolos de capas inferiores de las redes heredadas (protocolos de la capa dos del modelo OSI como Ethernet o Token Ring). De esta manera, están siendo desarrollados nuevos APIs capaces de soportar clases de aplicaciones aun no ampliamente utilizadas, tales como multimedia y videoconferencia.

En este trabajo, solo se explicará a detalle la primer forma en que ATM se integra a las tecnologías y protocolos heredados, es decir, los métodos de emulación de redes LAN.

6.1.5.4.2.1 Emulación de redes LAN (ELAN)

Dos estándares han emergido como la base para la emulación de red LAN sobre ATM, uno es responsabilidad del Forum ATM "Emulación de LAN ATM" (LANE: LAN emulation) y el segundo por el IETF (Internet Engineering Task Force) con el método "IP clásico sobre ATM" (classical IP over ATM) referido con el RFC 1577[123].

---

[122] Dado que la mayoría de las redes heredadas actuales son multipunto y sin conexión.

[123] Esto es conocido como operación en modo nativo, en este tipo de operación se utilizan mecanismos de resolución de direcciones para mapear las direcciones de la capa de red directamente a direcciones ATM y los paquetes de la capa de red son entonces conducidos a través de la red ATM.

Los dos estándares, LANE y el 1577 asumen que los usuarios de ATM tendrán adaptadores de sistema para sus computadoras de escritorio soportando una interface UNI[124] ATM (algunas veces llamada UNI privada). Los estándares de la UNI privada definidos hasta este momento incluyen velocidades de 25Mbps basados en medio de cobre, 100Mbps basado en medio fibra óptica, y 155 Mbps basados en medios de cobre y fibra óptica.

Ambos estándares asumen que los usuarios serán conectados hacia un conmutador ATM. Los conmutadores normalmente soportarán ambos puertos ATM, conexiones hacia estaciones o sistemas de servidor y troncales ATM[125] (usados para interconectar conmutadores ATM, o para conmutadores de backbone extenso). Algunos conmutadores ATM además soportarán estaciones no-ATM. Esto facilita la transición partiendo de redes LAN Ethernet y Token Ring hacia ATM.

6.1.5.4.2.2 Método de operación general de los sistemas de emulación de red (ELAN)

La emulación de red LAN ATM en cualquiera de sus formas ya sea LANE o RFC 1577, trabaja de manera similar ya que consisten principalmente en dos funciones de software. La primera, es una función **cliente** que se ejecuta sobre cada una de los sistemas conectados a la red LAN ATM emulada, y una segunda función referida como **servidor** que reside con cada grupo de estaciones clientes. Por lo tanto, una colección de clientes y el dispositivo servidor asociado es lo que se llama una **red LAN emulada** (ELAN: emulation LAN)[126].

Como se explico en el capítulo 2, los protocolos de red actúan en una capa en particular del modelo de referencia OSI, de esta manera, cualquier estándar que interactúe entre las redes LAN existentes y ATM deberá tener como objetivo una capa o nivel de protocolo específico. En este punto es donde divergen los dos estándares, LANE y el IP Clásico sobre ATM (RFC 1577). La Emulación LAN (LANE), el estándar del Forum ATM, tiene como objetivo la emulación de red LAN en el nivel de la capa dos del modelo de referencia OSI el nivel MAC/LLC (Control de Acceso al Medio / Control de enlace lógico). A partir de que este es un protocolo de nivel inferior para las redes LAN, el estándar LANE puede ser usado como base para cualquier protocolo de capa superior, incluyendo TCP/IP, Netware SPX/IPX, NetBEUI. Mientras que, el IP Clásico sobre ATM (RFC 1577) de otra manera tiene como objetivo el nivel tres del modelo de referencia OSI (capa de

[124] Interface de Red de usuario (UNI: User Network Interface).
[125] El Forum ATM (LANE) hace referencia a la interface entre conmutadores como Interface Red-a-Red Privada (P-NNI: private Network-Network Interface), la cual esta basada sobre la UNI pero además incluye mensajes especiales para enrutamiento y manejo de estado de ruta.
[126] ELAN es un termino que hace referencia a cualquiera de las dos metodologías de emulación, es decir el LANE y el 1577.

red) y es solamente especifico para el conjunto de protocolos TCP/IP (Internet). Aún cuando los dos métodos se enfocan en diferentes niveles del modelo de referencia OSI, cabe decir que ambas formas de emulación de red LAN ATM (ELAN) trabajan de manera similar. Esto es, cuando una red LAN ATM se establece, los sistemas cliente intentan contactar a un dispositivo con función de servidor para que se registre la información de dirección del cliente (dirección ATM del cliente y la dirección por la que son conocidos ya sea que se maneje en la capa 2 (dirección MAC) o en la capa 3 (por ejemplo dirección IP) según sea el caso). El dispositivo con función del servidor, de esta manera construye un directorio a partir de esa información, la cuál será utilizada posteriormente. Cuando se ha realizado completamente el registro de todos los sistemas cliente, estos y los servidores se ponen en un estado de espera del trafico de las aplicaciones del usuario.

El software del usuario que opera bajo el ambiente de una emulación de red LAN es ejecutado de la misma manera que en un ambiente de red local actual nativo, es decir, como si estuviese en una red local normal sin emulación. Esto es por que solamente los controladores de comunicación de las capas de bajo nivel son específicos para ATM. Por lo tanto, cuando una aplicación de usuario genera un mensaje, este fluye de pila de comunicaciones (modelo de referencia OSI) hacia el software ATM. Llegando en la forma de un datagrama (o mensaje sin conexión) al nivel dos o tres como sea apropiado para el tipo de emulación de LAN que se lleva a cabo. Y es en este momento que el software ATM debe emular la red LAN.

Una vez que el software ATM tiene información que transmitir, verifica la existencia de algún circuito virtual activo que realice la conexión hasta el dispositivo final deseado. Si se encuentra activo un circuito virtual desde el origen del datagrama hasta su destino, el datagrama debe simplemente ser conducido dentro del circuito virtual y este deberá llegar a su destino de manera correcta. En realidad, cada cliente ATM mantiene una tabla de direcciones (ya sea de capa dos o de capa tres) y los identificadores de circuitos virtuales específicos hacia el destino (VPI/VCI). Si una dirección destino es encontrada en la tabla, entonces el datagrama es enviado sobre la ruta virtual asociada. Un problema ocurre cuando no puede ser encontrada la dirección destino en esta tabla, en este momento es cuando la función servidor de la emulación de LAN se activa, para que de esta manera se pueda resolver la dirección ATM correspondiente al cliente destino. Esto se realiza de la siguiente manera: si no se encuentra un circuito virtual activo, es decir, que el sistema cliente no tiene una conexión de circuito virtual ATM hasta el destino, por lo que el siguiente paso es establecer uno (hay que notar que el datagrama es un mensaje de red LAN heredada, por tal motivo no tiene la información de la dirección ATM destino). Para poder obtener la dirección ATM correspondiente a la dirección de capa superior, el cliente envía un mensaje al dispositivo con función de servidor, identificando su destino proyectado ya sea en direcciones de la capa dos o tres y pidiendo la dirección ATM correspondiente. Esta dirección es entonces regresada por el servidor al cliente, una vez conocida la

dirección ATM del destino, el cliente establece un Circuito Virtual Conmutado ATM (SVC) hacia el destino, sobre el cual los datagramas fluirán encapsulados en celdas ATM.

La función servidor también deberá proveer una función de broadcast a través de la cual los clientes envían datagramas de broadcast o multicast. Esta función envía los datagramas recibidos a cada uno de los clientes registrados.

6.1.5.4.2.2.1 Dispositivos no-ATM (dispositivos heredados)

Los dispositivos de redes LAN actuales referidos como dispositivos de red LAN heredados (legacy LANs) se deben también comunicar con estaciones ATM, esto se lleva a cabo ejecutando una forma de emulación LAN; para lo cuál, los conmutadores proveen una función llamada **proxy client** (apoderado del cliente) sobre el nombre de aquellas estaciones no-ATM. En este caso, una estación ATM que llama a otra no-ATM debe obtener la dirección ATM del proxy client (por medio de una petición al dispositivo con función de servidor), y establecer así, un circuito virtual conmutado (SVC) hacia esa dirección. El proxy client debe entonces puentear o enrutar el datagrama según sea el caso hacia la estación correcta. En la práctica, este será actualmente el uso mas relevante de una red emulada partiendo del punto de que la gran mayoría de las conexiones hacia el área de escritorio de los usuarios será Ethernet, Token Ring, FDDI y Fast Ethernet durante los años venideros.

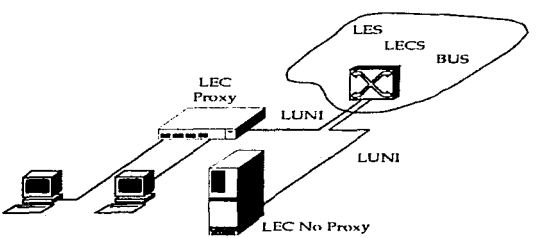


Figura 6.20 Dispositivos proxy y no proxy

6.1.5.4.2.2.2 Desventajas

El IP clásico sobre ATM da lugar a políticas de limitación sobre el tamaño de un dominio de emulación de LAN debiendo ser no mayor de una subred IP. Por otro lado, el estándar del Forum ATM LANE no tiene políticas de limitación; sin embargo el tamaño práctico del dominio es establecido por el número de mensajes multibroadcast generados, lo cual carga tanto al dispositivo con función servidor como al cliente y debido a que el método LANE se desenvuelve en la capa dos del modelo OSI, entonces de cierto modo se puede decir que es afectado por las mismas limitaciones que las redes puenteadas, es decir, el trafico de broadcast y multibroadcast es su principal factor limitante.

6.1.5.4.2.2.3 Conmutadores multivendedor

Las conexiones nativas ATM requieren rutas de conexión ATM desde el origen hasta el destino. Por lo que no se presentan problemas si las dos partes se encuentran sobre el mismo conmutador. De manera similar, no existen problemas si las dos partes se encuentran sobre la misma localidad y sobre conmutadores del mismo vendedor. Pero de manera contraria, conexiones multi-vendedor probablemente requerirán el uso de la interface P-NNI (interface red-a-red privada) para formar un puente entre dos o mas diferentes conmutadores ATM, y si la conexión ATM debe hacer un cruce a través de una red de área amplia. Algunos proveedores de servicio de acarreo ATM pueden ser también requeridos.

En suma, si un usuario desea llevar ATM hasta su área de escritorio en los próximos dos años, deberá estar seguro de que los conmutadores propuestos por los vendedores tienen una posición de escritorio de ATM y además, que soporten ATM desde 155Mbps a 622Mbps en una conexión conmutador-a-conmutador. Debiendo de otra manera, asegurar que los puertos ATM de los productos incluyen Emulación LAN ATM, además de que el vendedor del conmutador sea miembro del comité de desarrollo de protocolos como el RFC 1577 y MPOA. Finalmente, que la interface troncal entre los conmutadores debe tener soporte para el estándar P-NNI.

6.1.5.4.2.3 Emulación LAN ATM (LANE)

El objetivo principal del servicio de Emulación LAN (LANE: LAN Emulation) es la de habilitar el acceso de las aplicaciones actuales, sobre una red ATM por medio de pilas de protocolos como IP, NetBIOS, IPX, etc., como si estuviesen corriendo sobre una red LAN tradicional. LANE trabaja al nivel de la subcapa de Control de Acceso al Medio (MAC) y habilita al trafico de las redes heredadas Ethernet, Token Ring o FDDI correr sobre ATM sin tener que modificar las aplicaciones, sistemas operativos de red o adaptadores de escritorio. Es decir, como su nombre lo indica, emula una red de área local tradicional (heredada) sobre una red ATM.

De manera específica, el protocolo LANE define mecanismos para emular de manera lógica un segmento de red local Ethernet (802.3) o Token Ring[127]. De esta manera, el protocolo LANE define un servicio de interface para protocolos de capas superiores, con esto las estaciones finales de sistemas heredados puedan utilizar LANE para conectarse a otros sistemas heredados, como también a servidores conectados directamente a ATM, enrutadores, concentradores y otros dispositivos de red.

LANE versión 1.0 define una arquitectura cliente servidor que especifica, como el cliente de Emulación LAN (LEC) interactúa con el servidor de Emulación LAN a través de la Interface de usuario-a-red (UNI: User-to-Network Interface). Sin embargo, este no especifica los detalles de diferentes funciones dentro de servicio de Emulación LAN.

6.1.5.4.2.3.1 Funcionamiento de Emulación LAN

La función básica del protocolo LANE es la de resolver las direcciones MAC en direcciones ATM. Para esto, la Emulación de LAN es conformada por una colección de servicios que trasladan la información entre los protocolos de las capas superiores de servicios de protocolos orientados a la no conexión y los de capas inferiores (protocolos orientados a conexión de ATM).

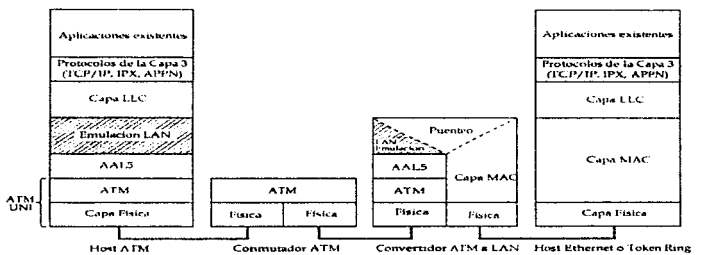


Figura 6.21 Estructura lógica de la Emulación LAN

[127] El protocolo actual de LANE no define una encapsulación individual para FDDI, por lo que un paquete FDDI debe ser mapeado dentro de una emulación de red LAN Ethernet o Token Ring a través de utilizar técnicas existentes de puentreo translacional. Las dos nuevas tecnologías predominantes en redes LAN, Fast ethernet (100Base T) y el 100VG-AnyLAN (IEEE 802.12) pueden ser mapeadas sin cambio dentro de los formatos y procedimientos LANE Ethernet y Token Ring, a partir de que ellos ocupan el mismo formato de datos.

Como se explicó anteriormente, la capa de adaptación ATM (AAL) se encuentra encima de la capa ATM. El AAL lleva a cabo el formateo de los datos dentro del campo de 48 bits referido como payload en un proceso conocido como segmentación. Como ATM puede llevar múltiples tipos de tráfico, varios protocolos de adaptación son requeridos, los cuales operan de manera simultánea (desde el AAL1 hasta el AAL5). El AAL5 es el protocolo de adaptación sobre el cuál trabaja la Emulación LAN.

La Emulación LAN se sitúa por encima del AAL5 en la jerarquía de protocolos. En la conversión ATM-a-LAN al nivel de red, la Emulación LAN resuelve los problemas de datos para todos los protocolos, ya sean enrutables o no enrutables, de otro modo, al resolver las direcciones ATM y LAN al nivel de la subcapa MAC. La Emulación LAN es completamente independiente de los protocolos de capas superiores, servicios y aplicaciones.

6.1.5.4.2.3.2 Componentes de LANE

La especificación LANE esta basado en una implantación de modelo cliente-servidor; una red LAN emulada se lleva a cabo en un servicio de Emulación LAN y múltiples LECs (clientes) comunicándose a través de un enlace llamado LUNI.

Una red LAN emulada es constituida por las siguientes entidades:

Cliente LANE

- Cliente de Emulación de LAN (LEC: LAN Emulation Client)
  Un LEC es una combinación de agentes de software y hardware implantados dentro de dispositivos de red o sistemas finales, para el manejo de envío de datos, resolución de direcciones y otras funciones de control. Un LEC también provee una interface de servicio de LAN estándar para cualquier protocolo de la capa superior del sistema final. Cada componente de red puede soportar múltiples instancias de un LEC[128], permitiendo de esta manera que múltiples redes LAN emuladas puedan existir simultáneamente sobre la misma red física.

  Cada LEC es identificado por una dirección ATM única, la cuál es asociada con una o más direcciones MAC, las cuales pueden ser alcanzadas a través de la dirección ATM. En el caso de una NIC ATM, por ejemplo, el LEC puede estar asociado con una sola dirección MAC, mientras en el caso de un conmutador de red LAN, el LEC debe estar asociado con todas las direcciones MAC que se pueden alcanzar a través de los puertos de ese conmutador de LAN, los cuales son asignados para una ELAN particular. Se debe notar que en el ultimo caso, este conjunto de direcciones puede cambiar (tanto direcciones de nodos MAC

[128] Un sistema final que se encuentre conectado a múltiples ELANs (quizá sobre la misma UNI) deberá tener un LEC por ELAN.

pueden darse de alta o de baja, y como rutas particulares son reconfiguradas ya sea por cambios lógicos o físicos en la topología de red LAN (por ejemplo, al utilizar el protocolo de árbol expandido o spanning tree).

Por último, mientras las especificaciones actuales de LANE definen dos tipos de red LAN emuladas, una para Ethernet y otra para Token Ring, esta no permite la conectividad directa entre un LEC que implanta una ELAN Ethernet y otra que implanta una ELAN Token Ring. Es decir, LANE no intenta resolver el problema de traslación (puenteo) entre tecnologías, el cual es intratable entre la interconexión Ethernet-a-Token Ring. Los dos tipos de ELANs solo pueden ser interconectados a través de un enrutador ATM que actúe como un cliente de cada ELAN.

Existen dos tipos de LECs:

Un LEC proxy es aquel que representa la dirección MAC de otros dispositivos además de la de él mismo. En otras palabras, actúa como un puente.

Un LEC no-proxy es un dispositivo como un anfitrión que tiene una dirección MAC única, es decir la dirección de él mismo solamente.
La versión 1.0 de LANE, permite a los servidores distinguir entre los tipos de LECs, para agregar eficiencia en la resolución de direcciones. En este caso, el servidor mantiene dos árboles punto-a-multipunto, uno para clientes LECs proxy y otro para LECs no-proxy. Los LECs se identifican así mismos como proxy o no-proxy cuando estos se conectan a una red LAN emulada.

Cuando un mensaje LE_ARP llega, el servidor LES verifica su tabla de direcciones y responde con la dirección ATM apropiada si este encuentra el mapeo. Si no encuentra el mapeo en sus tablas, el LES puede asumir que la dirección MAC está asociada a un LEC proxy. Este entonces direcciona la petición LE_ARP hacia aquellas estaciones sobre el árbol punto-a-multipunto proxy para su resolución.

Servicio LANE

El servicio LANE consiste de tres entidades, un servidor de Emulación LAN (LES), un servidor de broadcast y desconocido (BUS) y por último, un servidor de configuración (LECS). La especificación LANE no describe los detalles de la implantación de los componentes de servicio. Es decir, no especifica algún lugar en especial donde deban estar localizados los tres servidores, cualquier dispositivo o dispositivos con conectividad ATM deberán ser suficiente. Aun que, por desempeño y eficacia, la mayoría de los proveedores implantan los componentes con funciones de servicio sobre los equipos de red, tales como conmutadores o enrutadores ATM, en lugar de estaciones.

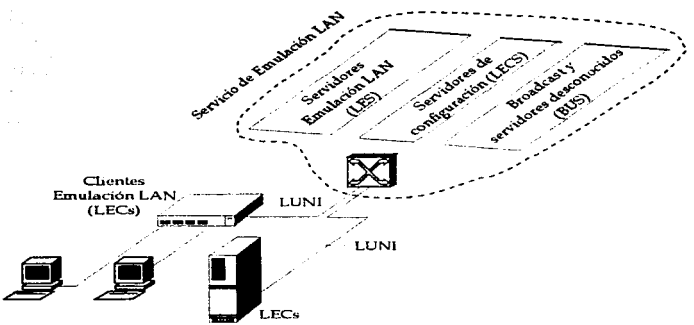


Figura 6.22 Componentes LANE y la interrelación

En la figura anterior, se representan dentro de una nube los servicios de Emulación LAN, significando las posibles opciones de para la implantación de los diferentes tipos de servicio.

- Servidor de Emulación de LAN (LES: LAN Emulation Server)

  La entidad LES, es el centro de control para una LAN emulada, ya que realiza el manejo de resolución de direcciones y control de información. Su primer tarea es la de registrar y resolver las direcciones MAC a direcciones ATM.

  El LES implanta la función de control para una ELAN particular. Existe solamente un LES lógico por cada red LAN emulada (ELAN), y para poder pertenecer a una ELAN particular significa tener un control de relación con ese servidor LES de una ELAN particular. Cada LES es identificado por una dirección ATM única.

  Todos los dispositivos registrados dentro de un mismo servidor LES llegan a ser parte de una misma red LAN emulada (ELAN). Una red LAN emulada es esencialmente una capa MAC basada en una red LAN virtual, definiendo un dominio de broadcast común entre todas las estaciones finales registradas en un mismo servidor LES.

- Servidor de Broadcast y Desconocido (BUS: Broadcast and Unknown Server)

  El BUS está diseñado para ser un servidor multicast, el cuál, es usado para llevar trafico hacia direcciones con destino desconocido, direccionar tráfico de broadcast y tráfico multicast, hacia clientes dentro de una ELAN particular.

  Cada LEC está asociado con un solo servidor BUS por ELAN pero pueden existir múltiples servidores BUS dentro de una ELAN particular, sin embargo, se deben comunicar y coordinar de la manera que el proveedor indique (función propietaria), ya que esta acción se encuentra fuera del alcance de la versión 1.0 de la especificación LANE[129].

  Los servidores LES y BUS, trabajan conjuntamente para transferir tanto tráfico unibroadcast como de broadcast. Generalmente, los servidores LES y BUS son localizados dentro de un solo dispositivo.

- Servidor de Configuración de Emulación de LAN (LECS: LAN Emulation Configuration Server)

  El servidor LECS, es una entidad que asigna clientes LANE individuales (LEC) a redes LAN emuladas particulares. Esto se lleva a cabo, al dirigir a estos clientes hacia el LES que corresponde a una ELAN determinada. Además, mantiene una tabla de las asociaciones resultantes.

  El LECS puede determinar la asignación de un LEC individual a una determinada red LAN emulada, basado en la locación física del LEC (como se especifica por la dirección ATM del LEC) o por su asociación lógica (cuando se definen VLANs o redes virtuales). Es por esta razón, que el servidor LECS es generalmente configurado por el administrador de la red con la información inicial principal, la cual indica a que red LAN virtual pertenece cada LEC (donde una LAN virtual corresponde a una ELAN).

  Existe lógicamente un servidor LECS por dominio administrativo, y este sirve a todas las ELANs dentro de ese dominio. Por lo tanto un solo servidor LECS puede administrar la información de configuración de una red ATM muy grande (partiendo de que sus responsabilidades son limitadas para la configuración inicial).

Como se puede observar, el software que entrega el servicio de Emulación LAN se encuentra implantado principalmente en los tres servidores lógicos: LES, BUS y el servidor LECS.

---

[129] Cabe hacer mención, que este tipo de configuración queda fuera del alcance de la versión 1.0 de LANE y se espera que la versión 2.0 formalice este requerimiento.

6.1.5.4.2.3.3 Como funciona el servicio de Emulación LAN ATM

A continuación se demuestra como trabajan conjuntamente los diferentes componentes del LUNI para implantar la especificación LANE.

Inicialización y configuración

Al encender un dispositivo final conocido como LEC, en principio debe obtener la información de configuración (su propia dirección ATM, la cual se realiza a través del registro de dirección) del servidor LECS[130], para poder unirse a una red LAN emulada. El LEC entonces establece una conexión de configuración directa con el LECS.

Una vez que el LEC localiza al servidor LECS y establece una conexión directa VCC, le dirige alguna información importante como es: su dirección ATM, su dirección MAC, su tipo de LAN y su máximo tamaño de frame. El servidor LECS responde con el tipo de LAN emulada actual (Ethernet o Token Ring), el tamaño máximo de frame actual[131], y la dirección ATM de un servidor LES (dependiendo del criterio de asignación que se siga, ya sea por redes virtuales o por localización física)[132].

Una vez que el LEC obtiene la dirección del servidor LES, posteriormente establece una conexión directa VCC con el servidor LES. Una vez hecho esto, el LES asigna al LEC con un identificador LEC único (LECID: LEC Identifier). El LES, entonces registra la dirección MAC y dirección ATM del cliente LEC[133]. A partir de este momento, el cliente LEC puede resolver el mapeo de direcciones MAC a direcciones ATM[134].

---

[130] La especificación LANE ofrece varias opciones para que un cliente LEC encuentre al servidor de configuración inicial LECS. Las opciones más importantes son: El primero, utilizando un procedimiento definido como Interface de Administración Local Provisional (ILMI: Interim Local Management Interface) para determinar la dirección LECS; el segundo, utilizando una conexión permanente referida como bien-conocida (well-known) al LECS (ruta virtual definida como VPI=0, VCI=1). Para mayor información de los otros métodos referirse al white paper: ATM LAN Emulation; 3Com; pp. 5-6.

[131] Es importante hacer notar, que todos los dispositivos conectados a una misma LANE deberán utilizar el mismo tamaño MTU.

[132] La especificación LANE, actualmente no define los dispositivos con múltiples direcciones ATM (tales como conmutadores ATM), deberán organizar esas direcciones. Similarmente, no especifica como el servidor LECS debe mantener su base. Estas decisiones se dejan para el manejo de una red LAN Emulada individual implantada y el administrador de la red.

[133] El anexo proxy contra no-proxy, describe la manera de como se puede utilizar esta información de dirección.

[134] El LEC puede realizar conexiones de control directo VCC y conexiones VCC distribuido para el procedimiento de resolución de direcciones Emulación LAN ARP (LE_ARP: LAN Emulation Address Resolution Protocol).

La primer dirección que necesita el LEC es la dirección del servidor BUS, para lo cuál envía una petición de la dirección MAC con el valor de todos los bits en uno (dirección de broadcast) al servidor LES. Cuando un LEC recibe un frame de datos unicast de las capas superiores para su transmisión, este primero verifica sus tablas locales para ver si conoce la dirección ATM asociada con la dirección MAC. Si no se encuentra en sus tablas locales, el LEC tiene entonces tres opciones:

- Este puede emitir el frame hacia la red para inicializar la resolución de la dirección MAC a una dirección ATM.

- Este puede retener el frame hasta que pueda aprender la dirección ATM del destino y establecer hasta entonces una conexión VCC directa.

- El LEC puede dirigir el frame hacia el servidor BUS para mantener los datos en movimiento. En este caso, el BUS responde de manera de servidor de broadcast (envía el paquete a hacia cada uno de los clientes de la red LAN emulada por medio de inundación) Esta opción se explica mas a detalle a continuación:

  Cuando un LEC origen envía los frames hacia el servidor BUS, de manera simultánea, el LEC envía una petición LE_ARP (LAN Emulation Address Resolution Protocol) hacia el servidor LES, tratando de que resuelva la dirección MAC desconocida, si el LES reconoce este mapeo, puede escoger contestar directamente sobre el Control Directo VCC al LEC origen. Si no reconoce el mapeo[135], este, redirige la petición hacia todos los clientes por medio de una conexión de control-distribuido VCC para solicitar una respuesta de un LEC que conozca la dirección MAC de la petición.

  El destino, al reconocer su dirección MAC envía un LE_ARP de respuesta hacia el servidor LES, el cuál incluye las direcciones ATM tanto del LEC originario de la petición como la del LEC destino. El servidor LES envía el mensaje de respuesta con la dirección ATM del destino hacia todos los LECs (en una modalidad de broadcast) para que todos los LECs puedan aprender esta dirección especial. El ciclo termina cuando el LEC fuente reconoce su propia dirección contenida en el mensaje de respuesta. En este punto, ha aprendido la dirección ATM de la dirección MAC desconocida y puede en este momento establecer una conexión directa entre él y el LEC destino.

---

[135] Generalmente, cualquier dirección MAC no conocida por el LES, deberá encontrarse solo en un cliente LEC proxy (un concentrador o un puente) y no dentro de una tarjeta NIC ATM, y solamente los LECs no ATM (es decir, dispositivos no-ATM detrás de un dispositivo proxy) dentro de tales dispositivos (proxy) necesitan necesariamente recibir LE_ARPs redirigidos por el dispositivo proxy.
Para llevar esto a cabo, algunos dispositivos LECs pueden registrarse con el LES como un nodo "proxy", indicando que este puede ser alcanzado a través de otra dirección (la dirección del dispositivo LEC proxy). El LES entonces tiene la opción de establecer controles distribuidos VCCs de manera que los LE_ARPs sean solo enviados a tales LECs proxy (para mayor referencia ver los tipos de clientes LECs en este mismo capítulo).

Mientras el cliente LEC origen, espera la respuesta de la petición del LE_ARP. el BUS correspondiente, por medio de inundación enviará paquetes hacia todos los LECs registrados. Esto debe ser llevado acabó, porque, en el caso de un dispositivo pasivo que se encuentre detrás de un conmutador LAN (LEC proxy), el LEC origen no puede saber donde se encuentra la dirección MAC[136]. Adicionalmente, la resolución a un LE_ARP puede tomar un poco de tiempo, y varios protocolos de red son intolerantes tanto a la perdida de paquetes (si el LEC escoge descartar el paquete mientras espera la resolución del LE_ARP) o a la latencia (si el LEC escoge almacenar o retener el paquete). De este modo, el servidor BUS provee la analogía del procedimiento de inundación utilizado por el mecanismo de árbol expandido usado por los puentes tradicionales (para mayor referencia ver el capítulo de los puentes) para paquetes con destino desconocido, de aquí el nombre del servidor.

Si un LE_ARP de respuesta es recibido, el LEC puede establecer una conexión VCC directa hasta el nodo destino, y utilizar este para transferir los datos en lugar de la opción de inundación del servidor BUS. Antes de que se realice la conexión directa, el LEC origen necesita dar de baja la ruta de inundación del BUS y utiliza el procedimiento llamado "desecho" (flush) para asegurar que todos los paquetes previamente enviados por medio del BUS hayan sido entregados al destino y posteriormente se de debaja el método de inundación, una vez realizado esto, se puede hacer uso de la nueva ruta con la conexión VCC directa de datos. Esta mecanismo se lleva a cabo para poder garantizar la preservación del orden de los frames.

Si no se recibe una respuesta del LE_ARP, el LEC continuará enviando paquetes vía el servidor BUS (por inundación), pero regularmente seguirá enviando peticiones de LE_ARP hasta que se reciba un LE_ARP de respuesta. Generalmente una vez que un paquete es inundado por medio del servidor BUS el destino responde con un LE_ARP de respuesta.

Cada LEC construye su propia tabla de direcciones MAC, direcciones ATM y conexiones VCC. Si una dirección MAC particular no ha estado activa durante algún tiempo, un LEC eventualmente desechará esta dirección de su tabla, es decir, cuando no existen mas direcciones MAC asociadas con una conexión VCC de datos directos, el LEC puede desechar la conexión.

Basándose en la versión 1.0 de LANE, todas las implantaciones de clientes LEC estandarizados son garantizados para interoperar, pero por otro lado, no existe una manera estandarizada por la cuál servidores de múltiples proveedores actualmente puedan intercomunicarse, la segunda versión de la Emulación LAN (versión 2.0 actualmente bajo desarrollo) definirá protocolos servidor-a-servidor

[136] Como un puente en modo de aprendizaje (capitulo 5), un LEC deberá aprender la localización del dispositivo, cuando este responda al paquete que fue inundado por todos los segmentos.

que permitirán el trabajo conjunto de servidores multiproveedor incrementando la escalabilidad y robustez de LANE. Mientras tanto los administradores de redes deberán escoger sus funciones de servicio de un solo vendedor para asegurar una amplia interoperabilidad ATM.

6.1.5.4.2.3.4 Múltiples redes LAN Emuladas

El estándar de Emulación LAN del Forum ATM, también soporta la implantación de múltiples redes LAN emuladas dentro de una sola red ATM. La Emulación LAN está basado en el modelo cliente-servidor, cada cliente se conecta al servidor a través de una conexión virtual. Solo aquellos clientes conectados al mismo servidor pueden aprender acerca de las otros clientes y comunicarse directamente. Lógicamente la segmentación de la red es a través de múltiples funciones de servidor (LECS, LES y BUS) los cuales pueden ser dispositivos en modo único (stand alone), o como software en los sistemas finales o en módulos de conmutador ATM. Permitiendo a múltiples redes LAN Emuladas coexistir simultáneamente sobre la misma red física.

Sin embargo, el protocolo LANE solamente define los mecanismos de operación dentro de una sola red LAN emulada (ELAN). Como se explico en el párrafo anterior, múltiples ELANs pueden coexistir simultáneamente sobre una sola red ATM por tal motivo, la intercomunicación entre redes LAN emuladas requiere de un puente o enrutador convencional[137]. Una red LAN Virtual (VLAN) resulta cuando existen varios dominios LANE diferentes a través de uno o mas conmutadores ATM. Las Redes LAN Virtuales, desarrollan grupos de trabajo mas seguros y pueden crear una protección contra ráfagas de broadcast (broadcast storms) para hacer un mejor uso de la red.

Un mensaje de broadcast proveniente de un LEC, solo puede alcanzar a otros LECs de la misma red VLAN, pero no a otros, de esta manera, estaciones finales que no pertenecen a la misma VLAN no desperdician recursos procesando datos no relacionados con su grupo de interés. Las redes Virtuales o VLANs[138] simplifican la administración de la red al permitir la estructuración de grupos de trabajo, basándose en el interés común de los usuarios y no en la locación física de las estaciones. Los administradores de la red, pueden adicionar, mover, cambiar o simplemente redefinir la agrupación de los grupos de trabajo, además de poder configurar los dispositivos finales a través de una forma remota. Todo esto se lleva a cabo sin la necesidad de cambiar el sistema de cableado o adicionar nuevos dispositivos a la red.

---

[137] Es decir, aun que las redes LAN emuladas coexistan en la misma red ATM, se necesita de un puente o un enrutador para que puedan intercomunicarse estaciones de diferentes redes LAN emuladas.

[138] Para mayor referencia, ver la parte referente a redes virtuales VLAN, que viene en el capitulo 5 referente a conmutadores.

6.1.5.4.2.3.5 Limitaciones de Múltiples redes LAN Emuladas

Como se puede observar, un número de conexiones VCCs son requeridas para establecer y mantener una red LAN emulada. Cada LEC tiene conexiones VCC desde y hasta el servidor LES y el servidor BUS, las cuales pueden ser bidireccionales o unidireccionales (en el peor caso, de conexiones unidireccionales, se requiere de cuatro por LEC).

Por otro lado, los servidores no son capaces de soportar un número infinito de VCCs, por tal motivo, existe un límite para el número de LECs que puede contener una red LAN emulada[139].

6.1.5.4.2.4 LANE versión 2.0

La segunda versión de la especificación LANE, está actualmente bajo desarrollo. En esta, se definirán los protocolos servidor-a-servidor (LNNI: NNI[140] Emulación LAN) que permitirá a los servidores de múltiples proveedores el poder trabajar conjuntamente, además de brindar la Calidad de Servicio (QoS), de esta manera, se piensa incrementar la escalabilidad y robustez de LANE. Esto es:

- La versión 2.0 de LANE empieza por distinguir los elementos dentro de la nube de servicios LANE. Con esto, se pretende poder acomodar múltiples pares de servidores LES/BUS al definir protocolos entre ellos. Estos protocolos proveerán un alto nivel de escalabilidad para LANE y soportarán una función de servidores redundantes.

- La versión 2.0 brindará los servicios de Calidad de Servicio (QoS)[141], que están diseñados para integrar trafico de voz, video y datos en un ambiente ATM, a través del uso de diferentes conexiones virtuales. La Calidad de Servicio QoS soporta aplicaciones que requieren diferentes tipos de ancho de banda (constante, variable, disponible y sin especificar). Además de que QoS es particularmente importante para el manejo de aplicaciones en tiempo real (videoconferencias, video sobre demanda).

Una característica importante que deberá cubrir la versión 2.0 es que debe ser compatible con la especificación LANE 1.0 existente.

---

[139] Este es un punto importante que se debe preguntar a los proveedores del equipo LANE.
[140] Interface Red-a-Red (NNI: Network-Network Interface).
[141] Los administradores pueden especificar el tipo de servicio en tráfico; LANE 1.0 soporta únicamente tráfico sin especificación de cantidad de bit.

6.1.5.4.2.5 Desventajas de LANE versión 1.0

Como se ha podido observar, el protocolo LANE solamente especifica la operación de la Interface de Usuario de Emulación LAN a la Red (LUNI: LAN Emulation User to Network Interface) es decir, la relación entre un LEC y la parte que provee el servicio de LANE (LES, BUS y LECS). Esto se puede ver de manera contrastante con la NNI[27] Emulación LAN (LNNI), que opera entre los componentes que realizan la función de servicio dentro de un solo sistema emulado ELAN y la cuál no ha sido especificada en esta versión de LANE.

Es por esto que en la actualidad, puede surgir un problema el utilizar conmutadores de más de un fabricante. Cuando un conmutador ATM se instala, determina si se conectará a un servidor LANE existente o si este actuará como servidor. Los productos de un mismo fabricante resuelven este problema fácilmente. Sin embargo, en los ambientes que tienen productos de varios fabricantes, dos conmutadores pueden entrar en conflicto tratando de determinar cual de ellos actuará como servidor LANE y con frecuencia será necesario configurarlos de manera manual.

Además, la fase 1 de protocolo LANE no permite el soporte de forma estándar de múltiples servidores de LES y BUS dentro de una misma ELAN. De aquí, que estos componentes de servicio representen ambos solamente puntos de falla y cuellos de botella potenciales, además de que no se proporciona ninguna redundancia, (por que no se puede especificar la configuración de servicio LANE de respaldo (espejo)). Actualmente, la iteracción entre cada uno de los componentes de servicio en la versión 1.0 del protocolo LANE han sido dejados sin especificar, y serán implantados de manera propietaria por los proveedores, por tal motivo, los mecanismos no quedaran estándarizados hasta que llegue la nueva versión de LANE (la versión LANE 2.0).

6.1.5.4.3 Multiprotocolo Sobre ATM (MPOA)

Una vez que el Forum ATM ha terminado su especificación de Emulación LAN versión 1.0 (la cuál define la manera de como puentear trafico proveniente de redes heredadas), pone su atención hacia un nuevo objetivo: definiendo como puede ser enrutado el tráfico sobre una red ATM. Desarrollando el estándar referido como Multiprotocolo Sobre ATM (MPOA: Multiprotocol Over ATM) el cual, es el proyecto más ambicioso que ha tenido el Forum ATM hasta la fecha.

El Múltiprotocolo Sobre ATM es un método nativo de protocolo de interconectividad en red para sintetizar, enrutar y puentear trafico de protocolos diversos sobre ambientes conmutados ATM. Es decir, provee métodos unificados para sobreponer los protocolos de capa 3 sobre ATM.

De acuerdo al documento, MPOA definirá una arquitectura de servidor de enrutamiento (arquitectura de enrutamiento virtual) en los cuales los conmutadores consultarán una entidad de enrutamiento central cuando ellos tengan la necesidad de conocer donde se deben enviar los datos. Para realizar esto, el MPOA espera que definan varios protocolos diferentes, incluyendo un protocolo conmutador-a-servidor (el cuál permitirá la comunicación entre el servidor de enrutamiento y el conmutador) y un protocolo interservidor (el cuál mantendrá la información en diferentes servidores de enrutamiento en la misma red).

6.1.5.4.4 Control de Flujo

La congestión es definida como el estado de elementos de red en el cual, debido a la sobre carga de tráfico, la red no es capaz de garantizar una Calidad de Servicio (QoS) en las conexiones establecidas en el momento de la congestión, ni tampoco las nuevas peticiones de conexión. El control de flujo trata de minimizar los efectos de la congestión.

Cuando varios conmutadores ATM se enfrentan a la congestión, descartan celdas de acuerdo al parámetro CLP (Cell Loss Priority). La voz y el video no son tolerantes a la perdida de celdas. Por otro lado, el trafico de datos es mas tolerante a la perdida y retraso de datos, pero si las celdas que contienen información de un paquete de alto nivel son desechadas, el paquete entero tiene que ser retransmitido. Considerando que los paquetes IP son 1500 bytes de largo y los paquetes FDDI son de 4500 bytes de largo, la perdida de una sola celda puede significar retransmisiones significantes, además de agravar mas la congestión.
Es por esto que para redes ATM de mayor tamaño y que lleven diferente tipo de trafico se hace necesario el manejo de mecanismos mas sofisticados para el control de la congestión.

El Forum ATM consideró dos enfoques. El primero, esta basado en un esquema salto-a-salto con concesión-de-crédito (credit-granting), donde el conmutador o una estación final no pueden enviar celdas sobre una conexión dada, hasta que ésta le haya proporcionado el crédito de ancho de banda. Este enfoque no fue ampliamente aceptado por varios vendedores, ya que su implantación requería de utilizar nuevos chips, ocasionando que los conmutadores actuales de ATM llegaran a ser obsoletos.

El segundo enfoque, esta basado en un control de velocidad fin-a-fin. En este enfoque, la celdas que pasan a través de un conmutador y que experimenten congestión serán marcados al establecer un bit en su encabezado. La estación destino observará el estatus de este bit y enviará una celda especial de regreso a la estación fuente, ocasionando que ésta, retarde o acelere el envío de las celdas. Esto es facil de implantar en los conmutadores, pero aumenta la tarea de procesamiento en las estaciones terminales.

En septiembre de 1994, el Forum ATM escogió el enfoque basado en control de velocidad, con esta decisión, ha planeado completar la especificación a finales de 1995.

6.1.5.5 Integración WAN sobre ATM

Existen cuatro protocolos primarios requeridos para la completa interconexión de ATM sobre una Red de Área Amplia (WAN).

1. Interface de usuario-a-red pública (UNI: User Network Interface)

El protocolo UNI de ATM provee múltiples clases de servicio y reservación de ancho de banda que se establece durante la llamada para establecer una conexión conmutada virtual (VCC). La interface UNI define la interoperabilidad entre el equipo del usuario y el puerto del conmutador ATM. Una interface UNI pública define la interface entre un servicio público de red ATM que usualmente soporta interfaces SONET o DS3. Este es el enlace entre el usuario ATM y conmutador ATM del proveedor de la red pública ATM.

Nivel	Velocidad de la línea (Mbps)
OC-1	51.84
OC-3	155.52
OC-9	466.56
OC-12	622.08
OC-18	933.12
OC-24	1244.16
OC-36	1866.24
OC-48	2488.32

Tabla 6.15 Jerarquía de nivel de señal óptica SONET

Nivel	Estados Unidos	Europa
1	1.544 (DS1)	2.048
2	6.312 (DS2)	8.448
3	44.736 (DS3)	34.368

Tabla 6.16 Jerarquía de la señal digital (en Mbps)

2. Interface Pública Red-a-Red (NNI: Network-to-Network Interface)
El protocolo NNI provee el arbitraje, el control de congestión y manejo de topología de la conexión virtual de conexiones ATM públicas y privadas. Es decir, es el enlace entre conmutadores ATM dentro de una red ATM pública.

3. Interface Interportadora (ICI: Intercarrier Interface)
El ICI define los mecanismos de interred sobre redes ATM de área amplia. Es decir, este permite poder enlazarse entre dos redes de proveedores de red ATM.

4. Interface de Intercambio de Datos (DXI: Data exchange interface)
El DXI provee una interface estándar para equipo heredado. El DXI soporta enrutamiento sobre ATM debido a que está basado en paquetes en lugar de celdas. Utiliza un protocolo de paquete estándar de Control de enlace de datos de alto nivel (HDLC, ver capitulo 2). Este protocolo permite conectar los dispositivos existentes (no-ATM) a redes ATM.

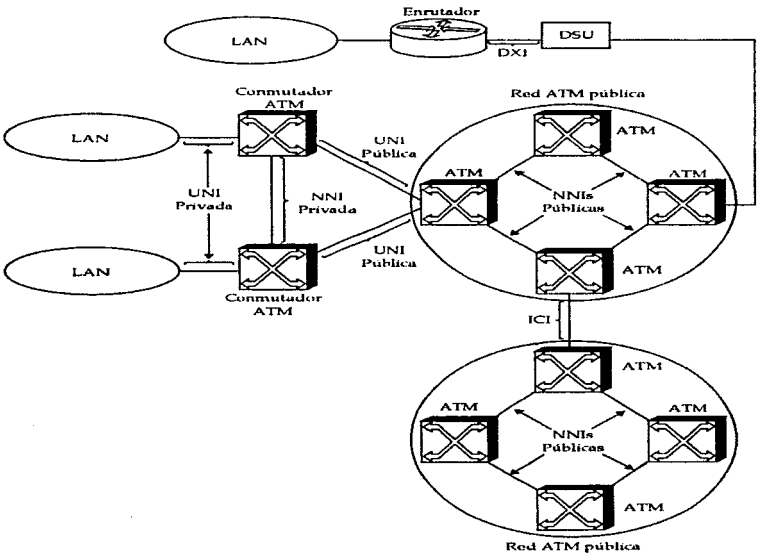


Figura 6.23 Red ATM de área amplia.

Aunque la mayoría de los proveedores de servicios digitales ofrecen ATM, todavía no es ampliamente disponible. Debido a que no todos los proveedores de intercambio local (LECs: local exchange carriers) y los proveedores de intercambio

(IXCs: Interexchange carriers) han instalado redes digitales ATM/SONET integradas para poder ofrecer servicios de red de datos privados virtuales de forma económica.

Los proveedores de servicio reconocen que ATM es definitivamente el futuro de las comunicaciones de redes de área amplia, debido a que quitara las fronteras entre redes LAN y las redes WAN.

Existen tres opciones para realizar una conexión real ATM para el cruce a través de redes de área amplia

Un servicio de línea digital alquilada del proveedor con línea T3, por ejemplo puede ser usado como un troncal entre dos conmutadores ATM, y estos dispositivos entonces crearán celdas y manejaran la señal y el flujo de trafico. De hecho esta es una red ATM privada.

Un proveedor de servicios ATM puede proveer en forma de una ruta virtual, una troncal entre el mismo par de conmutadores. En este caso, el proveedor solo transporta

6.1.5.5.1 Interconexión de redes WAN y ATM

En particular, se han realizado trabajos sobre la interconexión con ATM de redes orientadas a conexión Frame relay y redes sin conexión Servicio de Datos Multimegabit Conmutados[142] (SMDS: Switched Multimegabit Data Service).

Conjuntamente, el Forum Frame relay y el Forum ATM han especificado acuerdos para poder soportar interconexión PVC Frame relay/ATM basados sobre el estándar ITU-TI.555. El cual define el mapeo de paquetes Frame relay dentro de paquetes AAL5 como una unidad de interred Frame Relay-a-ATM.

La interconexión de redes SMDS con ATM está definida en el ITU-T I.364 y los acuerdos de implantación se llevan a cabo por el Forum ATM y el Grupo de Interés SMDS de Estados Unidos y Europa.

[142] SMDS es un servicio ofrecido en Estados unidos. Mientras que en Europa, un servicio casi idéntico es conocido como el CBDS (Connectionless Broadband Data Service).

6.2 Redes de Área Amplia (WAN)

6.2.1 Introducción

En el pasado, las redes de área amplia fueron construidas usando facilidades analógicas de baja velocidad, utilizadas primeramente para trafico de voz, posteriormente, para llevar a cabo una transmisión eficaz de datos, redes públicas y privadas de conmutación de paquetes[143] fueron utilizadas.

Actualmente, la tendencia ha sido ir hacia las facilidades digitales, especialmente de los servicios T1 y T3.

Con la conversión actual de la mayoría de las redes públicas hacia la conmutación y transmisión digital, existe una menor necesidad de protección contra errores. Actualmente las redes publicas de fibra óptica tienen un número muy bajo de errores, al mismo tiempo los dispositivos de los usuarios finales han sido dotados con un nivel mayor de inteligencia, poder de procesamiento y mayor almacenamiento, haciéndolos mas adeptos al manejo de control de errores y soporte de diversos protocolos. Consecuentemente, las funciones de los protocolos de comunicaciones utilizados sobre la red pueden ser reducidos a funciones de portador de manera esencial, permitiendo un mejor rendimiento.

El interconectar redes locales (LANs) en diferentes sitios, frecuentemente se necesita el uso de servicios de área amplia (WANs). Pero teniendo en cuenta que el ancho de banda de una red de área amplia es mas caro que el ancho de banda de una red local. Además de que los circuitos de redes de área amplia son mas delgados y mas largos también, esto es, ellos soportan menor tráfico que los canales de redes locales, por medio de esto se limita el rendimiento. De esta manera el objetivo principal es el de optimar los servicios de red de área amplia.

Una red de área amplia (WAN) utiliza conexiones dedicadas o conmutadas para enlazar las computadoras que se encuentran localizadas en sitios geográficamente remotos que se encuentran de cierta manera en forma dispersa. Estas conexiones de área amplia se pueden realizar a través de redes públicas o a través de redes privadas.

[143] Para mayor información referirse al Anexo D.

6.2.2 Una red WAN

Un enrutador envía tráfico en dirección a una localidad remota desde una red local sobre la conexión de área amplia hacia su destino remoto. El enrutador es conectado hacia una línea analógica o de otra forma a una línea digital[144] (servicios digitales). Dependiendo del servicio del portador (carrier service), se determina el tipo exacto del equipo de área amplia necesario.

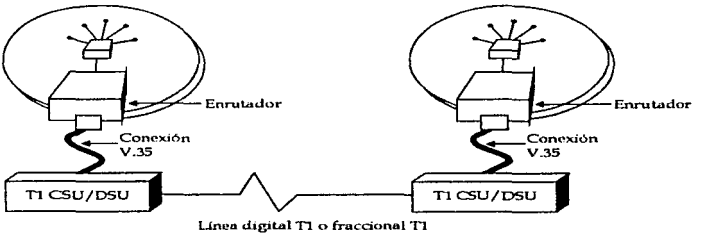


Figura 6.24 Conexiones de red WAN a través de servicios digitales T1.

Servicios digitales

Los servicios digitales son frecuentemente utilizados para llevar voz, video y datos. Los circuitos digitales pueden transmitir datos a velocidades mayores de 45Mbps. Usualmente, las líneas digitales son posibles al acondicionar líneas analógicas para manejar grandes velocidades de datos. Las líneas son generalmente alquiladas con un portador de intercambio local e instalados entre dos puntos para proveer un servicio dedicado.[145]

Las redes de área amplia pueden incluir ya sea líneas dedicadas o conmutadas. Una línea dedicada es una conexión permanente entre dos puntos que usualmente es alquilada. Mientras que, un servicio de línea conmutada no requiere de conexiones permanentes entre dos puntos. Es decir, permite a los usuarios establecer conexiones temporales entre múltiples puntos que se mantienen solamente en el tiempo de duración de la transmisión de los datos. Existen dos

[144] Un enrutador es conectado a líneas analógicas vía un módem o a líneas digitales por medio de unidad de servicio de canal/unidades de servicio de datos (CSU/DSUs: channel service unit/data service units).
[145] Para mayor información referirse al Anexo E.

tipos de servicios conmutados disponibles **servicios de conmutación de circuitos y servicio de conmutación de paquetes** (el cual es mejor utilizado para la transmisión de datos).[146]

6.2.3 Líneas digitales

Las líneas digitales son diseñadas para llevar trafico de datos a una velocidad mayor de 45 Mbps y son disponibles tanto en servicios dedicados o en servicios conmutados.

6.2.4 Servicios de WAN o servicios de portador

Diferentes tipos de redes requieren diferentes velocidades de transmisión, prioritización de los datos y niveles de calidad de servicio. A continuación se describirá brevemente los mas populares.

6.2.4.1 Servicios de conmutación de circuitos

Estos son servicios portadores conmutados, que establecen una conexión virtual antes de transferir datos. Dos de los mas comúnmente usados son los servicios **conmutación 56** (switched 56) y la **Red Digital de Servicios Integrados** (ISDN).

6.2.4.2 Servicios de conmutación de paquetes

En este tipo de servicio no es necesario el establecimiento previo de la conexión antes de que la transferencia de datos comience. En lugar de ello, todos los paquetes son transmitidos de manera separada, y cada uno puede tomar una ruta por separado a través de la malla de rutas de red que establecen la red de conmutación de paquetes. Aun que este tipo de servicios no es muy eficiente para trafico sensitivo al tiempo, de otra manera, la conmutación de paquetes es el mejor servicio para el manejo de trafico de ráfaga (bursty). Dentro de los mas populares, se encuentran **X.25** y **Frame relay**.

6.2.4.3 Servicios de conmutación de celdas

En servicios de conmutación de celdas, la unidad mas pequeña de datos es de tamaño fijo (celda), en lugar de un tamaño variable. Esta tecnología basada en celdas permite que la conmutación se lleve a cabo por medio de hardware sin complicaciones y sin el consumo de tiempo en el calculo de rutas frame por frame. Lo que hace a la conmutación mas rápida y menos cara.

---

[146] Para mayor información referirse al Anexo D.

6.2.5 Red Digital de Servicios Integrados (ISDN)

El origen de ISDN es el estándar **ISDN de banda estrecha** (narrowband ISDN). El primer estándar ISDN que define interfaces digitales fin-a-fin apareció en 1984 bajo el CCITT (Consultive Committee for International Telegraph and Telephone. La ISDN ha sido considerada como un mejor avance al especificar servicios de red digital que pueden ser entregados sobre la existente red telefónica digital integrada, además de ofrecer un alto desempeño de 2Mbps en un enlace local y de 64Kbps o 128Kbps sobre área amplia.

La **Red Digital de Servicios Integrados** (ISDN: Integrated Services Digital Network) es una red de telecomunicaciones pública con una infraestructura flexible diseñada para integrar voz, datos, vídeo, imágenes y otras aplicaciones y servicios. La ISDN se puede pensar como un reemplazo de la red de telefonía analógica existente. **ISDN de banda estrecha** (narrowband ISDN) provee servicios de baja velocidad, desde 56 Kbps hasta 2 Mbps; mientras que el **ISDN de banda ancha** (broadband ISDN), basada en la tecnología de celdas de tamaño fijo o **Modo de Transferencia Asíncrono** (ATM), para necesidades de servicio de direccionamiento de alta velocidad puede ser desde 2 Mbps hasta 600 Mbps.

6.2.5.1 Desarrollo del ISDN

La Unión de Comunicaciones Internacionales - Sector de estandarización de Telecomunicaciones (ITU-TSS), formalmente conocido como (CCITT), ha definido a ISDN como una red que evolucionó de la telefonía de **Red Digital Integrada** (IDN: Integrated Digital Network), que además, provee un conectividad digital fin-a-fin para soportar una amplia variedad de servicios. Dos características principales que distinguen a la ISDN de las redes de telefonía tradicionales son:

- Esta es digital desde un punto de la conexión hasta el otro.
- Este define un pequeño conjunto de protocolos de interface usuario/red de estándar internacionalmente, de esta manera, todos los dispositivos ISDN pueden usar el mismo tipo de conexión física y el mismo conjunto de protocolos de señal.

ISDN combina el tratamiento de red de telefonía extensa geográficamente con la capacidad de acarreo de datos de redes de datos digitales dentro de una estructura bien definida, que puede soportar simultáneamente aplicaciones de voz, datos, vídeo imágenes y multimedia.

La tecnología ISDN ha estado disponible durante años, pero solamente en los pasados años ha llegado a un desarrollo tal, que es una opción viable para redes de área amplia (WAN), principalmente en Estados unidos.

6.2.5.2 Estructura de ISDN

ISDN es un servicio compuesto por dos tipos de canales: canales portadores (bearer channels) y canales de señalización (signaling channels). Los proveedores han combinado estos dos tipos de canales para construir dos diferentes tipos de servicios ISDN: **Interface de Tasa Básica** (BRI: Basic Rate Interface) y la **Interface de Tasa Primaria** (PRI: Primary Rate Interface).

6.2.5.3 Canales lógicos ISDN

ISDN define dos tipos de canales lógicos distinguiéndose ambos por su función y capacidad. Un tipo para la transmisión de datos y el otro para el manejo de la administración de señal y control de llamada.

Canales portadores (canal B)

- Canal B (canal portador). Los canales B transmiten a 64Kbps en modo de circuitos o modo de paquetes para llevar la información del usuario (voz, datos, fax y flujos de información multiplexada de los usuarios). Todos los servicios de red están disponibles a través de canales tipo B (los canales H son funcionalmente equivalentes a los canales B pero operan a velocidades mayores de 64Kbps). Todos los servicios de red son disponibles a través de este tipo de canal. El canal B puede ser usado en la conmutación de circuitos y conmutación de paquetes. Para la conexión por conmutación de circuitos, el canal B es dado por completo a un sola interface de usuario en modo transparente y no se permite información de señalización para el control de la conexión en el canal B. Para la conexión por conmutación por paquetes, el flujo de datos del canal B puede ser conmutada en diferentes circuitos virtuales para la separación de destinos.

- Canal H. Este tipo de canales son funcionalmente equivalentes a los canales B pero operan a velocidades mayores de 64Kbps. La función principal es la de transmitir la información del usuario que requiere tasas mayores a 64Kbps y un poco mas de 100Mbps, como por ejemplo, video digital y audio a alta velocidad, resolución para televisión, teleconferencia, transferencia de archivos a alta velocidad, etc. existen varios tipos de canal H:

Canal	tasa de transmisión (Kbps)	tasa múltiplo de canales B	tasa múltiplo de canales H0
H0	384	6	1
H11	1536	24	4
H12	1920	30	5
H21	32768	512	-
H22	44160	690	115
H4	135168	2112	352

La tasa de transmisión de cada uno de ellos se una combinación del canal B o canales H

Tabla 6.17 Ejemplo de canales tipo H

Canal de señalización (canal D)

- Canal D (señalización). Los canales D transmiten a 16Kbps para la interface BRI y a 64Kbps para interface PRI. La Función principal es la de llevar la información de señalización para el establecimiento de llamada, control de la conexión y terminación de la llamada. Es decir, lleva la señal de llamada y configuración para establecer una conexión de red, petición de servicios de red, enrutamiento de datos sobre canales B y la terminación de la llamada cuando se ha completado la transferencia de datos. El canal D es totalmente separado (fuera de banda) de los canales B, es esta señalización fuera de banda (out-of-band) la que proporciona un tiempo de conexión más rápido a ISDN. Sin embargo, para una eficiencia completa, el ancho de banda no requerido para la señalización y control sobre el canal D puede ser utilizado para transportar paquetes de usuario o frames de datos cuando sea necesario. La señalización del canal D es una función de las capas de nivel físico, de enlace de datos y de red del modelo de referencia OSI.

  Diferentes operaciones son desarrolladas para cada nivel del modelo de referencia OSI. A continuación se da una breve explicación de como el canal de señalización D trabaja dentro de cada uno de estos niveles.

6.2.5.4 Funciones de capa física

El protocolo de capa física de ISDN establece una conexión de conmutación de circuitos de 64Kbps. Este también soporta la interface física por el **adaptador terminal de red** (NTA: Network Terminal Adapter), el cual soporta la conexión de múltiples dispositivos simultáneamente. Finalmente, este protocolo administra la verificación del circuito y funciones de monitoreo.

6.2.5.5 Funciones de la capa de enlace de datos

La capa de enlace de datos de ISDN establece rutas virtuales a través de la red para los frame de datos. Este protocolo también maneja el control de llamadas y funciones de señalización por medio del **Procedimiento de Acceso al Enlace por el Canal** D (LAP-D Link access Procedure for D Channel), el cual es el procedimiento que trabaja cruzando la señalización o canal D.

6.2.5.6 Funciones de la capa de red

El protocolo de capa de red del ISDN maneja todos los servicios tanto de conmutación de circuitos como de conmutación de paquetes. La capa de red crea el direccionamiento y determina la información de ruta que la capa de enlace de datos usara para establecer las rutas virtuales.

6.2.5.7 Estándares de interface de usuario

El ITU-TSS ha definido dos estándares de interface de usuario ISDN:
ISDN ha desarrollado dos servicios estándar, llamados **Interfaces de Tasa**, las cuales combinan canales portadores y el canal de señalización en diferentes densidades. Estos son los llamados BRI y PRI.

6.2.5.7.1 Interface de Tasa Básica (BRI)

La **Interface de Tasa Básica** (BRI: Basic Rate Interface) consiste usualmente[147] de dos canales B y un canal D de 16Kbps para la señalización (2B+D), dando una tasa de datos en conjunto de 144 Kbps[148]. Los canales B se usan de forma simultánea pero independiente una de otra en conexiones diferentes o en la misma conexión.

Con esta finalidad se tiene la posibilidad de enviar de manera simultánea e independiente voz y datos de una sola o de diferentes terminales sobre una misma interface de usuario. El hecho de enviar la información de control por un canal distinto (o sea, el canal D) permite crear una tercera conexión para la transmisión de información de control y datos de baja velocidad a un usuario final.

La Interface de Tasa Básica fue diseñada para los dispositivos caseros o de pequeños negocios, tales como telefonía digital, terminales de datos, computadoras personales, fax e impresoras, debido a que la tasa de datos pico generadas en las aplicaciones que envuelven estos dispositivos están por abajo de 100Mbps.

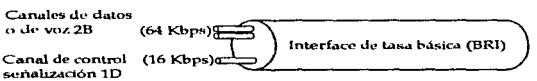


Figura 6.25 Interfaz de Red/Usuario BRI

[147] Algunos proveedores de ISDN, también pueden ofrecer un solo canal B y otro D (1B+D).
[148] Con velocidades hasta de 128Kbps, ISDN BRI provee una mucho mayor velocidad de ancho de banda que las soluciones basadas en módem analógicas con rangos desde 4.8 Kbps a 28.8 Kbps. Utilizando una proporción de compresión desde 2:1 a 4:1, este puede entregar tasas de transmisión efectiva desde 256Kbps hasta 632 Kbps.

6.2.5.7.2 Interface de Tasa Primaria (PRI)

La Interface de Tasa Primaria (PRI: Primary Rate Interface). Esta es una interface (23B+D)[149] en los Estados Unidos y Japón, y una interface (30B+D) en Europa.
Los canales B pueden ser adicionados para formar las configuraciones referidas en una terminología de intercambio local como servicios H (tabla 6.17 de servicios H). El canal D es un canal de 24 Mbps (o 31Mbps dependiendo del país), y controla los procedimientos de señalización para algunos o todos los canales B.

Las líneas pueden ser usadas como troncales para transferencia de archivos largos y flujos de datos continuos o ser subdivididos con un multiplexor para proveer múltiples canales para varios dispositivos.

La Interface de Tasa Primaria fue diseñada para ajustarse al manejo de video comprimido, dispositivos de audio de alta calidad y terminales gráficas de alta velocidad y dispositivos fax digitales, video teléfonos y teleservicios. Por ultimo cabe mencionar, que la tasa de datos transmitidos para los dispositivos que usan PRI llegan al rango de hasta los 2Mbps, esta es la interface ISDN equivalente a una interface de línea T1/E1 de 1.544 Mbps o 2.048 Mbps.

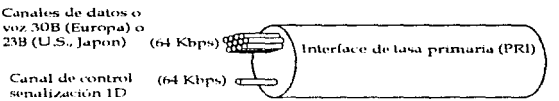


Figura 6.26 Interfaz de Red/Usuario PRI

6.2.5.7.3 Interface de Tasa de Banda Ancha

La interface de Banda Ancha es un tipo de estructura que esta basada en un par de formatos del llamado **Red Óptica Síncrona** (SONET: Synchonous Optical Network) definido por ANSI. La tasa de bits y la combinación de canales se eligen para unir la tasa de datos de algunas señales de televisión estándar que han sido digitalizadas ya sea por PCM o por alguna de las codificaciones de reducción de tasa (PCM diferencial adaptativo por ejemplo).

[149] Generalmente en la versión de 1.544 Mbps se obtiene como una combinación de los canales B y H0 y puede o no contener un canal D de 16Kbps, el más utilizado es el de 23+D (canal D=64Kbps) obteniendo 1536Kbps. La información del usuario se transmite por canales B y las señales de control por el canal D, además en cada trama se agrega un bit para señalización obteniéndose de esta forma una tasa global de 1.544 Mbps

Existen únicamente dos estructuras definidas:

- La primera equivale a 2016 canales B para una tasa de 129.024 Mbps.
- La segunda equivale a 8064 canales B para una tasa de 516.0096 Mbps.

La interface de banda ancha provee la capacidad requerida para la transmisión de cuadros de movimiento, televisión estándar y de alta definición, videoconferencias y datos de vídeo. La tasa de transmisión se puede extender hasta varios cientos de Mbps.

6.2.5.8 Como trabaja ISDN

En una red analógica, un ciclo de dos-alambres que van desde la oficina central de la compañía local hasta el usuario, soporta un solo canal de transmisión, el cual puede acarrear solamente un servicio (voz, datos o vídeo) a la vez. En cambio con ISDN, este mismo par de alambres de cobre trenzado es dividido lógicamente dentro de múltiples canales lógicos lo que permite tener varios servicios simultáneamente.

Por otro lado, el trafico de larga distancia entre oficinas de conmutación de teléfonos corren sobre enlaces troncales T1/E1 que consisten de cuatro alambres lógicamente divididos dentro de múltiples canales. ISDN utiliza la misma conexión canalizada para su transmisión de larga-distancia.

6.2.5.8.1 Designación de ancho de banda dinámico

La arquitectura de ISDN permite la designación de ancho de banda para ayudar a una velocidad de transmisión efectiva. Ancho de banda dinámico o designación de canal es la agregación lógica de ambos canales B dentro de BRI, para una capacidad total de 128Kbps, y cualquiera de todos los canales B para líneas PRI, para un rendimiento efectivo de hasta 1.536 Mbps en Estados Unidos y de 1.92 Mbps en Europa. También conocida como ancho de banda sobre demanda (bandwitdth on demand) o multiplexaje inverso, La agregación de canales es frecuentemente abreviada como Nx64 Kbps, donde N es el número de canales lógicos combinados.

6.2.5.9 Servicios sobre ISDN

La CCITT define en tres categorías de servicios de ISDN :

- **Servicios de portadora** (Bearer services): Estos son esencialmente las existentes redes analógicas o digitales que siempre se han especializado en entregar información de un punto a otro (incluyendo voz y datos ya sea de conmutación de circuitos o conmutación de paquetes).

Telefonía digital, incluyendo "toll free" inbound/out bonund.
Datos de conmutación de circuitos (a 64Kbps).
Datos de conmutación de paquetes (X.25) y datos Frame relay.

- **Teleservicios**: Los teleservicios son servicios sofisticados que ISDN puede proveer gracias a que ISDN opera a niveles muy altos en el modelo de referencia OSI y aun que todavía no se encuentran ampliamente utilizados, se espera que ellos sean la dirección hacia el futuro y el valor real de ISDN. Algunos de estos servicios son: correo electrónico, videotex, telefax, teletex y fax (facsimile) almacenamiento y reenvío, y videotelefonía (provee servicios de transmisión de televisión sobre ISDN).

- **Servicios de suplementarios**: Estos servicios suplementarios amplían las funciones tanto de los servicios de portadora como los servicios de teleservicio (por definición, los servicios suplementarios no se pueden encontrar solos). Estos comprenden mas las características asociadas con llamadas: fast dialing, calling line I.D, calling waiting, call forwarding, conferencing, etc. Cabe hacer notar que estos servicios suplementarios varían dependiendo del proveedor de ISDN el cual los puede ofrecer o no.

6.2.5.10 Los beneficios de ISDN para aplicaciones intensivas de datos

ISDN es cada vez más utilizada para proveer facilidades de redundancia para redes de área amplia en casos tales como recuperación de desastres y respaldo por marcaje en caso de saturación (backup overflow). Una conexión ISDN puede actuar como respaldo de bajo costo para una línea alquilada sobre una conexión dial-up de "pago solo por uso" basado en velocidad de línea comparable con las líneas alquiladas actuales como T1/E1. ISDN elimina el gasto de una segunda línea alquilada que puede estar sin utilizar la mayoría del tiempo.

Además, ISDN interopera con otros servicios de red de área amplia tales como, X.25, Frame Relay, como servicios existentes analógicos, **Servicio de Datos Multimegabit Conmutado** (SMDS: Switched Multimegabit Data Service), y servicios de más alta velocidad como ATM.

6.2.5.11 ISDN equipo para LANs

La instalación de equipo ISDN para redes LANs requiere de un puente o un enrutador con una interface ISDN. El enrutador ISDN es conectado directamente al cable ISDN, de manera que debe ser configurado no solo para enrutar tráfico hacia los segmentos apropiados, sino también para interoperar con la red ISDN.

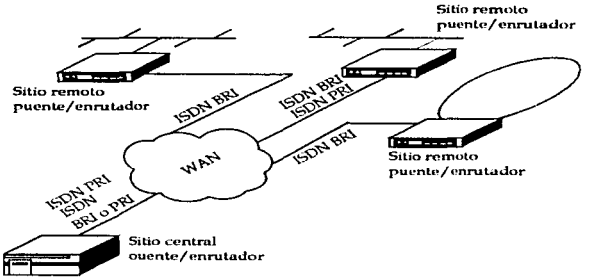


Figura 6.27 Interconexión remota de LAN a LAN a través de ISDN

6.2.5.12 Servicios Soportados por ISDN

ISDN soporta servicios de **conmutación de circuitos** (circuits-switched) y **conmutación de paquetes** (packets-switched). Además, dos servicios a nivel de frames, uno conocido como **Frame relay** y otro conocido como **Conmutación de Frames**, son también soportados.

Los dos servicios de modo de frame asociados con ISDN son: **Frame relay** y **Conmutación de frames**. El mismo esquema de señalización es usada por ambos servicios. La principal diferencia es que la red desarrolla procedimientos de control de error y flujo para cada frame dentro de la **Conmutación de frames**, en cambio en el servicio **Frame relay** no se desarrolla ninguna tarea de este tipo en los nodos intermedios y simplemente soporta un servicio de **mejor esfuerzo** (best-try). En la practica, Frame relay es por mucho el servicio dominante. Los procedimientos asociados con los servicios de frames son definidos en la recomendación CCITT I.122/Q.922.

6.2.5.13 El futuro de ISDN : Broadband ISDN

El ITU-T esta actualmente trabajando sobre las especificaciones para el modelo **ISDN de banda ancha** (B-ISDN: Broadband ISDN). El cuál entregará hasta 62.08 Mbps en una transmisión de datos de modo full dúplex. Por medio de estas altas velocidades se soportaran transmisiones interactivas sofisticadas, almacenamiento y envío de difusión multimedia, mensajes multimedia y servicios de reparación.

El estándar B-ISDN es también la base para el **Modo de Transferencia Asíncrono** (ATM: Asynchronous Transfer Mode).

6.2.6 Frame Relay

Frame relay es una red publica, de servicios de datos a nivel de área amplia y metropolitana. Enfocado al alto desempeño de las líneas alquiladas en el área amplia, pero minimizando el costo y con una mayor flexibilidad. Frame relay utiliza un avanzada tecnología de conmutación de paquetes lo cual lo hace una forma eficiente para proveer servicios orientados a la conexión entre localidades con características de ráfaga de trafico de diferentes tamaños y patrones impredecibles.

6.2.6.1 Historia de Frame Relay

Antes de que **Frame relay** apareciera como un protocolo en 1989, este fue una parte del estándar **ISDN** como el componente de **conmutación de paquetes** de ISDN, Frame relay fue diseñado para proveer un servicio de transmisión de datos por medio de conmutación paquetes a muy alta velocidad (como tal es mejor situado para transferencias de datos a velocidades debajo de 2 Mbps)[150] para proveer conectividad entre dispositivos; fue entonces que los que desarrollaron Frame relay hicieron posible que los principios detrás del protocolo pudieran ser aplicados fuera del esquema de ISDN.

Frame relay es un protocolo que conecta redes de área local sobre una red publica o privada de conmutación de paquetes. En esencia, un frame proveniente de una red LAN es encapsulado en un paquete de Frame relay, posteriormente es transmitido a través de la red hacia su destino. Frame relay utiliza técnicas de **multiplexaje estadístico** para cargar los datos provenientes de múltiples orígenes a la salida de una sola línea hacia la red, es decir, los flujos de datos son partidos en bloques de datos (frames) y entonces, multiplexados estadísticamente sobre una ruta de transmisión.

El servicio Frame relay comúnmente esta disponible en velocidades de fraccional T1 (fraccional E1) y T1 (E1) completo, aun que algunos proveedores ofrecen velocidades de hasta T3 (45Mbps). [151]

6.2.6.2 Estandarización de Frame Relay

Actualmente dos importantes comités llevan a cabo el estándar de Frame Relay. En Estados Unidos, el trabajo es manejado por ANSI (trabajo T1S1) y el segundo es el

[150] Cabe hacer notar que nada limita a frame relay ser definido a velocidades mayores de 2 Mbps, pero esto no ha sido llevado a cabo.
[151] Para mayor información referirse al Anexo E.

CCITT y el grupo LMI (Local Management Interface). El trabajo técnico sobre Frame relay fue terminado en 1991.

6.2.6.3 Principios de Frame Relay

En Frame relay, los datos son divididos dentro de frames de longitud variable (que no excedan de 8,189 bytes) como la unidad básica para la transmisión de datos, donde cada uno contiene información de direccionamiento que es utilizada por la red para enrutar estos a través de los conmutadores.

Frame relay tiene la apariencia de ser un protocolo de conmutación de paquetes común[152]. De hecho la diferencia entre Frame relay y las redes de conmutación de paquetes, es que estas ultimas, operan hasta el nivel 3 del modelo de referencia OSI, mientras que Frame relay opera hasta el nivel 2 (haciendo notar además, que Frame relay, no desarrolla todas las funciones que se especifican en el nivel 2), esto significa que Frame relay es un protocolo mas sencillo que otros protocolos de conmutación de paquetes (ej. X.25).

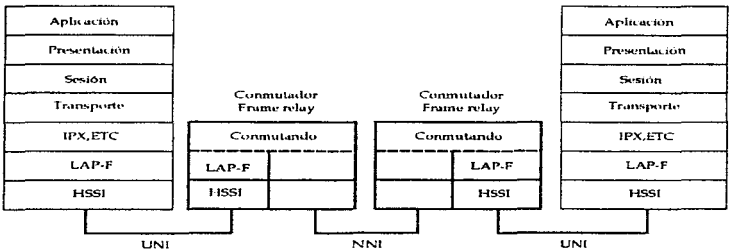


Figura 6.28 Frame relay en el modelo de referencia OSI

Al ser desarrollado bajo el pensamiento de que el medio de transmisión es eficaz y relativamente libre de errores y teniendo en cuenta, que las aplicaciones del usuario final pueden detectar y recobrar los paquetes erróneos. Tales motivos son por los cuales, Frame relay delega sobre los protocolos de las capas superiores de los sistemas finales (punto a punto) el desarrollo de la retransmisión y recuperación de errores, significando que Frame relay requiera menos procesamiento en los nodos intermedios y en consecuencia un menor retraso al cruce de la red. Debido a esto, todos los frames validos son procesados muy

[152] Para mayor información referirse al Anexo D.

rápidamente (como ellos van pasando al cruzar la interface de red). Al usar solamente la mitad de la capa 2, Frame relay desarrolla únicamente la detección de errores (no lleva a cabo la corrección de estos, es decir, no tiene la función de retransmisión ni desarrolla alguna función de control de flujo) por lo que los frames inválidos son simplemente desechados, ya que espera que estos sean retransmitidos por los sistemas finales (end systems). Esta capacidad habilita a los nodos de Frame relay a pasar trafico de datos mas rápidamente, permitiendo transmitir altos volúmenes de tráfico a mas grandes velocidades de canal sin la necesidad de incrementar el tamaño y el costo de los equipos.

La conmutación de Frame relay tiene tres funciones principales:
- Enrutar frames de entrada y escoger el puerto de salida apropiado.
- Examinar el campo de verificación del frame para determinar si el frame contiene un error, y de resultar erróneo, descartarlo.
- Verificar si la memoria de almacenamiento (buffer) esta llena, de ser así, descartar los frames de entrada hasta que llegue a descongestionarse.

6.2.6.4 Interfaces de acceso a Frame Relay

Frame relay actualmente es un servicio **orientado a conexión**, por lo tanto una transferencia de datos conducida entre dos puntos finales sobre una red Frame relay requiere del establecimiento de una ruta virtual. Estas rutas son los llamados **circuitos virtuales** o **rutas virtuales** (VC: virtual circuit o virtual paths) que en el caso específico de Frame relay son referidos como **conexión de enlace de datos** (DLC: Data Link Connection).

Los dos tipos de circuitos virtuales soportados por el estándar Frame relay son: **circuitos virtuales conmutados** (SVC: switching virtual circuit) y **circuitos virtuales permanentes** (PVC: permanent virtual circuit).[153]

Un **Circuito Virtual Permanente** (PVC: permanent virtual circuit) es una ruta de conexión punto-a-punto a través de la red Frame relay de manera permanente desde el momento en que el usuario hace una subscripción a la red Frame relay.

Circuitos Virtuales Conmutados (SVC: switching virtual circuit) es un circuito virtual que se establece de manera dinámica sobre una base de demanda, es decir, se establece la conexión cuando sea necesario y se dará de baja una vez que la sesión de comunicaciones se haya terminado.

Con los Circuitos Virtuales Conmutados (SVCs), el usuario es capaz para usar paquetes de control para establecer o terminar circuitos virtuales aun cuando se lleva a cabo la transferencia de datos.

---

[153] Para mayor información referirse al Anexo D.

Cada DLC (sea PVC o SVC) tiene un numero de identificación de canal lógico llamado **Identificador de Conexión de Enlace de Datos** (DLCI: Data Link Connection Identifying). El cual permite enrutar cada frame de manera enlace-a-enlace (salto a salto por su significado local) perteneciente a una ruta virtual definida. Por su alcance local, este identificador va cambiando como el frame va atravesando los enlaces (mapeandose en cada conmutador intermedio por medio de tablas de enrutamiento) de la ruta virtual. [154]

Las tablas de enrutamiento en cada conmutador Frame relay que interviene en la ruta toma cuidado de enrutar los frames hacia su destino propio, alternando la lectura del DLCI del que provienen y asignándole al frame la información del nuevo valor del DLCI de salida.

Los DLCIs forman el esquema de direccionamiento de Frame relay. Cada conexión virtual permanente (PVC) sobre una UNI tiene su propia DLCI. Por lo tanto, El DLCI es una dirección de alcance local y solo hace razón cuando combinado dentro de la UNI sobre el PVC que esta[155]. Al conocer el UNI y el numero DLCI, se puede conocer el PVC sobre el que se esta tratando. Los números DLCI en cada punto final del PVC pueden ser los mismos, o pueden ser diferentes.

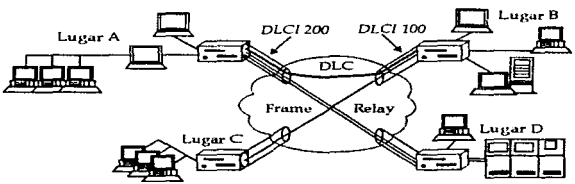


Figura 6.29 Vista conceptual del esquema de direccionamiento de Frame Relay

6.2.6.5 Ancho de banda sobre demanda (Multiplexaje estadístico)[156]

La capacidad de proveer el ancho de banda sobre demanda hace que Frame relay sea un buen protocolo para trafico de ráfagas de datos (bursty). El ser eficaz para proveer ancho de banda agregado es el resultado del uso del multiplexaje estadístico de Frame relay, el cual no requiere que el enlace se encuentre

[154] Por su naturaleza local, los DLCI de una conexión frame relay pueden ser iguales o diferentes en el sitio origen y el del final remoto.
[155] Conociendo el DLCI de un PVC sin conocer el correspondiente UNI deberá ser análogo a conocer en que calle vive una persona y el numero pero sin conocer la ciudad en la que vive.
[156] Para mayor información referirse al Anexo B.

establecido y dedicado todo el tiempo. Por el contrario, Frame relay utiliza el ancho de banda solo cuando existen datos que requieren transmitirse. [157]

A diferencia de las líneas alquiladas, en Frame relay se pueden establecer dos velocidades de conexión: **tasa de información de entrega** (CIR: committed information rate) y la **tasa de información excedente** (EIR: excess information rate).

El CIR es el mínimo ancho de banda disponible, determinado por una estimación del trafico normal del usuario, si el trafico de red incrementa pasando el CIR, la nube Frame relay intentará abrir circuitos adicionales y completará la transmisión (esto se realiza solo cuando la red no se encuentra congestionada).

El multiplexaje y el esquema de direccionamiento utilizados por Frame relay permiten a grandes sitios ser conectados a la nube por medio de un solo puerto de enrutador y una sola conexión de alta velocidad hacia la nube.

6.2.6.6 Acceso a Frame relay (dispositivos de acceso)

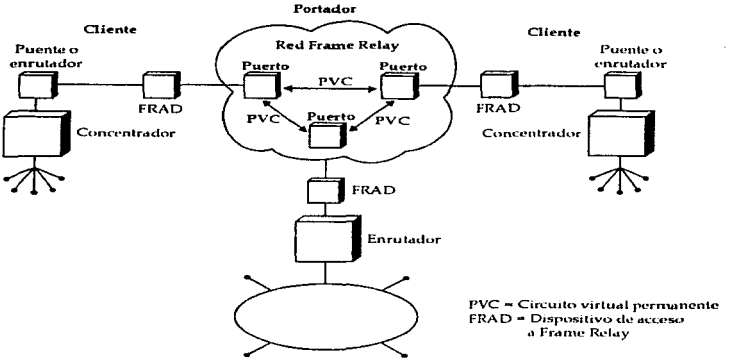
Las redes Frame relay están construidas de manera externa al equipo de los clientes, por lo que se debe tener una línea de acceso a Frame relay, es decir, los puntos origen y destino se comunican desde sus localidades hacia la nube Frame relay, sobre conexiones de líneas alquiladas (puntos de acceso), las cuales son generalmente :

56/64 Kbps sobre conmutación 56 o líneas ISDN.
128 Kbps sobre líneas ISDN premisa.
384Kbps a 1.544 Mbps sobre T1 fraccional o líneas T1.

6.2.6.7 Equipo del usuario

Una red LAN tiene acceso a Frame relay a través de un dispositivo llamado **Interface de Red de Usuario** (UNI: Unit Network Interface). Las interfaces UNI más comúnmente utilizadas, son los llamados **Dispositivo de Acceso a Frame Relay** (FRAD: Frame relay Access Device) o en otros casos los enrutadores. Estos deberán ser conectados a una **Unidad de Servicios de Datos** (DSU: Data Service Unit), si el usuario es conectado a un punto de acceso 56Kbps, o a un **DSU/CSU** (Unidad de servicio de Datos / Unidad de Servicios de Canal), si es conectado a un punto de acceso ISDN o una línea T1.

[157] Otros, transportadores de redes WAN mas tradicionales ocupan multiplexaje por división de tiempo, por medio del cual, cada transmisión de datos requiere un ancho de banda dedicado para el cruce por la red



6.30 Ejemplo de una conexión Frame Relay

6.2.6.7.1 FRAD

Un **Dispositivo de Acceso a Frame relay** (FRAD: Frame relay Access Device) es generalmente un dispositivo unitario (stand alone) que recibe los datos que provienen de la red LAN sobre uno o mas puertos seriales, encapsulando los datos dentro de paquetes de Frame relay y los envía hacia el punto de acceso a través de la DSU o DSU/CSU. De manera contraria, este recibe paquetes que provienen del punto de acceso, separa a cada paquete de su encabezado y suma de verificación para que posteriormente los envíe al puerto serial de salida apropiado.

6.2.6.7.2 Enrutadores

Un enrutador es un dispositivo de red local dentro del cual el usuario puede insertar una tarjeta de expansión que provea el acceso a Frame relay. La tarjeta encapsula los datos de entrada de la red LAN dentro del enrutador desde el ambiente de computación interno (LAN) en paquetes Frame relay y los envía al DSU/CSU hacia el punto de acceso de la central telefónica. De manera contraria, recibe los paquetes de la red provenientes del punto de acceso, separando a cada uno de su encabezado y suma de verificación, y los maneja dentro del enrutador mismo, el cual los envía hacia el puerto salida de red LAN apropiada.

En general, los enrutadores y los FRADs soportan muchas de las características de Frame relay. Los FRAD son utilizados para aplicaciones y protocolos específicos, mientras que los enrutadores son designados para manejar múltiples protocolos e integrar tráfico de datos dentro de una red de backbone. Por lo anterior, cabe hacer notar que los FRADs son mas baratos que los enrutadores, pero estos últimos son frecuentemente utilizados en ambientes multi-LAN que requieren un punto de acceso a Frame relay.

6.2.6.7.3 DSU y CSU/DSU

Los DSU y CSU/DSU son dispositivos usados para terminar la conexión física 56 Kbps o T1 provenientes de la compañía telefónica local. Todos los FRADs y enrutadores requieren un DSU o un DSU/CSU para conectarse a los servicios de Frame Relay.

Por último, se debe saber que un solo CSU/DSU y un puerto de enrutador o FRAD son necesarios solamente para que cada sitio tenga múltiples conexiones lógicas, salvando el costo de equipo y de circuitos[158].

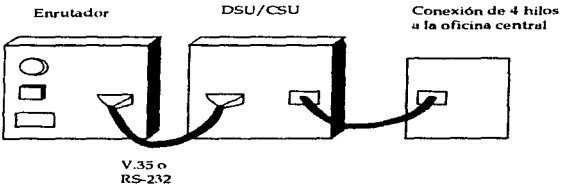


Figura 6.31 Equipo de acceso a Frame Relay

6.2.6.8 Usando Frame relay para la comunicación de red LAN a LAN

Frame relay soporta múltiples protocolos y su habilidad para manejar ráfagas de tráfico (bursty traffic) hace de éste, un transporte ideal para llevar trafico en una comunicación LAN-a-LAN. Esto provee los siguiente beneficios:

El ancho de banda de Frame relay puede ser escalado fácilmente desde menos de 56Kbps hasta 1.5Mbps, habilitando a los usuarios para conectar mas y mas redes LAN en la disposición de compartir los datos y construir aplicaciones cliente servidor de área amplia.

[158] A diferencia de un canal físico, el cual es un puerto sobre una computadora o un multiplexor, un canal lógico es solamente una conexión temporal que es hecha entre porciones de la red.

Frame relay simplifica las conexiones a redes WAN al proveer una interface estándar, habilitando a los usuarios a conectarse a varios tipos diferentes de equipos de interconexión de red, incluyendo FRADs, enrutadores, puentes y concentradores.

Además, cuando es usado para interconectar redes locales de una organización a su oficina principal, habilita a la organización a administrar las redes LAN de manera remota, reduciendo el número de personal de administración de red requerido para cada sitio.

6.2.6.9 Usando Frame relay sobre ISDN

Algunos proveedores de servicios Frame relay actualmente habilitan a sus usuarios a conectarse a sus servicios sobre una línea ISDN. Frame relay sobre ISDN, está en la espera de un crecimiento significativo por las siguientes razones: Frame relay está basado fuertemente sobre el protocolo de capa de enlace de datos de ISDN llamado **Protocolo de Acceso a Enlace Llamada de Señalización D** (LAP-D: signaling called Link Access Protocol D) ya que fue originalmente destinado a ser un portador de servicio ISDN. Además de que, Frame relay puede ser usado para acarrear datos sobre servicios ISDN ofreciendo conexiones de conmutación de circuitos a 64 Kbps, 384Kbps y 1536 Kbps. En otras palabras Frame relay es completamente compatible con ISDN.

Las líneas BRI de ISDN generalmente tienen un costo substancial menor y proveen mas que dos veces el ancho de banda que las líneas alquiladas de 56Kbps.

6.2.6.10 Frame relay y Cell Relay: Relación con ATM

Frame relay y Cell Relay son protocolos orientados a paquetes, la diferencia consiste en que Frame relay es un protocolo de acceso a red para tráfico de datos[159], y cell relay es un método de conmutación diseñado para llevar voz, datos y video cruzando un backbone de red de área amplia de alta velocidad (que promete ser el mas grande integrador de servicios). Las ventajas de Frame relay llegan a ser significativas en una red de cell relay. Uniendo los dos protocolos, estos ofrecen: una interfaz estándar para equipo existente y un movimiento eficiente sobre la red de área amplia ya que los datos de Frame relay son capaces de tomar ventaja de la conectividad lógica y características de enrutamiento de un backbone de red cell relay.

Dos principales consorcios industriales han estado trabajando cooperativamente para definir el estándar de convenios de implantación de relación de trabajo Frame

[159] Aun que actualmente ya se encuentran trabajos de transporte de tráfico de voz sobre Frame relay.

Relay/ATM en 1994. El desarrollo de este estándar significa que el equipo Frame relay sea capaz de enviar datos a equipo basado en ATM y viceversa. Esto también significa que el equipo Frame relay puede enviar datos a otro equipo Frame relay a través de una red basada en ATM. La función principal por tanto, es la de trasladar el protocolo Frame relay dentro de los apropiados protocolos ATM y viceversa.

6.2.7 Otros Servicios de interconexión de Redes de Área Amplia (WAN)

La interconexión de sitios remotos hacia sistemas principales de redes locales en sitios-centrales requieren enlaces de redes de área amplia de alta velocidad. Los administradores de red tienen un número de opciones de servicios de WAN para escoger, como son:

ISDN
Dial-up Analógico
Conmutación 56
X.25
Líneas alquiladas dedicadas punto-a-punto
Frame Relay
Cable
SMDS
ATM (cell relay)

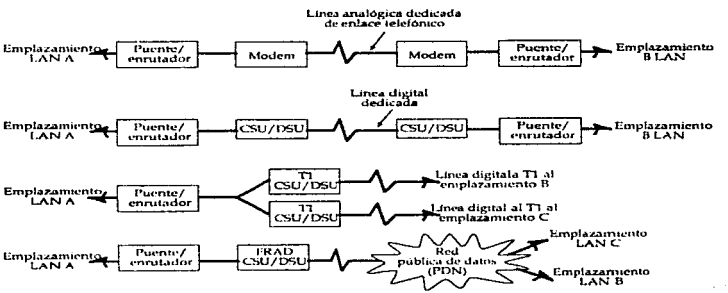


Figura 6.32 estrategias de conexión de WAN

Algunas de estas tecnologías y servicios tienen normalmente un costo-efectivo de conectividad hacia aplicaciones hacia sitios distantes LAN-a-LAN. En el México actual las necesidades de comunicación y transmisión de información han crecido enormemente y en un corto tiempo la tecnología ha permitido que el volumen de datos y la rapidez con que éstos se transmiten sea cada vez mayor. Por otro lado, México está experimentando la globalización en el ámbito de las telecomunicaciones, muchas compañías tanto nacionales como extranjeras comienzan a ofrecer sus servicios. Es por esto, que escoger la mejor opción envuelve la evaluación con factores tales como disponibilidad de servicios en locaciones, tipos de aplicaciones de red a ser soportadas, el ambiente de interconexión entre otros puntos.

A continuación se hace una breve explicación de los servicios de interconexión WAN existentes actualmente en el mundo.

6.2.7.1 La red telefónica pública conmutada (Servicio de Dial-up analógico)[160]

El servicio de red telefónica pública conmutada referido también como Dial-up analógico es un servicio de conmutación de circuitos que corre sobre líneas telefónicas estándares y es optima para comunicaciones de voz[161]. Este, es el servicio mas ambiguo de transmisión de que provee conectividad a través de todo el mundo. Los servicios de Dial-up son generalmente utilizados cuando el acceso a uno o mas dispositivos remotos no justifica el costo de una línea dedicada alquilada. Las aplicaciones típicas incluyen telecomunicaciones, interconexión de redes de nodo-a-LAN remota, dial-up automático como recuperación a desastre para una línea alquilada que se encuentra en fallo, e Internet u otro acceso de servicio de información en línea.

En la mayoría de los casos, los proveedores de servicio de Dial-up analógico no garantizan un soporte para velocidades específicas de transmisión de datos, aun cuando los usuarios se conectan por medio de modems analógicos a tasas de transmisión de 28.8 Kbps o mas; debido a que la máxima tasa de transmisión es generalmente de 19.2 Kbps. También, la calidad de línea varia ampliamente y la cantidad de ruido sobre una línea tiene un decremento directo sobre la velocidad máxima de transmisión de datos.

---

[160] Para mayor información referirse al Anexo E.

[161] Cuando levantamos el telefono e intentamos comunicarnos a un punto distante estamos utilizando la red telefónica pública conmutada. Una comunicación consta de tres fases que son: el establecimiento del circuito (se marca), la transmisión de la información(se habla) y la liberación del circuito (se cuelga). Sobre esta red se puede, adicionalmente, transmitir datos utilizando un módem. Para la transmisión de datos por módem, la cantidad de datos que se pueden transportar y la velocidad para enviarlos se encuentra limitada (a 33.6 Kbps en 1996), además de tomar en cuenta que la velocidad máxima que puede lograrse depende de la calidad de la trayectoria utilizada para cada llamada.

6.2.7.2 Servicio de conmutación 56 (SW56)

El servicio de Conmutación 56 (SW56: Switched 56 Service) provee una alternativa de bajo costo para líneas digitales privadas. Su operación es similar al estándar del servicio Dial-up analógico, excepto que la transmisión es digital, a una velocidad de 56 Kbps y es utilizado para aplicaciones de transmisión de datos únicamente. Por último, cabe mencionar que el servicio de conmutación 56 puede ser utilizado para enlazar redes ISDN en lugares donde ISDN aun no ha sido desarrollado.

6.2.7.3 Servicio de conmutación X.25[162]

X.25 es quizá el protocolo estándar más ampliamente utilizado. Este ha sido usado como una manera costo efectivo para proveer interfaces entre sistemas anfitrión y redes de conmutación de paquetes durante varios años. Basado en estándares internacionales provee transferencia de datos síncronos sobre una red conmutada pública a velocidades de transmisión de datos de hasta 56 Kbps. X.25 es comúnmente usado para comunicación de anfitrión de terminal remota, para aplicaciones tales como ordenamiento de entrada, mensajería electrónica, verificación de tarjetas de crédito, etc.

La tecnología de conmutación de paquetes X.25, automáticamente designa el acceso de ancho de banda disponible y maneja de manera eficiente las ráfagas de tráfico inherente en el ambiente de redes LAN. Además, X.25 provee seguridad de datos, una detección de errores de manera automática y facilidades de corrección; aun que cabe mencionar que por estas características se consume una parte del ancho de banda disponible.

6.2.7.4 Servicio de líneas dedicadas alquiladas punto a punto[163]

Líneas privadas alquiladas. Una línea privada es una línea alquilada a una empresa de telecomunicaciones por cierto período de tiempo, lo que permite tenerla disponible las 24 horas del día y evita el acceso de alguien más a ella. Hay dos tipos de líneas privadas: las analógicas y las digitales. Estas últimas se usan en mayor medida para la comunicación de datos por la calidad de transmisión que ofrecen. La oferta en México incluye el uso de pares de cobre, radio-enlaces, microondas, enlaces satelitales y fibra óptica.

Actualmente, la mayoría de las conexiones de redes WAN en el mundo, consisten de líneas digitales privadas alquiladas operando a 56Kbps o 1.544 Mbps (tasa T1) en los Estados Unidos y a 64 Kbps o 2.048 Mbps (tasa E1) en Europa. Las transmisiones punto-a-punto de alta velocidad, son utilizadas en ambientes donde la seguridad y control son de principal importancia. Las líneas alquiladas punto-a-

[162] Para mayor información referirse al Anexo C.
[163] Para mayor información referirse al Anexo E.

punto, consisten de una línea de comunicación digital dedicada entre dos puntos y provee una cantidad constante de ancho de banda a una velocidad fija.

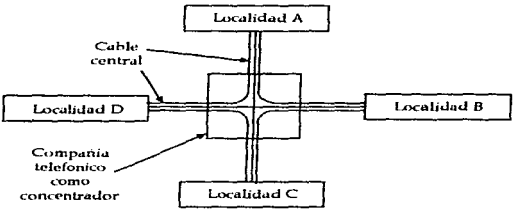


Figura 6.33 Red privada de línea dedicada

Generalmente, las tarifas de cobro se encuentran basadas en la combinación del ancho de banda provisto y la distancia entre las localidades.

Por ultimo, cabe señalar que las líneas privadas dedicadas no proveen ninguna forma de eficiencia inherente en la transmisión de tráfico de ráfaga y son frecuentemente subutilizadas, algunas veces corren tan solo a un 5 o 20 por ciento de su capacidad total. En adición a una conexión punto-a-punto, una interconectividad redundante completa requiere de una muy cara topología de malla y equipo del usuario.

Por lo anterior, Fraccional T1 (E1 en Europa) ofrece una capacidad alta, ya que su diseño de servicio digital privado soporta múltiples canales de 64 Kbps. Con este servicio, los subscriptores a WAN pueden alquilar uno de varios canales de 64 Kbps en lugar de un tubo completo T1 (T1 pipe). Este servicio ofrece el mismo tipo de control, administración y características de seguridad como el tubo T1 completo. Pero por otro lado, con sus mismas desventajas; aun que los costos son menores para la topología de malla completa.

Es importante mencionar que la oferta de telecomunicaciones en México incluye un servicio relativamente novedoso de conducción de señales punto a multipunto que permite comunicar a un punto central con hasta 30 puntos remotos. En el punto central se tiene acceso E1 canalizado y en cada uno de los puntos remotos un acceso E0.

6.2.7.5 Servicio de Cable

La industria de transferencia por cable, esta empezando a construir enlaces WAN TCP/IP. Estos, pueden soportar velocidades de línea que van desde 500Kbps hasta 30Mbps. Aun que actualmente se encuentran bajo desarrollo, los usuarios a los que principalmente va dirigido este servicio de WAN por cable son los usuarios de computadoras personales que se encuentran en su hogar, los cuales requieren acceso a información sobre una línea mas rápida o de televisión interactiva. El dispositivo de acceso al cable, incluye una tecnología de módem para convertir la señal analógica en datos digitales que son usados por la computadora. El tubo de red mismo es incrementalmente una fibra óptica o un híbrido de fibra óptica y coaxial diseñado por dos maneras de comunicación en una configuración asimétrica.

La desventaja de las redes sobre cable, son su reputación de un servicio no muy confiable y el hecho de que el ancho de banda es compartido. Si uno de los usuarios en el enlace WAN corre una aplicación que consume un gran ancho de banda, otros usuarios sufrirán. Es por esta razón que las compañías de transferencia por cable están actualmente diseñando modelos de red distribuidos que deberán conectarse a pequeños grupos de usuarios hacia múltiples puntos de presencia para resolver este problema. Por último, cabe mencionar, que las redes de transmisión por cable no están actualmente estandarizadas por lo cual faltan algunos años para que el proceso de estandarización se lleve a cabo.

6.2.7.6 SMDS

SMDS es una servicio de transporte de datos de conmutación de celdas sin conexión utilizado para interconectar múltiples nodos LAN de empresas través de la red de telefonía pública. De hecho, SMDS fue diseñado para ser el servicio de datos sin conexión para la tecnología ATM. SMDS es un servicio estándar que puede ser usado como un backbone de red, que de igual manera puede conectar redes Ethernet, Token Ring y FDDI. Debido a su naturaleza sin conexión, SMDS elimina la necesidad de conmutadores para establecer una llamada de conexión entre dos puntos antes de que se transmitan los datos. Los dispositivos de acceso SMDS pasan datagramas de 53 bytes que incluyen información de direccionamiento hacia el conmutador que reenvía las celdas sobre cualquier ruta disponible hacia su destino. Los datos viajan sobre rutas menos congestionadas en una red SMDS, brindando de esta manera transmisiones mas rápidas, seguras y una gran flexibilidad.

SMDS es algunas veces referido como CBDS (Connectionless Broadband Data Service).

A continuación demuestran algunas características de los servicios de WAN.

6.2.8 Comparación de servicios de WAN

	Red Telefónica Pública	Conmutación 56	X.25	Líneas privadas alquiladas
Tipo	Conmutación de circuitos, público	Conmutación de circuitos, digital, privado.	Conmutación de paquetes, público o privado	Conmutación de circuitos punto-a-punto, privado
Ancho de Banda	64 Kbps voz 9.6-28.8 Kbps datos	56 Kbps	<= 56 Kbps datos	T1:1544Mbps datos (E.U). E1: 2.048Mbps datos (Europa)
Aplicaciones	Voz y datos sobre líneas separadas	Voz y datos sobre líneas separadas	Protocolo para ambientes de transmisión de datos de terminal-a-anfitrión	Alta velocidad transmisión voz y datos para aplicaciones basadas en transacción y acceso a Internet
# de sitios por costo efectivo	Ilimitado	Ilimitado	Ilimitado	Pocos
Ventajas	*Amplia disponibilidad *Conectividad cualquier-a-cualquier *Bajo costo	*Amplia disponibilidad *Conectividad cualquiera-a-cualquiera *Costo moderado *Números telefónicos de uso estándar	*Amplia disponibilidad *Eficiente para ráfagas de tráfico *Conectividad cualquiera-a-cualquiera *Detección de error, corrección automática y seguridad *Protocolos actualmente estándar. *Fácil implantación de múltiples conexiones y expansión sin necesidad de altos costos *Tecnología madura	*Alta velocidad *Eficacia *Alto grado de administración y seguridad *Estándar *Conexión directa a Internet
Limitantes	*Ancho de banda limitado *Ganancia ineficiente soportando explosión de trafico versus trafico continuo	*Solo para datos *Ancho de banda limitado Requiere CSU/DSU.	*Ancho de banda limitado a partir de que la detección de error limita la velocidad *Incrementa el costo; marginal para la interconexión a LAN	*Completa topología de malla muy cara
Disponible en México	Sí	No	Sí	Sí

Tabla 6.18a Comparación de WAN

servicios

	Frame relay	Cable	SMDS	ISDN	ATM (Broadband ISDN)
Tipo	Conmutación de paquetes, público o privado	punto-a-punto, privado	Conmutación de celdas, público	Conmutación celdas o paquetes, público	Conmutacion de celdas, tecnologia de conmutación pública
Ancho de Banda	64 Kbps-1.544 Mbps de datos	500 Kbps - 30 Mbps datos y video	N×56/64 Kbps datos (o paquetes de voz o video) (1.544-45 Mbps generalmente)	64-128 Kbps para BRI voz, video y datos. 1.544-2,0 Mbps para PRI voz, video y datos.	11 Mbps- 622 Mbps voz, video y datos (25-155 Mbps generalmente)
Aplicacion	*Optimo para datos *Ambiente punto-a-punto	*Internet en-linea y acceso a información *Conexion a redes locales, video	*Optimo para datos, *Ambiente multipunto	*Optimo para voz, datos y video integrado sobre una sola linea digital.	*Optimo para conmutación de voz, datos y video.
# de sitios por costo efectivo	*Reemplazamiento de linea alquilada privada *Costo efectivo para pocos sitios fijos	Ilimitado	Costo-efectivo desde cuatro o más sitios	Ilimitada	Para usuarios poderosos, adoptado precozmente; inicialmente aplicaciones del sistema principal para red local
Ventajas	*Alta velocidad, baja latencia *Ancho de banda sobre demanda. *Fácil escalabilidad *Protocolos estándar *Conectividad punto-a-punto *Eficiente para ráfagas de tráfico	*Alta velocidad *Infraestructura existente *Configuración de llamada rapida	*Alta velocidad, baja latencia *Conectividad cualquiera-a-cualquiera *Económico para redes de malla virtuales *Actualmente estándar *Fácil para realizar cambios.	*Alta velocidad *Datos digitales, voz, imagenes video integrado sobre linea *Configuración de llamada rapida *Seguro, eficaz, estable, conectividad digital *Eficaente para ráfagas de tráfico *Actualmente estándar.	*Muy alta velocidad *Datos, voz video integrados sobre linea *Configuración de llamada rapida *Segura, eficaz *Conexión digital estable *Eficiente para ráfagas de tráfico.

Tabla 6.18b Comparación servicios de WAN

	Frame relay	Cable	SMDS	ISDN	ATM (Broadband ISDN)
Limitantes	*Requiere un acceso de línea dedicado *No ampliamente desarrollado en Europa *Caro y complicado para hacer movimientos o cambios *Confía en que los usuarios finales se encarguen de la corrección de errores y control de flujo *Es propenso a sufrir congestionamiento en la red[164]	*Voz sobre línea separada *Ancho de banda dividido entre usuarios sin capacidad de firewall (paredes de fuego) *Servicio delicado *Frecuentemente una manera de transmisión.	*No ampliamente usado en stados Unidos y Europa.	*Tarifa de tasas inconsistente *Puede ser complicado para instalar y configurar *No es aún universal.	*No es aún ampliamente disponible *Bajo desarrollo aún los detalles de estandarización *Productos actuales caros *Productos propietarios tienen problemas de compatibilidad multiproveedor debido a la carencia de estándares.
Disponible en Mexico	Si	No	No	No	No

Tabla 6.18c Comparación servicios de WAN

[164] Esto puede ocurrir, si en ciertos momentos la mayoría de los usuarios mandan simultáneamente sus ráfagas de tráfico.

CAPÍTULO 7
ESTADO ACTUAL DE LA RED DEL INSTITUTO DE INGENIERÍA

Es importante para cualquier estudio, realizar una etapa de revisión del sistema actual para así poder desarrollar un diagnóstico que sirva de base para diseñar soluciones técnicas o administrativas de acuerdo a la naturaleza del problema.

7.1 Red del Instituto de Ingeniería

El Instituto de Ingeniería de la UNAM cuenta con una red de área local en el campus de Ciudad Universitaria y que forma parte de Red UNAM. El Instituto utiliza una plataforma de computo distribuido cliente-servidor, es por esta razón que uno de los pilares principales sobre el que se basa la tecnología de cómputo en el Instituto es su infraestructura de red, también conocida como REDII. La cuál se encuentra basada en una tecnología de red tipo Ethernet a 10 Mbps.

El Instituto cuenta actualmente con alrededor de 300 puntos de red distribuidos en 5 edificios[165] que están unidos por una estructura de backbone de bus con cable coaxial grueso tipo RG/58 cumpliendo las normas especificadas en el estándar Ethernet 10Base5 de IEEE 802.3.

En el interior de cada uno de los edificios se tiene una tecnología Ethernet 10BaseT basado en un sistema de cableado estructurado que cumple con las normas del estándar EIA/TIA 568 y se conectan al backbone a través de dispositivos de comunicación tales como concentradores y puentes, estos dispositivos cumplen con las normas de monitoreo y administración SNMP[166]. Por último, cabe mencionar que la REDII se enlaza a RedUNAM a través de un enlace de fibra óptica (multimodo 62.5/125) a un enrutador Cisco (modelo AGS +). De esta manera, nuestra comunidad puede utilizar los recursos de cómputo de toda la UNAM incluyendo la supercomputadora CRAY YMP y mantenerse comunicada con universidades, centros de investigación, entre otros organismos tanto a nivel nacional como internacional. [167]

---

[165] El Instituto de Ingeniería esta comprendido por 8 edificios de los cuales solo 5 se encuentran actualmente conectados a la REDII, los 3 edificios restantes se planea integrarlos en un futuro cercano por lo cual entran dentro de los planes de este trabajo escrito.

[166] Protocolo de Administración de Red Simple (SNMP: Simple Network Management Protocol).

[167] Por medio de REDUNAM se tiene salida hacia redes nacionales como MEXNET y RUTYC e internacionales como BITNET, INTERNET, NSFNET, EARN entre otras.

Se tiene un total de 35 estaciones de trabajo sobre plataforma Unix (WorkStations) interconectadas (de los cuales 3 son los servidores principales de servicios de TCP/IP Internet), 4 computadoras personales servidores con plataforma Novell Netware (ver 3.11) y alrededor de 500 equipos entre computadoras personales y periféricos.

A continuación se muestra dos figuras 7.1 y 7.2, en la primera se muestra la ubicación física de los edificios que componen el Instituto de Ingeniería, y en la segunda figura se esquematiza la situación actual de la REDII

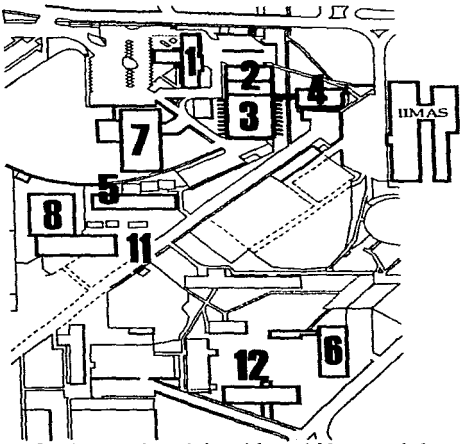


Figura 7.1 Ubicación física de los edificios del Instituto de Ingeniería.

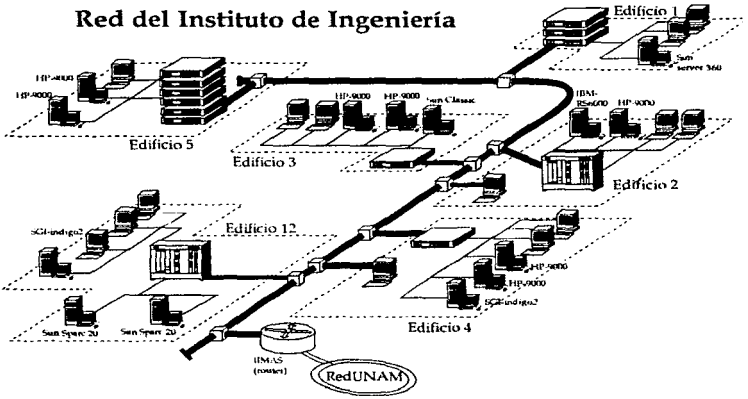


Figura 7.2 Estado actual de la red del Instituto de Ingeniería

En primer lugar, solo están interconectados al backbone 5 edificios del Instituto de Ingeniería a la REDII. Teniendo planes dentro del estudio que este trabajo comprende, de poder integrarlos a esta. Los edificios interconectados son : el edificio 1, 2, 4, 5 y 12. Que como se mencionó anteriormente, están conectados por medio del backbone de cable coaxial RG/58.

El sistema de cableado intraedificio cumple con las normas del estándar de cableado estructurado EIA/TIA 568 a través de cable par trenzado sin blindar (UTP: Unshielded twisted pair).

Edificio	Categoría del cable UTP
1	3
2	3
4	3
5	3,5
12	5

Tabla 7.1 Resumen de categoría de cable UTP utilizado por edificio

7.1.1 Equipos de intercomunicación

A continuación se describen las características de los principales dispositivos de intercomunicación por edificio.

Edificio 1

Este edificio se conecta al backbone por medio de un concentrador SEHI-24 (Cabletron). Además, de 2 concentradores conectados en cascada de modelos SEH-24 y SEH-34 (Cabletron).

Edificio 2

Este edificio se conecta al backbone por medio de un chasis MMAC-M5FNB (Cabletron) con una tarjeta de conexión a red IRBM (Cabletron).

Edificio 4

Este edificio se conecta al backbone por medio de un concentrador MMAC-M3FNB con salida de tarjeta IRBM (Cabletron).

En este mismo edificio se tiene el enlace de salida hacia la conexión con RedUNAM, este enlace se lleva a cabo por medio de cable fibra óptica[168] hasta un repetidor Cisco AGS plus.

Edificio 5

Este edificio se conecta al backbone por medio de un concentrador MMAC-M3FNB (Cabletron) con una tarjeta de conexión a red IRBM (Cabletron). Además tienen conectados en cascada 5 concentradores con los siguientes modelos, un HP-48 (J2602A), MRXI (Cabletron), 2 concentradores SEH-24 y un SEHI-24 (Cabletron).

Edificio 12

Se conecta al backbone por medio de un chasis MMAC-M8FNB (Cabletron) con una tarjeta de conexión a red IRBM (Cabletron).

En el anexo 2 se explican con mayor detalle las características técnicas de los equipos de intercomunicación de la REDII.

[168] La conversión de cable coaxial ha fibra óptica se realiza por medio de un dispositivo llamado ODS localizado en el edificio 4.

7.1.2 Principales equipos conectados a red

Edificio 1

Sus principales equipos de computo son: Una estación de trabajo Sun (modelo Sunserver 360).

Edificio 2

Sus principales equipos de computo son: una estación de trabajo HP9000 (modelo 720) y una IBM RS6000. Al igual, que el edificio 5 este cuenta con un gran numero de nodos instalados (que tienden a crecer) por lo que se piensa que se tendrá un gran volumen a futuro.

Edificio 4

Sus principales equipos de computo son: dos estaciones de trabajo HP9000 (modelos 720 y 710) y una SGI[169] (modelo Indigo 2).

Edificio 5

Sus principales equipos de computo conectados son: Dos estaciones de trabajo HP9000 (modelos 750 y 720).

Este edificio es el que cuenta con el mayor número de nodos conectados por lo se piensa que tendrá un gran volumen de tráfico en el futuro.

Edificio 12

En este edificio, se pueden observar los tres servidores generales conectados, siendo los principales del Instituto[170] (estaciones de trabajo marca Sun modelos, Sparcserver 20, Sparcstation 20 y una Ultrasparc), además se encuentra una estación de trabajo de monitoreo (marca Sun modelo SparcClassic con el software de administración de red SunNetManager), otra de visualización (SGI modelo Indigo 2) y por último el servidor de nombres DNS (marca Sun modelo SparcClassic).

Como se puede observar, en este edificio es donde se concentran la mayoría de los servicios prestados a todo el Instituto por lo que es el edificio de mayor importancia.

---

[169] SGI: Silicon Graphics.

[170] Las demas estaciones de trabajo del plano, son en las que se tienen la mayor carga de trabajo y transferencia de paquetes (por lo que son consideradas como los servidores de segundo orden de importancia).

7.1.3 Protocolos de comunicación en el Instituto de Ingeniería

La red del Instituto de Ingeniería tiene como protocolos de comunicación: TCP/IP (Internet), IPX/SPX (Novell Netware) y NetBEUI (Microsoft). Los cuales, fueron explicados en el capítulo 4 "Protocolos de Comunicación".

7.1.4 Aplicaciones especificas de usuarios y de administración en el Instituto de Ingeniería

A continuación se realiza una breve explicación de los servicios de aplicación que mas se utilizan en el Instituto de Ingeniería[17]. Estos servicios de aplicación se han subdividido en 6 secciones para poder ser explicados y entendidos con mayor facilidad.

7.1.4.1 Servicios básicos

Sesión remota

Las sesiones remotas se efectúan mediante emulaciones de terminales que proveen al usuario un mecanismo de enlace remoto con la mayoría de los equipos con que cuenta el Instituto (las estaciones de trabajo que se encuentran conectadas a la REDII) o aquellas maquinas localizadas en el mundo o red Internet.

Dada la gran aceptación que ha tenido TCP/IP como un estándar en las comunicaciones a nivel mundial, el servicio de sesión remota mejor referido como **Telnet** se ha convertido en la herramienta más empleada para efectuar sesiones remotas en Internet y redes que trabajan con esta familia de protocolos. Telnet permite al usuario acceder a una computadora remota desde su computadora local, una vez conectado el usuario al equipo remoto, éste puede introducir datos, ejecutar programas y llevar a cabo todas aquellas tareas que desee como si estuviese trabajando directamente en el equipo remoto.

Comunicaciones electrónicas

Las comunicaciones electrónicas aprovechan las herramientas de comunicación en línea y de transferencia de mensajes, como el **correo electrónico**, con las cuáles el usuario puede entablar, en forma confiable y de manera eficiente la comunicación con otros usuarios dentro de la misma Institución u otras personas en otras organizaciones nacionales o extranjeras que se encuentren integradas a una red mundial (como la Internet) y que cuenten con los mismos servicios.

---

[17] Si se desea una explicación mas a profundidad, referirse al capítulo 4 "Protocolos de Comunicación".

La aplicación más utilizada dentro de los servicios de comunicación electrónica entre los usuarios es el correo electrónico (E-mail), que se utiliza para intercambiar mensajes con una o varias personas, y se considera la herramienta de comunicación que más se utiliza en el mundo[172]. La mayoría de los mensajes contienen en su mayoría solo texto, pero también es posible enviar archivos conteniendo imágenes, sonido y hasta animaciones.

El conjunto de protocolos TCP/IP especifica un estándar para el intercambio de correo electrónico entre anfitriones, este es referido como el **Protocolo de Transferencia de Correo Simple** (SMTP: Simple Mail Transfer Protocol), que describe las características bajo las cuales el correo electrónico debe ser implantado.

Los sistemas basados en la plataforma Unix usan el programa **sendmail**, el cuál utiliza el protocolo SMTP, este programa es capaz de comunicarse con otros servicios de correo basados en el SMTP, así mismo, puede operar como un intérprete[173] entre diferentes sistemas de correo.

Todas las estaciones de trabajo del Instituto de Ingeniería utilizan el programa sendmail como servicio para el correo electrónico, de esta manera, se encuentran configuradas para la recepción y envío de mensajes a cualquier punto del mundo a través de la red Internet y otras redes. Otros servicios adicionales dentro del servicio de correo electrónico son soportados, tal es el caso del protocolo de servicio referido como POP (Post Office Protocol), el cual es el encargado de atender a los clientes de POP instalados en las computadoras personales (PC's). Es importante señalar que fue necesario utilizar estos servicios adicionales ya que permiten que el servidor de correo electrónico (sendmail) también pueda entregar y recibir mensajes hacia/desde computadoras personales (cliente) que utilizan el cliente POP.

La mayoría de los usuarios nunca emplean el programa sendmail directamente, en su lugar utilizan aplicaciones de interface (referidos como front-end's) que permiten una forma mas fácil de interacción con él, algunos ejemplos de estos programas son: PINE, elm, Mail; los cuales son ejecutados en las mismas estaciones de trabajo y por otro lado programas como Eudora y Minuet instalados en computadoras personales (por lo cual son clientes del servicio POP).

Por otro lado, el Instituto de Ingeniería maneja otros servicios de comunicación electrónica a través de la red, como son los servicios: talk, finger, write, wall, IRC, entre otros.

---

[172] Esta forma de envío de mensajes representa grandes ventajas sobre otros métodos de envío tradicionales como lo son el fáx, mensajería común y telefonía, ya que los costos son menores, pero sobre todo por que es una forma más rápida y confiable de entrega de mensajes.
[173] Referido como gateway en el lenguaje técnico utilizado por TCP/IP.

Todos estos servicios de comunicación electrónica se proporcionan a todos los usuarios del Instituto que así lo requieran y de manera implícita a todos aquellos usuarios que tengan cuenta en alguna estación de trabajo. Con estas herramientas se provee al personal del Instituto, el acceso a los más diversos servicios de comunicación electrónica a nivel local, nacional e internacional.

Transferencia de archivos (FTP)

Uno de los grandes beneficios que se tiene al contar con una red de cómputo, es la facilidad de transferir archivos entre computadoras, convirtiéndose así en una de las aplicaciones de uso principal que se tienen en la red. Los archivos a transferir pueden ser datos, imágenes, programas, texto o cualquier otro tipo de información. La aplicación estándar utilizada para transferir archivos en redes que emplean TCP/IP es el programa **ftp** (file transfer program) que se basa en el protocolo FTP (File Transfer Protocol).

Entre las características más relevantes del ftp se encuentran:

- Acceso interactivo: La mayoría de las implantaciones de ftp proveen una interface interactiva que permite al usuario interactuar fácilmente con servidores remotos. Entre las operaciones que se pueden efectuar en una sesión de ftp son: listar archivos, crear y eliminar directorios remotos, etc.

- Especificación de formato: ftp permite al cliente especificar el tipo de formato de los archivos a ser transferidos, es decir, el usuario puede emplear diferentes modalidades de transferencia (modo binario para formatos especiales o modo ascii para archivos de texto), con esta característica la transferencia de datos puede hacerse incluso entre computadoras que empleen sistemas operativos diferentes o formatos de almacenamiento distintos.

- Control de autenticidad: ftp requiere que los clientes verifiquen su autenticidad enviando su nombre de usuario y su clave de acceso al servidor antes de iniciar una sesión de transferencia de archivos. El servidor niega el acceso a aquellos clientes que no cuenten con un nombre de usuario y una clave de acceso válida.

El programa ftp es una de las principales herramientas empleadas en el Instituto de Ingeniería ya que sirve para transferir información entre los diferentes equipos de cómputo conectados. Cada equipo conectado a la red del Instituto está provisto de esta herramienta, ya sea computadora personal o estación de trabajo. En lo que se refiere a computadoras personales se cuenta con diferentes versiones de clientes de ftp, mientras que para estaciones de trabajo cada una cuenta con una propia implantación del ftp tanto para el cliente como para el servidor.

También se ha implantado una cuenta pública en una estación de trabajo del Instituto para efectuar ftp de libre acceso, esta cuenta mantiene un conjunto de

programas y documentos de interés general y que son de libre distribución, entre estos se encuentran manuales, programas antivirus, compactadores de información y diversas utilerías de dominio público. Este tipo de cuenta pública utilizada para efectuar la transferencia de archivos es conocida como ftp anónimo.

7.1.4.2 Servicios de recursos compartidos

Sistema de archivos en red (NFS)

El **Sistema de Archivos en Red** (NFS: Network File System), permite que directorios y archivos sean compartidos a través de una red. Esta herramienta fue inicialmente desarrollada por SUN Microsystems en los inicios de los años ochenta, sin embargo, ya ha sido adoptado como un estándar por otros fabricantes de software y actualmente forma parte del sistema operativo UNIX[174] y otros sistemas operativos, existiendo incluso versiones de NFS para computadoras personales (como PC-NFS para el sistema operativo DOS y Windows 95).

Mediante NFS, usuarios y programas pueden acceder a sistemas de archivos localizados en sistemas remotos y tratarlos como si fueran sistemas de archivos locales. Una vez implantado el ambiente de NFS, el usuario no conoce donde se encuentra su información y ni le interesa, esto es, no se entera si la información a la que accede esta guardada localmente (en el disco duro de su máquina) o si está en un disco duro de una máquina remota, es decir, la gestión de la información que hace NFS es completamente transparente desde el punto de vista del usuario e incluso al de las aplicaciones.

Dentro del Instituto el protocolo NFS juega un papel muy importante, ya que a través de esta herramienta es posible dotar de espacio de almacenamiento a equipos que no cuentan con medios de almacenamiento propios o sus medios sean limitados, tal es el caso de terminales gráficas (utilizadas para procesos de visualización y simulación) y computadoras personales con pocos recursos de disco duro. Es por esto, que el Instituto, cuenta con dos estaciones de trabajo que utilizan UNIX como servidores de archivos basados en NFS que permiten prestar este servicio de préstamo de recurso de disco duro a computadoras personales que utilizan el sistema operativo MS-DOS o Windows 95.

---

[174] Pese a que NFS se ha convertido en la herramienta por excelencia para compartir sistemas de archivos a través de una red, existen otras aplicaciones que permiten llevar a cabo esta misma tarea, tal es el caso de AT&T RFS (Remote File Sharing) y de AFS (Andrew File System) que fueron explicados en el capítulo 4 de este trabajo.

Impresión remota

La impresión remota es uno de los mecanismos más empleados en ambientes de red para proporcionar a los usuarios de una organización el acceso a impresoras de características diferentes, tales como manejo de lenguajes de impresión (Postscript, HPCL, etc.), impresión a color o bien impresión de alta resolución; obteniéndose de esta forma un mejor uso y disponibilidad de estos periféricos. La impresión remota es efectuada por los usuarios como si ellos tuviesen conectada la impresora directamente al puerto paralelo de su computadora personal o estación de trabajo.

En ambientes de red, cuando un usuario desea imprimir un trabajo puede optar porque éste se lleve a cabo localmente (si cuenta con una impresora) o bien redireccionar su impresión hacia un equipo encargado de las tareas de impresión en la red, llamado servidor de impresión (print server). Éste ultimo se encarga de recibir cada una de las tareas de impresión de los diferentes usuarios de la red, una vez que ha llegado un trabajo de impresión el servidor verifica si existen trabajos de impresión esperando a ser procesados, en caso de que así sea, el nuevo trabajo será guardado en una cola de impresión (esta cola es realmente un archivo guardado bajo cierta estructura de subdirectorios que el propio servidor se encarga de crear) en espera de ser procesado y será almacenado ahí hasta que el servidor lo envíe a la impresora; en caso de que el servidor no este atendiendo otra impresión previa, el trabajo será enviado inmediatamente hacia la impresora. Cabe aclarar que la impresora puede encontrarse conectada directamente al servidor de impresión o bien puede hallarse conectada a la red como un nodo más de ella, sin que esto afecte a su funcionamiento y disponibilidad, esta ultima opción de conectar la impresora a la red como un nodo más presenta grandes ventajas ya que permite que una impresora se localice en lugares en donde los usuarios puedan acceder fácilmente y al mismo tiempo se evita que personal no autorizado tenga contacto con los servidores.

El servidor de impresión no solo se encarga de recibir trabajos provenientes de la red y enviarlos a impresión, este efectúa otras tareas como: monitorear el estado de las colas de impresión, manipular el orden en que se encuentran los trabajos en las colas de impresión, cancelar trabajos y llevar un estricto control de trabajos de impresión efectuados para un determinado usuario o departamento.

El uso de impresión remota en el Instituto de Ingeniería se ha convertido en una tarea relevante, para ello se han implantado diferentes mecanismos que permitan llevar a cabo esta actividad. Uno de ellos se basa en el uso de servidores de impresión del sistema operativo Novell Netware versión 3.11, mientras que un segundo mecanismo emplea las facilidades de impresión en red que la plataforma Unix proporciona. Ambos mecanismos, tanto el basado en Netware como el basado en Unix, emplean para el control de tareas de impresión, servidores dedicados a procesarlas (print server), la configuración de cada uno de estos

servidores requiere que las siguientes tareas sean efectuadas antes de ponerlos en operación:

1. Determinar de forma estratégica la ubicación de impresoras dentro del Instituto, ya sea que estas se encuentren conectadas directamente a los servidores de impresión o bien sean conectadas a la red como un nodo más en lugares accesibles únicamente para los usuarios autorizados.
2. Establecer que equipos se emplean como servidores de impresión remota.
3. Definir para cada servidor las colas de impresión, así como las impresoras que atenderán a cada una de estas colas.
4. Especificar las características de operación de cada una de las impresoras que los servidores utilizaran para canalizar las tareas de impresión.
5. Finalmente, definir los usuarios a los que cada servidor atenderá.

Servidor de impresión de NetWare Ver. 3.11	Servidor de impresión de Unix
Soporte de impresoras conectadas a red	Soporte de impresoras conectadas a red
Cada servidor puede atender máximo 16 impresoras a la vez.	El límite de impresoras soportadas esta determinado por la carga de trabajo de cada estación de trabajo
Para contar con impresión remota, es necesario iniciar sesión con el servidor de archivos	Para acceder a impresoras remotas, no se requiere iniciar sesión con ningún servidor
Solo soporta a clientes que emplean NetWare	Facilidad de impresión a clientes de Unix y clientes de otras plataformas (DOS, Windows, Macintosh, etc) que empleen TCP/IP
El usuario está limitado a emplear el servidor de impresión asociado al servidor de archivos que lo atiende.	El usuario puede redireccionar su impresión hacia cualquiera de los servidores de impresión disponible.
El redireccionamiento de trabajos hacia el servidor de impresión puede ser activado/desactivado en cualquier momento	El redireccionamiento de trabajos hacia el servidor de impresión puede ser activado/desactivado en cualquier momento

Tabla 7.2 A continuación se muestran algunas características propias de cada mecanismo dependiendo sobre que plataforma se desempeñe:

7.1.4.3 Sistemas de Información Distribuida

Formalmente un sistema de información distribuida es una colección de módulos de software ejecutándose en varias computadoras interconectadas por una red, los cuales administran todos los datos distribuidos (archivos y bases de datos) y las transacciones asociadas. Básicamente estos sistemas incluyen la funcionalidad de un sistema de administración de base datos, un sistema de administración de archivos distribuidos y un sistema de administración de transacciones distribuidas.

Diferentes protocolos y herramientas de obtención de información de información en Internet han sido desarrolladas en los últimos años. Estas herramientas pueden

ser clasificadas en varias categorías: servicios interactivos de entrega de información y servicios de índices.

A continuación se describen las principales herramientas de navegación y exploración en Internet con que cuenta el Instituto de Ingeniería.

7.1.4.3.1 Servicios interactivos de entrega de información

Gopher

Originalmente el servicio Gopher fue desarrollado por el Departamento de Servicios de Cómputo e Información de la Universidad de Minesota, como un sistema de información en línea dentro de la universidad, que permitía difundir de manera eficiente información dentro del campus. Gopher actualmente es considerado uno de los servicios de información más importantes dentro de la red Internet, ya que permite integrar una amplia variedad de servicios y herramientas para búsqueda y adquisición de información.

Gopher combina características de los boletines electrónicos (referidos como BBS) y bases de datos en un sistema de información distribuido que permite examinar información y efectuar búsquedas utilizando índices. Gopher está basado en el uso de menús jerárquicos para el acceso de información, las opciones contenidas en los menús pueden ser ligadas a otros servidores Gopher, esto permite que el volumen de información pueda ser incrementado gradualmente, creando así una red mundial de información referida usualmente como el espacio de Gopher.

La información obtenida con Gopher usualmente es de tipo texto, sin embargo, otros tipos de información son también soportados, tales como imágenes, video y audio, aunque el acceso a estos dependa exclusivamente de la capacidad de los programas cliente. Gopher también provee acceso a través de traductores (gateways"), a otros servicios de adquisición de información como son FTP, WAIS, Usenet y Archie.

World Wide Web

Desarrollado en Suiza, por el European Particle Physics Laboratory. El WWW, también referido como W3 o WEB, combina la obtención de información y uso de hipertextos para ser un simple pero poderoso sistema de información. El WWW consiste en documentos virtuales que pueden contener otros documentos con ligas a otros servidores WWW. Los índices son considerados como documentos especiales que pueden ser examinados. Los servidores de WWW soportan documentos en una amplia variedad de formatos como por ejemplo, PostScript, audio, imágenes y video, o ligas a otros servidores WWW.

WWW utiliza el protocolo HTTP (Hyper Text Transport Protocol como un programa de examinación que solicita documentos o búsquedas por medio de palabras claves de un servidor remoto. Estos programas son diseñados para acceder datos usando el HTTP (conexión TCP utilizando el puerto lógico 80) y protocolos existentes como FTP y el NNTP usado en Usenet. Originalmente WWW incluía un cliente modo línea para utilizarse con el telnet y una interface gráfica limitada, actualmente la mayoría de los clientes WWW se encuentran basados en interfaces gráficas (GUI o navegadores) que pueden desplegar imágenes, video y agregar audio al hipertexto de calidad PostScript, los clientes GUI más destacados actualmente para WWW son el Mosaic, Netscape y Internet Explorer (Microsoft).

7.1.4.3.2 Servicios de índices

Archie

Desarrollado en la Universidad de McGill en Montreal, Canada. Archie es una especie de biblioteca gigantesca que automáticamente consulta un gran número de servidores de ftp anónimos en Internet para que de esta manera haga un índice de los archivos encontrados, creando así, una enorme base de datos, en realidad esta base de datos es una recopilación de los archivos disponibles en cada uno de los servidores de ftp anónimos que se encuentran asociados a Archie. Como Archie consulta estos servidores regularmente, entonces la base de datos es actualizada constantemente. Actualmente, Archie no es un solo servidor, sino una colección de servidores Archie, en donde cada uno de ellos es responsable de consultar su propio conjunto de servidores de ftp anónimo de Internet para construir su base de datos, como Archie ha sido diseñado para compartir y coordinar la recolección de información, entonces es posible tener varios servidores de Archie en varias locaciones de Internet cada uno con una copia similar de las bases de datos. Para poder encontrar archivos con Archie se utilizan dos estrategias: Si se conoce el nombre del archivo, entonces se puede preguntar a Archie donde encontrarlo, o bien, si se desconoce el nombre del archivo, entonces Archie puede buscar los nombres de los archivos y directorios que contienen palabras relacionadas a la información requerida.

Una limitante de Archie es que solo pueden hacer búsquedas de un solo tema por medio de una palabra clave. Cuando la búsqueda tiene éxito, Archie muestra la información acerca de los archivos encontrados relacionados al tema pedido, desplegando el nombre de los anfitriones donde se puede localizar el archivo, los directorios y subdirectorios donde el archivo se localiza, así como el tamaño de cada archivo, su fecha y la hora en que fue actualizado, además de los atributos del archivo. Es importante destacar que Archie no conoce el contenido y el tipo de archivos que él despliega.

WAIS

WAIS (Wide Area Information System), desarrollado por Thinking Machines en colaboración con Apple Inc. y KPMG Peat Marwick, es un sistema que intenta hacer fácil la búsqueda y obtención de la gran cantidad de información que existe en diversas bases de datos dentro de Internet. Para muchos usuarios de Internet, WAIS ofrece una solución real al problema de buscar algo cuando no se esta seguro de donde esta.

En términos básicos WAIS trabaja como el bibliotecario de una enorme biblioteca, pero ha sido diseñado para automatizar este procedimiento. El usuario formula una pregunta en inglés, selecciona la base de datos que quiera consultar, y entonces recibe una respuesta a su petición.

Para construir una búsqueda, muchos sistemas de bases de datos emplean un lenguaje especial, WAIS en particular utiliza un lenguaje natural como el inglés, además de que incorpora palabras de funciones booleanas como AND, OR, NOT, GREATHER THAN, LESS THAN, etc. lo que permite realizar un modo de búsqueda mas flexible y eficiente.

Catálogo de libros

Múltiples bibliotecas ofrecen en línea los catálogos de su acervo, es decir, que estos pueden ser accedidos vía sesión remota telnet o hytelnet.

7.1.4.6 Servicios de monitoreo y administración de la REDII

7.1.4.6.1 Administración

Aprovechando las características de TCP/IP un conjunto de herramientas de diagnóstico y monitoreo en redes TCP/IP han sido empleadas, estas herramientas permiten monitorear el estado de la red y el comportamiento de las aplicaciones. Algunas de estas herramientas se incluyen con los sistemas operativos y otras más son software de dominio público. Una pequeña relación de estas herramientas y su función de detección y corrección de fallas se explica a continuación:

Ifconfig (Interface configuration): Provee información acerca de la configuración básica de la interface, es utilizado para detectar direcciones IP, máscaras de subred y direcciones de envío de mensajes de broadcast (broadcast address) incorrectas. Esta herramienta es provista con el sistema operativo Unix.

Arp (address resolution protocol) Permite efectuar traducciones de direcciones IP a direcciones Ethernet. Es utilizado para detectar sistemas en una red

local que se encuentren configurados con una dirección IP incorrecta o repetida. Arp es considerado como parte de Unix, sin embargo también esta disponible en otros sistemas operativos.

Netstat Provee varios tipos de información, es utilizado comúnmente para desplegar estadísticas detalladas acerca de cada interface de red, sockets y tablas de enrutamiento. Forma parte de los servicios de red que provee Unix.

Ping **(Internet control message protocol):** Indica cuando un anfitrión remoto puede ser accedido, también es útil para verificar la comunicación con otros dispositivos de red como puentes, compuertas y enrutadores. Despliega algunas estadísticas como son los paquetes perdidos y el tiempo de envío. Es parte de Unix, aunque también está disponible en otros sistemas operativos como VMS, MS-DOS y System 7.

Nslookup Provee información acerca del Servidor de Nombres (DNS). Permite hacer consultas sobre dominios, anfitriones, registros MX, etc. Forma parte del software BIND de Unix.

Traceroute Indica que rutas toman los paquetes de información desde el sistema origen hasta el sistema destino. La información acerca de cada salto (hop) es desplegada. Es de gran utilidad para trazar rutas o detectar fallas en redes remotas. Traceroute es una herramienta de dominio público.

Etherfind (Analizador de protocolos) Esta herramienta, analiza los paquetes individuales que se intercambian entre anfitriones en la red. Etherfind es un protocolo TCP/IP que puede examinar el contenido de los paquetes incluyendo sus cabeceras de información, es muy útil para analizar problemas relacionados con la implantación de protocolos. Otros analizadores de protocolos son el **tcpdump** (para sistemas Unix) y el **lanwatch** (para sistemas MS-DOS).

7.1.4.6.2 Monitoreo

El servicio de monitoreo es una de las tareas más importantes dentro de las actividades de administración de toda red de cómputo, sus funciones engloban la extracción e interpretación de datos relacionados con el estado de los dispositivos conectados a la red.

El operador de la red deberá siempre tener cuidado de correcciones rápidas de fallas en la red, manteniendo un alto desempeño de ésta y sin olvidar el aspecto de la seguridad.

El desarrollo de una buena función de monitoreo permitirá llevar a cabo una planeación de posibles crecimientos de la red, de la manera más adecuada, basándose en un buen diseño.

Los tipos de monitoreo se pueden agrupar en dos clases:

Monitoreo de red físico: Se encargan de los elementos físicos de la red, como son interfaces de comunicación, puertos, canales, etc. Este tipo de monitoreo se basa en que todos los cambios de estado (cambios de voltaje por ejemplo) pueden ser medidos y comparados con umbrales de operación. Las funciones de monitoreo de la red física son capaces de analizar los tres primeros niveles del modelo OSI.

Monitoreo de red lógico: En este, se analizan los estados lógicos de los elementos de la red para garantizar el buen funcionamiento de todo el equipo como son: colas, uso de procesador, utilización de puertos, utilización de enlaces, memorias, tráficos, etc.

Dependiendo del tipo de monitoreo se deben considerar otros criterios más específicos como protocolos soportados, etc.

Para facilitar las tareas de administración y monitoreo de la red del Instituto de Ingeniería, ha sido necesario la adquisición de dos sistemas de administración de redes, estos son: el SunNet Manager y el LANVIEW; los cuales permiten los dos tipos de monitoreo. Los dos sistemas utilizan el protocolo SNMP (Simple Network Management Protocol) como protocolo de administración, de esta manera, los dos permiten una oportuna detección de fallas, adecuada configuración de los equipos y de los dispositivos, así como un constante monitoreo del desempeño de la red. Todos los resultados arrojados por este sistema permiten efectuar cambios y considerar modificaciones en la infraestructura de la red,

Entre las características principales que se tiene con estos sistemas de administración es que se puede tener un despliegue de una vista jerárquica de la red del Instituto. Además de que aprovechan la compatibilidad que tienen los equipos con el protocolo de administración SNMP, con esto se pueden monitorear todos los dispositivos sin importar sobre que protocolo de comunicación se desempeñe, es decir máquinas con TCP/IP Unix, Novell Netware SPX/IPX o Microsoft NetBEUI pueden ser monitoreables si estos tienen habilitado el protocolo SNMP. De esta forma se pueden monitorear sobrecargas en los segmentos, fallas en los servicios y parámetros como porcentajes de errores, colisiones por cada salida lógica etc., esto ha permitido un monitoreo del estado de estos dispositivos muy completo y confiable, además de que se han logrado minimizar los tiempos en el monitoreo de desempeño, detección y corrección de fallas de la red.

7.1.4.6.3 Implantación de herramientas de seguridad en el Instituto de Ingeniería

En los ambientes de computo distribuido y sobre todo aquellos que tiene conexión hacia redes externas como la red global Internet, deben tener en cuenta en sus políticas, medidas de seguridad a dispositivos de conexión, equipos que brindan soporte de servicios públicos (ftp, sesión remota, finger, correo electrónico, etc.) o que mantienen información crítica para la organización, es por esto que deben ser provistos de medidas de seguridad muy rigurosas con la finalidad de mantener su buen funcionamiento y evitar daños o intromisiones no deseadas por parte de personal no autorizado.

En el Instituto de Ingeniería se están llevando a cabo el establecimiento de nuevas políticas de uso y prioridades en los equipos conectados. Además de llevar a cabo la instalación de herramientas que llevan a cabo el monitoreo y control de ciertos aspectos del sistema. Estas herramientas cubren en la medida de lo posible, los puntos principales que pueden ser automatizados en la seguridad de los anfitriones.[175]

De acuerdo a las necesidades básicas principales de seguridad en el Instituto, se decidió instalar y configurar herramientas de seguridad[176], algunas de ellas serán descritas a continuación.

NPASSWD[177]: es un programa que forza a que las claves secretas (passwords) de los usuarios cumplan ciertas reglas de seguridad, antes de que estos sean dados de

[175] Las medidas de seguridad han sido implantadas únicamente en sistemas basados en plataforma Unix, debido a que éstos desempenan la tarea de anfitriones de servicios de usuarios locales y externos.
[176] Todas las herramientas son de dominio público y son disponibles en la Internet global.
[177] Npasswd está disponible vía FTP anónimo en ftp.cc.utexas.edu bajo /pub/npasswd.

alta. Npasswd no es un generador aleatorio de claves secretas, el usuario es libre de elegir su clave, pero debe de cumplir con ciertos criterios como son que la clave contenga un número mínimo de caracteres, que la clave no contenga caracteres ilegales, que la clave sea una combinación de letras mayúsculas y minúsculas, que no este formado por información personal, etc.

COPS (Computer Oracle and Passwd System)[178]: es una herramienta de seguridad que permite el diagnóstico y reporta el estado de una máquina Unix. Escrito en el interprete de comandos Bourne shell utiliza comandos como awk, sed y C. El sistema es básicamente un programa de interprete de comandos (shell script) que ejecuta varios subprogramas, en general analiza los permisos de los archivos, directorios dispositivos, de claves, grupos de archivos, el contenido del archivo /etc/rc y archivos cron, cambia el estado SUID, los permisos de escritura de los directorios hogar (home), archivos de inicialización de los usuarios (.profile, .cshrc), etc. Cabe mencionar que COPS no corrige ningún problema que encuentra y no es necesario tener la clave del administrador del sistema para correrlo.

TCP-Wrapper[179]: Una de las técnicas más utilizadas para limitar el acceso entre sistemas conectados a la red es el **control de acceso**, esta técnica consiste en verificar la dirección IP del anfitrión que solicita un servicio contra una lista de control de acceso. Si la lista indica que el anfitrión visitante puede utilizar el servicio solicitado entonces su acceso es permitido, en caso contrario, el acceso al anfitrión es denegado[180]. En sistemas Unix existe un software para el control de acceso, el más utilizado es el llamado TCP_Wrapper cuya principal caraterística es el control de acceso a servicios de red tales como FTP, Telnet, Finger, etc.

TCP-Wrapper realiza dos funciones básicas: registrar las peticiones de servicios (independientemente del si tienen acceso o no), y proveer un mecanismo de control de acceso a servicios de red. El registro de peticiones de servicio es una excelente herramienta para monitorear el uso de los servicios de red, de gran ayuda para la detección de actividades ilegales (personal no autorizado), pero su poder real es su habilidad para controlar el acceso a servicios de red.

Finalmente es importante destacar que aunque estas herramientas ayudan a mejorar la seguridad del Instituto, se siguen probando otros esquemas y herramientas de seguridad.

---

[178] COPS está disponible vía FTP anónimo en cert.sei.cmu.edu en /pub/cops.
[179] TCP-Wrapper está disponible vía ftp anónimo en cert.sei..cmu.edu bajo /pub/network_tools.
[180] Esta técnica es utilizada en anfitriones que necesitan validar al cliente antes de proporcionarle un servicio, es también utilizada por algunos enrutadores como los fabricados por CISCO Inc.

7.2 RedUNAM: Actual y tendencias

7.2.1 Estado actual de RedUNAM[181]

RedUNAM es el proyecto desarrollado para la transmisión de datos entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias que conforman a la Universidad Nacional Autónoma de México.

7.2.2 Objetivos de RedUNAM

- Promover el intercambio de ideas, pensamientos y opiniones que enriquezcan a los pueblos, instituciones e individuos.
- Apoyar el crecimiento de la UNAM y de México, brindando una opción tangible para el libre tránsito de información entre las diversas instituciones generadoras y transformadoras de conocimientos en México y el mundo.
- Acercar los bancos de información y otras fuentes de conocimiento a todo estudiante, personal académico, administrativo, y en general, a todo aquel que así lo requiera.

7.2.3 Principales características de RedUNAM

- Transmite indistintamente voz y datos, mediante sistemas digitales basados en las más modernas normas internacionales.
- Las principales instalaciones de la Universidad están integradas a la Red. Esto significa que a nivel licenciatura, posgrado e investigación, alrededor del 90% de sus miembros se encuentran en instalaciones cubiertas por la RedUNAM, independientemente de su ubicación geográfica.
- El sistema es descentralizado, redundante y esta integrado por 31 Nodos de Cómputo y Telecomunicaciones enlazados entre sí por medio de un sistema de cableado de fibra óptica.
- Así mismo tiene una infraestructura instalada para más de 170 redes locales de cómputo. La Red enlaza a cerca de 8000 computadoras en la UNAM entre sí y alrededor de un millón de computadoras en el resto del mundo.

[181] DGSCA, Dirección de Telecomunicaciones Digitales, pagina de web: http://www.dtd.unam.mx/home.html

7.2.4 Topologías y medios de comunicación

El backbone de la red universitaria de datos:

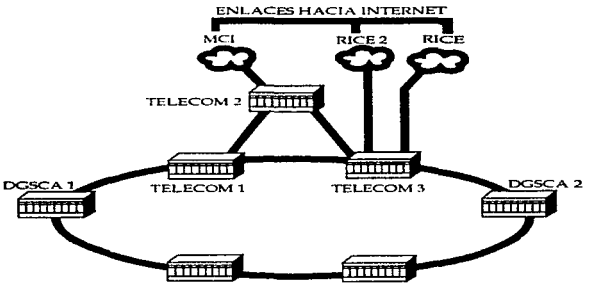


Figura 7.3 Topología de REDUNAM

En la siguiente figura 7.4 se muestra las dependencias que se conectan a REDUNAM por medio del IIMAS, entre ellas se encuentra el Instituto de Ingeniería.

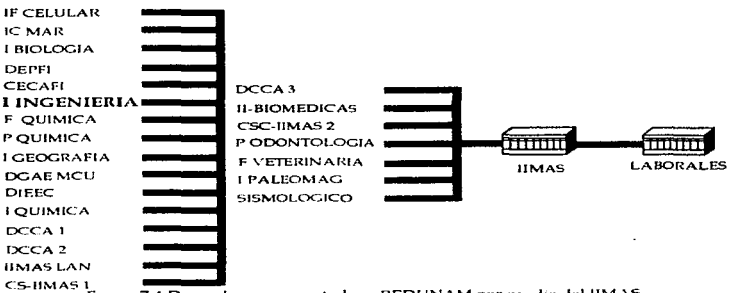


Figura 7.4 Dependencias conectadas a REDUNAM por medio del IIMAS.

La estructura principal de RedUNAM es un anillo de FDDI (un anillo de fibra óptica activo y otro de respaldo que pueden transportar información de hasta 100 Mbps, enlazando a 5 enrutadores principales). Conectadas a ellos se encuentran las redes locales de cada dependencia: las cuales se encuentran en el campus de Ciudad Universitaria, estas redes locales son enlazadas por medio de fibra óptica. Aquellas que se encuentran fuera de él, se comunican con RedUNAM a través de alguno de las siguientes formas:

Dentro del área metropolitana	Radio modem Lineas conmutadas o privadas Microondas RDI
Interior de la República Mexicana	Enlaces Satelitales RDI

En las redes propias de la UNAM las topologías más empleadas son variantes de la tecnología Ethernet: en primer lugar se tienen las redes tipo estrella (conocidas también como red de par trenzado pues éste es el medio físico con el que se construyen). Es posible encontrar este tipo de redes complementando con verticales de coaxial grueso en edificios de varios pisos. El segundo medio más empleado es el coaxial delgado, aunque su uso empieza a decaer debido a sus desventajas frente al par trenzado. Y por último, se puede decir que las redes del tipo Token Ring se encuentran en franca desaparición.

7.2.5 Conexión RedUNAM a la red Mundial Internet

La UNAM por medio de la Dirección de Telecomunicaciones Digitales tiene la conexión a la red mundial Internet mediante enlaces directos y permanentes con:

Enlaces directos	SESQUINET	Internet MCI
Operado por	Rice Univesity	Enlace E1
Núm. enlaces	2 enlaces (Houston, Texas),	1 enlaces (Houston, Texas),
Tasa de transmisión	1544 Kbps	2048 Mbps.

Tabla 7.3 Enlaces directos hacia la red mundial Internet

7.2.6 Protocolos y sistemas operativos

Una red de datos como lo es RedUNAM requiere un protocolo de comunicación tal que:

- Permita la conexión transparente entre diferentes clases de computadoras: PC's, mainframes, sistemas Unix, Macintosh, etc. así como, que pueda convivir con sistemas operativos de red que se utilizarán en las redes locales de la Universidad.
- Que sea fácil de configurar y requiera pocos ajustes de acuerdo al crecimiento de la red.
- Sea altamente confiable bajo cualquier condición operativa y en caso necesario, cuente con herramientas poderosas para la corrección de errores. También deberá brindar al administrador facilidades para el monitoreo y mantenimiento preventivo del funcionamiento de la red.
- Que este diseñado expresamente para redes de área amplia o metropolitana, ofreciendo también la posibilidad de atender apropiadamente las redes de área local.

Es por esta razón, que el conjunto de protocolos TCP/IP se perfila como la solución natural a esta lista de requisitos. Es además el protocolo para la comunicación en Internet; sobre el cuál pueden instalarse sistemas operativos de red tales como Windows NT (NetBEUI) y sus variantes, LAN Manager, Lantastic, así como Novell NetWare (SPX/IP).

7.2.7 Servicios ofrecidos por RedUNAM

- **Enrutamiento:** sin el cual no sería posible la comunicación con los anfitriones de otras redes nacionales y extranjeras. El enrutamiento se encarga de que los archivos de los usuarios no se extravíen en alguna parte del mundo o le lleguen a la persona equivocada. También es posible limitar el acceso de usuarios no autorizados a algún anfitrión importante dentro de alguna red.

- **Servidor de Nombres (DNS: Domain Name Service):** se encarga de resolver la conversión o mapeo entre las direcciones numéricas y los nombres lógicos de las máquinas, de forma tal que el usuario por ejemplo, pueda utilizar el nombre servidor.dgsca.unam.mx para comunicarse con su servidor de correo en lugar de la dirección 132.248.10.4. A continuación se muestran los Servidores de Nombres de la UNAM que se tienen para el dominio **.unam.mx**:

    - ns.dgsca.unam.mx
    - noc.noc.unam.mx
    - danzon.astrocu.unam.mx
    - dns2-u.ans.net

- **Centro de operación de la Red (NOC: Network Operation Center):** El cuál se encarga de monitorear el comportamiento de la RedUNAM, así como la óptima operación de ésta y darle el mantenimiento necesario. Además de ser el que se encarga de verificar los enlaces que tiene RedUNAM con las diversas dependencias internas y externas.

  El objetivo primordial del NOC es el mantener en óptimas condiciones la operación de la red y de los dispositivos conectados a ella. Entre las actividades que se realizan para llevar a cabo ese objetivo está la detección, determinación, atención y solución de fallas en la red.

  Dentro del Departamento de Redes y Comunicaciones se llevan acabo las siguientes actividades concernientes al área de NOC: monitoreo, administración, operación y crecimiento.

  De igual manera dentro del NOC se realizan paralelamente actividades tales como: pruebas de la red, enrutamiento, distribución de Información y funciones de mantenimiento

- **Centro de Información de la RedUNAM (NIC-UNAM):** el propósito de este centro es el de proporcionar servicios de soporte informativo, administrativo y procedural a los usuarios de la RedUNAM primordialmente, ya que se pretende que el servicio se extienda a los usuarios de la red académica nacional y mundial.

  A continuación se dan algunas de las funciones que se tienen en el Centro de Información:

  Proveer recursos de información: el Centro de Información deberá proveer a los usuarios el acceso a la información de diversas Formas Nic, para ello:

  * Será el responsable de la obtención de información de otros sitios y de almacenarla localmente para que los usuarios puedan tener acceso a ella.
  * Proporcionará referencias a los usuarios sobre la información localizada en otras localidades de Internet. Esta información deberá mantenerse actualizada.
  * Deberá crear documentos tales como boletines informativos, tutoriales, de información comercial, etc. y ponerlos a disposición de los usuarios que así lo requieran.

  En todos los casos descritos anteriormente, se deberá mantener la autenticidad y actualidad de la información.

Proporcionar soporte a los usuarios finales a través de contacto directo: el Centro de Información de la RedUNAM es el principal recurso de información de los usuarios. Donde se reciben un gran número de peticiones tales como: procedimiento de conexión a Internet, como localizar y acceder cierta aplicación, como determinar una dirección electrónica o como resolver problemas operacionales.

El Centro de Información deber ser capaz de contestar a todas esas preguntas proporcionando al usuario una referencia sobre la fuente de información apropiada. Asimismo deber coordinarse con el Centro de Operación de la RedUNAM (NOC) para resolver problemas de conectividad.

Mantenimiento de soporte a la infraestructura del Centro de Información: Es esencial que el Centro de Información tome parte activa en el soporte de la Infraestructura de NIC/INTERNET. Para ello debe:

- Atender el "IETF USER SERVICES WORKING GROUP (USWG)". Este organismo es el encargado de identificar, discutir y recomendar soluciones a problemas de servicio de red.
- Participar en la lista de correo "nic-forum" con el propósito de intercambiar información con otros centros similares de Internet.

En base a estos servicios el usuario puede hacer uso de otros, tales como:

- **Correo electrónico:** es uno de los servicios de mayor demanda, el cual como se explico anteriormente permite la comunicación entre usuarios de cualquier parte del mundo a través de la colocación de mensajes en el buzón electrónico del destinatario. RedUNAM cuenta con varios servidores de correo[182], dos de los cuales están destinados al público universitario y académico en general.

- **Gopher:** Se trata de menús jerárquicos que permiten buscar información en RedUNAM e Internet a través de conexiones transparentes al usuario. En la UNAM se cuenta con una gran variedad de servidores Gopher, por ejemplo el servidor Condor y el servidor NOC.

- **Archie:** búsqueda electrónica en los servicios anunciados para tal fin. Basta con definir el tema a buscar y en pocos minutos se obtendrá una lista que contiene los nombres y direcciones de las máquinas que contienen archivos referentes al

[182] El principal de ellos, es un equipo SUN Sparc CENTER 2000 para uso de correo electrónico, destinado tanto para la comunidad universitaria como para público en general. Este es conocido como el anfitrión: **servidor.unam.mx**.

tema y que son de dominio público. Dichos archivos pueden ser copiados por el usuario vía el cliente de ftp Anónimo.

- **Telnet:** Sesiones remotas a grandes computadoras para aprovechar sus altas capacidades de cálculo y otros recursos.

- **World Wide Web:** Sin duda uno de los servicios más interesantes y completos que se pueden encontrar en Internet. Este servicio aprovecha la tecnología de multimedia para ofrecer una presentación de la información mucho más interesante mediante el uso de imágenes, texto y audio desde cualquier punto de Internet directamente a la computadora del usuario. Existe una gran cantidad de Servidores WWW en la UNAM, los cuales ofrecen información de gran interés.

- **Otros servicios relacionados:** La UNAM cuenta con un servicio de almacenamiento masivo de información. Además de un equipo de impresión láser disponible para la comunidad universitaria.

  Para llevar a cabo una investigación científica y desarrollo tecnológico de una manera competitiva se requieren servicios de cómputo modernos. Con el propósito de proporcionar este tipo de servicio a la comunidad universitaria y productiva del país, la Universidad Nacional Autónoma de México a puesto en operación desde 1991 el servicio de la Supercomputadora CRAY Y-MP/43 2

7.2.8 Formas de conexión a RedUNAM-Internet

La UNAM ha puesto en disposición tres formas básicas de conexión:

- **La conexión directa:** es la más simple, consiste en tener acceso a una red LAN que esté conectada directamente a la red mundial Internet.

- **La conexión conmutada/por vía telefónica:** cuando se requiere la conexión a la red desde un lugar remoto, la computadora personal del usuario se utiliza para establecer el enlace a través de un módem y una la línea telefónica convencional. Además, cabe mencionar que se necesita de un software apropiado que proporcione el cliente del protocolo Slip o PPP y un módem.

- **Una conexión dedicada:** En este tipo de conexión se hace uso de un circuito de telecomunicaciones dedicado punto-a-punto y enrutadores IP (un dispositivo de red dedicado), que enlace la localidad remota con la RedUNAM-Internet. El rango de velocidad de una línea dedicada varía desde 9.6 Kb hasta 45 Mb, siendo las velocidades de conexión más comunes entre 56 Kb y 2 Mb. Una conexión dedicada a Internet se utiliza principalmente para interconectar a la red de un campus que incluye una gran cantidad de computadoras y estaciones de trabajo.

Requerimientos para un enlace dedicado a la RedUNAM-Internet
Si alguna organización requiere integrar su red a través de una conexión dedicada, la UNAM provee la conexión una vez que la organización haya elegido e instalado su medio de enlace a la RedUNAM. Los medios de enlace pueden ser:

- Línea privada
- RDI
- DSO
- Microondas
- Radio módems
- Enlace vía satélite

El medio de enlace dependerá de las necesidades y de la distancia que exista entre la localidad remota y la UNAM. Uno de los factores decisivos al seleccionar la opción apropiada, además del costo y el propósito de la organización, son el tamaño (ancho de banda), y los usos proyectados (relacionados con el tráfico) de la conexión.

Una vez instalado el medio de enlace se requiere de dos dispositivos enrutadores con una configuración mínima que incluya un puerto V35 y un puerto Ethernet; y una computadora que opere bajo ambiente Unix para que trabaje como Servidor de Nombres DNS primario.

La UNAM por medio de la Dirección de Telecomunicaciones Digitales puede proporcionar la conexión a Internet mediante enlaces directos y permanentes hacia SESQUINET (dos enlaces) y **Internet MCI** (un enlace):

7.2.9 Tendencia de RedUNAM

Como se mencionó anteriormente, RedUNAM actualmente tiene un backbone con tecnología FDDI, esta tecnología solo soporta velocidades de hasta 100 Mbps, sin opción a crecimiento. Además de no soportar los requerimientos de las nuevas aplicaciones y ser una tecnología no escalable, tendiendo a ser desplazada en los próximos años por nuevas tecnologías de red.

Es por esto, que RedUNAM teniendo el compromiso de seguir ofreciendo un servicio de red adecuado a las nuevas necesidades que tanto la educación como la investigación requieren, contempla en sus planes futuros una migración hacia una tecnología de red que permita la convivencia tanto de redes heredas (Ethernet) como de redes de altas especificaciones que permitan el empleo de las nuevas aplicaciones (por ejemplo, videoconferencias, multimedia transferencia de datos a altas velocidades, etc.), por tal motivo la única tecnología de red que permite una escalabilidad de este tipo, además de garantizar una solución a largo plazo es la tecnología ATM.

7.3 Internet: actual y tendencias[183]

7.3.1 Historia de Internet

En 1969 la Agencia de Investigación de Proyectos Avanzados (ARPA: Advanced Research Projects Agency) mas tarde llamada DARPA (Defence Advanced Research Projects Agency) la cual formaba parte del Departamento de Defensa de Estados Unidos (DoD), fundó un proyecto de investigación y desarrollo[184] para crear una red experimental de conmutación de paquetes, conocida como ARPANET. La red fue diseñada para requerir un mínimo de información de las computadoras que forman parte de ella. Para enviar un mensaje en la red, una computadora sólo tiene que poner la información en un sobre, referido como paquete de Protocolo Internet (IP) y asignarle el domicilio destino en forma correcta. Las computadoras que se comunican tienen la responsabilidad de asegurar que la comunicación se lleve a cabo de manera eficiente. La filosofía era que cada computadora en la red se pudiese comunicar, como un elemento individual, con cualquier otra computadora.

En 1972, cuando ARPANET fue mostrada públicamente, 50 universidades y organizaciones de investigación estaban ya conectadas, todas envueltas en proyectos de tecnología militar.

En 1975 ARPANET pasó de ser una red experimental a una red operacional, y la responsabilidad de administrarla recayó en la Agencia de Comunicaciones de la Defensa (DCA: Defense Communications Agency). La tecnología desarrollada por DARPA incluyó un conjunto de protocolos de comunicación y una serie de convenciones para interconectar redes y enrutar tráfico, que fue referido como TCP/IP. ARPA comenzó a trabajar como una tecnología de red de redes a mediados de los años setenta; su arquitectura y protocolos tomaron su forma actual entre 1977 y 1979. En ese tiempo, ARPA era conocida como la principal agencia en proporcionar fondos para la investigación de redes de paquetes conmutados y fue pionera de muchas ideas sobre la conmutación de paquetes con su red conocida como ARPANET. ARPANET utilizaba interconexión convencional de línea alquilada punto-a-punto. [185]

---

[183] Douglas E. Comer; TCP/IP; 3ª. Edición; Prentice Hall; p. 458. Tesis de licenciatura de Rosa Alva Martínez P. y Fernando Mendoza; "Facilidades de cómputo distribuido en el Instituto de Ingeniería: Implantación y desarrollo de mecanismos de información, procesamiento y administración"; p. 55.

[184] La primera configuración reunió cuatro computadoras y fue diseñada para demostrar la flexibilidad de construcción de redes utilizando computadoras que se encontraban distribuidas en una área amplia. Esta red sirvió para estudiar técnicas de comunicación de datos que fueran robustas, confiables y sobre todo no propietarias.

[185] ARPA también ofreció fondos para la exploración a través de redes de radio y mediante canales de comunicación por satélite. De hecho, la diversidad creciente de tecnologías de hardware de red obligó a ARPA a estudiar la interconexión de redes y alentó al enlace de redes.

La Internet global se inició alrededor de 1980 cuando ARPA comenzó a convertir las máquinas conectadas a sus redes de investigación en máquinas con el nuevo protocolo TCP/IP. ARPANET, una vez en su lugar, se convirtió rápidamente en la columna vertebral del nuevo Internet, y fue utilizada para realizar muchos de los primeros experimentos con el TCP/IP. La transición hacia la tecnología Internet se completó en enero de 1983, cuando la Oficina del Secretario de Defensa ordenó que todas las computadoras conectadas a redes de largo alcance utilizaran TCP/IP. Al mismo tiempo, la Agencia de Comunicación de la Defensa (DCA), dividió ARPANET en dos redes separadas, una para la investigación futura y otra para la comunicación militar. La parte de investigación conservó el nombre de **ARPANET** y la parte militar, que era un poco mas grande, se conoció como la red militar **MILNET**. Entonces el término **Internet** fue utilizado para referirse a la red entera : MILNET y ARPANET.

Para alentar a otras instituciones a adoptar TCP/IP, especialmente universidades y centros de investigación, DARPA fundó la compañía Bolt, Benarek y Newman Inc. (BBN) para implantar TCP/IP en la Distribución Berkeley de Software de la Universidad de California (Unix BSD)[186]. A partir de este momento comenzó la gran relación entre TCP/IP y el sistema operativo Unix. Y ARPA fue capaz de llegar a más del 90% de los departamentos universitarios de ciencias de la computación[187].

La distribución Berkeley de software se volvió popular ya que ofrecía los protocolos básicos TCP/IP y un grupo de programas de utilidades, Unix Berkeley proporcionó una nueva abstracción de sistema operativo conocida como **socket** , la cual permite que programas de aplicación accedan a protocolos de comunicación. Como generalización del mecanismo Unix para I/O, el socket tiene opciones para muchos tipos de protocolo de red además del TCP/IP. Por lo tanto alentó a los investigadores a experimentar con TCP/IP.

El éxito de la tecnología TCP/IP y de Internet entre los investigadores de ciencias de la computación guió a que otros grupos la adoptaran. Dándose cuenta de que la comunicación por red pronto sería una parte crucial de la investigación científica, la Fundación Nacional de Ciencias (NSF) tomó un papel activo al expandir el Internet TCP/IP para llegara la mayor parte posible de los científicos. Iniciando en 1985, se comenzó un programa para establecer redes de acceso distribuidas alrededor de sus seis centros con supercomputadoras. En 1986 se aumentaron los esfuerzos para el enlace de redes al proporcionar fondos para una red de columna vertebral de área amplia, llamada NSFNET, que eventualmente alcanzó todos los centros con supercomputadoras y los unió a ARPANET. Por último, en 1986, la

[186] En ese tiempo, la mayor parte de los departamentos universitarios de ciencias de la computación utilizaban una versión del sistema operativo Unix, disponible en Distribución Berkeley de Software de la Universidad de California (Unix BSD).
[187] Llegando en un momento significativo, debido a que los departamentos necesitaban protocolos de comunicación y no había otros generalmente disponibles.

NSF proporcionó fondos para muchas redes regionales cada una de las cuales conecta en la actualidad importantes instituciones científicas de investigación. Todas las redes con fondos de la NSF utilizan los protocolos TCP/IP y todas forman parte de la Internet global.

En 1990, ARPANET formalmente desapareció, y el término Internet tomo un nuevo significado: Internet es la colección mundial de redes interconectadas, que crecieron fuera de la original ARPANET, y que utilizan el conjunto de protocolos TCP/IP para enlazar las distintas redes físicas en una sola red lógica coordinada.

A siete años de su concepción, Internet había crecido hasta abarcar cientos de redes individuales localizadas en los Estados unidos y en Europa. Conectaba casi 20,000 computadoras en universidades, así como a centros de investigación privados y gubernamentales. El tamaño y la utilización de Internet ha seguido creciendo mucho más rápido de lo esperado. A finales de 1987, se estimó que el crecimiento había alcanzado un 15% mensual. En 1994, la Internet global incorporaba más de 3 millones de computadoras en 61 países.

7.3.2 Internet Actual

Actualmente Internet es la red de datos mas importante en el mundo. La adopción de los protocolos TCP/IP y el crecimiento de Internet no se ha limitado a proyectos con fondos del gobierno e instituciones educativas. Grandes corporaciones computacionales se han conectado a Internet, así muchas otras grandes corporaciones, incluyendo: compañías petroleras, automovilísticas, empresas electrónicas, compañías farmacéuticas y de telecomunicaciones, etc. Las compañías medianas y pequeñas se empezaron a conectar en los años noventa. Además, muchas compañías han utilizado los protocolos TCP/IP en sus redes corporativas (Intranets), aunque no han optado por ser parte de la Internet global.

7.3.3 Seguridad en Internet

La seguridad en un ambiente como Internet es algo muy delicado, pues la información es lo mas importante y por tanto tiene un valor significativo y difícil de cuidar, debido a que implica entender cuándo y cómo pueden confiar los usuarios, las computadoras, los servicios y las redes, uno en otro, también implica entender los detalles técnicos del hardware y los protocolos de red. Algo muy importante, dado que TCP/IP soporta a una amplia diversidad de usuarios, servicios y redes, y debido a que Internet global puede abarcar muchas fronteras políticas y organizacionales, los individuos y las organizaciones participantes pueden no estar de acuerdo en lo que un nivel de confiabilidad se refiere o en las políticas para el manejo de datos.

7.3.3.1 Mecanismos para la seguridad de Internet

Los problemas de seguridad en Internet y los mecanismos de software que ayudan a que la comunicación en Internet sea segura, se pueden dividir en términos generales en tres conjuntos. El primero, se enfoca a los problemas de autorización, autenticación e integridad. El segundo, se enfoca al problema de la privacía y el tercero, se orienta hacia el problema de la disponibilidad mediante el control de acceso.

7.3.3.2 Mecanismo de autenticación

Los mecanismos de autenticación resuelven el problema de verificar la identificación. Muchos servidores, están configurados para rechazar una solicitud a menos que la origine un cliente autorizado. Para validar la autorización, un servidor debe conocer la identidad del cliente, por ejemplo una forma débil de autenticación en Internet es utilizar la dirección IP. La autenticación de fuente IP es débil debido a que se puede romper fácilmente. En una red como Internet en la que los datagramas pasan a través de enrutadores y redes intermedias, la autenticación original puede ser atacada desde una máquina intermedia.

Una forma mas segura de saber si un cliente o un servidor se están comunicando o no como un impostor, es utilizando un sistema de cifrado de clave pública.

7.3.3.3 Mecanismos de privacía

El cifrado también puede manejar problemas de privacía. Por ejemplo, si un emisor y un receptor utilizan esquemas de cifrado de clave pública, el emisor puede garantizar que sólo el receptor involucrado pueda leer un mensaje. Si es así, el emisor utiliza la clave pública del receptor para codificar el mensaje y el receptor su clave privada para descodificar el mensaje. Dado que solo el receptor involucrado tiene la clave privada necesaria, en ningún otra parte se puede descodificar el mensaje. Así, la privacía puede reforzarse aun cuando una tercera parte obtenga una copia de los datagramas conforme éstos pasan entre el emisor y el receptor.

Los mecanismos de cifrado de clave pública pueden utilizarse para ayudar a resolver los problemas de autenticación, autorización y privacía. Por otra parte, es necesario que tanto el software del cliente como el del servidor deben ser modificados para poder usar estos mecanismos.

Antes de que una organización pueda elegir un mecanismo para reforzar la seguridad, es necesario establecer una política de información.

El mecanismo de paredes de fuego (fire wall) para la seguridad se utiliza para controlar el acceso a Internet. Esto se lleva a cabo de la siguiente manera, una organización coloca una pared de seguridad en cada enlace que realice la conexión de salida hacia el mundo exterior (Internet global), esto es para garantizar que la red interna de la organización se mantenga libre de tráfico no autorizado. Una pared de seguridad consiste en dos barreras y una computadora o dispositivo seguro, llamada anfitrión baluarte. Cada barrera utiliza un filtro para restringir el tráfico de datagramas. El anfitrión baluarte ofrece servicios visibles desde el exterior y corre clientes que acceden a servidores externos. La organización utiliza su información y sus propias políticas de acceso a Internet para determinar cómo configurar el filtro. Por lo general, la pared de seguridad bloquea todos los datagramas que llegan desde el exterior, excepto los destinados al anfitrión baluarte en donde este verifica ciertos datos de información del datagrama y determina si le da acceso o no a la red protegida.

7.3.4 Crecimiento y tendencias del futuro de Internet

Tanto la tecnología TCP/IP como Internet continúan evolucionando. Se siguen proponiendo nuevos protocolos; los mas antiguos se están revisando. La NSF añadió una considerable complejidad al sistema al introducir una red de columna vertebral, redes regionales y cientos de redes a nivel de campus. Otros grupos alrededor del mundo se conectan día con día a Internet. Sin embargo, el cambio más significativo no viene de la adición de conexiones de redes, sino del tráfico adicional. Cuando nuevos usuarios se conectan a Internet y aparecen nuevas aplicaciones, los patrones de tráfico cambian. En el pasado, cuando los físicos, químicos y biólogos comenzaron a utilizar Internet, intercambiaban archivos de datos sobre sus experimentos. Dichos archivos parecían muy grandes comparados con los mensajes de correo electrónico. Cuando Internet se volvió más popular y los usuarios comenzaron a rastrear información utilizando servicios como gopher, World Wide Web, el tráfico se incremento de nuevo.

En la actualidad, es difícil visualizar un fin de la necesidad de mayor capacidad. El crecimiento en las demandas para las redes no debe ser una sorpresa. La industria de la computación ha disfrutado por muchos años de una demanda continua de mayor poder de procesamiento y de mayor almacenamiento de datos. Los usuarios apenas han comenzado a entender cómo utilizar las redes. En el futuro podemos esperar incrementos continuos en la demanda de comunicaciones. Por lo tanto, se necesitarán tecnologías de comunicación con mayor capacidad para incorporar el crecimiento.

En la siguiente tabla se demuestra el crecimiento de la Internet conectada. Además de los incrementos en el tráfico que resultaron del incremento en tamaño, Internet afronta la complejidad resultante del manejo descentralizado del desarrollo y operación.

Año	Número de redes	Número de computadoras
1980	10	10^2
1990	10^3	10^5
1997	10^6	10^8

Tabla 7.4 Crecimiento de la Internet conectada

7.3.4.1 Necesidad de una nueva versión de los protocolos TCP/IP[188]

La red Internet global ha tenido varios años de crecimiento exponencial, duplicando su tamaño cada nueve meses o mas rápido. La evolución continúa conforme se conectan más columnas vertebrales de redes nacionales, produciendo un incremento complejo de políticas que regulan la interacción.

La versión 4 del protocolo Internet (IPv4) proporciona los mecanismos de comunicación básicos del conjunto TCP/IP y la red global Internet; se ha mantenido casi sin cambio desde su inserción a fines de los años setenta. La antigüedad de la versión 4 muestra que el diseño es flexible y poderoso. Desde el momento en que se diseñó el IPv4, el desempeño de las computadoras se ha incrementado en de magnitud y desempeño, las tecnologías LAN han emergido y el número de anfitriones en Internet ha crecido hasta llegar a un total de mas de 4 millones. Además, los cambios no ocurren de manera simultánea, el IP se ha adaptado a los cambios de una tecnología antes de adaptarse a los cambios de otras. Es por esto, que a pesar de su diseño, el IPv4 también debe ser reemplazado, debido al inminente agotamiento del espacio de direcciones[189]. Actualmente, muchas organizaciones tienen varias redes LAN o incluso cuentan con una red WAN. En consecuencia, el espacio de 32 bits que se usa actualmente no puede adaptarse al crecimiento proyectado de la red Internet global.

Aun cuando la necesidad de un espacio de direcciones extenso está forzando un cambio inmediato en el IP, hay otros factores que también contribuyen. En particular, gran parte de éstos se refieren al soporte de nuevas aplicaciones. Por ejemplo, debido a que el audio y el video en tiempo real necesitan determinadas garantías en los retardos, una nueva versión del IP debe proporcionar un mecanismo que haga posible asociar un datagrama con una reservación de fuente pre-asignada. Además , como varias de las nuevas aplicaciones de Internet necesitan comunicaciones seguras, una nueva versión del IP deberá incluir capacidades que hagan posible autenticar al emisor. Es por esto que los grupos en el ITEF han estado trabajando para formular una nueva versión del IP por varios años. La próxima generación se llamara IPv6, la cuál conservará muchas

[188] Douglas E Comer. TCP/IP, 3ª. edición; Prentice Hall; pp. 497-518.

[189] Cuando IP se diseñó, un espacio de 32 bits era mas que suficiente ya que pocas organizaciones utilizaban las redes LAN y muy pocas tenían una red WAN corporativa.

características que contribuyeron al éxito del IPv4 pero con unas cuantas modificaciones[190].

7.3.4.2 Nuevas aplicaciones[191]

Conforme otras tecnologías hacen su arribo, en un futuro se verán nuevas aplicaciones, algunas de ellas ni siquiera imaginables por la mayoría de los usuarios. Pero indudablemente el uso de multimedia y las bases de datos distribuidas serán algunas de las áreas de mayor atención tengan por parte de los desarrolladores. Por otro lado el objetivo de a red Internet será acercar hasta el último usuario y el último dispositivo de la red de área amplia al escritorio de los administradores, de tal manera que sea transparente si se encuentra en la oficina de junto o al otro lado del mundo.

Las nuevas aplicaciones constituyen una de las áreas de mayor interés por parte del usuario de la red Internet, estas nuevas aplicaciones cada ves mas poderosas e interesantes requerirán un mayor número de recursos de los equipos y de las redes actuales, a continuación hablaremos un poco de las áreas donde se espera que se desarrollen estas nuevas aplicaciones.

Comercio:

Con el auge comercial de Internet, cada vez es más frecuente el establecimiento de centros comerciales virtuales incluso algunas compañías están vendiendo sus productos directamente por medio de páginas web. Además de poder realizar compras se pueden realizar transacciones de diversos tipos, por tal motivo se requerirá de un manejo muy eficaz sobre la seguridad del paso de información de alta confidencialidad, es por esto en las aplicaciones futuras deberán incluir mecanismos con alto grado de seguridad en el paso de la información a través de la Internet global.

Educación:

Actualmente se encuentran en exploración las posibilidades de la educación a distancia por medio de Internet. Este medio se presenta como una herramienta de gran valía en la educación a los usuarios de las redes Institucionales educativas y corporativas, pues, sí es correctamente utilizada, permitirá ahorros substanciales en la contratación de instructores y en el desplazamiento de los usuarios hacia los centros educativos (que muchas veces pueden estar incluso en otro país).

---

[190] Si desea una mayor información referirse al capitulo 4 de este trabajo, "Protocolos de Comunicación".

[191] "Internet el servicio para la empresa"; Revista RED, ano VI, septiembre 1996 Núm. 76.

CAPÍTULO 8
ESTUDIO DE LAS SOLUCIONES POR ETAPAS PARA LA REDII: ANÁLISIS, EVALUACIÓN Y SELECCIÓN

8.1 Metodología de planeación y evaluación de proyectos de informática (adaptado a proyectos de redes de computadoras)

8.1.1 Introducción

La finalidad de esta metodología es indicar como planear, preparar y evaluar proyectos de informática. En este caso se adecuó para el estudio de la red del Instituto de Ingeniería enfocándose a los requerimientos del mismo, proporcionando una pauta que permitiera determinar una configuración que realmente cubriera las necesidades de los usuarios, además de seguir las normas y restricciones que impone actualmente la institución.

8.1.2 Metodología para la evaluación de equipamiento computacional

La metodología, tiene como objetivo servir al diseñador de redes como un fundamento estructurado de como llevar a cabo la planeación de una red y por otro lado el de contribuir a la toma de decisiones del proyecto, de la manera mas conveniente, utilizando como herramientas algunos criterios de evaluación económica.

8.1.2.1 Problemáticas detectadas en los proyectos de informática

Particularmente en proyectos de informática en donde se requiere efectuar un análisis mas profundo realizando una evaluación económica, existen algunos problemas comunes, los cuales se relacionan con el tipo de análisis que se debe llevar a cabo (un análisis costo-beneficio o un costo-efectivo). Cuando se tiene que tomar una decisión de asignar recursos a una alternativa de inversión, es decir, cuando se tiene que decidir entre aceptar un proyecto o no, lo ideal sería realizar un análisis tanto de los costos como de los beneficios y compararlos, este es referido como un análisis **costo-beneficio**.

El análisis costo-beneficio implica que tanto los costos como los beneficios son medibles y valorables, ya que es necesario compararlos entre sí; esto quiere decir que deben poder ser expresados en unidades monetarias. Así la evaluación costo-beneficio indicaría cuál es la riqueza adicional que se tienen por llevar a cabo el proyecto (cuanto dinero más se obtiene); también se sabría que tasa interna de rendimiento genera el proyecto (o alternativa de inversión). Un beneficio directo (y posiblemente el mas importante) es la liberación de horas-hombre (H-H) o un aumento en la productividad; el problema se presenta al tratar de medirlo. Esto nos lleva a decir que no siempre es posible medir y aún más difícil valorar los beneficios en un proyecto de informática como el que se está llevando a cabo, por ejemplo, como se puede medir el ¿Cuanto vale para el Instituto de Ingeniería el tener una red de mayor velocidad? o ¿Cuanto estarían dispuestos a pagar los usuarios de la red por tener un mejor servicio?. Es por esto, que en los proyectos donde se requiera un estudio económico además de un estudio técnico, se recomienda hacer un análisis costo-efectividad[192] para realizar dicho estudio, ya que este tipo de evaluación se lleva a cabo a partir del planteamiento de unos objetivos bien definidos a los que se quiere llegar, y posteriormente se elige la opción de menor costo que alcance todos los objetivos.

8.1.2.2 Análisis Costo-efectivo o costo-efectividad

El análisis costo-efectivo se encuentra basado en la idea de que la evaluación económica de proyectos de computo generalmente muestran rentabilidades altas, es decir, siempre traen beneficios por ende, y por tanto, solo cabe centrarse en la optimización del proyecto por medio de una buena selección de las alternativas.

La metodología costo-efectivo plantea que la conveniencia de llevar a cabo un proyecto se determina por la observación conjunta de dos parámetros:

- El **costo**[193] que involucre la implantación de la solución informática, desde la adquisición del equipo hasta la puesta en marcha del sistema hardware y/o software, además de los costos de operación asociados.
- La **efectividad**, que se entiende como la capacidad del proyecto para satisfacer la necesidad, solucionar el problema o lograr el objetivo para el cuál se ideó; es decir, un proyecto será superior o inferiormente efectivo en relación al mayor o menor grado del cumplimiento del objetivo final para el cual fue creado.

---

[192] La limitación de este tipo de análisis es que no se conoce el incremento monetario que se tiene por realizar dicho proyecto.

[193] La cuantificación y medición de los **costos** en cualquiera de los dos análisis, no reviste mayor complejidad; en cambio, en la cuantificación de los beneficios son en su mayoría intangibles o de difícil medición.

Como nota final, cabe mencionar que los objetivos a los que se quiere llegar, los debe plantear alguna autoridad dentro de la organización, en este caso, el Instituto de Ingeniería. También deben decidir sobre el momento optimo de realizar la inversión y hacer el cambio (de la tecnología de red) dentro del Instituto.

Esta metodología se encuentra al nivel de preinversión de un proyecto[194]. Ya que establece la preparación y evaluación de un proyecto, a fin de determinar la conveniencia en su inversión y posterior puesta en operación.

8.1.2.3 Nivel de preinversión

El estado de preinversión tiene por finalidad el efectuar algunos estudios relativos a los aspectos **técnicos, económicos y de mercado.**[195]

Dependiendo del nivel de análisis que se desea alcanzar y en base al monto disponible a invertir en cada proyecto, la preinversión se puede subdividir en tres etapas sucesivas. Estas son: nivel perfil, prefactibilidad y factibilidad.

Para un proyecto que no requiera de grandes sumas de dinero para lograr sus objetivos[196], bastará con efectuar un estudio a **nivel de Perfil**, es decir, su información no deberá ser muy exhaustiva en la descripción de los puntos por analizar, pero si debe permitir formarse un juicio respecto de la conveniencia y factibilidad técnico-económica de llevar a cabo el proyecto. Cuando el proyecto en análisis involucre muy pequeñas cantidades dinero y su perfil muestre la conveniencia de realizarse, se debe ir directamente a la etapa de implantación.

Si el monto del proyecto es superior al anterior[197], se debe efectuar un **estudio de prefactibilidad**, en el cual se deberá analizar con mayor grado de detalle aspectos identificados en la etapa anterior (nivel de perfil), tanto en los aspectos técnicos como económicos y en especial los que inciden en la factibilidad y rentabilidad del proyecto. Además, se deben examinar en detalle las alternativas más convenientes seleccionadas en la etapa anterior.

---

[194] Existen tres estados posibles en la trayectoria de un proyecto, estos son: preinversión, inversión y operación.

[195] Conviene abordarlos en el orden antes expuesto, a fin de lograr coherencia en la información necesaria para efectuar la evaluación.

[196] Este rango de monto de dinero, depende de la normas administrativas de cada institución, en este trabajo se recomienda como base de referencia 25,000 dólares, no obstante puede estar sujeto a cambio según el evaluador de proyectos de cada organismo.

[197] Este rango también depende de cada organismo, en este trabajo se recomienda como base de referencia una cantidad que fluctúe entre los 26,000 y los 150,000 dólares.

Por último, cuando el monto del proyecto supere la cantidad requerida para efectuar el estudio de prefactibilidad[198], se deberá llevar a cabo un **estudio de factibilidad**, que es la última etapa. En este punto se abordan los mismos aspectos de las etapas anteriores, pero se profundiza el análisis y la descripción de las variables que inciden en el proyecto. Se deberá minimizar la holgura esperada en aspectos económicos, tales como la determinación de costos, beneficios, calendario de inversiones, fuentes de financiamiento, etc. y en lo técnico puntos tales como la capacidad de expansión, vida útil, compatibilidad, etc. Si la empresa no posee personal capacitado para realizar un estudio con la profundidad que se exige en este nivel, se aconseja contratar asesoría externa para cumplir con tal objetivo.

8.1.2.4 Etapas de la metodología para el estudio de preinversión

- Antecedentes generales.
- Diagnóstico.
- Optimización de la situación actual.
- Definición de requerimientos y presentación de problemas.
- Alternativas de diseño y proyecto.
- Selección y proyección de alternativas.
- Método de implantación.

8.1.2.4.1 Antecedentes generales

En esta etapa, se hace un estudio de los datos referentes a la organización y el medio ambiente en donde se desarrollara el proyecto, con esto se pretende:

- Conocer el sistema en que se insertará la solución informática. Identificando sus finalidades, restricciones y variables que determinan su actual desempeño.
- Conocer el entorno en que se desenvuelve actualmente el sistema sujeto a estudio.
- Identificar la necesidad que da origen al problema y los objetivos existentes.

Un claro planteamiento de este último punto, apoyado por la descripción general del entorno organizacional ayudarán a la justificación, análisis y comprensión del problema en estudio y por ende, de las distintas alternativas de solución.

[198] Es decir que supere los 150,000 dólares, esto también depende de cada institución.

Para esta etapa, en los antecedentes se debe presentar:

1. Identificación y descripción del problema.

Que problema se intenta solucionar o que objetivo se pretende alcanzar (en términos generales, ya que el análisis en detalle se abordará en la etapa de diagnóstico). Es importante aclarar este punto, por cuanto constituirá el motivo por el cuál se origina el proyecto.

2. Análisis del entorno de la organización:

- Institución: objetivos de la organización, funciones, estructura de la organización y flujos de información mas relevantes.
- Área en que se inserta: señalar las áreas que se verán afectadas por el proyecto y describir brevemente de que forma se afectan.
- Procedimientos y funciones afectadas: profundizar dentro de las áreas afectadas cuáles son los procedimientos y funciones involucradas.
- Recursos utilizados: recursos humanos y de capital, incluidos los recursos computacionales existentes.

8.1.2.4.2 Diagnóstico

La información que resulte de esta etapa es clave para las etapas posteriores, por lo cuál, se deben analizar las áreas problema del sistema actual y diferenciar claramente cuáles corresponden a problemas de gestión administrativa y cuáles a problemas de gestión de información o de requerimientos de información, desarrollando de esta manera, un diagnóstico que sirva de base para diseñar soluciones técnicas o administrativas de acuerdo a la naturaleza del problema. Una fuente de información importante para el diagnóstico podrían ser las opiniones de los usuarios actuales o potenciales y del equipo de administración.

El diagnóstico debe presentar como resultado, la traducción del problema en estudio en términos de requerimientos informáticos. Estos justificarán la inversión en soluciones tecnológicas, y para estos efectos se pueden distinguir entre:

- Entendimiento del sistema actual: en este punto se definirán las problemáticas, deficiencias y limitaciones que se tienen en la arquitectura actual y que se desean resolver con el nuevo sistema.
- Definición de requerimientos: en esta sección se deben especificar los requerimientos del sistema a diseñar tomando en cuenta tanto a los usuarios como al equipo de administración. Estos deberán ser descritos de manera estructurada y lo mas detallado posible.

Como resumen de este punto, deben quedar justificados los problemas y requerimientos, diferenciando claramente cuales están asociados a problemas de informática y cuales a problemas de gerencia; para los primeros se recomienda sintetizar los resultados en requerimientos técnicos, a objeto de poder con posterioridad seleccionar entre distintas alternativas tecnológicas la solución; con respecto a los segundos, esto deberían superarse previamente a la introducción de soluciones tecnológicas.

8.1.2.4.3 Optimización de la situación actual

En base a la etapa de diagnóstico anterior se determinará si es posible mejorar la situación actual, ya sea con medidas administrativas de la red misma, rediseño de organización de la red o con inversiones marginales, teniendo en cuenta que la modificación no es de manera drástica. Es decir, cuando a la situación actual se incorporan inversiones mínimas y medidas de administración de red (pudiéndose considerar también aquellos proyectos que se están llevando a cabo o que se tiene aprobada su ejecución y tienen relación con el proyecto en estudio) que mejoran la eficiencia actual.

8.1.2.4.4 Definición de requerimientos y presentación de problemas para la licitación

Existen dos alternativas en que se puede encontrar el encargado de realizar el proyecto, éstas dependerán de la existencia de equipos computacionales en la organización. Por lo tanto, la determinación de los requerimientos puede ser abordada bajo dos modalidades distintas.

Primero, si la organización no ha poseído nunca equipo computacional, los requerimientos se deben obtener en base a la información generada por los bosquejos del sistema requerido, efectuados con anterioridad al presente documento.

La segunda alternativa debe ser utilizada en los casos que la organización tenga experiencia en el manejo de equipos computacionales. Los requerimientos se deben fundamentar de acuerdo a la información proporcionada por el diagnóstico técnico efectuado en la red bajo análisis, más la suma de las nuevas necesidades que a partir de ellos se detectaron.

El objetivo que se persigue con esta información, es el permitir confeccionar una pauta de requerimientos técnicos, que determine las necesidades que deben satisfacer él o los proveedores que se presenten a la licitación, esta pauta debe estar compuesta por información proveniente del diagnostico técnico más las nuevas necesidades que se presenten. Toda esta información se hará especialmente necesaria cuando se hable de proyectos de inversión con estudio

de factibilidad, exigiéndose el análisis de muchos de estos puntos de una forma más general, realizadas en los estudios de perfil y de prefactibilidad.

Los resultados obtenidos del diagnóstico nos permitirán determinar las características del equipamiento que la organización requiere, incluyendo las nuevas características que surjan de los diseños lógicos y físicos. Debiendo ser respaldado este análisis por aspectos exclusivamente técnicos. Además, se debe presentar en este punto, de manera explícita el problema que debe resolver la organización.

El resultado arrojado en este punto, es la de llegar a explicar cuál es el problema en concreto al que se enfrentara la organización y que con anterioridad no se había podido definir. Luego, con esta información se puede tener una idea clara de lo que persigue la organización.

8.1.2.4.5 Alternativas de diseño y proyecto

Basados en los resultados de la etapa de diagnóstico hechos anteriormente, y realizado un **análisis previo** de especificación de las bases técnicas de las diferentes tecnologías de redes de alta velocidad, aunado con la determinación de las necesidades de la organización, se deben planear distintas alternativas de solución al problema detectado. En resumen, en este punto de la metodología, se deberá incluir el conjunto de **requerimientos** que la organización tenga que satisfacer con la nueva configuración, basándose en el diagnóstico técnico resultante.

Además, esta información está resumida en un conjunto de parámetros y atributos, que permiten confeccionar la **ficha técnica**, la que dándole un adecuado manejo, permitirá determinar el diseño y especificaciones del equipo requerido. En este punto se presentan dos alternativas factibles de llevar a la práctica:

En primer lugar, se presenta la alternativa que dicta la relación con la preparación del diseño del equipo necesario por parte del personal encargado de efectuar el proyecto completo, sea éste propio de la empresa o perteneciente a consultores externos contratados para tal efecto.

Una segunda alternativa que se presenta, es la que dicta la relación al efectuar un llamado a propuesta pública a las empresas proveedoras de sistemas computacionales (licitación), con el objeto que sean ellas las encargadas de efectuar los diseños respectivos, basándose en los requerimientos presentados por la organización, y entreguen sus proposiciones al o los evaluadores del proyecto. Este tipo de solución se presenta en forma atractiva para aquellos proyectos de gran tamano y complejidad, en los cuales se deban efectuar

estudios de prefactibilidad o factibilidad. Pero la determinación de necesidades y requerimientos debe ser efectuada por el equipo evaluador del proyecto, fijando los marcos de referencia dentro de los cuales se deberán limitar los proveedores. Toda esta información, más la proveniente del exhaustivo diagnóstico técnico de la situación actual, permitirá confeccionar la base para la llamada a propuesta pública o privada para los proveedores de hardware o software.

Otro aspecto que merece ser considerado en este punto, es el carácter dinámico e interactivo que posee este tipo de estudio, es decir, se pueden realizar modificaciones de los procesos durante el desarrollo del estudio. Es por esto que debe existir predisposición por parte del evaluador de la organización, o de los proveedores, a fin de efectuar cambios en el momento que éstos se hagan necesarios y en el momento oportuno, con el objeto de alcanzar la meta u objetivo de la mejor forma posible.

La elección del equipamiento debe ser tal que se complete y sea compatible con los sistemas existentes en la organización y que se deseen mantener en operación a futuro.

Una vez presentado un conjunto de alternativas técnicamente factibles, debe realizarse el prediseño respectivo. Este corresponde a la presentación de cada alternativa con un resumen de sus puntos técnicos y económicos más importantes.

8.1.2.4.6 Selección y proyección de alternativas

Todas las alternativas que sean técnicamente factibles de implantar en la institución u organización, sean éstas obtenidas por estudios propios o proporcionadas por terceros, deberán ser rigurosamente evaluadas. Estos análisis deben ser del tipo técnico-económico, es decir, deben relacionar aspectos tales como capacidad de operación, crecimiento, velocidad, etc., con aspectos tales como costos, tipo de financiamiento, entre otros.

Cuándo se quiera efectuar una aproximación del comportamiento futuro de cada alternativa estudiada, se puede utilizar técnicas de simulación, las que permitirán obtener una proyección del comportamiento de las alternativas bajo análisis, en el horizonte predeterminado para ésta.

Toda esta información irá produciendo una diferenciación entre las alternativas de equipos postulados.

Como criterio general, y tal como se planteó en los puntos referidos al análisis y selección de alternativas, la propuesta debe ser sobre una opción de configuración optima de red, es decir, una alternativa tecnológica y nunca una alternativa de marca específica de equipos. Este criterio con mayores motivos aún debe mantenerse en las especificaciones referidas en la licitación.

Cuando se presente el conjunto de alternativas técnicamente factibles, se puede recurrir a distintas técnicas a modo de seleccionar la mejor alternativa. Un mecanismo muy utilizado, y recomendable a su vez, es la de trabajar con el **método de puntuación aditiva**, el cuál consiste en hacer matrices compuestas de parámetros y atributos con ponderaciones (esta técnica se explicará posteriormente).

Si en la preselección de alternativas anterior, quedara alguna incertidumbre respecto a la selección entre dos o más alternativas por tener razones de costo-efectividad similares, se deberá hacer la evaluación costo-beneficio para todas ellas. Si por el contrario en el análisis de alternativas tecnológicas ya se pudo seleccionar una, se realizará la evaluación para dicha alternativa solamente.

Por lo explicado anteriormente referido a la medición de beneficios, es aconsejable que la medición y valoración de beneficios se aborde solo para proyectos que por su magnitud tengan un impacto económico significativo en la organización, es decir que el monto sea mayor a los $250,000 dólares. Para los proyectos "pequeños", podría ser preferible llegar sólo hasta la identificación de los beneficios sin cuantificarlos.

Obviamente, la selección final se hace sobre el proceso de licitación. Sin embargo, el análisis previo de generación y selección de alternativas que se está proponiendo debería ayudar a una mejor especificación de las bases técnicas para la licitación, evitando conflictos por vacíos en las bases y acotado el espacio de alternativas; permitiendo un análisis más minucioso de las propuestas.

La selección entre alternativas se puede hacer en forma cualitativa en proyectos "pequeños". Para proyectos "grandes" se recomienda usar el método que se propone a continuación, que correspondería a un nivel de prefactibilidad o factibilidad.

8.1.2.4.6.1 Método de puntuación aditiva

Se propone un método de selección jerárquico, en particular un **método de puntuación** (aditivo) en el cual se definen los atributos más relevantes de la configuración, asignándoles puntuaciones a cada atributo en cada configuración y ponderaciones a cada atributo. Finalmente se estudia el puntaje de cada

alternativa propuesta con la siguiente función referida como función de modelo aditivo:

$$P_j = \sum W_i U_{ij}$$

Pj: Puntaje de la alternativa j
Wi: Ponderador del atributo i.
Uij: Puntuación de la alternativa j respecto al atributo i.

Volviendo al modelo aditivo, podemos representar las puntuaciones y ponderaciones en una matriz. Si algún atributo es irrelevante para el evaluador se le asigna un ponderador igual a cero. A la matriz anterior se le pueden agregar atributos tales como los resultados de las pruebas por empresas independientes (benchmarks) y pruebas de carga cuando sea factible hacerlas (para proyectos que por su complejidad lo requieran, se recomienda usar una matriz más compleja y realizar las pruebas de carga pertinentes[19]).

A los atributos medibles en **puntajes** se les deben asignar puntos de acuerdo a tablas como la siguiente:

Porcentaje	Calidad
< 50	Mala
50-70	Regular
70-80	Buena
80-90	Muy buena
90-100	Excelente

Tabla 8.1 Ejemplo de una tabla con rango de calificaciones

Un problema posible de presentarse en la aplicación de un modelo como este, es la estimación de los ponderables Wi. En efecto, el proceso de asignación de puntajes y ponderaciones, presupone claridad respecto a los requerimientos; problemas del actual sistema, objetivos del nuevo sistema, funciones administrativas y sistemas administrativos a ser apoyados por la configuración, ya que de lo anterior dependerán los ponderadores que se le asignen a cada atributo. Si se dan las condiciones anteriores, y lo que es tanto o mas importante, si los evaluadores disponen del tiempo necesario para acceder a la información relevante y hacer los análisis correspondientes, debería esperarse que el valor asignado a los ponderadores refleje las necesidades de la organización con respecto al sistema informático.

Al no darse esas condiciones queda abierto la posibilidad de que el evaluador "maneje" los ponderadores para "seleccionar" alguna alternativa preconcebida, lo que hace que la herramienta resulte inservible para los objetivos de acercarse a la

[19] Resulta de gran interes poder hacer simulaciones que permitan proyectar el funcionamiento del equipo en situaciones ficticias (por ejemplo, ante el aumento de la carga).

selección de una buena configuración computacional. Como una posible forma de salvar esta dificultad podría seguirse un proceso interactivo entre el evaluador y la persona encargada de revisar el proyecto hasta acercarse a algún valor adecuado para los Wi.

8.1.2.4.7 Método de implantación

Por último se debe desarrollar un plan apropiado para llevar a cabo la implantación, de acuerdo a la organización, el sistema y el problema que se está buscando resolver.

8.2 Objetivo

La implantación de una red de computo de altas especificaciones capaz de adaptarse las exigencias actuales y futuras del Instituto, guardando ciertos lineamientos como son, el ser estándar, segura, administrable, además de ser escalable de manera flexible.

8.3 Funciones y requerimientos de la REDII

Para poder llegar a nuestro objetivo de la implantación de una red de altas especificaciones es necesario primero definir las funciones y requerimientos que debe cubrir el nuevo sistema. Con esto nos referimos a tener en claro las deficiencias, problemáticas y limitaciones que se tienen en la arquitectura actual y que se desean resolver con el nuevo sistema y por otro lado las necesidades futuras por cubrir y para las cuales queremos estar preparados.

8.3.1 Problemas y limitaciones de la REDII

Como se explico anteriormente en el capitulo 7, el Instituto de Ingeniería tiene una red Ethernet 10Base5 (bus de cable coaxial grueso) en el backbone principal y Ethernet 10BaseT en el interior de los edificios. Antes de entrar en detalles, se explicara de manera breve la forma de operación de este tipo de tecnología y posteriormente se procederá a definir los problemas y limitaciones que se tienen actualmente en la REDII.

Las redes Ethernet son redes de difusión (broadcast) o medio compartido, es decir, que todos los nodos sobre la red comparten una ruta de comunicación común y que solo un dispositivo puede usarlo en un momento dado, ya que la transmisión de datos de este se propaga hacia todos lados sobre el segmento. Si un nodo se está comunicando, entonces todos los demás deberán esperar, creando cuellos de botella y contención por el acceso al medio. En el caso que dos dispositivos intenten transmitir al mismo tiempo ocurrirá una colisión y todos los dispositivos deberán esperar un tiempo aleatorio para intentar

transmitir de nuevo. Cabe mencionar que el redimiendo de este tipo de red se degrada cada vez que se conecta un nuevo dispositivo debido a que disminuye la probabilidad de transmisión de todos los dispositivo conectados y aumenta la probabilidad de que ocurran colisiones.

En este tipo de red como se puede observar tiene varias deficiencias y limitaciones generales, además de que existen problemas particulares de la red misma del Instituto, los cuales se explicaran con mas detalle a continuación.

Dentro de las problemáticas fundamentales que se tienen en la red, son las deficiencias ocasionadas por el cable coaxial utilizado en el backbone, como la vulnerabilidad a interferencias electromagnéticas y la dificultad para localizar y aislar fallas debido a su topología de bus físico, afectando la confiabilidad y disponibilidad de toda la red. Asimismo el estándar 10Base5 en particular, tiene un crecimiento limitado a un cierto número de nodos sin la posibilidad de ser escalada.

Las redes tipo Ethernet como se explico anteriormente se encuentran basadas en el protocolo de acceso al medio referido como CSMA/CD[200], por lo cual el crecimiento de dispositivos conectados dentro de la red del Instituto a llevado al problema de mayor número de colisiones y un mayor retraso en la transmisión de información entre dispositivos. Afectando directamente en gran medida a los servidores de aplicaciones que deben competir por el medio de transmisión teniendo de esta manera un desempeño ineficiente y pobre de tiempos de respuesta para las peticiones de los usuarios.

Además de que la red del Instituto ha crecido en complejidad y tamaño, y aunado a que los patrones de trafico de las aplicaciones de los usuarios han cambiado (manejo datos, imágenes y audio en una misma aplicación), ocasionando de esta manera que la red actual alcance mas fácilmente los niveles de congestionamiento durante momentos de cargas de trafico altos, ya que este tipo de redes fue diseñada pensando en un pequeño numero de dispositivos y con un tipo de aplicaciones que demandaban un menor ancho de banda (basadas principalmente en transferencia de datos tipo texto).

Otra de las deficiencias que se tiene dentro de la red del Instituto, es que no existe ningún esquema de administración y monitoreo de los diferentes dispositivos conectados a esta, lo cual con lleva a una mala prevención, detección y corrección de fallas, además de no saber de que manera están siendo aprovechados los recursos de la red.

---

[200] En el método de control de acceso al medio CSMA/CD cada uno de los dispositivos conectados a un mismo segmento compite por el derecho a transmitir.
Se ha comprobado matemáticamente que las colisiones limitan el rendimiento de una red Ethernet operando cerca del 40% de su capacidad total, es decir, una red traslada solo 4Mbps sobre una red Ethernet a 10Mbps.

En relación a la seguridad se tienen deficiencias tanto físicas como lógicas con respecto a la red en sí, por ejemplo, que el cable coaxial utilizado no se lleva a través de ductos especiales únicos para protección de este, así mismo, los elementos que conforman la red como son los concentradores y puentes no se encuentran localizados en sitios seguros como son closets de acceso restringido. Con respecto a la seguridad lógica, las redes tipo Ethernet tienen la desventaja de poder operar en modo promiscuo, de esta manera se permite a cualquier persona el monitorear todo el trafico que fluye a través de la red.

Por otro lado, existen muchos dispositivos de interconexión de red (concentradores, etc.) que no cuentan con sistemas tolerantes a fallas (módulos intercambio rápido (hot swap)[201], fuentes redundantes), Fuentes de Poder Ininterrumpible (UPS) etc. lo cual afecta directamente la disponibilidad de la red.

En lo concerniente a las capas superiores, en el Instituto se manejan diferentes protocolos de comunicación de alto nivel como son: TCP/IP, IPX/SPX y NetBEUI[202], los dos ultimos protocolos estan encaminados a realizar funciones similares, ocascionando deficiencias en la administración, tales como tener duplicidad de información, desperdicio de recursos (p. ej. servidores con diferentes plataformas, entre otros) y la falta de estandarización en la manera de trabajar para los usuarios y administradores, etc.

8.3.2 Requerimientos futuros de la REDII

Una vez señaladas las limitaciones y deficiencias existentes en el sistema actual[203], se deben definir los requerimientos pretendidos que se tienen en el Instituto y que deberán ser resueltos por el nuevo sistema.

Dado que todas las redes de comunicaciones son diferentes y que cada una tiene su propio conjunto de necesidades y expectativas, se definirán los requerimientos en base a los puntos que son principales y que deben tomarse en cuenta para el diseño de la red.

---

[201] El término "Hot swap", quiere decir que no es necesario apagar el dispositivo para poder cambiar dicho modulo.
[202] Para mayor información referirse al capitulo 4 "Protocolos de Comunicación"
[203] Cabe mencionar que pueden existir otros problemas dentro de la red pero que no se abarcarán dentro del contexto de este trabajo, ya que no se considera que tengan una importancia relevante.

8.3.2.1 Acceso a usuarios

El nuevo sistema a implantar deberá manejar un backbone de alta velocidad además de ofrecer otras características como son calidad de servicios y/o manejo de prioridades si es necesario, para poder soportar aplicaciones tanto de consumo intensivo de ancho de banda como las orientadas a clases de servicios. En la tabla 9.1 se muestran algunos ejemplos de este tipo de aplicaciones las cuales se desea brindar en el Instituto de Ingeniería.

	No multimedia	Multimedia
En tiempo real	• Servicios de información de tiempo crítico (p.ej monitoreo de la red en tiempo real) • Control de procesos (p.ej. monitoreo de procesos en tiempo-real)	• Videoconferencias • Educación a distancia • Colaboración de aplicaciones compartidas de escritorio
En tiempo no real	• E-mail • Gestión de bases de datos convencionales • Transferencia de datos • Sesiones remotas • Herramientas con interfaces gráficas	• Documentos con manejo de voz (p.ej. correo de voz) • Reproducción de video • Manejo de imágenes • Páginas de Web (imágenes, audio y texto)

Tabla 8.2 Servicios y aplicaciones que serán soportados en el Instituto de Ingeniería

Por otro lado, es necesario que siga soportando los protocolos de comunicación de alto nivel como son TCP/IP, NetBEUI e IPX/SPX y de esta manera mantener de una manera transparente una completa compatibilidad entre la nueva arquitectura de red, las aplicaciones y los usuarios.

8.3.2.2 Conectividad

Los equipos de interconexión que conformen la arquitectura de la red deberan permitir una escalabilidad ordenada por medio de productos apilables o modulares para que puedan satisfacer el crecimiento en el número de usuarios del Instituto.

De igual manera las tecnologías utilizadas deberan cumplir los requisitos de distancia de cableado necesarios para que la red pueda ser accesible desde cualquier parte del Instituto.

El tipo de cable adecuado así como las instalaciones para esté, deberán satisfacer los requerimientos actuales y futuros relativos a la velocidad de transmisión de datos, la topología del nuevo sistema a ser implantado, además de cumplir con las normas de cableado estructurado (EIA/TIA 568) y las medidas de seguridad

físicas requeridas como son: ductos especiales de cableado, armario de telecomunicaciones de acceso restringido, inmunidad a interferencias electromagnéticas, etc.

Se deberá asegurar la existencia de adaptadores de red para los los diferentes tipos de plataformas (computadoras personales, estaciones de trabajo: Sun, HP9000, SGI e IBM), utilizadas en el Instituto de Ingeniería para la o las tecnologías seleccionadas para la arquitectura de red.

Un punto importante que debe tener el sistema, es que permita la organización lógica de los usuarios por medio de uso de redes virtuales (VLANs), no debiendo estar limitados por la localización física de estos[204]. Asimismo, una organización logica permitirá llevar un eficiente control de trafico al poder realizar control multicast, limitar las tormentas de broadcast además de mantener una mayor seguridad de transmisión y una manera mas fácil de realizar las funciones de administración de grupos de trabajo.

8.3.2.3 Interoperabilidad

Los elementos de hardware y software de red utilizados, deberán cumplir con los estándares abiertos, y de esta manera garantizar la interoperabilidad entre las diferentes plataformas usadas en el Instituto y con RedUNAM, además, de asegurar la no dependencia de un solo proveedor.

8.3.2.4 Capacidad de desempeño

La rápida evolución en el poder de procesamiento de los equipos conectados aunado con la reciente proliferación de múltiples aplicaciones cada vez mas sofisticadas y que demandan un incesante consumo de ancho de banda, todo esto sin realizar modificaciones en la infraestructura de red actual ha llevado a que se alcance mas fácilmente los niveles de congestionamiento durante momentos de cargas de trafico altos y degradando sus niveles de desempeño. Es por esto que la nueva arquitectura de red deberá ser lo suficientemente flexible para que nos permita manipular su configuración y usar esta para llevar a cabo alteraciones hasta alcanzar un nivel de desempeño óptimo cuando sea necesario.

---

[204] Por ejemplo, los equipos de los usuarios que participen en un proyecto conjunto requieren del acceso compartido de recursos de computo comunes, pero los miembros de los grupos de trabajo no siempre se encuentran físicamente cercanos, este tipo de inconvenientes puede dar lugar a presiones significativas en la red actual, la cual esta organizada de manera física mas que lógica dando como resultado cuellos de botella y desperdicio innecesario de ancho de banda.

8.3.2.5 Administración

Se requiere una plataforma de administración que sea capaz de extraer información del estado, configuración y rendimiento de los distintos dispositivos[205] conectados a la red. Esta plataforma deberá estar basada en los estándares de administración SNMP y RMON. Lo anterior servirá para que los administradores de red puedan consultar la información en diversos formatos y utilizar métodos estadísticos para evaluar de que manera están siendo aprovechados los recursos de red, además, el sistema de administración ayudará a los administradores a medir el rendimiento de la red, diagnosticar fallas y control recursos, igualmente a mantener un nivel mayor de seguridad.[206]

NOTA: Debido que realizar un esquema completo de administración y monitoreo se encuentra fuera del alcance de este trabajo. Solo se tendrá la responsabilidad de que los equipos contemplados soporten los estándares de administración y monitoreo SNMP y RMON, y que los proveedores proporcionen una herramienta que interopere con la plataforma de administración que se maneja dentro del Instituto a través de las aplicaciones SunNet Manager y LanView.

8.3.2.6 Seguridad

Las principales políticas a considerar en el sistema de seguridad requerido dentro de la red del Instituto son:

- Servicios de confidencialidad: estos servicios ocultan los datos al acceso no autorizado y aseguran al emisor y al receptor que la información no sea vista por personal no autorizado.
- Servicios de autentificación: estos servicios identifican a los usuarios cuando acceden a la red y proporcionan la prueba de autenticidad a los dispositivos de la red.
- Servicios de integridad: Estos servicios son especialmente importantes para la transacción de información de alta confidencialidad ya que proporciona la garantía de que los mensajes son auténticos y no están modificados.
- Servicios de autorización: estos servicios proporcionan a los usuarios autentificados el acceso a los servicios de la red por medio de derechos de acceso.
- Filtrado de paquetes: este servicio evita el acceso no autorizado tanto a información como dispositivos críticos.

---

[205] Es necesario que los dispositivos de interconexión de la red también cumplan con los estándares de administración SNMP y RMON para que puedan ser monitoreados y administrados completamente.

[206] Se debe tomar en cuenta, que los sistemas de administración pueden añadir un exceso de tráfico a la red, dependiendo de las funciones de administración que se encuentren activadas.

- Administración de llaves: el cual incluye la distribución y mantenimiento de las llaves seguras utilizadas para la encriptación y autentificación, la creación y mantenimiento del acceso y sistemas de protección de claves de acceso (passwords), además de la integración de éste con la infraestructura de administración completa de la red.

NOTA: solo se verán las características que ofrecen los dispositivos de interconexión referente a la seguridad que estos soportan, quedando fuera del alcance de este trabajo la implantación del esquema completo de seguridad contemplado en los puntos anteriores.

8.3.2.7 Tolerancia a fallas

Por la importancia que ha tomado la red dentro del Instituto de Ingeniería es indispensable que la infraestructura a implantar tenga los mas altos niveles de disponibilidad y confiabilidad. Esto se lleva a cabo en gran medida al tener una red tolerante a fallas.

Debido a lo anterior, no es permisible que la falla de un solo componente afecte a toda la red, por lo que hay que tomar en cuenta varios puntos para tener una red de estas características:

- Enlaces múltiples: De esta manera se asegura que todos los dispositivos principales estarán interconectados por lo menos a dos rutas. Además de proveer un incremento en la capacidad de transmisión de la red excediendo la capacidad requerida (balanceo de cargas[207]). Estos enlaces pueden ser usados como parte de la operación normal de la red y si falla un enlace, el otro estará de respaldo.
- Dispositivos de red: Los equipos de interconexión que conformen la arquitectura de red deberan incluir componentes que ofrezcan características de tolerancia a fallas (modulos redundantes) y modulos de intercambio hot swap para la corrección en tiempo de operación.
- Fuentes de Poder Ininterrumpible (UPS: Uninterrumptible power supplies): Estos son capaces de soportar una red durante unos minutos o unas horas. Su principal propósito es proteger a la red cuando se suspende el suministro de energía eléctrica durante un período corto.

8.3.2.8 Flexibilidad topológica

La red deberá ser capaz de absorber los cambios que demande el Instituto sin la necesidad de un rediseño total o de sufrir cambios abruptos en el diseño de ésta. Es decir, que una simple actualización no requiera cambios significativos y de esta manera realizar la protección de la inversión en lo mas posible. Además, la

[207] Esta caracteristica solo es soportada por algunos equipos.

flexibilidad establecerá los principales puntos para que las tecnologías de las próximas generaciones puedan ser integradas sobre la base del sistema ya instalado.

8.3.2.9 Documentación

Por último, se requiere que la arquitectura de red este documentada en su totalidad ya que esto servirá de base para futuras expansiones, soporte de ésta e interpretación de los objetivos originales de la red.

8.4 Diseño e implantación de la arquitectura de red del Instituto de Ingeniería

Para llevar a cabo nuestro objetivo de dar una solución óptima de una red de altas especificaciones para el Instituto de Ingeniería es importante desarrollar una arquitectura de red que nos permita un diseño de alto nivel con tecnologías de red apropiadas, esquemas de interconexión, protocolos de transporte, sistemas de administración y servicios, los cuales serán la base para la implantación de ésta.

Entendiendo como arquitectura de red, la planeación donde se establecen las estrategias y anteproyectos para definir mejor los elementos de la red y la relación que estos mantendrán entre sí.

Uno de los factores importantes que tenemos que considerar en este tipo de proyectos en los cuales se desea tener una red local de altas especificaciones y que sin lugar a dudas tendrá un esquema complejo de configuración, es que ésta pueda ser instalada en una serie de etapas, debido a que no todos los requerimientos antes mencionados tienen la misma prioridad en la actualidad y por tanto se tienen que llevar a cabo cuando sean necesarias por el Instituto. Por otro lado, si el proyecto se implantara en una sola etapa implicaría realizar una gran inversión.

Además, un diseño por etapas guiará al Instituto hacia el futuro de la forma mas ordenada y controlada posible, y al mismo tiempo asegurará la protección de la inversión, salvando el mayor valor de los costos.

Antes de determinar las etapas en las que se implantara la red de altas especificaciones para el Instituto, es necesario definir una arquitectura modular que nos permita dividir las funciones de la red por componentes que puedan ser implantados o modificados según sean los requerimientos y prioridades del Instituto y de esta manera sirvan de fundamento para la definición de las etapas.

8.4.1 Definición de la arquitectura modular

Para poder definir una arquitectura modular adecuada, es necesario realizar el diseño teniendo como base el Modelo de Referencia OSI (arquitectura por niveles).

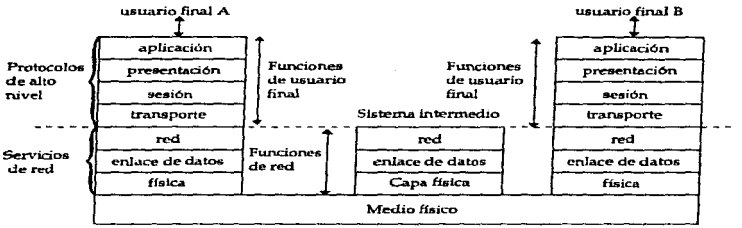


Figura 8.1 Modelo de Referencia OSI

El modelo de referencia OSI consta de siete niveles, los cuales a su vez se pueden dividir en dos grupos:

- Los **protocolos de servicios de red** que están formados por las tres capas inferiores, las cuales se encargan de todas las funciones de comunicación y transmisión propios de la red.
- Los **protocolos de alto nivel** que están formados por las cuatro capas superiores, las cuales ofrecen los servicios propios de los usuarios finales.

En este trabajo, nos enfocaremos principalmente a los **protocolos de servicios de red** y en menor grado a los protocolos de alto nivel debido a que en una buena planeación de las 3 capas inferiores se pueden sobreponer cualquier conjunto de protocolos de nivel superior que se adapten a las necesidades de los usuarios del Instituto de Ingeniería.

Una vez planteado lo anterior, es necesario hacer un diseño basado en las funciones que realizan cada uno de las partes que integran una red (arquitectura modular), es decir, dividir la red dentro de una serie de componentes en la cual cada uno tiene una función especifica dentro de la red.

Los siguientes componentes, pueden servir como principales puntos de referencia para fundamentar la arquitectura modular deseada.

Los componentes en que se dividió la red del Instituto son[208]:

- Backbone: este modulo comprende el sistema de cableado principal que interconecta a los edificios y los principales servidores.

- Conexión a RedUNAM: este comprende el enlace hacia el equipo de RedUNAM (IIMAS).

- Grupo de servidores: este modulo comprende al conjunto de estaciones de trabajo principales que proporcionan los servicios mas importantes del Instituto.

- Infraestructura dentro de los edificios: este modelo se comprende de tres partes, cableado del edificio, tecnología de red y usuarios finales.

- Grupo de protocolos de alto nivel: es el conjunto de protocolos que definen la forma en que se comunican las aplicaciones de los usuarios.

Esta arquitectura modular proporcionará la flexibilidad requerida por la red, para absorber futuras actualizaciones sin la necesidad de hacer cambios abruptos o un rediseño total de la red, además de que permite minimizar los riesgos a fallas y reduce grandemente las interrupciones hacia la red completa.

8.4.2 Definición de las etapas para la red de altas especificaciones del Instituto de Ingeniería

Una vez determinados los módulos en que se puede dividir la REDII, se procederá a definir las etapas necesarias para llegar a nuestro objetivo. La definición se realizara tomando en cuenta las prioridades observadas en la red. Se debe tener en cuenta que cada una de las etapas tiene como meta cubrir diferentes necesidades y por lo cual se pueden tener distintas soluciones posibles, donde cada una de estas soluciones ofrece beneficios específicos para cubrir un conjunto particular de necesidades. Es por esto que en esta sección se realizara el análisis y evaluación de las posibles soluciones de cada una de las etapas, seleccionando posteriormente la que mejor se adecue a nuestras necesidades en base a un análisis costo-efectivo.[209] Posteriormente, en el siguiente capítulo, se planteará el esquema de solución para cada una de las etapas y que beneficios traerá a la red de Instituto.

---

[208] Esta definición de componentes fue hecha a partir de puntos vista y requerimientos particulares de los diseñadores de red de este trabajo. Por lo cual se deja bajo criterio, el uso de estos para otros trabajos.

[209] Cabe señalar que una solución atractiva comercialmente no significa escoger la oferta mas barata.

8.4.3 Etapa 1 Nuevo esquema para el backbone de la REDII

8.4.3.1 Alcance de la etapa

En esta etapa se pretende obtener un backbone confiable y con mayor grado de disponibilidad, a través de llevar a cabo una reestructuración tanto en la topología como en la tecnología actual de la red. Con esto se pretende además tener un mejor aprovechamiento y optimización del uso del ancho de banda actual solucionando el problema de congestionamiento debido al incremento de usuarios sin una planeación adecuada. Por último, que este backbone debe, soportar las nuevas tecnologías sin necesidad de realizar cambios significativos en su esquema.

El monto disponible de inversión en esta etapa es menor a $25, 000 dlls. entrando en el rango de un estudio a nivel perfil.

8.4.3.2 Desarrollo

8.4.3.2.1 Etapa 1.A Sistema de cableado

Dadas las deficiencias que se tienen en el backbone de la red actual (bus de cable coaxial), se considera de suma importancia el cambio de esquema de cableado[210], además de que es prioritario para llevar a cabo cualquier transición hacia una red de altas especificaciones.

8.4.3.2.1.1 Comparación de los medios de comunicación

Los diferentes sistemas de cableado ofrecen distintas características de funcionamiento para distintas áreas dentro del diseño de una red, es por esto que a continuación se comparan y evalúan las posibles soluciones del sistema de cableado mas importantes.

	Cable par trenzado sin blindar (UTP)	Cable Coaxial Grueso 50 ohms	Fibra óptica
Topología soportada	Anillo, estrella, bus	Bus y árbol	Anillo, estrella y árbol
Max. distancia permitida por el estándar EIA/TIA 568	800m	500m	2000m

Tabla 8.3 Comparación de los diferentes tipos de medios

[210] Nos referimos a esquema de cableado al tipo de cable a usar y la topología a configurar.

	Cable par trenzado sin blindar (UTP)	Cable Coaxial Grueso 50 ohms	Fibra óptica
Tipo de senal	canal-unico, unidireccional, dependiendo del tipo de modulación puede ser analogico o digital; half o full dúplex	Multi-canal, unidireccional, RF analogico, half dúplex (full dúplex cuando son usados dos canales o dos cables)	Un canal-unico; unidireccional; half dúplex, senal codificada en luz por fibra; múltiples fibras por cable; full dúplex cuando se usan dos fibras
Máx. Ancho de banda	155 Mbps.	155 Mbps.	Mas de 155 Mbps.
Susceptibilidad a interferencias	alto	media	ninguno
Confiabilidad	media	media	alta
Seguridad	baja	baja	alta
Soporte a nuevas tecnologías	alta	media	alta
Flexibilidad	flexible	rigido	flexible
Duración de vida	3-5	3-5	10-15

Tabla 8.3 Comparación de los diferentes tipos de medios; (continuación)

Siguiendo las características requeridas del backbone en la red del Instituto de Ingeniería, los factores a evaluarse y las calificaciones de cada uno de los medios se demuestran en la siguiente tabla.

	Cable par trenzado sin blindar (UTP)	Cable Coaxial Grueso (50 Ω)	Fibra óptica	Ponderación
Ancho de banda	1	4	5	30
Confiabilidad	1	2	5	30
Seguridad	1	2	5	20
Flexibilidad	5	3	4	10
Costo	5	4	3	10
Calificación	1.8	2.9	4.7	

Nota: Se debe tomar en cuenta que las calificaciones asignadas en la tabla, están en base a como se comportarían los diferentes tipos de cable en un ambiente de backbone principal con las características de la REDII.

Tabla 8.4 Tabla de calificaciones de los tipos de medios

En la siguiente tabla se muestra la escala de calificaciones con sus respectivos criterios, los cuales se utilizaran en todos los casos de selección de la mejor alternativa por medio del método de puntuación aditiva.

Criterio	calif.	Explicación del criterio
Excelente	- 5:	Se asigna a aquellas casos en que el funcionamiento supera en gran medida las expectativas deseadas.
Bueno	- 4:	Satisface los criterios estándar e incluye algunas características especiales.
Suficiente	- 3:	Su función o características son las esperadas.
Pobre	- 2:	Escaso cumplimiento en las funciones o características esenciales.
Inaceptable	- 1:	Es seriamente deficiente.

Tabla 8.5 Criterios de calificación que se tomaron para este proyecto

La fibra óptica al utilizar luz en lugar de señales eléctricas la hace totalmente inmune a las interferencias electromagnéticas, además de ser altamente seguro al resistir accesos no autorizados debido a que no se puede interceptar o interferir la señal[211]. Asimismo le permite alcanzar grandes distancias en el contexto de LANs, sin la necesidad de uso de repetidores. Por otro lado le permite tener un alta integridad de datos (baja tasa de error en la transferencia de datos). Debido a su gran ancho de banda virtualmente ilimitado puede ser usado para la transmisión de todo tipo de datos. El único inconveniente que tiene es que es caro respecto a los empalmes en la interconexión y los generadores de las señales ópticas (sin embargo estos costos son menores). Todo esto lo hace el medio óptimo y justificable para todas las tecnologías de red y telecomunicaciones del futuro.

Existen a su vez, dos tipos de cable de fibra óptica: mono modo y multimodo.

Tipo de fibra	Multimodo	Mono modo
Emisión de senal	por LED	por láser
Ancho de banda*	500 Mbps	Multimegabit
Distancia de transmisión*	2,000 metros**	10,000 metros **
Sensible a la temperatura	Menor	Mayor
Apoyo a multimedia	Si	Si
Facilidad de identificación de fallas y pruebas de instalación	Simple	Simple
Costo de la fibra óptica (cable)	Bajo	Alto (2 veces más que multimodo)
costo de generadores de senal y dispositivos de interconexión	Bajo	Alto (7 veces más que multimodo)

* Fuente: Anixter (http://www.anixter.com)
** Sin uso de repetidores

Tabla 8.6 Tabla de las principales diferencias entre fibra óptica multimodo y monomodo

Dados los requerimientos del Instituto y siguiendo la metodología costo efectivo, se eligió el cable de fibra óptica **multimodo** debido a que cumple con las necesidades de distancia entre los edificios, al mismo tiempo que soporta un

[211] La fibra óptica no permite llevar a cabo derivaciones, ya que cualquier ruptura en el cable ocasionaría fallas en la señal luminosa resultando una caída en la señal de manera instantánea.

ancho de banda satisfactorio para las nuevas y existentes tecnologías y aplicaciones. Otro factor decisivo fue el apoyo que brindo DGSCA para la adquisición de este tipo de fibra ya que se redujeron los costos significativamente, por compra a nivel masivo por parte de la UNAM.

El esquema de cableado para el backbone que se escogió es muy flexible, ya que puede ser configurado en una topología de estrella o anillo, dependiendo de la tecnología que se quiera soportar o implantar en las siguientes etapas (por ejemplo, ethernet conmutado,FDDI o ATM).

8.4.3.2.2 Etapa 1.B Alternativas para optimizar el uso del ancho de banda

Una vez resuelto el problema del tipo de medio de comunicación a utilizar en el backbone y que servirá como base para la siguiente parte de la etapa, se considera como segunda prioridad el resolver la reestructuración que nos permita tener un mejor aprovechamiento del ancho de banda actual y dé solución al congestionamiento debido al incremento no controlado que se tiene de los usuarios, a menor costo y permita escalar. Por ultimo, la solución a la que se llegue, debe ser adaptable a nuevas modificaciones y tecnologías, sin necesidad de realizar cambios significativos en su esquema.

Existen dos enfoques para solucionar el congestionamiento en las redes locales actuales y la optimización del ancho de banda.

El primer enfoque el cual se piensa que es el mas adecuado para esta etapa, es el uso de un dispositivo de interconexión que permita la segmentación de la red[212] y de esta manera optimizarla, al reducir el número de usuarios por segmento y el movimiento de trafico entre las subredes. Los dispositivos que nos permiten llevar esto a cabo son: los conmutadores y enrutadores. Según los requerimientos de cada red se debe escoger el tipo de dispositivo tomando en cuenta como este realiza la segmentación.[213]

El segundo, es instalar una tecnología de red de alta velocidad. Esta solución tiene la gran desventaja de que sería muy cara y todavía no es justificable en estos momentos para el Instituto, además de que se requeriría un cambio abrupto en la mayoría de los módulos de la red.

---

[212] La segmentación es el proceso de dividir un segmento con un gran número de dispositivos conectados en dos o mas segmentos con menor numero de dispositivos, mejorando así el desempeño de la red.

[213] Para mayor información de las diferencias de como realizan la segmentación cada uno de estos dispositivos, referirse al capitulo 5 "Dispositivos de interconexión de redes", en la sección "segmentación con conmutadores y enrutadores".

8.4.3.2.2.1 Selección de la tecnología adecuada

Teniéndose claro que el objetivo es realizar un mejor aprovechamiento del ancho de banda actual[214], y tomando en cuenta que la red del Instituto es del tipo Ethernet y que no tiene que realizar ninguna función de enrutamiento por si misma[215] (red plana), se ha llegado a la conclusión de que la tecnología que mejor satisface estos puntos es la **Ethernet conmutada** (Ethernet switch).

Adicionalmente, Ethernet conmutada nos proporciona un esquema de segmentación adecuado para administrar de mejor manera el ancho de banda que se tiene y al mismo tiempo ofrece una estructuración para tener un mejor control del aumento de usuarios en los edificios. Además, es una tecnología mas barata y requiere menos tiempo de configuración de los dispositivos que una tecnología basada en enrutadores

Por otro lado, el cambio será transparente para los usuarios, soporta la topología de estrella basada en fibra óptica acoplándose a la solución del backbone propuesto anteriormente y además asegura la protección de la inversión de todos los equipos al ser capaz de interoperar al 100% con la tecnología con que se cuenta actualmente y ser reutilizable para modificaciones futuras.

En la siguiente tabla se muestran las características de cada uno de los equipos posibles para la solución Ethernet conmutado, y posteriormente se llevará cabo la evaluación de ellos.

Marca	Modular	redundancia	Protocolos utilizados en el Instituto	Protocolo de Monitoreo /Software	Tipo de cable
ADC Fibermux	Si	Si	Transparente	SNMP LighWatch	UTP, STP, F.O., Coaxial
Cabletron	Si	Si	Transparente	SNMP LanVIEW	UTP, STP, F.O., Coaxial
Intersys	Si	Si	Transparente	SNMP	UTP, STP, F.O., Coaxial

Tabla 8.7 Características principales de los posibles equipos para Ethernet conmutado

[214] Como se explico anteriormente la implantación de una tecnología de red de alta velocidad todavía no es justificable en estos momentos, además de que el ancho de banda actual todavía es el adecuado para las necesidades actuales de los usuarios del Instituto.
[215] Este servicio lo lleva a cabo la RedUNAM.

Marca	Modular	redundancia	Protocolos utilizados en el Instituto	Protocolo de Monitoreo /Software	Tipo de cable
HP	No	Si	Transparente	Si SNMP OpenVIEW	UTP, F.O., Coax. delgado y grueso
RAD LANNET	Si	Si	Transparente	Si SNMP MultiMAN	UTP, STP, F.O., Coax. delgado y grueso

Tabla 8.7 Caracteristicas principales de los posibles equipos para Ethernet conmutado (continuación)

Marca	Rendimiento (%)	Calidad	Mantenimiento y Soporte técnico	Apoyo UNAM
ADC** Fibermux	95	Excelente	Bajo contrato	Cursos de capacitación
Cabletron	95	Excelente	Bajo contrato, después de terminada la garantía	Descuento, mejor servicio, mantenimiento y soporte.
Intersys**	100	Excelente	NO incluido en la garantía	Si
HP*	-	-	-	-
RAD LANNET	90	Muy buena	Incluido dentro del periodo de garantía	No

* No proporciono la suficiente información para poder ser evaluado, además su propuesta estaba comprendida por concentradores repetidores y puentes, por lo cual no puede ser considerado como una tecnología Ethernet Conmutado.
** Es necesario senalar que las empresas ADC Fibermux e Intersys no presentaron su cotización respectiva.

Tabla 8.8 Caracteristicas principales de los proveedores de los equipos para Ethernet conmutado

Entre las principales características por las que se eligió el producto de Cabletron (MMAC-M5FBN con ESXMIM) es que era el único proveedor que ofrecía un esquema completo monitoreo de todos sus equipos y componentes a partir del protocolos de administración SNMP y el CMIP el cual se podía administrar remotamente ya sea a través de productos que manejen estos protocolos o por medio del software LANVIEW o SPECTRUM, por otro lado su diseño modular con componentes hot-swap, permite llevar a cabo de manera rápida y sencilla reparaciones o mantenimientos. Asimismo, permite adaptarse a diferentes tipos de necesidades de expansión ya que su chasis con plano posterior (backplane) de Bus de Red Flexible (FNB: Flexible Network Bus), tiene la capacidad de soportar enlaces hacia tecnologías como FDDI y ATM dependiendo de los módulos con que se configure el MMAC.

Cabe mencionar, que Cabletron fue el único proveedor que soportaba un esquema completo de redundancia a través de la conexión de dos equipos MMAC, con el cual se aseguraba que todos los datos tuvieran al menos dos vías de acceso por medio de conexión de dos o mas dispositivos. Así mismo también tenía la opción de fuentes de energía redundantes y monitoreables por medio del estándar SNMP.

El módulo de conmutación de Ethernet utilizado en el MMAC-5FBN es el modelo ESXMIM-F2, el cuál cumple con las especificaciones FOIRL de Ethernet a 10Mbps sobre fibra óptica, y da un soporte a varias funciones de puenteo, entre las que se incluyen: administración de puenteo a través del algoritmo de árbol expandido (spanning tree, IEEE 802.1d) y filtros de tráfico por destino.

Un último punto, pero el cuál fue muy determinante en la selección que se hizo, fue la interoperabilidad entre los equipos ya instalados en los edificios, y se debe a que todos eran de la marca Cabletron, por lo cual hubo el mínimo de ajustes y era lo mas transparente para los usuarios y se tenía experiencia previa tanto en el funcionamiento y desempeño de los equipos, así como en el tipo de servicio de soporte que proporcionaba dicho proveedor[216]. Permitiendo además, cubrir todo el equipo de interconexión de red en el mismo contrato de mantenimiento.

Selección: Tecnología Ethernet conmutada con topología en estrella basada en fibra óptica multimodo para el backbone principal de la red del Instituto.

8.4.4 Etapa 2 Incremento en el desempeño del grupo de servidores de REDII

8.4.4.1 Introducción

Una vez mejorado el aprovechamiento del ancho de banda por parte de los usuarios en la etapa 1, es necesario incrementar el desempeño hacia las conexiones de los principales servidores del Instituto. Esto es debido a que un servidor puede generar 30 Mbps de tráfico o más, según el numero de clientes que realicen peticiones, llegando a convertir en insuficientes los 10Mbps de ancho de banda para absorber tal carga de conexión. Es decir, si se conectan N clientes simultáneamente, un servidor deberá tener un ancho de banda de N*10 Mbps para poder proporcionar un servicio adecuado a los clientes, si no de otro modo el enlace hacia el servidor puede convertirse en un gran cuello de botella.

Por otro lado, hay que tener en cuenta que, aunque el grupo de servidores se vio beneficiado por la segmentación de la etapa 1, esto no fue del todo suficiente, ya

[216] Además de que brindaban tratos especiales para las dependencias de la UNAM.

que estos, se encuentran en el mismo segmento con todos los usuarios del edificio 12 compitiendo por el medio de transmisión. Por lo que se puede observar que no todos los 10 Mbps del ancho de banda son dedicados para los servidores y por tal motivo se degrada de mayor manera su desempeño.

8.4.4.2 Alcance de la etapa

En esta etapa, se pretende incrementar el desempeño de las conexiones del grupo de servidores[217] principales del Instituto por medio de un enlace de alta velocidad, que además cumpla con un alto nivel de eficacia, disponibilidad y seguridad debido a la gran importancia que tienen estos dentro de la Institución.

El monto disponible de inversión en esta etapa es menor a $25, 000 dlls. entrando en el rango de un estudio a nivel perfil.

8.4.4.3 Desarrollo

Como se explico anteriormente, las necesidades de los clientes y los servidores, son asimétricas. Dependiendo de la cantidad de clientes que accedan al grupo de servidores a través de la red Ethernet de 10 Mbps, puede ocurrir una congestión masiva. Dado que en un ambiente cliente/servidor como el del Instituto, los servidores experimentan graves cuellos de botella al estar restringidos a las limitaciones de desempeño de 10Mbps de Ethernet. Es por esto que los servidores de alto desempeño requerirán de una solución con un alto nivel de confiabilidad.

Una arquitectura conmutada 10/100 y una topología de red adecuada proveerá a los clientes sobre múltiples segmentos Ethernet con 10Mbps conectarse hacia servidores de alto desempeño sobre una red con ancho de banda de 100Mbps. En este momento, los estándares de tecnologías de red a 100 Mbps adecuados para soportar dicha topología son FDDI y Fast Ethernet.[218]

Debido a que FDDI y Fast Ethernet operan de distinta manera proporcionando así diferentes ventajas y desventajas, a continuación se comparan algunos de los parámetros mas importantes y que servirán como fundamento para una posterior evaluación y selección de estas dos tecnologías.

---

[217] Comúnmente este termino también es referido como "server farm" o finca de servidores.
[218] 100GV-AnyLAN no fue tomado en cuenta en esta etapa, debido a que es una solución de un solo proveedor con un soporte de industria limitado. Por otro lado tecnologías mas rápidas como ATM (155Mbps) es relativamente nueva, por tal motivo aun es costosa y difícil para instalar y soportar en estos momentos.

	100Base-T	FDDI/CDDI
Estandarización	802.3u (aprobado el 14 de julio de 1995)	ANSI X3T9.5 1996
Asociación que la soporta	Alianza Fast Ethernet	No existe organización que lo soporte
Método de acceso	CSMA/CD	Rotación de senal (token) por tiempo (Timed Token)
Velocidad (Mbps)	100	100
Desempeño*		
1 servidor	hasta 82 Mbps	hasta 84 Mbps
2 servidores	hasta 77 Mbps	hasta 90 Mbps
3 servidores	hasta 74 Mbps	hasta 90 Mbps
4 servidores	hasta 70 Mbps	hasta 90 Mbps
Tipo de frame	Ethernet 802.3	FDDI ANSI X3T9.5
Máximo tamano de paquete (bytes)	1,500	4,500
Medios soportados		
cable UTP	Si	Si
Fibra óptica	Si	Si
Redundancia	No	Dual homing MAC ring
Servicio	Asíncrono	Asíncrono y síncrono
Administración	SNMP y MIBs ethernet	SMT, SNMP
Madurez del estándar	Apenas comenzando	Estable
Productos disponibles	1994	Desde 1990
Proveedores en 1995	20	Mas de 100
Aplicaciones en la cobertura geográfica	Grupo de trabajo y área de trabajo	Grupos de trabajo, áreas de trabajo, backbone (LAN y WAN)
Aplicaciones	Transferencia de datos	Datos, multimedia y aplicaciones de video conferencia
Flexibilidad topológica: reutilización de equipo (en base a la existencia de 10baseT)	Reutilización tanto del cableado existente como de las tarjetas 10BaseT (pero requiere cambio de concentradores)	Se aprovechan ciertos concentradores y conmutadores que tengan la opción de soportar FDDI (requiere el reemplazo de alguna tarjetas de estos dispositivos) reutilización del sistema de cableado UTP categoría 5.

*Fuente: Network Peripherals (HTTP://www.npix.com/product/fe-fddi4.html)

Tabla 8.9 Principales caracteristicas de las posibles tecnologías de conexión para el módulo de servidores del Instituto de Ingeniería

Aunque FDDI y Fast Ethernet son ambas tecnologías de 100 Mbps, sus características de desempeño son muy diferentes. Fast Ethernet es basado en CSMA/CD al igual que Ethernet 10Mbps, por lo tanto al conectar mas sistemas, incrementa la tasa de colisiones, decrementando sobre todo las capacidades de

desempeño. FDDI por otro lado, esta basado sobre un esquema[219] timed token garantizando el acceso al anillo FDDI para cada dispositivo sobre la red, lo cual lo hace una tecnología libre de colisiones, determinístico y con un alto grado de desempeño.

Con respecto a la topología de red física, tanto Fast Ethernet como FDDI soportan 100 mts. sobre cable UTP y 2Km sobre fibra, aunque existen diferencias en el esquema de tecnología que hacen adecuarse mejor a FDDI en esquemas de servidores distribuidos en varias áreas geográficas. Sin embargo, en ambientes de servidores centralizados dentro de un mismo centro de computo (misma área geográfica), tanto FDDI como Fast Ethernet pueden ser instalados de igual manera utilizando cable par trenzado sin blindar (hasta 100 metros).

En el caso donde se requiere un total nivel de disponibilidad debido a la naturaleza critica de las funciones de los servidores, FDDI es mejor ubicado que Fast Ethernet debido a su diseño de anillo doble, que le permite seguir operando aun cuando falla un cable.

Por ultimo, en un ambiente compartido, FDDI sostiene de mejor manera su rendimiento en desempeño que en Fast Ethernet compartido en el aumento de dispositivos conectados. Es decir, mientras el numero de dispositivos se incrementa en el anillo de FDDI su desempeño no llega a degradarse en un gran porcentaje debido a su método de acceso Rotación de señal por tiempo (Timed Token). De otra manera, como el número de usuarios se incrementa sobre un segmento de Fast Ethernet compartido, el desempeño se degrada con el incremento de colisiones.

Una vez explicados algunos puntos de importancia, a continuación se hace la evaluación de las dos tecnologías de acuerdo a los parámetros requeridos por el Instituto.

Tecnología	FDDI	Fast Ethernet	Ponderación
desempeño	5	4	30
Recuperación a fallas	5	2	20
Administración	4	4	15
incremento de servidores	5	3	15
Instalación y configuración	2	4	10
Costo	2	4	10
Calificación	3.7	3.1	

Tabla 8.10 Tabla de calificaciones de las tecnologías para el modulo de servidores

[219] No se debe confundir la estructura de anillo de FDDI con la tecnología Token Ring. FDDI, utiliza una variación sobre una idea llamada Rotación de señal por tiempo (Timed Token), en la cuál cada maquina envía datos al siguiente nodo durante un periodo de tiempo definido (el cual fue negociado anteriormente).

En la siguiente tabla se muestra la escala de calificaciones con sus respectivo criterios. Los cuales se utilizaran en todos los casos de selección de la mejor alternativa por medio del método de puntuación aditiva para seleccionar.

Criterio	calif.	Explicación del criterio
Excelente	- 5:	Se asigna a aquellas casos en que el funcionamiento supera en gran medida las expectativas deseadas.
Bueno	- 4:	Satisface los criterios estándar e incluye algunas características especiales.
Suficiente	- 3:	Su función o características son las esperadas.
Pobre	- 2:	Escaso cumplimiento en las funciones o características esenciales.
Inaceptable	- 1:	Es seriamente deficiente.

Tabla 8.11 Criterios de calificación que se tomaron para este proyecto

Además de la calificación obtenida por FDDI, otro factor determinante para la selección de FDDI fue la protección de la inversión del chasis MMAC-M8FBN, ya que este solo tiene capacidad de soportar tecnologías como Ethernet 10Mbps conmutado, Token Ring, ATM y FDDI, reduciendo grandemente los costos de instalación y compra de módulos. Por otro lado, en el tiempo cuando se llevo a cabo la evaluación de esta etapa, Fast Ethernet era una tecnología relativamente nueva[220], por lo se penso que su implantación llevaría a tener varios riesgos innecesarios para el grupo de servidores y sus funciones de servicio crítico.

Selección: Tecnología FDDI para el enlace del grupo de servidores principales de la red del Instituto.

NOTA: Se debe mencionar que en el tiempo cuando se realizo la evaluación para esta etapa, no se habia desarrollado completamente el Fast Ethernet Conmutado. El cual, actualmente proporciona un mejor desempeño que Fast Ethernet Compartido, y está ganando mayor aceptación sobre FDDI/CDDI para conexiones cliente/servidor debido a su bajo costo, y alto rendimiento, además de que ha desarrollado un perfil de desempeño y características de redundancia necesarias para este tipo de topologías de servicio crítico.

[220] Desarrollado en 1992, y aprobado como un estándar por el comité IEEE 802.3 en el ano de 1995.

8.4.5 Etapa 3 Base para la red de altas especificaciones del Instituto de Ingeniería

8.4.5.1 Introducción

A diferencia de las etapas anteriores en donde se tenía un problema especifico que solucionar, en esta etapa, no se tiene una problemática como tal, si no que se pretenden implantar los inicios de una infraestructura de red de alta velocidad que soporte los requerimientos a mediano plazo del Instituto y por otro lado sea la base para la evolución de la red del Instituto hacia el futuro.

Esta etapa de la red del Instituto deberá establecer los principales puntos para que las actualizaciones de las próximas generaciones puedan ser integradas sobre la base de los sistemas ya instalados. Es por esto, que esta etapa es de suma importancia ya que de ésta dependerá el éxito que tenga la REDII en su desarrollo hacia el futuro.

8.4.5.2 Alcance de la etapa

En esta etapa se pretende obtener una infraestructura de alta velocidad tanto en el backbone como en la conexión hacia RedUNAM, además de que sean confiables y que tengan altos niveles de disponibilidad. Al mismo tiempo se pretende extender los beneficios de una mayor segmentación a hacia la red completa y por ultimo, proporcionar enlaces de alta velocidad para los servidores y usuarios finales que así lo requieran.

El monto disponible de inversión en esta etapa es de alrededor de $150,000 dlls. entrando en el rango de un estudio de prefactibilidad.

8.4.5.3 Desarrollo

El nuevo sistema a implantar deberá manejar un backbone de alta velocidad, con esto nos referimos a que proporcione por lo menos un ancho de banda de 100 Mbps para poder soportar las nuevas aplicaciones que se caracterizan por su consumo intensivo de ancho de banda, además de que debe ofrecer facilidades de calidad de servicio o manejo de prioridades para aquellas aplicaciones que así lo requieran como multimedia, videoconferencia, aplicaciones en tiempo real etc.

También deberá de cumplir con normas (estándares) que garanticen la completa interoperabilidad entre las diferentes plataformas utilizadas tanto en el Instituto como con la RedUNAM. Al mismo tiempo, es deseable que el sistema se base en tecnologías que permitan un crecimiento gradual en su ancho de banda (escalabilidad) para poder obtener un mayor aprovechamiento del esquema a implantar.

Por otro lado, siguiendo la orientación de segmentación, el nuevo sistema debe permitir un mayor grado de segmentación en el interior de los edificios y establecer las bases para el manejo de redes virtuales.

Por ultimo, el sistema deberá ofrecer las facilidades de administración y seguridad adecuadas para una buena disponibilidad y confianza de la red.

8.4.5.3.1 Análisis de las tecnologías de red de alta velocidad

Actualmente existen varias tecnologías disponibles para llevar a cabo nuestro objetivo, sin embargo son pocas las opciones viables a las que nos hemos limitado tomando en cuenta su estandarización, madurez, asociación de desarrollo que la soporta, además de ciertos parámetros como posición y expectativas en el mercado. Esto nos ha llevado a tomar en cuenta solamente tecnologías como 100Base-X/T4, 100VG-AnyLAN, FDDI y ATM para realizar nuestro estudio. Aun que las cuatro son tecnologías de alta velocidad, la manera en que estas funcionan son muy diferentes, lo que hace que cada una ofrezca beneficios específicos para ciertas áreas de la red o que soporten de una mejor manera un conjunto particular de funciones, aplicaciones y servicios.

8.4.5.3.2 Descripción de las tecnologías de alta velocidad respecto a ciertos parámetros.

A continuación, se hace una breve descripción de cada una de las tecnologías de alta velocidad con respecto ciertos parámetros que se pensaron como esenciales para el desarrollo de una red de altas especificaciones con las características que necesita la red del Instituto de Ingeniería.

8.4.5.3.3 ATM

Ancho de banda: ATM soporta diferentes anchos de banda. Para redes tipo LAN, en el mercado actual se manejan velocidades de 25Mbps, 155Mbps, 622 Mbps.[221]

Soporte a aplicaciones: ATM tiene varias características de transmisión que la convierten en una tecnología que hace un manejo adecuado para el trafico de voz, datos y video (procesamiento de imágenes, videoconferencias, multimedia, etc.). La mas importante de estas características es su capacidad de ofrecer Calidad de Servicio (QoS: Quality of Service)[222] dependiendo del tipo de trafico a transmitir.

---

[221] Para mayor información referirse al capitulo 6, Tecnologías de redes de alta velocidad en el apartado de capa física de ATM.

[222] Se tiene las siguientes categorías de servicio: Tasa de Bit Constante (CBR: constant Bit Rate), Tasa de Bit Variable Tiempo-Real (rt-VBR: Real-Time Variable Bit Rate), Tasa de Bit Variable

NOTA: Aunque ATM, puede manejar trafico de voz por de facto, muy poco se ha hecho en el desarrollo de una tecnología ATM para voz en ambientes LAN. Actualmente ATM no tiene una capa o protocolo que sea optimo para manejar trafico de voz. El protocolo AAL que existe actualmente hace un manejo ineficiente de este tipo de trafico.

Seguridad: Debido a que su tecnología es orientada a la conexión, ATM adiciona una ventaja potencial con respecto a la seguridad. La red puede determinar inteligentemente que trafico deberá ser pasado basándose en su identificación fuente y destino (punto a punto). Además, se puede implantar un sistema de autentificación de usuario que los restrinja a tener acceso a solo una parte o a todos los recursos de la red (filtrado de celdas)[223]. La naturaleza de ATM de orientación a la conexión también asegura que el trafico solamente será enviado al destinatario (de esta manera no se desperdician recursos de la red con innecesarios broadcast o el filtrado de protocolos y así incrementar la eficiencia).

Por otro lado, ATM al ser una tecnología de conmutación proporciona las ventajas del manejo de las redes virtuales, las cuales pueden incrementar el nivel seguridad sobre las redes ATM. Los administradores de red pueden usar las redes virtuales para definir filtros para restringir el acceso entre los grupos y dispositivos, proporcionando una seguridad muy alta. Además, los conmutadores ATM ofrecen seguridad a nivel de puerto para permitir a los administradores restringir a las subredes virtuales a puertos físicos específicos.

Estandarización: La mayor parte de las especificaciones principales y estándares para redes ATM privadas han sido desarrolladas por el Forum ATM y el Fuerza de Tarea de Ingeniería Internet (IETF: Internet Engineering Task Force). En la practica el Forum ATM ha considerado extender tales estándares a los requerimientos específicos de redes privadas, por lo que se han creado nuevas especificaciones, como son LANE y el protocolo P-NNI. Las especificaciones del Forum ATM pueden ser considerados estándares de facto para el desarrollo de redes privadas ATM. Mientras que por otro lado, el IETF se ha enfocado principalmente en aspectos de interoperabilidad del manejo del protocolo IP sobre ATM.[224]

La mayor desventaja de la tecnología de ATM para redes LAN ha sido su lento desarrollo en sus estándares. Esto es debido a que las fechas para la aprobación de las especificaciones pendientes no han sido cumplidas totalmente, además de que los esquemas de desarrollo necesarios no pueden comenzar antes de la

---

No-Tiempo-Real (nrt-VBR: Non-Real-Time Variable Bit Rate), Tasa de Bit Disponible (ABR: Available Bit Rate), Tasa de Bit Sin Especificar (UBR: Unspecified Bit Rate).

[223] Cabe mencionar que todas las técnicas de filtrado basado en direcciones son vulnerables a ataques de indagación de paquetes por parte de personas no autorizadas.

[224] Actualmente, otros protocolos de capa 3 como por ejemplo IPX tiene soluciones propietarias para la interoperabilidad sobre ATM. Sin embargo, el Forum ATM esta desarrollando la especificación MPOA (Multiprotocol Over ATM) para dar solución para que los protocolos de capa tres interoperen sobre ATM.

finalización de estándares previos, teniéndose de esta manera que el desarrollo de los estándares completos generalmente se retrasen para su liberación final.

Madurez en el mercado: Los inicios de ATM fueron pensados en redes de área amplia a partir del año de 1986 [225], haciendo que los conceptos en que se basa esta tecnología sean maduros. Sin embargo, en el área de redes locales, el Forum ATM fue fundado en el año de 1991, aunado con que los estándares desarrollados por éste, han llevado una evolución lenta, además de no permitir un amplio desarrollo tanto en la interoperabilidad entre proveedores como con la relación de ATM con las redes heredadas. Por lo anterior se puede decir que ATM en el campo de redes LAN es una tecnología en evolución.[226]

Confiabilidad: ATM al poder utilizar una topología de malla, permite proveer varios enlaces entre componentes y de esta manera tener varias rutas redundantes. Sin embargo, ATM para ofrecer una red lo suficientemente rápida, no provee detección de errores ni tampoco esquemas de retransmisión.

Administración: El protocolo ILMI (Interim Local Management Interface) provee una interface para administración basado en SNMP (Simple Network Management Protocol) para ATM. ILMI requiere que cada estación final (UNI 3.0 y UNI 3.1) o red ATM implante una Entidad de Administración UNI (UME: UNI management entity). El UME funciona como una MIB ILMI (Management Information Base). Este responde a peticiones de las aplicaciones de administración SNMP. El estándar de administración SNMP puede utilizar los niveles AAL 3/4 o AAL 5 para encapsular los comandos SNMP en unidades de datos del protocolo ATM (PDUs).

Desempeño: ATM al ser una tecnología de conmutación y proporcionar características de Calidad de Servicio (QoS) ofrece un alto desempeño en el manejo de ancho de banda. Al mismo tiempo ofrece una transmisión full dúplex incrementando al doble el ancho de banda donde se pueda aprovechar esta característica. Además, al permitir una topología de malla y por su característica de operación, los conmutadores ATM pueden utilizar el balanceo de cargas a través de las múltiples rutas disponibles.

Por otro lado, de acuerdo a la relación entre el tamaño de la celda y el encabezado de información, ATM tiene un desempeño del 90.5% en cuanto a la transferencia real de datos por celda.

---

[225] El CCITT decide emplear a ATM como la tecnología principal para el ISDN de Banda Ancha (B-ISDN).

[226] Para obtener una mayor información del estado en evolución de los estándares de ATM para redes LAN, referirse al Forum ATM (http://www.atmforum.com).

Control de flujo: ATM define varios esquemas simples para el control de la congestión, entre ellos se encuentran GFC (Generic Flow Control), CLP (cell Loss Priority) y el EFCI (Explicit Forward Congestion Indicator). Sin embargo, se hacen necesarios mecanismos mas sofisticados para el manejo de la congestión en redes mas grandes y que lleven diferentes tipos de trafico. El Forum ATM recientemente ratifico la estrategia de manejo del trafico basado en velocidad (rate-base) que trabaja sobre los conmutadores y las estaciones finales regulando la velocidad transmisión cuando se llega a un cierto nivel de congestión.

Garantía de entrega: En la capa ATM no existe un servicio de garantía de entrega fin-a-fin, ya que esta no realiza ninguna función de retransmisión y por tal motivo se delega esta función a los protocolos de capas superiores.

Flexibilidad topológica: La tecnología ATM soporta topologías de malla y estrella, sobre diferentes medios de transmisión como son: fibra óptica, par trenzado y cable coaxial. Además es la única tecnología que ofrece soluciones potencialmente de usuario final a usuario final, esto significa que puede ser empleado tanto para conexiones WAN, backbones de redes LAN, como para soluciones de usuario final.

Sin embargo, hay que tener en cuenta que su instalación y configuración es compleja, además los retos de interoperabilidad en ambientes LAN han limitado la implantación inicial a backbones de campus, backbones de intraedificios, conexiones de servidores de alto desempeño y conexiones hacia redes de área amplia.

Escalabilidad: ATM al soportar una topología de malla, puede aumentar el numero de conmutadores conectados al backbone sin limite (cabe hacer notar solo se tienen las restricciones físicas de los equipos, como son el numero de direcciones MAC que manejan, así como las características de no bloqueo de los mismos, etc.). De igual manera ATM permite tener una escalabilidad en el ancho de banda, haciéndola de esta manera una de las tecnologías de red mas escalable.

Redes virtuales: ATM al ser una tecnología por naturaleza conmutada proporciona un amplio manejo de redes virtuales. La principal ventaja del uso de redes virtuales, es que permite a los administradores poder agrupar los dispositivos lógicamente, sin importar la localización física, además de prever un ancho de banda y servicio dedicado a cada uno los dispositivos, así mismo, la administración de redes virtuales puede definir filtros entre las redes virtuales mismas (como lo hace un enrutador). Además de la capacidad de filtrado, las redes virtuales proveen facilidades de administración como son: simplicidad para la administración (movimientos, adiciones y cambios de los dispositivos y usuarios finales), manejo del ancho de banda por usuario y características de seguridad.

Costo: ATM es una tecnología en pleno desarrollo, por lo que los precios al principio pueden parecer altos comparados con otras tecnologías de red actuales. Sin embargo, la participación de muchos fabricantes y la tendencia que tiene ATM de ser una de las tecnologías con mayor respaldo hacia el futuro, hacen que los precios tiendan a disminuir.

Es recomendable para:
- ✓ Aplicaciones de multimedia y video gracias a su habilidad de asignación dedicada de ancho de banda para aplicaciones y su capacidad de calidad de servicio.
- ✓ Backbone, por ser una tecnología escalable, que proporciona un alto desempeño, seguridad y el manejo de rutas redundantes (con balanceo de cargas).
- ✓ Para redes de área amplia, ya que no tiene problemas o no necesita de mas cosas protocolos o tecnologías para integrar tanto redes tipo WANs y LANs.

No es recomendable para:
- × Pequeñas redes, por su alto precio.
- × Para redes que deban conservar su base instalada de diferentes protocolos de red, ya que actualmente ATM carece de especificaciones estándares para la integración de varios protocolos.

Es fuerte en:
- ✓ Alto desempeño
- ✓ Escalabilidad
- ✓ Ancho de banda dedicado
- ✓ Potencialmente para empleo universal (WAN, MAN y LAN)
- ✓ Seguridad
- ✓ Redes Virtuales

Es débil en:
- × Interoperabilidad (actualmente por la falta de terminación de estándares)
- × Alto costo
- × Tolerancia a fallas moderado (ya que se tienen que crear los enlaces redundantes)

Arquitectura de red	Aplicaciones de red
Para grupos de trabajo de alto desempeño	Aplicaciones de Bases de datos
Para grupos de servidores	Multimedia
Backbone	Procesamiento de imágenes
Redes de área amplia (WAN)	Redes de área amplia (WAN)

Tabla 8.12 Soluciones que da ATM

8.4.5.3.4 FDDI

Ancho de banda: El ancho de banda soportado por FDDI es de 100 Mbps.

Soporte a aplicaciones: FDDI dispone de dos modos de transmisión. El primero es el modo asíncrono que soporta el manejo de datos, mientras el segundo, referido como modo síncrono, permite darle prioridad al trafico sensible al tiempo pero no de una forma eficiente ya que no se garantiza que la señal token llegara a la estación en el tiempo establecido para transmitir la información (es decir, puede llegar retrasado). De esta manera, podemos decir que FDDI puede soportar la transmisión de datos, y solo cierto tipo de trafico de voz y video.

Seguridad: FDDI al ser una tecnología de medio compartido, no proporciona ningún tipo de seguridad en la transmisión de los paquetes, ya que cualquier estación no autorizada puede analizar el contenido de los paquetes al fluir por el anillo de FDDI.

Estandarización: En 1982, un subcomité del Grupo de Trabajo Técnico X3T9 del Instituto Nacional Americano de Estándares (ANSI), estuvo encargado del desarrollo de un estándar de redes de datos de alta velocidad. En 1986, ANSI había revisado el documento original y publicó una propuesta que finalmente sería el FDDI que se conoce actualmente.

Madurez en el mercado: Al ser estandarizado a mediados de los años ochentas, FDDI cuenta con un desempeño probado durante varios años, convirtiéndose así, en una tecnología madura y estable.

Confiabilidad: FDDI es una tecnología extremadamente tolerante a fallas debido a su topología de doble anillo redundante, por lo que los dispositivos pueden tener dos conexiones al anillo dual, de esta manera se puede tener una ruta alterna si llegase a fallar una conexión.

Administración: FDDI define su propio protocolo de monitoreo y administración, llamado Administrador de Estación (SMT: station management). A diferencia del resto de las tecnologías, FDDI fue diseñado con SMT como parte integral de este. Además de soportar los protocolos estándares de administración como son SNMP y RMON.[227]

Desempeño: De acuerdo a la relación entre el tamaño del paquete y el encabezado de información, FDDI tiene un desempeño del 99.5 % en cuanto a la transferencia real de datos por paquete.

---

[227] El IETF no ha estandarizado una MIB RMON para FDDI, sin embargo, varios fabricantes proporcionan una solución propietaria.

El diseño de medio compartido de FDDI impone algunas desventajas, debido a que todos los nodos de la red deben obtener una porción de los 100Mbps comunes, la capacidad disponible para cada usuario decrece en proporción al tamaño de la LAN.

Cabe hacer notar que aunque FDDI consta de un anillo dual, solo un anillo permanece activo mientras el otro solo sirve de respaldo.

Control de flujo: Debido a las características de transmisión que maneja FDDI permite que este no se vea afectado por ningún tipo de congestión. En ambientes FDDI conmutados el ajuste del TTRT (Timed Target Rotation Time) permite el manejo de grandes cargas de trafico sin tener problemas de congestionamiento.

Garantía de entrega: FDDI al igual que Ethernet delega las funciones de garantía de entrega a los protocolos de capas superiores.

Flexibilidad topológica : La flexibilidad topológica que ofrece FDDI no es muy grande ya que solo soporta una configuración en anillo, además, de que solo es posible utilizar fibra óptica o par trenzado categoría 5 en el caso de CDDI.

FDDI soporta una distancia de 100 Km totales de diámetro por anillo en fibra óptica multimodo y 2 Km de distancia entre nodos. Por otro lado, soporta 100 metros de distancia entre estaciones sobre cable par trenzado.

Además, la instalación de FDDI es relativamente difícil. No obstante, a causa de que FDDI ha estado disponible por varios años, es fácil encontrar asistencia técnica. Asimismo, puede haber algunos problemas al inicializar las estaciones, sin embargo, una vez funcionando la red FDDI es muy estable y requiere de muy poco mantenimiento.

Por ultimo, actualmente los estándares de ANSI e ISO no soportan algoritmos de puenteo de encaminamiento fuente lo que conduce a esquemas de solución propietaria y consecuentemente con la incompatibilidad.

Escalabilidad: Un punto importante, es que FDDI no ofrece escalabilidad para un mayor ancho de banda. Al mismo tiempo, solo soporta un total de 500 nodos conectados directamente al anillo dual sobre la distancia citada anteriormente.

Conmutación: El FDDI conmutado proporciona todas las ventajas de cualquier tecnología conmutada como es el ser full dúplex (obteniéndose un ancho de banda de 200Mbps), manejo de redes virtuales (VLAN), etc. Sin embargo en el caso de FDDI la tecnología de conmutación es sumamente costosa[228], por lo que solo se recomienda para ambientes donde su inversión en FDDI es muy grande y

[228] El precio de FDDI conmutado supera incluso a la tecnología ATM.

de esta manera proteger la inversión de estos equipos. Por otro lado, muy pocos proveedores lo soportan.

Costo: Debido a su alta complejidad FDDI es una tecnología cara en comparación con otras tecnologías de redes locales existentes en el mercado.

Es recomendable para:
- ✓ Para cierto tipo de multimedia y vídeo por los mecanismo de asignación del ancho de banda síncrono que pude asegurar el ancho de banda adecuado.
- ✓ Para grupos de servidores y backbone por las características de administrabilidad y su esquema tolerante a fallas.
- ✓ Segmentos de backbone

No es recomendable para:
- × Para el área de trabajo con computadoras de escritorio por el alto costo y los grandes encabezados que maneja asociado con el SMT.

Es fuerte en:
- ✓ Soporte de extensiones para la administración construidos dentro del protocolo SMT.
- ✓ Un diámetro grande de la red.
- ✓ El soporte de varios vendedores.

Es débil en:
- × Relativamente caro
- × Relativamente difícil de instalar
- × Un gran encabezado al utilizar el SMT.

Arquitectura de red	Aplicaciones de red
✓ Grupos de trabajo de alto desempeño (CDDI)	✓ Multimedia
✓ Para grupo de servidores (CDDI)	✓ Procesamiento de imágenes
✓ Backbone (FDDI)	

Tabla 8.13 Soluciones que da FDDI

8.4.5.3.4 Fast Ethernet conmutado

Ancho de banda: El ancho de banda soportado por Fast Ethernet es de 100Mbps.

Soporte a aplicaciones: Fast ethernet soporta un modo de transmisión asíncrono, con lo cual ofrece su mejor desempeño para trafico que sea intermitente entre el cliente y el servidor (un ejemplo son las aplicaciones de bases de datos). También es bueno para aplicaciones estándares de oficina (procesadores de texto, hojas de calculo, etc.). Sin embargo por las características que proporciona la

conmutación, aunado con el ancho de banda que maneja, se pueden llevar cierto tipo de trafico multimedia no sensible al tiempo (esto se aplica principalmente a dispositivos que tienen el ancho de banda dedicado, es decir que están conectados directamente a un puerto del conmutador).

Seguridad: Se puede decir que Fast Ethernet conmutado proporciona cierto margen de seguridad, al partir del principio de conmutación donde los paquetes viajan a través de una conexión virtual solo entre el nodo transmisor y el nodo receptor, es decir, que en esencia se crea un segmento privado entre los puertos origen y destino.

Estandarización: Fast ethernet conmutado cumple los mismos estándares que el Fast ethernet compartido (802.3u). Sin embargo, actualmente no existen estándares para regular los mecanismos tanto de control de flujo como para el de conmutación en el plano posterior (backplane) de los conmutadores.

Madurez en el mercado: A pesar de que Fast ethernet conmutado salió al mercado en el año de 1995, gracias al apoyo por parte de los fabricantes así como a la gran aceptación que ha tenido en los usuarios, su desarrollo a sido muy acelerado, haciéndolo una tecnología relativamente nueva pero con un amplio soporte.

Confiabilidad: Fast Ethernet conmutado puede proporcionar mecanismos de redundancia al permitir llevar a cabo rutas redundantes siendo administradas por el protocolo de árbol expandido (spanning tree, 802.1d).

Administración: Debido a que Fast Ethernet es muy similar a 10baseT muchas de las familias de herramientas de administración de éste último están disponibles para usarse en redes 100BaseT, como son los sistemas de administración de dispositivos y los analizadores de protocolos.

Desempeño: Fast Ethernet conmutado, proporciona un mejor desempeño que Fast Ethernet compartido, esto es debido a que la conmutación nos proporciona una mejor asignación del ancho de banda y un menor nivel de degradación en el incremento de usuarios. Por otro lado existen características opcionales que dependen del diseño de una red Fast Ethernet, como son el modo de operación full dúplex y la reducción o completa eliminación de colisiones.[229]

[229] Estas características dependen del tipo de segmentación que se lleve a cabo, es decir, segmentación dedicada, donde se eliminan completamente las colisiones y se puede realizar el modo full dúplex, y por otro lado la segmentación compartida donde solo se reduce el numero de colisiones dependiendo del numero de estaciones que se conecten.

De acuerdo a la relación entre el tamaño del paquete y el encabezado de información, Fast Ethernet tiene un desempeño del 98.4% en cuanto a la transferencia real de datos por paquete.

Control de flujo: Los conmutadores pueden llegar a un punto de congestión en los puertos de salida y de esta manera la técnica empleada para manejar la congestión afecta directamente el desempeño de la red. Los conmutadores Fast Ethernet ocupan uno de dos técnicas[230], la primera es conocida como backpressure, la cual envía una señal para reducir la carga del trafico proveniente de la fuente y así evitar la congestión, mientras que la segunda técnica está basada en grandes buffers de almacenamiento. Por otro lado, fast ethernet conmutado esta basado en el protocolo CSMA/CD con el cual se lleva a cabo el manejo de las retransmisiones.

Garantía de entrega: Fast Ethernet es una tecnología de mejor esfuerzo de entrega y la mayoría de las funciones de recuperación de error son delegadas a los protocolos de capas superiores por lo que no garantiza una entrega de datos eficaz. Los conmutadores Fast Ethernet realizan la verificación de problemas relacionados a Ethernet comunes tales como corrección de errores.

Flexibilidad topológica: Fast Ethernet conmutado soporta las topologías de estrella y malla, ambas sobre fibra óptica y par trenzado sin blindar (en categorías 3, 4 y 5 con diferentes configuraciones, lo cual puede representar algunas desventajas dependiendo del sistema de cableado existente y el tipo de tecnología Fast ethernet que se quiera desarrollar).

Debido a su limitada cobertura geográfica, Fast Ethernet se ubica mejor en redes tipo LAN ya que soporta una distancia de 2 Km totales entre usuarios finales sobre fibra óptica multimodo (en modo full dúplex) y por otro lado, soporta 100 metros sobre cable par trenzado (full dúplex / half dúplex).

La instalación de Fast Ethernet en cualquiera de sus tipos es relativamente sencilla. Además de que gracias al apoyo proporcionado por los proveedores y a la experiencia previa de los usuarios con Ethernet 10BaseT, es fácil encontrar asistencia técnica.

Escalabilidad: Fast Ethernet no tiene una escalabilidad de ancho de banda como tal, si no que existen desarrollos que se encuentran basados en el mismo principio de CSMA/CD, utilizado por Ethernet original y Fast Ethernet, tal es el caso de Gigabit Ethernet el cual proporciona un ancho de banda de 1Gbps.

Por otro lado, cualquier tecnología ethernet basada en conmutación, desarrolla esquemas que permiten una mejor escalabilidad tanto en el numero de usuarios,

[230] Ambas técnicas tienen sus ventajas y desventajas.

así como por las características full dúplex que permiten incrementar la distancia entre dos dispositivos.

Redes Virtuales: Fast Ethernet conmutado permite el manejo de redes virtuales, con lo que se proporciona una poderosa herramienta de administración y seguridad. Con el manejo de redes virtuales se pueden llevar a cabo una reestructuración lógica de las estaciones y dispositivos, no importando la localización física de estos y al mismo tiempo un mecanismo de filtrado de paquetes entre las redes virtuales.

Costo: Fast Ethernet conmutado al utilizar el mismo esquema que Ethernet 10baseT, le permite ofrecer un menor precio que otras tecnologías de redes de alta velocidad. Además de realizar una migración costo efectivo en la mayoría de las redes existentes, con la máxima reutilización del equipo, como es la infraestructura de cableado, sistemas de administración de redes, etc. Al mismo tiempo, su gran apoyo en el mercado ha permitido que se reduzcan los costos grandemente.

Es recomendable para:
- ✓ Aplicaciones que requieran una comunicación intermitente entre el cliente y el servidor, ya que el protocolo CSMA/CD ofrece su mejor desempeño bajo éste tipo de trafico (opuesto al trafico continuo).
- ✓ Para aplicaciones estándares en áreas de trabajo en computadoras de escritorio.
- ✓ Para grupos de servidores de alto desempeño y que se encuentren centralizados geográficamente a causa de su limitada distancia.
- ✓ Para ser implantado en el backbone con ciertas consideraciones, como por ejemplo, con la característica de full dúplex habilitada y la configuración de rutas redundantes.

No es recomendable para:
- * Para aplicaciones que requieran comunicación sensible al tiempo o constante entre el cliente y el servidor, como son aplicaciones de multimedia y vídeo. Esto es a causa de que la arquitectura del protocolo CSMA/CD no puede realizar la entrega de paquetes de manera predecible.

Es fuerte en:
- ✓ No es caro
- ✓ Fácil de integrar dentro de instalaciones existentes de 10Base-T.
- ✓ Usa los mismos tipos de conexiones (pinouts) como 10Base-T.
- ✓ Utiliza muchas de las reglas de cableado que 10Base-T.

Es débil en:
- * Limitada escalabilidad.
- * Permite solo dos repetidores por segmento

- Máxima distancia de la red de solo 210 m entre el nodo final y el conmutador.
- El método de acceso CSMA/CD impide respuestas a tiempo para usuarios y aplicaciones que requieren de un ancho de banda alto.

Arquitectura de red	Aplicaciones de red
Para grupos de trabajo de alto desempeño	Aplicaciones de Bases de datos
Para grupos de servidores	Aplicaciones de grupos de trabajo
Backbone (bajo ciertas consideraciones)	Cierta clase de multimedia

Tabla 8.14 Soluciones recomendables para Fast Ethernet conmutado

8.4.5.3.6 100VG-AnyLAN

Ancho de Banda: 100VG-AnyLAN es una tecnología que ofrece 100Mbps de ancho de banda.

Soporte de aplicaciones: 100VG-AnyLAN esta basado en un nuevo método de control de acceso central referido como Método de Acceso de Prioridad por Demanda (Priority Access) el cual permite tener dos niveles de prioridad para el manejo de trafico, con esta característica se proporciona un mejor manejo de aplicaciones para voz, datos y cierto tipo de multimedia.

Seguridad: 100VG-AnyLAN ofrece cierto rango de seguridad, ya que con su esquema de prioridad por demanda los paquetes de datos solo son dirigidos a los puertos indicados de destino, dando así cierto nivel de seguridad no provista por redes como Ethernet original o FDDI.

Estandarización: La tecnología de 100VG-AnyLAN fue aprobada como la especificación 802.12 del IEEE en el año de 1995. Actualmente el comité 802.12 esta discutiendo algunas posibles extensiones para VG, tales como tasas de transferencia de datos mayores como 400Mbps en cobre y 1Gbps para fibra, enlaces redundantes entre concentradores y enlaces en modo full dúplex y transferencia de paquetes de tipo ráfaga (burst).

Madures en el mercado: el estándar 100VG-AnyLAN aunque fue aprobado en el año de 1995, esta tecnología ha sufrido la falta de publicidad, asimismo del respaldo por parte de las grandes compañías fabricantes, que combinado con la falta de productos a la venta (conmutadores, analizadores de red, concentradores o adaptadores) han hecho que el desarrollo de 100VG-AnyLAN en el mercado sea lento.

Confiabilidad: Recientemente 100VG-AnyLAN empezó a ofrecer el servicio de rutas redundantes controladas por el protocolo de árbol expandido (spanning tree 802.1).

Administración: Al estar basado en las tecnologías de Ethernet y Token ring, 100VG-AnyLAN permite el manejo de administración basado en SNMP.

Para propósitos de diagnóstico y de administración de red, la tecnología 100VG-AnyLAN permite activar puertos individuales del concentrador para monitorear todo el trafico que pasa a través del concentrador.

Desempeño: A diferencia de Ethernet original, 100VG-AnyLAN debido a su método de transmisión que utiliza poléo (round robin), la convierte en una tecnología libre de colisiones además de ser una tecnología con transmisión determinística y ofrecer un esquema rudimentario de prioridad de trafico.

De acuerdo a la relación entre el tamaño del paquete y el encabezado de información, 100VG-AnyLAN tiene un desempeño del 98.4% (en modo de manejo de paquetes Ethernet) y de 99.5% (en modo de manejo de paquetes Token Ring) en cuanto a la transferencia real de datos por paquete.

Control de flujo: 100VG-AnyLAN lleva a cabo el control de flujo por medio de su esquema de prioridad por demanda.

Garantía de entrega: 100VG-AnyLAN es un protocolo de mejor esfuerzo de entrega, por lo cual las funciones de garantía de entrega son delegadas a las capas de protocolos superiores.

Flexibilidad Topología: Las redes 100VG-AnyLAN utilizan una topología de estrella escalable sobre cable de par trenzado y fibra óptica. Sin embargo, se debe tener en cuenta que las reglas de cableado no son totalmente compatibles con las permitidas por 10BaseT, además de ser necesario el uso de puentes traductores para la operación entre 10BaseT y 100VG-AnyLAN.

Por otro lado, aunque no existen limitantes con respecto al numero de nodos conectados a un segmento de la red, es conveniente tener solo 250 nodos como máximo para mantener un alto desempeño. Del mismo modo otra limitante es el numero de hubs que se pueden tener en cascada, ya que solo soporta hasta 4 hubs (conectados en fibra óptica), aunque se recomienda solo tener 3 niveles, ya que cada nivel en cascada adicional, suma un encabezado, disminuyendo de esta manera el desempeño de la red.

Costos: La tecnología 100VG-AnyLAN es aproximadamente dos veces mas cara que su antecesor Ethernet original. Por lo que ofrece ser una tecnología viable para su instalación.

Es recomendable para:

- ✓ Para instalaciones que no tengan cables de 25 pares, ya que 100VG-AnyLAN no opera sobre cables de 25 pares donde estén conectados dispositivos que este corriendo en modo promiscuo.
- ✓ Aplicaciones de multimedia y vídeo gracias a la capacidad de priorización y la entrega segura de paquetes.
- ✓ Para grupos de trabajo de poder, gracias a su esquema de acceso de datos determinístico que asegura un desempeño constante con alto trafico.

No es recomendable para:

- * Backbone, por que el diseño de poléo centralizado (round robin) puede causar potencialmente un punto de retardo (cuello de botella) o riesgo si llegase a fallar. Además de que actualmente no ofrece servicios de rutas redundantes.
- * Para redes que no cumplan con las especificaciones de 100VG-AnyLAN

Es fuerte en:

- ✓ Componentes de bajo precio
- ✓ Puede prioritizar el trafico de paquetes

Es débil en:

- * Seguridad limitada
- * Tecnología limitada en el crecimiento y el soporte de vendedores
- * Requerimientos de preparación considerables antes de su implantación dentro de una red 10Base-T.

Arquitectura de red	Aplicaciones de red
Grupos de trabajo	Aplicaciones de bases de datos
Para grupos de trabajo de alto desempeño	Aplicaciones de grupos de trabajo
	Multimedia
	Procesamiento de imágenes

Tabla 8.15 Soluciones que da 100VG-AnyLAN

8.4.5.3.7 Resumen

Para finalizar esta sección de descripción de las tecnologías, a continuación se muestran unas tablas comparativas. Las tablas 8.16 a la 8.20 se obtuvieron del libro: The McGraw-Hill High-Speed LANs Handbook (Data Communications Magazine) de Stephen Saunders editorial McGraw-Hill 1996.

	Tipo de redes donde es recomendable utilizarla	Tipo de redes donde no es recomendable utilizarla
ATM	Todas	Ninguna
FDDI	LAN, MAN	WAN
Fast Ethernet conmutado	LAN	MAN, WAN
100VG-AnyLAN	LAN	MAN, WAN

Tabla 8.16 Tipo de redes soportadas por las distintas tecnologías

	Característica de latencia	Características del ancho de banda	Aplicaciones recomendadas	Aplicaciones no recomendadas
ATM	Variable y baja; menos de 30 microsegundos en una red bien diseñada	Velocidad muy alta, conmutado	Datos, multimedia sensitiva al tiempo, voz	Ninguna
FDDI	Variable y alta; típicamente se mide en milisegundos	Velocidad alta, medio compartido	Datos	Multimedia sensitiva al tiempo, voz
Fast Ethernet conmutado (cut through)	Variable y bajo; alrededor de 30 microsegundos	Velocidad alta, conmutada	Datos, multimedia sensitiva al tiempo	Voz
Fast Ethernet conmutado (store-and-forward)	Variable; bajo (microsegundos) con paquetes cortos, alto (milisegundos) con paquetes largos	Velocidad alta, conmutada	Datos, algún tipo de multimedia sensitiva al tiempo	Algún tipo de multimedia sensitiva al tiempo, voz
100VG-AnyLAN	Variable y alto; típicamente se mide en milisegundos	Velocidad alta, medio compartido	Datos, algún tipo de multimedia sensitiva al tiempo	Algún tipo de multimedia sensitiva al tiempo, voz

Tabla 8.17 Capacidades de manejo de multimedia

	Nodos instalados en 1995	Nuevos nodos en 1996 (predecido)	Nuevos nodos en 1997 (predecido)	Nuevos nodos en 1998 (predecido)
ATM	33,000	93,000	440,000	840,000
FDDI	87,000	93,000	80,000	75,000
100Base-T conmutado	5,000	110,000	330,000	760,000
100VG-AnyLAN	40,000	165,000	250,000	500,000

Tabla 8.18 Soporte de las distintas tecnologías por la industria a nivel mundial

	Trabaja con los adaptadores instalados (NICs)	Trabaja con el cable de cobre instalado	Trabaja con las aplicaciones existentes
ATM	No	Si, categoría 3 y 5 de UTP y STP	Si; todas, usando emulación de LAN
FDDI	No	No, solo fibra óptica	Si, todas
CDDI	No	Si, categoría 5 UTP y STP	Si, todas
100Base-T conmutado	Si	Si, categoría 3 y 5 de UTP y STP	Si, todas
100VG-AnyLAN	No	Si, categoría 3 y 5 de UTP y STP	Si, todas

Tabla 8.19 Facilidad de integración de las tecnologías con respecto a la base ya instalada

	Velocidad (Mbit/s)	Conmutado o medio compartido	Full dúplex	Network overhead	Distancia para conectar nodos sobre cable de cobre	Topolog.
ATM	25, 50, 155 y 622	Conmutado	Si	9.5 %	100 m	Malla, punto-punto, estrella
FDDI	100	Medio compartido	No	0.5 %	n/a	Punto-punto, arullo, estrella
CDDI	100	Medio compartido	No	0.5 %	100 m	Punto-punto, anillo, estrella
100Base-T conmutado	100	Conmutado	Si	1.6 %	100 m	Malla, punto-punto, estrella
100VG-AnyLAN	100	Medio compartido	No	1.6 o 0.5 %	200 m (UTP 5)	Punto-punto, estrella

Tabla 8.20 Arquitectura

	100 Base T conmutado	100 VG-AnyLAN
Estandarización	802.3u (aprobado el 14 junio 1995)	802.12 (aprobado el 14 junio 1995)
Asociación que lo soporta	La alianza de Fast ethernet	Forum de 100VG-Any LAN
Velocidad (Mbps)	100	100
Método de acceso	conmutación y CSMA/CD	Demanda de prioridad
Tipo de frame	Ethernet 802.3	Ethernet 802.3 y Token Ring 802.5 (no simultáneamente)
Máximo tamaño de paquete (bytes)	1,500	1,500 o 4,500
Medios soportados:		
UTP Categoría 3	4 pares	4 pares
UTP Categoría 4	4 pares	4 pares
UTP Categoría 5	2 o 4 pares	4 pares y 2 pares
STP Categoría 1	2 pares	2 pares
Fibra óptica	Si	Si
Full dúplex	Si	No
Diámetro de la red	2.2Km.	2.2 Km.
Nodos por segmento	-	1024
Redundancia	Por método de Árbol expandido (spanning tree)	No aplica actualmente
Manejo de prioridades	No	Si
Servicios	Asíncrono	Asíncrono y síncrono
Aplicación en la cobertura geográfica	Para grupos de trabajo y áreas de trabajo. Algunas implantaciones de backbone si se tiene la característica de Full dúplex activa	Área de trabajo, backbone

Tabla 8.21 Resumen de los parámetros mas importantes de las tecnologías de red de alta velocidad.

	FDDI / CDDI	ATM
Estandarización	ANSI X3T9.5 1986	No tiene
Asociación que lo soporta	No existe organización que lo soporte	ATM Forum
Velocidad (Mbps)	100	Desde 25 hasta 622
Método de acceso	Rotación de señal token por tiempo	Conmutación
Tipo de frame	FDDI ANSI X3T9.5	Ninguno (basado en celdas)
Maximo tamaño de paquete (bytes)	4500	53 (tamaño de las celdas)
Medios soportados:		
UTP Categoría 3	No	Si
UTP Categoría 4	No	No
UTP Categoría 5	4 pares	Si
STP Categoría 1	2 pares	No
Fibra optica	Si	Si
Full dúplex	No	Si
Diámetro de la red	Desde 100 m hasta 200 Km	Desde 100 mts. hasta múltiples kilómetros
Nodos por segmento	500	-
Redundancia	Dual homing MAC ring	Rutas múltiples (topología de malla) con balanceo de cargas
Manejo de prioridades	Si	Maneja Calidad de Servicio (QoS)
Servicios	Asincrono y sincrono	Isócrono, asincrono y sincrono
Aplicación en la cobertura geográfica	Area de trabajo, grupos de trabajo, backbone (LAN y WAN)	Areas de trabajo, grupos de trabajo, backbone (LAN y WAN)

Tabla 8.21 Resumen de los parámetros mas importantes de las tecnologías de red de alta velocidad (continuación).

	100 Base T conmutado	100 VG-AnyLAN
Aplicaciones (voz, datos y video)	Transferencia de datos	Datos, multimedia y aplicaciones de video (debido a su capacidad de priorización y seguridad en la entrega de paquetes)
Flexibilidad topológica: reutilizacion de equipo (en base a la existencia de 10Base T)	Reutilización del cableado existente, reutilización de NICs de 10BaseT en la transición del cambio (pero requiere cambio de concentradores)	Reutilización de sistema de cableado mientras se encuentren disponibles los cuatro pares de cable UTP, reutilización de NICs en la transición del cambio, (requiere cambio de concentradores)[23]
Administración	SNMP y MIBs Ethernet	SNMP, MIB
Productos disponibles	1994	1994
Madurez del estándar	Apenas comenzando	Apenas comenzando
Inicio de la tecnología	En 1992 Grand Junction (actualmente una división de Cisco)	Noviembre de 1992
Costo aproximado por nodo(en base al precio de 10Base T	2 veces	2 veces
Proveedores mas importantes	3Com AT&T Global system Bay Networks Cabletron Systems Chipcom Cisco Systems Digital Equipment	AT&T microelectronics Cisco Systems incluyendo Compaq Hewlett-Packard NEC Thomas Conrad

Tabla 8.21 Resumen de los parámetros mas importantes de las tecnologías de red de alta velocidad (continuación).

[23] En la migración por etapas apartir de 10BaseT hacia 100VG, primeramente se requiere un puente translacional entre 100VG y 10BaseT.
Se debera explorar el sistema de cableado existente de manera de remover cualquier cable par trenzado de 25 pares conectado a dispositivos que operen en modo promiscuo.

	FDDI / CDDI	ATM
Aplicaciones (voz, datos y video)	Datos, multimedia y aplicaciones de video (debido a la designación de ancho de banda síncrono)	Datos, multimedia y aplicaciones de video (debido a la designación de ancho de banda síncrono)
Flexibilidad topológica: reutilización de equipo (en base a la existencia de 10Base T)	Se aprovechan ciertos concentradores y conmutadores que tengan la opción de soportar FDDI (requiriendo el reemplazo algunas tarjetas de estos dispositivos), reutilización del sistema de cableado UTP categoría 5; cambio de NICs	Se aprovechan ciertos concentradores y conmutadores que tengan la opción de soportar ATM (requiriendo el reemplazo algunas tarjetas de estos dispositivos). sistema de cableado?
Administración	SMT, SNMP	SNMP y MIBs propietarias
Productos disponibles	Desde 1990	1993-1994
Madurez del estándar	Estable	Evolucionando
Inicio de la tecnología	1986	1984 se empezó a desarrollar el concepto de ATM
Costo aproximado por nodo(en base al precio de 10Base T	6 veces	8 veces
Proveedores mas importantes	3com Anixter Bros. Cabletron Cisco Systems Digital Equipment Corp. Hewlett-Packard IBM Corp. SynOptics	3com Cabletron Systems Cisco Systems Digital Equipment Corp. Hewlett-Packard Motorola SynOptics Fore Systems

Tabla 8.21 Resumen de los parámetros mas importantes de las tecnologías de red de alta velocidad (continuación).

[1] En la migración por etapas a partir de 10BaseT hacia 100VG, primeramente se requiere un puente traductor entre 100VG y 10BaseT. Se deberá explorar el sistema de cableado existente de manera de remover cualquier cable par trenzado de 25 pares conectado a dispositivos que operen en modo promiscuo.

8.4.5.3.8 Análisis y evaluación

Como se explico en la introducción, se pretende llevar una migración gradual hacia una red de altas especificaciones, por lo que esta etapa se puede decir, que es solo el principio de esta red.

Se debe tener en cuenta que las necesidades no son iguales en todos los módulos de una red, es decir, mientras se requiere de mayor ancho de banda, disponibilidad y eficiencia tanto en el backbone principal, conexión a RedUNAM y el grupo de servidores, por otro lado, son menores los requerimientos de ancho de banda y otros parámetros en la mayoría de los usuarios finales. La esquema anterior es lo que se conoce como "jerarquía de áreas de red".

Tomando en cuenta esta jerarquía y para realizar un estudio mas estructurado que nos guíe a una mejor solución de esta etapa, hemos decidido dividir en dos secciones principales el análisis de ésta. La primera sección, tendrá en cuenta el backbone y la conexión a RedUNAM, mientras una segunda estudiará los segmentos en edificios donde se encuentran los usuarios finales. Al realizar esta división, se tendrá un mayor margen de libertad para poder establecer que tecnologías se adecuan mejor para cada una de las dos secciones y posteriormente puedan ser evaluadas. Al mismo tiempo, se podrán asignar con mayor libertad los ponderadores de acuerdo a los diferentes parámetros tomando en cuenta las necesidades y requerimientos de la sección que se este evaluando.

Tomando en cuenta lo anterior, se debe observar que la tecnología que se escoja para estas secciones, no debe ser necesariamente la misma que se seleccione para toda la red, ya que como se mencionó con anterioridad, existen jerarquías y al mismo tiempo, en la institución los requerimientos y necesidades son diferentes dependiendo de cada área o servicio, es por ello que tal vez una sola tecnología de redes no sea la adecuada para cubrir todas las necesidades operacionales que demanda el Instituto y por lo que tal vez sea preciso llegar a una solución de red híbrida.

8.4.5.3.8.1 Evaluación para la tecnología del backbone y conexión a RedUNAM

El backbone al ser la sección mas importante y donde se presenta de mayor manera los efectos de flujo de tráfico excesivo, nos conduce a prestar mayor atención en éste para poder mantener alto el nivel del desempeño de la red.

Asimismo, una mejor calidad y mayor ancho de banda en el backbone permitirá un mejor desempeño en la conexión hacia el grupo de servidores, ya que estos

captaran simultáneamente un mayor número de peticiones y de igual manera proporcionarán un mejor tiempo de respuesta a las aplicaciones, además de poder soportar los nuevos servicios requeridos por los usuarios.

Por otro lado, el principio de jerarquía no se había llevado tan profundamente en la conexión a RedUNAM en las etapas anteriores, ya que así como las necesidades y las aplicaciones cambian, lo mismo sucede con el flujo de tráfico. En las etapas anteriores, la red del Instituto tenía un comportamiento donde el mayor porcentaje del tráfico se quedaba localmente y un pequeño porcentaje solo cruzaba el backbone hacia RedUNAM, sin embargo debido a las nuevas necesidades requeridas por los investigadores, aunadas con el éxito que ha tenido Internet, este comportamiento de tráfico a cambiado, teniendo que un mayor porcentaje del tráfico cruza el backbone hacia RedUNAM, es por esto que se debe tener un ancho de banda adecuado en este enlace y en el backbone para poder soportar la carga de peticiones de los usuarios y no llegar a tener cuellos de botella en estos puntos, además de que por su función crítica ambos deben tener un máximo de disponibilidad y eficiencia.

De acuerdo a las características requeridas por el backbone y la conexión a RedUNAM, y basándose en el estudio que se realizo anteriormente, solo se tomaran en cuenta las siguientes tecnologías para su evaluación en está sección: ATM, FDDI y 100Base-X conmutado.

BACKBONE	ATM	FDDI	Fast Ethernet conmutado	Pond.
Ancho de banda/ desempeño	4	3	3	25
Soporte aplicaciones	5	3	4	20
Confiabilidad	5	4	3	17
Costo	3	3	4	10
Escalabilidad	5	2	3	10
Seguridad / administracion	4	3	4	10
Estandarizacion /Madurez mercado	3	4	4	8
Calificación	4.29	3.15	3.48	

Tabla 8.22 Calificaciones de las tecnologías para la sección backbone y conexión a RedUNAM

Criterio	calif.	Explicación del criterio
Excelente	- 5:	Se asigna a aquellas casos en que el funcionamiento supera en gran medida las expectativas deseadas.
Bueno	- 4:	Satisface los criterios estándar e incluye algunas características especiales.
Suficiente	- 3:	Su función o características son las esperadas.
Pobre	- 2:	Escaso cumplimiento en las funciones o características esenciales.
Inaceptable	- 1:	Es seriamente deficiente.

Tabla 8.23 Criterios de calificación que se tomaron para este proyecto

La tecnología ATM ha sido seleccionada como la solución óptima para el backbone de la REDII y la conexión hacia RedUNAM. Esto es a partir de que puede ser vista como una continuación del esquema de conmutación seguido por la red del Instituto de Ingeniería en las etapas anteriores. No obstante, debido a que su funcionamiento difiere en gran medida de la tecnología utilizada actualmente (Ethernet conmutado) y de otras tecnologías de redes LAN tradicionales, ATM proporciona capacidades superiores a todas ellas en varios aspectos.

Las tecnologías LAN de medio compartido, utilizan protocolos orientados a la no conexión haciéndolas adecuadas para aplicaciones de transmisión de datos. Lo mismo sucede para las tecnologías conmutadas de alta velocidad, que se encuentran basadas fundamentalmente en tecnologías de medios compartidos y por tanto orientadas a la no conexión. ATM es una tecnología de comunicación orientado a la conexión lo cuál lo hace efectivo para el buen manejo de las nuevas aplicaciones tanto de uso intensivo de ancho de banda como las que demandan Calidad de Servicio (multimedia y videoconferencias). Además, también ofrece beneficios considerables para la ejecución de aplicaciones heredadas que sean orientadas a la no conexión, ya que éstas pueden obtener ventaja del alto y dedicado ancho de banda que ofrece ATM.

Con respecto a la conmutación, en un conmutador LAN tradicional, se procesa cada paquete independientemente ya que este puede tener una longitud y dirección destino diferente, además la capacidad de rendimiento de un conmutador es directamente dependiente del poder y limitaciones del procesador. Aunque actualmente existen técnicas de conmutación como la cut-through con la que se puede mejorar la latencia del conmutador sobre una base puerto a puerto, existen ciertas funciones como son el filtrado, la adaptación de velocidad de puerto (10 Mbps a 100Mbps, por ejemplo) y la tasa de errores sobre el medio, que frecuentemente impiden llevar a cabo una conmutación de este tipo[232]. En cambio, en la conmutación ATM los datos son repartidos dentro de celdas de longitud fija y las características de la conexión son negociadas antes de la transferencia (si la red puede garantizar la Calidad de Servicio, la llamada entonces es aceptada y la ruta es establecida), de esta manera, las celdas son transmitidas a la velocidad de hardware sin la necesidad de reexaminar el contenido de las celdas o desarrollar acciones de conmutación almacenamiento-y-reenvío (store-and-forward) entre la fuente y el destino.

Por otro lado, en ambientes LAN ya sea compartidos o conmutados, las aplicaciones de una estación toman turno para el envío de los datos sobre el medio. Con esto, se puede tener el caso en que una aplicación de baja prioridad pueda retrasar la transmisión de un frame corto que es sensible al tiempo. ATM

[232] Teniéndose que llevar a cabo una conmutación del tipo almacenamiento-y-reenvío (store-and-forward).

en cambio, divide la información en celdas de tamaño fijo de 53 bytes con lo que se puede tener un mayor control del retraso, además de que las celdas de diferentes fuentes pueden ser entremezcladas y encoladas de acuerdo a su prioridad individual. De esta manera, retrasos fijos pueden ser respetados y la calidad de servicio puede ser establecida según los requerimientos de la aplicación, en lugar de aquellos que tenga el dispositivo.

ATM por otra parte, con su arquitectura de conmutación full dúplex, ofrece un mejor desempeño, no así otras tecnologías conmutadas que aunque también ofrecen el modo full dúplex, requieren ciertas características (como son buffers para el almacenamiento-y-reenvío, etc.) que reducen la capacidad real del ancho de banda que ofrecen. Al mismo tiempo, en ATM el ancho de banda es un parámetro a definir al momento de establecer la conexión de circuito virtual, convirtiéndose de esta manera en un aspecto independiente de la conexión física y por lo que no son necesarios buffers intermedios.

Por otro lado, si un enlace llegara a alcanzar su capacidad máxima, ATM ofrece la característica de poder conectarse por medio de una topología de malla y manejar balanceo de cargas, de esta manera, se pueden construir conexiones adicionales para el manejo de rutas redundantes y para ampliar el ancho de banda soportando el trafico adicional. Esto ultimo es una cualidad muy poderosa y que es un recurso fundamental en el manejo de alta calidad para el trafico sensible al tiempo y una solución para cuellos de botella entre conmutadores de grupos de trabajo y el conmutador del backbone central de alta velocidad.

Además de todas las características antes mencionadas, ATM por su mecanismo de multiplexaje y su característica de ser un protocolo orientado a la conexión, puede soportar transferencia de trafico con requerimientos diversos de ancho de banda y retraso. Esta característica de diseño permite a las redes ATM soportar voz, video y datos sobre un mismo enlace.[233]

Como una característica adicional, ATM ofrece el manejo de redes virtuales (VLANs) lo cual ayudara a mejorar aun mas el desempeño y eficacia de la red, al mismo tiempo, reduce el costo de operación y simplifica las tareas de administración.

Con la capacidad de multicast que proporciona ATM y el manejo de redes LAN emuladas (LANE) se pueden construir árboles de broadcast para redes virtuales, siendo así un fundamento tanto para la distribución de video como para videoconferencias, ya que a diferencia del manejo de broadcast que se realiza en

[233] La Calidad de Servicio se establece en el momento en que se llevan a cabo las negociaciones para efectuar la conexión. El Forum ATM ha definido cuatro tipos de Calidad de Servicio para los diferentes tipos de tráfico (CBR, VBR, UBR y ABR).

redes LAN de medio compartido, en ATM solo aquellos usuarios quienes quieran recibir el mensaje lo recibirán. Por otro lado, en las redes LAN conmutadas tradicionales, se pueden utilizar filtros para el control de trafico de broadcast en los conmutadores, pero estos tienen un efecto adverso sobre el desempeño total de la red.

Por ultimo, ATM es la tecnología que ofrece la mayor escalabilidad en varios aspectos como son, ancho de banda, distancia geográfica, numero de nodos conectados, numero de enlaces, etc. Además es la tecnología propuesta como solución en el backbone de RedUNAM, con lo cual se podrá tener una homogeneización de la REDII con esta.

8.4.5.3.8.2 Evaluación para la tecnología de conexión en el interior de los edificios

Como se mencionó anteriormente, los requerimientos que demandan los usuarios son menores que en otras áreas de la red, sin embargo, son obviamente el factor mas importante, y por el cual se debe realizar una continua actualización de la red, adaptándose así a ambientes expandibles tanto en tamaño como en diversidad al soporte de aplicaciones (teniendo cuidado al mismo tiempo de aspectos como el mejoramiento y simplificación de las tareas de administración y mantenimiento).

También se debe tener en cuenta que las mismas necesidades de los usuarios varían dependiendo del área de desarrollo y la coordinación, teniéndose de esta manera, diferentes categorías entre las estaciones de los usuarios finales. Es por esto que en esta sección de la evaluación se debe escoger una tecnología que cubra los diferentes niveles de necesidad y requerimientos de los múltiples usuarios. Es decir, la tecnología a implantar debe interoperar con la tecnología actual (Ethernet 10BaseT) para aquellos usuarios que sus requerimientos no sean mayores al ancho de banda de 10Mbps, pero que permita una ruta de escalabilidad para cuando estos usuarios lo deseen. Al mismo tiempo, la nueva tecnología proporcionará enlaces de alta velocidad que permitan la conexión para aquellos usuarios o grupos de trabajo de alto desempeño que necesiten una conexión con mayor ancho de banda además de otras características. Por otro lado, la tecnología también debe ser ampliamente interoperable con la tecnología a implantar en el backbone y la conexión ha RedUNAM, teniéndose de esta manera el mejor aprovechamiento de los beneficios de la nueva arquitectura y expandir hasta los usuarios finales ciertas características de la tecnología utilizada en el backbone.

De acuerdo a las características mencionadas en el párrafo anterior y basándonos en el estudio que se realizo anteriormente, cabe mencionar que solo se tomaran

en cuenta las siguientes tecnologías para su evaluación: CDDI, 100Base-X conmutado y 100VG-AnyLAN.

		Fast Ethernet		
INTRA EDIFICIOS	CDDI	conmutado	100VG-AnyLAN	Pond.
Ancho de banda/ desempeno	3	4	3	20
flexib. topológica./interoper. 10baseT	3	5	3	20
Costo	2	3	3	20
Soporte aplicaciones	3	4	3	15
Estandarizacion /Madurez mercado	4	3	2	10
Escalabilidad	2	4	3	10
Seguridad / administracion	3	4	3	5
Calificacion	2,8	3,9	2,9	

Tabla 8.24 Calificaciones de las tecnologías para la sección de la conexión intraedificios

Criterio	calif.	Explicación del criterio
Excelente	- 5:	Se asigna a aquellas casos en que el funcionamiento supera en gran medida las expectativas deseadas.
Bueno	- 4:	Satisface los criterios estándar e incluye algunas características especiales.
Suficiente	- 3:	Su función o características son las esperadas.
Pobre	- 2:	Escaso cumplimiento en las funciones o características esenciales.
Inaceptable	- 1:	Es seriamente deficiente.

Tabla 8.25 Criterios de calificación que se tomaron para este proyecto

Con respecto a la evaluación anterior, se ha seleccionado la tecnología Fast Ethernet conmutado como la tecnología para la interconexión de los usuarios finales y el backbone principal, ya que brinda principalmente una ruta de migración flexible hacia una red de alta velocidad de acuerdo a las necesidades requeridas por los diversos usuarios del Instituto de Ingeniería proporcionando una mejor protección de la inversión.

A partir de que Fast Ethernet es una extensión de Ethernet, este preserva ciertas características como son la utilización del mismo tamaño y formato del paquete de transmisión, de esta manera no se hace necesario realizar una traducción de paquetes entre estas dos tecnologías, ahorrándose así, tiempo de latencia y retrasos innecesarios. Por otro lado, al estar basado en protocolos usados por Ethernet, es posible seguir utilizando todas las herramientas de administración y monitoreo sin la necesidad de modificar los protocolos de las capas superiores, además, se puede seguir aprovechando la experiencia del personal en este tipo de tareas.

Al mismo tiempo, Fast Ethernet soporta un amplio rango de tipos de cables, lo cual lo hace una opción viable y flexible para su implantación en las zonas donde exista un sistema de cableado previo. Por otro lado, el estándar Fast Ethernet define un protocolo de autonegociación el cual permite que el adaptador y el conmutador puedan negociar la velocidad de operación (10Mbps o 100Mbps) del enlace de comunicación entre ellos, permitiéndose la reutilización de las tarjetas adaptadoras de 10Mbps según sea el caso.

Las anteriores, son las características que hacen que Fast Ethernet conmutado pueda brindar una ruta de migración fácil y flexible hacia la tecnología de alta velocidad, tomando en cuenta los requerimientos de las aplicaciones y el presupuesto de los usuarios, además de esta manera se garantiza ofrecer un alto grado de protección a la inversión.

Con respecto al incremento en el numero de dispositivos conectados, el desempeño del ancho de banda se llega a degradar en las redes del tipo de medio compartido, no así en Fast Ethernet conmutado donde por su modo de operación se puede ofrecer un mejor aprovechamiento del ancho de banda ya que permite seguir el esquema de microsegmentación donde a cada usuario se le puede designar un ancho de banda dedicado.

Al ser una versión conmutada, Fast Ethernet incluye características mas avanzadas como son el modo de operación full dúplex, lo que permite obtener dos veces el desempeño del ancho de banda en un enlace, además del filtrado de paquetes y el manejo de redes virtuales. Esta ultima característica, permite reducir los costos de operación, facilitar las tareas de administración y seguridad y proporciona un mejor aprovechamiento del ancho de banda.

Con respecto a la tolerancia a fallas, Fast Ethernet puede soportar múltiples enlaces entre dispositivos, previendo de esta manera enlaces redundantes controlados por el protocolo de árbol expandido (STP: Spanning Tree Protocol).

Por ultimo, cabe mencionar que Fast Ethernet conmutado al ser una tecnología ampliamente respaldada en el mercado, con una fácil instalación y configuración, aunado al amplio grado de protección a la inversión que ofrece, además de que permite seguir aprovechando la experiencia del personal, sea una tecnología que se pueda implantar y mantener a un precio muy razonable.

8.4.5.3.8.3 Selección y proyección de alternativas

Una vez que se han seleccionado las tecnologías que comprenderán esta etapa en la red del Instituto de Ingeniería, se procedió a realizar una licitación por invitación restringida a los siguientes proveedores:

3Com
Bay Networks
Cabletron Systems
Cisco Systems
NewBridge

Se escogieron estos proveedores por ser empresas líder en el área de redes de datos a nivel mundial, tener sucursales en México, además de pertenecer a los grupos de desarrollo de las tecnologías seleccionadas.

A las empresas se les pidió realizar una propuesta con las tecnologías seleccionadas en el backbone y en el sistemas intraedificios además de alinearse a ciertos requerimientos , para poder realizar posteriormente un análisis y evaluación de cada una de estas.

De estas empresas, las compañías Bay Networks y NewBridge fueron excluidas del la siguiente etapa. Esto es debido a que Bay Networks proporcionó una pobre explicación de su propuesta y además mostró poco interés para resolver esta situación, por otro lado, el producto de monitoreo que ofrecía no era compatible con la plataforma SunNet Manager que se maneja en el Instituto. En el caso de NewBridge, la línea de productos que ofrecen son relativamente nuevos, por lo que no han sido probados ampliamente en el mercado, así mismo, la solución que proponían sobrepasaba en un amplio margen nuestro presupuesto.

8.4.5.3.8.3.1 Tablas de especificaciones

A continuación se presentan las tablas con las características técnicas mas importantes de los equipos de acuerdo a cada proveedor.

8.4.5.3.8.3.2 Dispositivos para el backbone

La tabla 8.A presenta los parámetros mas importantes del equipo de cada proveedor que se utilizara como dispositivo central en el backbone ATM.

Proveedor Modelo	3com CoreBuilder 7000HD	Cisco Lightstream 1010	Cabletron MMAC Plus 6
Tipo	Conmutador para backbone	Conmutador para backbone	Conmutador para backbone
Capacidad de conmutación	5.0 Gbps 7000 HD (Backplane pasivo de 20.48 Gbps)	5 Gbps	5 Gbps
Max. numero de VCCs	64,000	32,000	-
Señalización	UNI 3.0, UNI 3.1	UNI 3.0, UNI 3.1, Q.2931	UNI 3.0, UNI 3.1
Señal de conmutador a conmutador	PNNI, IISP	PNNI, IISP	PNNI,IISP
Interfaces ATM	OC3, OC12	OC3,STM-1	OC3, OC12
Interfaces Ethernet	Conmutado 10/100 Mbps	N/A	-
Máximo numero de puertos ATM por chasis	32	32	48
Máximo numero de puertos Fast Ethernet por chasis	64	N/A	72
Máximo numero de puertos Ethernet por chasis	144	N/A	256
FDDI	N/A	N/A	14
No de VLANs soportadas	16 por conmutador	-	-
Tipo de arquitectura	Non-blocking	Non-blocking	Non-blocking
VPI/VCI	4,096 por puerto	32,000 pto-pto 1985 pto.-multipto.	
Soporte para ELAN	LANE 1.0	LANE 1.0	LANE 1.0
Mmoria principal (local)	16Mb	16 (actualización hasta 64)	16 (actualización hasta 32)
buffers de salida	600 celdas por puerto 19,200 para los 32 ptos.	65,536 celdas de memoria compartida	13,312 celdas por módulo de red
Arquitectura de conmutación	Matriz conmutada	Memoria compartida	Matriz conmutada (CTM)
Software de administración	Transend: SUN Sunnet Manager, HP Openview, IBM Netview.	Ciscowork: SUN Sunnet Manager, HP Openview, IBM Netview.	Spectrum: SUN Sunnet Manager, HP Openview, IBM Netview.

Tabla 8.26 Principales características del dispositivo central para el backbone ATM.

8.4.5.3.8.3.3 Dispositivos para la conexión intraedificios

En seguida se presentan las tablas por proveedor con las características mas importantes de los equipos que conforman el esquema de interconexión en el interior de los edificios.

3com		LANplex 2500 (enrutador)	Superstack switch 1000	Superstack switch 3000
Arquitect.	Mecanismo de conmutacion	Medio compartido	Medio compartido	Medio compartido
	Tipo de arquitectura	Non-blocking	-	-
	Tipo de reenvio	Almacenamiento-y-reenvio	Cut through / Almacenamiento-y-reenvio	Almacenamiento-y-reenvio
	Capacidad de conmutacion	290 Mbits/seg	800 Mbits/seg	800 Mbits/seg
	Memoria	8MB	2MB	2MB
Conexiones físicas	Tipo de chasis	Modular	Fijo, apilable	Fijo, apilable
	Ranuras utilizables	4 (2 para Ethernet conmutado, cada uno con 8 puertos y 2 para interfaces de alta velocidad (ATM, Fast Ethernet y FDDI)	N/A	N/A
	Max. No. de puertos a 10bps por conmutador.	16	24	12 (10/100)
	Max. No. de puertos a 10bps por módulo	8	N/A	N/A
	Max. No. de puertos a 100bps o mas por conmutador	2	2	12 (10/100)

Tabla 8.27 Caracteristicas de los dispositivos propuestos por 3com para la conexión intraedificios.

3com		LANplex 2500 (enrutador)	Superstack switch 1000	Superstack switch 3000
Conexiones físicas	Max. No. de puertos ATM por conmutador o por módulo	1 OC-3c (155Mbps)	1 OC-3c (155Mbps)	1 OC-3c (155Mbps)
	Max. No. de puertos FDDI	1	N/A	N/A
	Tipo de puertos a 10 Mbps	10Base-T,-2,-5,FL conmutados	10Base-T,-2,-5,FL conmutados	10/100 conmutados
	Tipo de puertos a 100 Mbps	100Base-TX, -FX, FDDI DAS (SM y MM) TP-DDI DAS y	100Base-TX, -FX, FDX y OC-3c ATM	100Base-TX, -FX, FDX y OC-3c ATM
	Uplinks	Fast Ethernet, FDDI, TP-DDI (CDDI) y OC-3c ATM	Fast Ethernet y OC-3c ATM	Fast Ethernet y ATM (OC-3) Gigabit Ethernet
Conexiones lógicas	Número de direcciones MAC	8,192	500 por conmutador, sin límite para el puerto de backbone	4,080
	VLAN	Si, agrupamiento por puertos (hasta 32), por direcciones MAC y basados en protocolos	Si	Si, hasta 16 VLANs
	En el caso de soportar ATM, que tipo de protocolos soporta	UNI3.0-3.1; LANE 1.0; soporte LES/BUS; RFC 1577;	UNI3.0-3.1; LANE 1.0;	UNI3.0-3.1; LANE 1.0;
Tolerancia a fallas	Intercambio rápido de módulos (hot swap)	Si	N/A	N/A
	Redundancia	Fuentes de poder	Como parte de la pila	Como parte de la pila
	Manejo de puertos espejo	Si	Si	Si
	Protocolos de puenteo/enrutamiento	802.1d	802.1d	802.1d
Administración	RMON	Si	Si , para 7 grupos	Si, para 7 grupos
	SNMP	Si	Si	Si

Tabla 8.27 Características de los dispositivos propuestos por 3com para la conexión intraedificios (continuación).

Cisco		Catalyst 3000	Cisco 2900 (enrutador)	Catalyst 5000
Arquitect.	Mecanismo de conmutación	Medio compartido	Medio compartido	Medio compartido
	Tipo de arquitectura	Nonblocking;	-	Nonblocking;
	Tipo de reenvío	Cut through / Almacenamiento-y-reenvío dependiendo de la tasa de error	Almacenamiento-y-reenvío	Cut through / Almacenamiento-y-reenvío dependiendo de la tasa de error
	Capacidad de conmutación	520 Mbps (bus Axis) (Catalyst Matrix 3.84Gbps)	1.2Gbps (con tres niveles de . prioridad)	1.2Gbs (con tres niveles de prioridad)
	Memoria	-	-	-
Conexiones físicas	Tipo de chasis	Apilable (stackable) hasta (hasta 8 por medio de Catalyst 3000 matrix,	Configuración fija	Modular
	Ranuras utilizables	2	N/A	4
	Max. no. de puertos a 10bps por conmutador	16 fijos 10BaseT 8 opcionales 10baseT 3 opcionales 10baseFL	12 (half o full dúplex) 10/100	96 (Ether. Switched) 192 (Group switching)
	Max. no. de puertos a 10bps por módulo	N/A	N/A	24 (Ether. conmutados) 48 (Grup conmutados)
	Max. no. de puertos a 100bps o mas por conmutador	1 o 2 ptos. opcionales: 100baseTx / 100baseFX / 100VG-AnyLAN	14 (half o full dúplex)	50
	Max. no. de puertos ATM por conmutador/ por módulo	1 pto. Opcional ATM (OC-3 155Mbps)	N/A	3 o 1 (OC-3 155Mbps)
	Max. no. de puertos FDDI	N/A	N/A	4 o 1 (DAS o SAS)

Tabla 8.28 Características de los dispositivos propuestos por Cisco para la conexión intraedificios.

Cisco		Catalyst 3000	Cisco 2900 (enrutador)	Catalyst 5000
Conexiones físicas	Tipo de puertos a 10 Mbps (compartidos o conmutados)	Conmutado	N/A	Conmutado
	Tipo de puertos a 100 Mbps	Conmutado	Conmutado	Conmutado
	Uplinks	Ethernet Fast Ethernet 100VG-Anylan OC-3 ATM (155Mbps) WAN	N/A	Fast Ethernet (half o full dúplex) FDDI/CDDI (half dúplex) OC-3 ATM con LANE
Conexiones lógicas	Numero de direcciones MAC soportadas	1700 por puerto 6000 o 10,000 direcciones por sistema dependiendo la versión	16000	16,000 por puerto
	VLAN	64 por switch	1024	-
	En el caso de soportar ATM, que tipo de protocolos soporta.	-	-	UNI 3.0, UNI 3.1 ILMI IISP (default) PNNI (opcional) PVC
Tolerancia a fallas	Capacidad para el intercambio rápido de módulos (hot swappability)	-	N/A	Si
	Redundancia	Fuentes redundante (con catalyst matrix)	?	-Fuente de poder redundantes -procesadores de conmutación -ventiladores -conexiones tolerantes a fallas (con balanceo de cargas)

Tabla 8.28 Características de los dispositivos propuestos por Cisco para la conexión intraedificios (continuación).

Cisco		Cisco Catalyst 3000	Cisco 2900 (enrutador)	Cisco Catalyst 5000
Tolerancia a fallas	Manejo de puertos espejo	Si	-	Si
	Protocolos de puenteo/enrutamiento	802.1d	-	802.1d
Administración	RMON	Si	Si	Si
	SNMP	Si	Si	Si

Tabla 8.28 Caracteristicas de los dispositivos propuestos por Cisco para la conexión intraedificios (continuación)

Cabletron		SmartStack 10	SmartSwitch 2200	SmartSwitch 6000
Arquitect.	Mecanismo de conmutación	Memoria compartida	Memoria compartida	Memoria compartida
	Tipo de arquitectura	-	-	Non blocking
	Tipo de reenvío	Almacenamiento-y-reenvio	Almacenamiento-y-reenvio	Almacenamiento-y-reenvio
	Capacidad de conmutación	-	640Mbps	3.2 Gbps
	Memoria	-	Memoria compartida entre puertos 4Mb	Memoria compartida entre puertos 4Mb
Conexiones físicas	Tipo de chasis	Apilable	Apilable	Modular
	Ranuras utilizables	N/A	N/A	5
	Max. No. de puertos a 10bps por conmutador	25	24	130
Conexiones físicas	Max. No. de puertos a 10bps por modulo	N/A	N/A	24
	Max. no. de puertos a 100Mbps o mas por conmutador	1 fijo 100Base-TX 1 opcional	2 opcionales	40

Tabla 8.29 Caracteristicas de los dispositivos propuestos por Cabletron para la conexión intraedificios.

Cabletron		SmartStack 10	SmartSwitch 2200	SmartSwitch 6000
Conexiones físicas	Max. no. de puertos ATM por conmutador/ por modulo	N/A	2 opcionales	1 por modulo 5 totales
	Max. no. de puertos FDDI	N/A	2 opcionales	1 por módulo 5 totales
	Tipo de puertos a 10 Mbps	Conmutados (full dúplex)	Conmutados (full dúplex)	Conmutado (full dúplex)
	Tipo de puertos a 100 Mbps	Conmutados (full dúplex)	Conmutado (full dúplex)	Conmutado (full dúplex)
	Uplinks	Fast Ethernet, 100Base-(FX/TX) conmutado	ATM (OC-3 155Mbps), FDDI (full dúplex), Fast Ethernet	ATM (OC-3 155Mbps), FDDI (DAS) full duplex,
Conexiones lógicas	Número de direcciones MAC soportadas	1024	8,192	8,192
	VLAN	Si	Si	Si
	En el caso de soportar ATM, que tipo de protocolos soporta	N/A	LANE 1.0 UNI 3.0/3.1	LANE 1.0 UNI 3.0/3.1
Tolerancia a fallas	Intercambio rápido de módulos (hot swap)	N/A	-	Si
	Redundancia	N/A	N/A	Fuentes de poder
	Manejo de puertos espejo (Port Mirroring)	-	Si	Si
	Protocolos de puenteo/enrutamiento	802.1d	802.1d	802.1d
Administración	RMON	Si	Si	Si
	SNMP	Si	Si	Si

Tabla 8.29 Caracteristicas de los dispositivos propuestos por Cabletron para la conexion intraedificios.(continuación).

8.4.5.3.8.3.4 Evaluación y selección del proveedor

A continuación se presenta la tabla de evaluación de los proveedores con respecto a los parámetros mas importantes que deben observar para la red del Instituto de Ingeniería.

	3com	Cabletron	Cisco	Ponderador
Escalabilidad	5	5	3	20
Costo	5	2	3	20
Interoperabilidad con RedUNAM	5	3	3	20
Administración	4	4	4	10
Tolerancia a fallos / confiabilidad	3	4	5	10
Flexibilidad en la arquitectura	5	4	3	10
Desempeño del equipo	4	3	4	5
Atención al cliente	4	2	3	5
Calificación	4,6	3,45	3,35	

Tabla 8.30 Calificaciones de los proveedores para la implantación de la tercera etapa

Criterio	calif.	Explicación del criterio
Excelente	- 5:	Se asigna a aquellas casos en que el funcionamiento supera en gran medida las expectativas deseadas.
Bueno	- 4:	Satisface los criterios estándar e incluye algunas características especiales.
Suficiente	- 3:	Su funcion o características son las esperadas.
Pobre	- 2:	Escaso cumplimiento en las funciones o características esenciales.
Inaceptable	- 1:	Es seriamente deficiente.

Tabla 8.31 Criterios de calificación que se tomaron para este proyecto

De acuerdo a la evaluación anterior, se puede observar que 3com es la compañía que cumple con nuestros requerimiento a un menor costo, haciéndola de esta manera, la opción mas viable para este proyecto.

La solución propuesta por 3com ofrece un alto grado de escalabilidad, el equipo central CoreBuilder 7000HD es una chasis de alto desempeño con un backplane pasivo 20.5 Gbps que garantiza la escalabilidad a mayores tasas de transmisión de celdas de hasta OC-12 sin la necesidad de un cambio de este dispositivo, por otro lado, también soporta módulos de interconexión Gigabit Ethernet, teniéndose de esta manera un backbone colapsado con un amplio margen de escalabilidad.

Con respecto a los componentes SuperStack 3000 en el esquema intraedificios, son dispositivos apilables, lo que permite un amplio rango de crecimiento en el numero de servicios (cada uno de los SuperStack 3000 tiene un uplink ATM lo cuál asegura tener un enlace hacia el backbone por cada dispositivo, ya sea para redundancia o para balanceo de cargas).

Al mismo tiempo, estos dispositivos son autosensibles (Ethernet 10/100) obteniéndose un rango de escalabilidad según sean las necesidades de los usuarios. Por el lado de la conexión hacia el backbone, soportan enlaces uplinks a tecnologías como Fast Ethernet (half/full dúplex), ATM (OC-3, OC-12) y Gagabit Ethernet lo que aunado con las características observadas por el CoreBuilder 7000HD, permite una escalabilidad del backbone sin la necesidad de un cambio drástico en los equipos.

Actualmente DGSCA ha implantado la solución ATM en el backbone de RedUNAM propuesta por 3com, consecuentemente esta compañía permitirá una interoperabilidad completa entre RedUNAM y la REDII.

En cuanto a las tareas de administración, el Transend es una aplicación basada en estándares y aplicaciones abiertas por lo que puede trabajar sobre la plataforma de administración SunNet Manager. Este, permite la configuración remota de los equipos, administración y configuración de las redes virtuales (ATM LANE y Fast Ethernet), configuración de funciones de seguridad, salida de reportes de operación, etc.

Con relación al desempeño, los productos 3com han obtenido resultados sobresalientes en múltiples pruebas (benchmarks) de empresas independientes, mostrando de esta manera que los dispositivos de 3com tienen un alto grado de eficacia.

NOTA: Para obtener mayor información de las pruebas realizadas consultar las siguientes direcciones web.

The switched 10 Mbps - 100 Mbps Evaluation Report;
Strategic Networks; actualizado en mayo de 1997;
http://www.snci.com/reports/10_100_Phase3/q23-1_c.htm.

Forget the Forkflit (We rack and stack ATM switches and find LAN emulation really works);
Data Communications Lab Test; septiembre de 1996;
http://www.data.com.

Comparing LAN switch contenders: Beyond Performance;
NetworkWorld; enero de 1996.
http://www.networkworld.com.

Ethernet Switches: Quantity, not commodity;
Data Communications Lab Test; noviembre de 1996.
http://www.data.com

El CoreBuilder 7000HD al soportar módulos de tecnologías ATM, Fast Ethernet y Gigabit Ethernet, proporciona una amplia flexibilidad y libertad de realizar diferentes esquemas de configuración de tecnologías sobre el backbone (debido a que la translación entre tecnologías se lleva a cabo en el mismo dispositivo, se garantiza la menor degradación en el desempeño) tomando en cuenta las

necesidades futuras de la red de las áreas del Instituto. Al mismo tiempo al ser una solución conmutada, permite realizar en mayor grado la segmentación al nivel de los usuarios finales ya sea en 10Mbps o 100Mbps dedicados. De esta forma la solución de 3com ofrece una alta flexibilidad en la arquitectura.

Los componentes de 3com, ofrecen una plataforma muy madura que tiene varios años en el mercado, teniendo así un nivel de perfeccionamiento en sus arquitecturas, y al mismo tiempo muy confiables. De igual manera, 3com cumple con las jerarquías en los niveles de disponibilidad en las diferente áreas de la red.

De igual manera, 3com cumple con las diferentes necesidades de disponibilidad dependiendo del nivel de jerarquía de las áreas de la red. En el backbone, el CoreBuilder 7000HD es un chasis de alta disponibilidad que se conforma completamente de componentes que cumplen con la característica intercambio rápido (hot swap), el mecanismo de conmutación redundante (switch engine), fuentes de poder redundantes con balanceo de carga. Por otro lado, los dispositivos SuperStack 3000 en el interior de los edificios ofrecen fuentes de poder redundante.

Conforme se desarrollo esta ultima etapa del proyecto, se observo que la compañía 3com fue la que brindo mayor interés y apoyo a nuestras necesidades así mismo el nivel de capacitación de su personal reflejo un buen grado de conocimientos en el área, todo esto indica que 3com mantiene un buen nivel de servicio al cliente.

Finalmente, tomando en cuenta todas las características técnicas de alto nivel mencionadas anteriormente, se puede observar que 3com ofrece una solución que mantiene un alto grado de protección a la inversión a un costo aceptable.

NOTA: un factor determinante para la selección de este proveedor, fue la existencia de negociaciones que se llevaron acabo entre la DGSCA y 3com, y que se hace extensivo a todas las dependencias de la UNAM. Estos acuerdos incluyen garantía de 5 años en todos los equipos, descuentos mayores del 40%, contratos de mantenimiento global, cursos de capacitación, planes de sustitución de equipos de otras marcas por equipos 3com, etc.

Selección:

Backbone principal y la conexión hacia RedUNAM: Tecnología ATM.
Conexión intraedificios: Tecnología Fast Ethernet.
Proveedor: 3com.

CAPÍTULO 9
SOLUCIÓN POR ETAPAS PARA LA REDII

9.1 Introducción

La red de cómputo del Instituto de Ingeniería (REDII) ha tomado un papel muy importante al ser la columna vertebral de los sistemas de información y una herramienta de soporte para el desarrollo de las funciones dentro del Instituto como son la gestión de bases de datos, soporte a aplicaciones de misión crítica, acceso de información, compartición de archivos y periféricos entre otros servicios.

Hoy en día la red del Instituto debe experimentar cambios significativos debido a los requerimientos de los usuarios y las aplicaciones orientadas a la investigación científica y la ingeniería, además de los propios de administración. Asimismo debe poder adaptarse a nuevas aplicaciones y a los continuos progresos de la tecnología de las comunicaciones requeridas para un mejor desempeño en las tareas del Instituto. Es por esto, que la REDII está obligada a reestructurarse continuamente para estar preparada para estos cambios y poder servir de una mejor manera al personal del Instituto de Ingeniería cuando sea necesario.

9.2 Solución por etapas

Con la definición de los secciones en que se puede dividir la red del Instituto, se ha conseguido la flexibilidad adecuada para poder absorber modificaciones sin realizar cambios abruptos o un rediseño total de la red, minimizando al mismo tiempo los riesgos a fallas e interrupciones en la red completa.

Por otro lado la definición de una solución por etapas, creará los principales puntos de estabilidad en la red a través de los cuales las siguientes modificaciones se integraran dentro de la base del sistema ya instalado, dando como resultado un cambio transparente y casi sin interrupciones para los usuarios y el beneficio de una mayor protección a la inversión y justificando de una mejor manera la inversión para cada una de estas etapas, ya que cada una ellas, esta confinada a modificar algún o algunos módulos donde y cuando sea necesario.

Asimismo, la solución por etapas proporcionará una ruta de migración controlable hacia nuestro objetivo, creando al mismo tiempo una estrategia para el futuro, es decir, será el fundamento para una transición manejable, que adapta la tecnología actual al principio de las etapas e irá progresando a través de una transición gradual hacia las tecnologías mas avanzadas.

9.2.1 Etapa 1: Nuevo esquema para el backbone de la REDII

Esta primera etapa se dividió en dos partes, la primera que da solución al esquema de cableado y una segunda que es la implantación de la tecnología Ethernet conmutado en el backbone.

9.2.1.1 Etapa 1.A: Sistema de cableado para el backbone

El llevar a cabo una red de altas especificaciones, debe partir del desarrollo e implantación de un sistema de cableado que permita llevar a cabo una transición hacia una red de estas características, ya que de éste dependerá gran parte el funcionamiento de nuestra red.

Es por esto, que una vez llevado a cabo un estudio tanto de las instalaciones del Instituto, de la tecnología Ethernet conmutado a la que se planea migrar en ésta etapa y previendo la flexibilidad necesaria para futuras modificaciones, se llego a la conclusión de instalar la fibra óptica siguiendo el esquema que se muestra a continuación, sustituyéndose el cable coaxial existente.

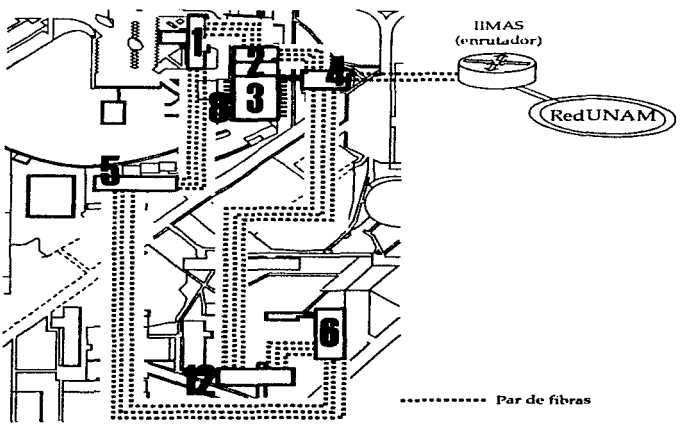


Figura 9.1 Tendido de la fibra óptica en la red del Instituto de Ingeniería

Como se puede observar en la figura 9.2 el esquema de cableado tiene un aspecto de anillo a través de tres pares de fibras ópticas multimodo entre la conexión de los edificios (nodos) que conforman el backbone.

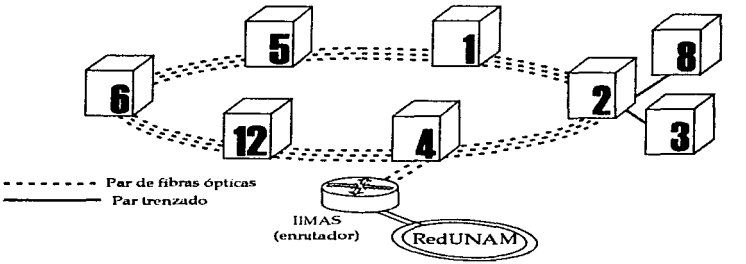


Figura 9.2 Tendido en forma de anillo de los 3 pares de fibras ópticas

Este esquema se puede configurar en una topología de estrella o anillo (figura 9.3), proporcionando la flexibilidad suficiente para poder adecuarse a futuras adaptaciones hacia otras tecnologías de alta velocidad.

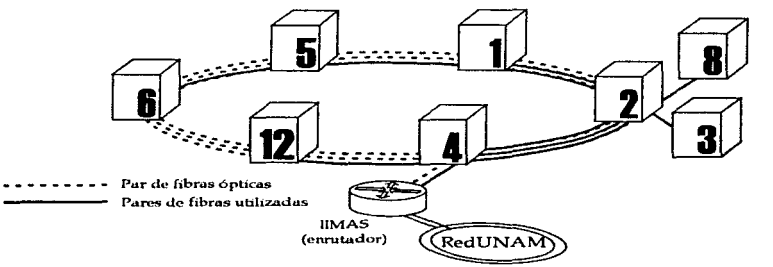


Figura 9.3 Configuración en estrella para la REDII

Por otro lado, los 3 pares tendidos entre edificios, proporcionan un sistema de redundancia básica al tener por lo menos una ruta alterna para la conexión de algún edificio en caso de que fallará su conexión original. Además, en el caso de configurar una topología en estrella se tiene la suficiente capacidad para poder ubicar el dispositivo central en cualquiera de los edificios que componen el backbone.

Con respecto, a la conexión hacia RedUNAM solamente se tendieron dos pares de fibras, de las cuales, una permanece como redundante o como medida de flexibilidad para una futura modificación.

Por ultimo, se debe hacer notar que no fue necesario modificar el esquema de cableado del interior de los edificios, ya que estos cumplen con la norma de cableado estructurado (EIA-TIA 568)[234], soportando así la compatibilidad hacia tecnologías de alta velocidad realizando solo pequeñas reconfiguraciones en las conexiones de los cables.

9.2.1.2 Etapa 1.B: Implantación de la tecnología Ethernet conmutado

Para llevar a cabo la ultima fase de esta etapa, la tecnología en que se basará el backbone de la REDII será a partir de Ethernet conmutado como se resolvió en la evaluación del capítulo anterior.

Con el propósito de realizar una mejor explicación de esta solución y sus beneficios, esta fase se dividió en tres partes principales: topología, dispositivo central de conmutación y delimitación de los segmentos.

9.2.1.2.1 Topología

La tecnología Ethernet conmutado, especifica una topología en estrella en nuestra configuración del cableado, por lo que se llevaron a cabo los empalmes y las conexiones necesarias, quedando de la manera que se demuestra en la figura 9.4.

Con esta configuración de topología se permitirá realizar de una manera mas simple y rápida la localización y corrección de fallas[235] y por otro lado, tener un mayor grado de disponibilidad y una red mas confiable.

---

[234] Para mayor referencia ver el capítulo 2 en el apartado de "Estándar de cableado estructurado EIA/TIA 568".

[235] Una de las mejores ventajas que se tiene con esta topología, es que un fallo en un nodo o segmento, o la ruptura de un cable de un segmento no incapacita el resto de la red, asimismo permite que la localización de fallas se realice de manera relativamente simple.

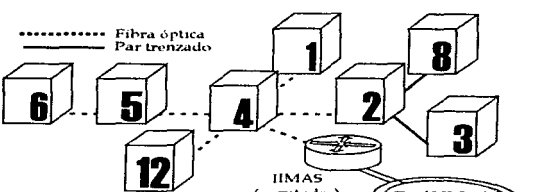


Figura 9.4 Configuración física de la fibra óptica en una topología en estrella implantada en la red del Instituto de Ingeniería.

9.2.1.2.2 Dispositivo central de conmutación

Este dispositivo junto con el esquema de cableado, tienen una importancia crítica dentro de la red, debido a que es el centro de la estrella y por tanto desempeñará las funciones de conmutación de la red.

La conmutación como se explico en el capitulo 4, permitirá un mejor control del trafico, al limitarlo solamente a los segmentos apropiados de destino sin alterar el ancho de banda de otros dominios. De esta manera, se tiene un incremento en el desempeño de la red ya que proporciona un mejor aprovechamiento del ancho de banda en los segmentos y por tanto de la red total.

Por su importancia y dado el análisis que se llevo a cabo en el capitulo anterior, el dispositivo central que realizará las funciones de conmutación entre segmentos, es un chasis marca Cabletron MMAC-5FBN con modulo de conmutación Ethernet ESXMIM-F2 y fuentes redundantes de energía. Además, proporciona un completo esquema de administración y monitoreo basado en los protocolos SNMP e CMIP, al mismo tiempo soporta enlaces (uplinks) hacia tecnologías como FDDI y ATM.[236]

Este dispositivo se ubicará en un cubículo del edificio 4 debido a que es el punto mas cercano hacia el nodo de RedUNAM designado por DGSCA (IIMAS) para el Instituto, teniendo asimismo la existencia de tubería para el cableado y ciertas estructuras que facilitaban la realización adecuada de este enlace. Por otro lado, el cubículo satisfacía los requerimientos de las dimensiones del equipo y las necesidades del grupo de administración.

[236] Se recomienda tener un segundo equipo de manera redundante en el nodo central, lo que incrementaría considerablemente la confiabilidad y disponibilidad del sistema.

9.2.1.2.3 Segmentación

La tecnología Ethernet conmutada proporciona una reestructuración a través de la delimitación de segmentos por dominios de colisión. En el caso particular del Instituto, se trato de llegar a tener un esquema de organización de segmentos adecuado a las necesidades de crecimiento de usuarios y sus aplicaciones, pero que al mismo tiempo ofreciera las facilidades de administración y monitoreo requeridas.

De esta manera, la segmentación se realizó de la manera mas balanceadamente posible, tomando en cuenta las cargas de tráfico, el número de usuarios actualmente conectados, la distribución geográfica del Instituto y una estimación tanto del crecimiento de usuarios como del trafico por edificio. La distribución de segmentos a la que se llego se muestra en la siguiente tabla.

Nombre del segmento	Edificios comprendidos
segmento 1	1
segmento 2	2, 3, 8
segmento 4	4
segmento 5	5, 6
segmento 12	12

Tabla 9.1 Definición de los segmentos de la red del Instituto de Ingeniería

Como se muestra en la tabla anterior, la mayoría de los segmentos comprende un solo edificio, excepto en los segmentos 2 y 5 debido a que los edificios 3, 6 y 8 tienen un número muy reducido de usuarios, y se espera que a futuro sus necesidades no sean muy crecientes por lo cual no sería justificable económicamente el gasto de un puerto extra en el conmutador y el cableado punto a punto que estos requerirían.

Una vez realizada esta segmentación, se ha reducido tanto el numero de usuarios por segmento como el numero de colisiones. Del mismo modo, el aumento de un usuario o dispositivo no repercutirá en la red total, tan solo en su segmento. Teniéndose como resultado un esquema de organización por segmentos sencillo pero eficiente para su administración, control y monitoreo.

A continuación se muestra el esquema final de la REDII, al final de la etapa 1.

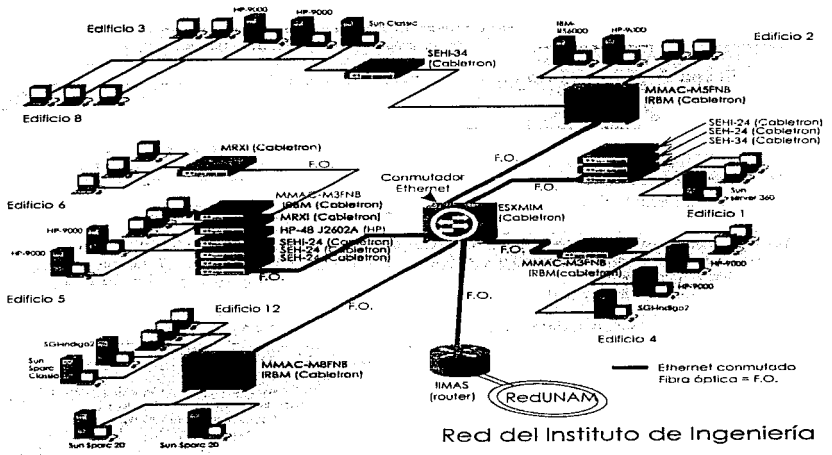


Figura 9.5 Esquema final de la etapa 1

9.2.1.2.4 Conclusiones de la etapa 1

Como conclusión a esta etapa, se puede decir que se ha obtenido un backbone con un mejor nivel disponibilidad y un incremento substancial en el desempeño de la red, debido a su topología y su esquema conmutado, pero por otro lado con la suficiente flexibilidad para mantener las opciones abiertas hacia el futuro. Todo esto se realizo sin la necesidad de requerir cambios significativos en la tecnología e infraestructura actual, satisfaciendo así la protección de la inversión.

9.2.2 Etapa 2: Incremento en el desempeño del grupo de servidores de la REDII

Como se explico en el capitulo anterior, se debe proporcionar un mayor ancho de banda al grupo de servidores principales para poder aprovechar de mejor manera las características de alto rendimiento y desempeño que estos ofrecen. Mejorando así el tiempo de respuesta de los servidores y las aplicaciones hacia los usuarios, además de poder realizar un mayor número de conexiones de manera simultánea. Teniéndose como resultado un desempeño óptimo y mayor eficiencia en la red.

De acuerdo al análisis efectuado, se resolvió poner un enlace de FDDI, desde el conmutador ethernet del edificio 4 hacia el edificio 12, además, el enlace que tienen los servidores principales se hace a través de CDDI, permitiéndoles tener un ancho de banda de 100Mbps en la conexión hacia estos.

Cabe hacer mención que para obtener el máximo rendimiento que puede ofrecer la tecnología FDDI en la configuración hacia los servidores, se aconseja tener un esquema balanceado de cargas entre los servidores del grupo.[237]

NOTA: La función del balanceo de cargas entre los servidores, tiene que llevarse a cabo por el grupo de administradores de estos equipos. Además, esta función tiene que ser llevada a cabo frecuentemente y de manera constante para que se pueda mantener en buen nivel el desempeño de los servidores.

Por otro lado, FDDI adicionalmente ofrece las ventajas de no degradar significativamente su desempeño al incrementar el numero de servidores conectados a su anillo lo que provee una gran escalabilidad a futuro. Así mismo con su esquema Dual homing Mac ring, proporciona un esquema tolerante a fallas lo suficientemente robusto para una excelente recuperación a estos lo cual mejora la confiabilidad y eficiencia necesaria para proporcionar un buen servicio.

A continuación se muestra el esquema final de la red del Instituto de Ingeniería una vez terminada la etapa 2.

---

[237] La función del balanceo de cargas entre los servidores, tiene que llevarse a cabo por el grupo de administradores de estos equipos. Además, esta función tiene que ser llevada a cabo frecuentemente y de manera constante para que se pueda mantener en buen nivel el desempeño de los servidores.

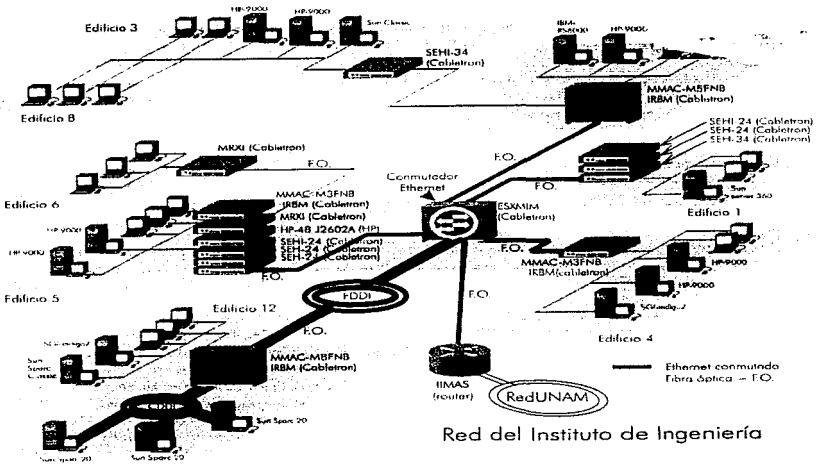


Figura 9.6 Esquema final de la etapa 2

9.2.2.1 Conclusiones de la etapa 2

Como conclusión a esta etapa, se puede decir que se ha obtenido una conexión de alta velocidad hacia los servidores principales del Instituto de Ingeniería con el máximo nivel de disponibilidad y eficiencia, lo cual traerá un mejor desempeño en el acceso a los servidores.

9.2.3 Etapa 3: Base para la red de altas especificaciones del Instituto de Ingeniería

En esta tercera etapa se establecen las bases de la estrategia en que se fundamentará la red de altas especificaciones del Instituto de Ingeniería. El desarrollo de esta etapa es de suma importancia ya que de ésta dependerá el éxito del desempeño de la red del Instituto de Ingeniería a futuro.

Como se explico en el capitulo anterior, esta etapa se enfocó en la modificación y actualización tecnológica de los módulos del backbone, la conexión hacia RedUNAM y finalmente al esquema de conexión de los usuarios en el interior de los edificios.

Asimismo, se establecieron las bases para la siguiente etapa (ya no comprendida en este trabajo) que tendrá como objetivo la integración de los servidores principales al backbone de la red.

Con el propósito de llevar a cabo una mejor explicación de la solución de esta etapa, se procedió ha dividirla en cuatro partes, la primera, comprende la configuración y ubicación de los dispositivos principales que conformarán la red para esta etapa. La segunda sección, explica la solución ATM en el backbone y conexión a RedUNAM, así como los ventajas que se obtuvieron en esta sección. La tercera sección, describe la conexión en el interior de los edificios por medio del esquema basado en Ethernet a 10/100 Mbps. Y por ultimo, en la cuarta sección, se explican las características de administración y seguridad que se obtienen con la infraestructura que se implantará en esta etapa.

9.2.3.1 Configuración y distribución física de los equipos

Una vez realizadas las selecciones tanto de tecnologías como de proveedor en el capitulo anterior, se procedió a realizar las adecuaciones pertinentes de la propuesta original del proveedor ya que esta incluía un mayor número de dispositivos y puertos de los requeridos, asimismo la ubicación y reutilización de los equipos no era la adecuada.

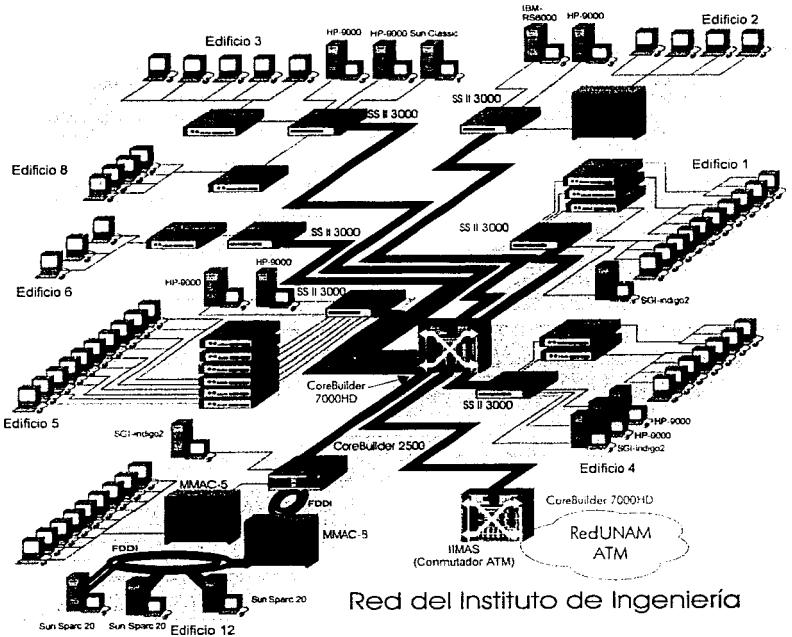


Figura 9.7 Esquema original de la propuesta de 3COM

En la configuración final de los equipos, se llevó a cabo la eliminación de algunos dispositivos que proponía 3com en su propuesta original, además de realizar una reubicación y reutilización de algunos dispositivos no contemplados en esta misma.

En primer lugar, se llevo a cabo la reubicación del conmutador central del backbone ATM (CoreBuilder 7000HD) hacia el edificio 12, donde se obtendrá un mayor control de seguridad, monitoreo, administración y tiempo de respuesta del personal de administración de la red a cualquier fallo que pudiera ocurrir en este dispositivo.

De esta manera, se establecerán las bases para la siguiente etapa, donde se planea emigrar los servidores principales a una tecnología de mayor ancho de banda (ATM OC-3 u OC-12 o Gigabit Ethernet, las cuales son soportadas por este dispositivo), teniéndose como beneficios adicionales, la integración de los servidores principales al backbone mismo y el ahorro del costo en el cableado.

Se reutilizará el dispositivo MMAC-5 (que se ubica en el edificio 4) al edificio 12, intercambiando al mismo tiempo todos los servicios Ethernet del edificio 12 a éste dispositivo. De esta manera se reducirá la carga en el MMAC-8 mejorando así el desempeño de la conexión FDDI hacia los servidores principales.

Para la conexión de los servidores principales (en FDDI) al backbone ATM, se instalo un conmutador/enrutador CoreBuilder 2500 configurado con dos enlaces uplink, uno ATM y otro FDDI a través de los cuales se llevará a cabo la integración.

Por ultimo, se ubicará un conmutador apilable SuperStack II 3000 (puertos Ethernet auto sensibles 10/100) en los edificios 1, 2, 4 y 5. Configurados con un enlace uplink ATM para la conexión hacia el backbone.

Se eliminaron los conmutadores SS II 3000 de los edificios 3 y 6, ya que como se mencionó con anterioridad tienen un numero reducido de usuarios y se espera que su crecimiento a futuro no sea muy grande, por lo cual no es justificable económicamente el gasto de un dispositivo individual para cada uno de estos edificios.

De esta manera se ha llegado a la configuración óptima mas acorde a los requerimientos de la red del Instituto, permitiendo además una escalabilidad ordenada a través de los productos apilables o modulares que absorberán la tasa de crecimiento del Instituto.

A continuación se muestra el diagrama de la configuración final de los dispositivos para la REDII.

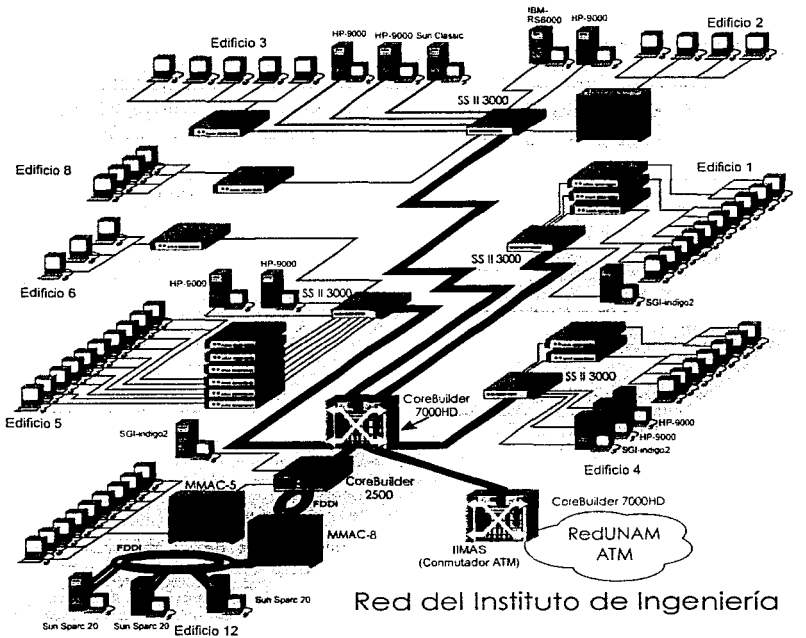


Figura 9.8 Esquema y configuración final de la ubicación de los dispositivos

Equipo	Descripción	Cant.	Ubicación
CoreBuilder 7000HD	Dispositivo central para el backbone ATM, con un módulo de 8 puertos OC-3 para fibra óptica	1	Edif. 12
CoreBuilder 2500	Dispositivo conmutador/enrutador, 1 módulo de 8 puertos. Ethernet 10Mbps dedicados 1 puerto. uplink ATM 1 puerto uplink FDDI	1	Edif. 12
Super Stack II 3000	Dispositivo conmutador Ethernet 10/100 1 puerto uplink ATM	4	Edificios 1, 2, 4, 5

Tabla 9.2 Equipos utilizados para el esquema de alta velocidad de la REDII.

9.2.3.2 Solución ATM en el backbone y conexión a RedUNAM

El backbone y la conexión hacia RedUNAM de la red del Instituto de Ingeniería se configurarán con una tecnología ATM a 155Mbps en modo full dúplex sobre una topología en estrella, a través de un dispositivo central modular CoreBuilder 7000HD.

En primer lugar con la implantación de este esquema de ATM se proporcionará un amplio margen de ancho de banda con buen desempeño y manejo de éste, el cuál garantizará el poder soportar la creciente carga de trafico ofreciendo un servicio adecuado tanto para aplicaciones de uso intensivo de ancho de banda como para las que requieran Calidad de Servicio (multimedia y video conferencias), de igual manera, se verán beneficiadas las aplicaciones heredadas no orientadas a conexión.

Asimismo esta solución será capaz de satisfacer las necesidades de disponibilidad del backbone, ya que el CoreBuilder 7000HD es un dispositivo de alta disponibilidad tolerante a fallas, conformado por partes de intercambio rápido (hot swap) y fuentes de poder redundantes. Por otro lado, ATM, al permitir el soporte de topología en malla, dará la libertad de poder realizar enlaces redundantes activos (con balanceo de cargas) entre dispositivos. Con esta última característica se obtendrá una mayor disponibilidad y al mismo tiempo se mejorará el desempeño entre los dispositivos con múltiples enlaces.

Por otro lado, el backbone que se implantará será capaz de adecuarse a los requerimientos del Instituto cuando y dónde sea necesario. Esto es debido a que ATM permite realizar múltiples enlaces entre dispositivos y al mismo tiempo no define un límite respecto al numero de equipos conectados al backbone. Por otro lado, el CoreBuilder 7000HD soporta módulos de tecnologías Ethernet, Fast Ethernet y Gigabit Ethernet, además de proporcionar una escalabilidad de ATM de hasta 622 Mbps. Con todas las anteriores características se garantiza que el backbone a implantar sea altamente flexible y escalable.

El CoreBuilder 7000HD proveerá todas las funciones de servicio de la Emulación LAN ATM (LES,BUS y LECS), sin la necesidad de otro dispositivo o servidor externo. Por otro lado, los conmutadores SS II 3000 llevarán a cabo la función de dispositivos LEC y proxy, y el Corebuilder 2500 (función de enrutador) realizará las operaciones de intercomunicación entre redes virtuales (LANEs) Con todo esto, se garantiza tener el esquema completo para la implantación y buen funcionamiento de redes Emuladas LAN ATM (LANEs), permitiéndonos de esta manera seguir soportando los protocolos de comunicación utilizados en el Instituto, como son: TCP/IP, NetBEUI e IPX/SPX, consecuentemente se podrá seguir utilizando las aplicaciones heredadas sin la necesidad de realizar modificaciones adicionales.

Un factor que cabe la pena mencionar, es que una vez seleccionada la misma tecnología tanto en el backbone de la REDII (ATM) y el backbone de RedUNAM (ATM), aunado a que cada uno de ellos se interconectan a través de dispositivos CoreBuilder 7000HD de 3Com, se obtendrá el mayor nivel de interoperabilidad y eficiencia entre estas dos redes, lo que traerá el máximo aprovechamiento de las ventajas y servicios que ofrezca RedUNAM e Internet.

9.2.3.3 Solución Ethernet 10/100 en la conexión en el interior de los edificios

El esquema de conexión en el interior de los edificios, se basará en la tecnología Ethernet 10/100 a través de conmutadores Super Stack II 3000 de puertos autosensibles. De esta manera, se establecen las bases para la estrategia de microsegmentación deseado para los usuarios, además de proporcionar un margen de escalabilidad de ancho de banda de 100Mbps para estos mismos. Sin embargo, hay que tener en cuenta que la microsegmentación o la migración a 100Mbps se llevarán a cabo en posteriores etapas de acuerdo a las necesidades y limitaciones de cada usuario.

Es por esto, que el primer paso, será agregar un segmento conmutado Ethernet/Fast Ethernet (puerto de conmutador SS II 3000), así la red original podrá ser segmentada en un mayor grado y proveer a cada concentrador de la pila de concentradores un segmento dedicado de 10Mbps, y reducir de esta forma el numero de usuarios en la contención por el ancho de banda por segmento, teniendo además un mejor desempeño para los usuarios.

Cabe señalar que de esta manera se garantiza una ruta de migración gradual de los usuarios y se amplia el tiempo de vida de la infraestructura existente.

9.2.3.4 Solución del esquemas de administración y seguridad

Se debe tener en cuenta que al implantar en el backbone una tecnología orientada a la conexión y utilizar en toda la red dispositivos que permiten el filtrado de trafico, se obtendrán mayores niveles de seguridad en la red, teniéndose de esta manera, una red mas confiable para la transmisión de información.

Por otro lado, con las herramientas SunNet Manager, LANview y Transend (módulo para el SunNet Manager), se obtendrá un sistema de administración y monitoreo mas robusto, eficaz y sencillo. Con esto, se eficientará el desempeño y confiabilidad de la red completa, además de facilitar las tareas del personal encargado.

Finalmente, al establecer una estrategia de arquitectura de conmutación en la REDII, se establecerán las bases para el manejo de redes virtuales (VLANs), lo cual permitirá tener una estructura mas flexible con una perspectiva de organización lógica de los componentes de la red (sin límites de su ubicación física). Al mismo tiempo, se mejorará el desempeño de la red, se facilitarán las tareas de administración y por ultimo, se aumentarán los niveles de seguridad.

9.3 Conclusiones

Con esta etapa, se obtendrá un backbone y conexión a la RedUNAM de alta velocidad. En la conexión interna de los edificios se tendrán las bases para la microsegmentación deseada y una tecnología de 10/100 Mbps que proporciona una ruta de escalabilidad gradual para los usuarios. De esta manera se puede decir que se ha obtenido una arquitectura de red con un amplio grado de flexibilidad y escalabilidad, además de obtener una red con un alto nivel de disponibilidad, confiabilidad y desempeño.

Una vez que se implante esta ultima etapa, se podrá soportar todo tipo de aplicaciones como las de consumo intensivo de ancho de banda y las sensibles al tiempo, además de ciertos servicios especiales como son: videoconferencias, reproducción de video, manejo de imágenes, páginas de Web (con un alto contenido de voz, datos y video, dándole manejo adecuado).

Por otro lado, el esquema a implantar, es completamente compatible con la RedUNAM, significando el mayor grado de interoperabilidad entre ésta y la REDII. De esta manera, se podrán aprovechar al máximo todos los recursos y servicios que proporcione el backbone de alta velocidad de RedUNAM y la DGSCA.

Asimismo, la arquitectura de red permitirá crear una ruta de migración gradual que ofrecerá al Instituto adecuarse a las necesidades presentes y futuras con un cambio mínimo en los dispositivos que la conforman, ganando de esta manera en la escalabilidad, un amplio grado de protección a la inversión de la infraestructura actual. También por otro lado, se asegura la reducción de riesgos a fallas, e interrupciones en la red y los usuarios.

Por ultimo, cabe mencionar que ésta etapa es la culminación de una serie de facetas que han establecido la estrategia principal a través de la cual se asegura guiar a la REDII hacia una red de altas especificaciones, ya que principalmente en esta etapa se establecen las bases para que las tecnologías de la próxima generación sean integradas dentro del esquema de los sistemas ya instalados.

CONCLUSIONES

La red de cómputo del Instituto de Ingeniería ha tomado un papel muy importante al ser la columna vertebral de los sistemas de información y una herramienta de soporte para las funciones dentro del Instituto.

En este trabajo se engloban, los cambios significativos que ha experimentado la red del Instituto debido a los requerimientos de los usuarios y las aplicaciones orientadas a la investigación científica y de ingeniería, además de los propios de administración. Al mismo tiempo se incluye la planeación de la estrategia hacia el futuro, ya que la REDII está obligada a reestructurase continuamente para poder adaptarse a las nuevas aplicaciones y a los continuos progresos de las tecnologías de comunicación requeridas y de esta manera seguir proporcionando el mejor desempeño a las tareas del Instituto.

El presente trabajo tuvo como objetivo la planeación e implantación de las bases para la red de altas especificaciones del Instituto de Ingeniería, un proyecto tan ambicioso como este, no solo implicó el análisis, evaluación, selección e implantación de la arquitectura tecnológica de la red, sino que involucró otros factores relevantes como son la participación activa de los usuarios y del personal de administración, ya que son éstos los que harán evolucionar en gran medida la red del Instituto con sus nuevas necesidades.

En conclusión, se ha obtenido una arquitectura de red de alta velocidad, con un amplio grado de flexibilidad y escalabilidad, además de obtener una red con un alto nivel de disponibilidad, confianza y desempeño.

Asimismo se proporciona una ruta de migración gradual y transparente hacia la red de altas especificaciones que adecuará al Instituto a las necesidades futuras con un cambio mínimo en los dispositivos que la conforman, asegurando de esta manera la protección a la inversión en todo momento. También por otro lado, se asegura la reducción de riesgos a fallas y una mínima interrupción del servicio de red a los usuarios.

Además se ofrece a los usuarios el poder soportar todo tipo de aplicaciones como son las de uso intensivo de ancho de banda, las sensibles al tiempo y las que requieran calidad de servicio. Con estas características se podrán proporcionar servicios tales como, videoconferencias, educación a distancia, colaboración de aplicaciones de escritorio compartidas, correo de voz, reproducción de video, soporte adecuado a aplicaciones de procesamiento de imágenes y visualización (especificaciones por las que se caracterizan las aplicaciones de ingeniería que se manejan en el Instituto), etc.

Asimismo, se ha obtenido que el backbone y la conexión hacia RedUNAM sean completamente homogéneas con la RedUNAM lo cual proporcionará el mayor aprovechamiento de los recursos de ésta y los servicios que ofrezca DGSCA.

Por ultimo, se ha dejado la documentación completa que servirá de base para las futuras modificaciones, soporte y administración de la red misma.

BIBLIOGRAFÍA

Libros

Alfred Halshall; Data Communications, Computer Networks & Open Systems; Addison Wesley.

Andrew S. Tanenbaum; Computer Networks 3a. ed. ; Prentice Hall 1996.

Colin Smythe; Internetworking Designinig the right Architectures; Addison Wesley 1995.

Colin Smythe; Internetworking Designing the Right Architectures; Addison Wesley 1995.

David A. Stamper; Business Data Communications; The Benjamin Cummings 1991.

Davidson Muller; Internetworking LANs Operation, Design y Management; Artech House.

Douglas E. Commer; Redes globales de información con Internet y TCP/IP 3a. ed.; Prentice Hall 1996.

Drew Heywood; LAN connectivity (Enterprise Series); NRP New Riders Publishing.

Gary Dickson, Alan Lloyd; Open Sytems Interconnection, Computer communication standars and gosip explained; Prentice Hall 1992.

Karanjit Siyan; Netware the professional reference 3a. ed. ; NRP New Riders Publishing.

Kornel Terplan, Shaku Abre; Effective Mangement of local Area Networks; McGraw Hill 1992.

Michael Santifaller; TCP/IP and NFS (Internetworking in Unix enviroment); Addison Wesley 1991.

Mischa Schwartz; Redes de telecomunicaciones (protocolo, modelado y análisis); Addison Wesley.

R. J. Cypser; Communications for Operating Systems OSI, SNA and TCP/IP.
Stan Schatt; Linking LANs; McGraw Hill 1995.

Stephen Saunders; High-Speed LANs Handbook (Data Communications magazine); McGraw Hill 1996.

Terè Parnell; LAN TIMES Guide to building high-speed networks; McGraw Hill 1996.

Tom Sheldon; Guía de interoperabilidad (soluciones para la interconectividad en la red); Mcgraw Hill 1994.

Uyless Black; Computer Networks Protocols, Standars & Interfaces; Prentice Hall

Uyless Black; OSI a Model for Computer Communications Standars; Prentice Hall 1992.

William Stallings; ISDN & BISDN with Frame Relay and ATM 3a. ed.; Prentice Hall 1995.

William Stallings; Local & Metropolitan Area Networks 4a ed.; MACMILLAN 1993.

William Stallings; Data & Computer Communications 2a. ed.; Addison Wesley

Revistas

Terè Parnell; Shopping for a High-Speed Vehicle (comparison); LAN TIMES; vol. 12, número 11; 5 junio 1995; pp 81-96.

Russ Sharer; A Switch in time; LAN, The network solution magazine; vol. 10 número 5; mayo 1995; pp 109.

Mejía Olvera Marcelo y Flores Ramiro Alejandra; Tecnologías de Área Amplia para la comunicación de Datos (una descripción comparativa de la oferta actual en México; Soluciones Avanzadas; Año 5 número 40; diciembre 96; p 24.

Tesis

Morchio Secul Javier E. ; Metodología de preparación, presentación y evaluación de proyectos de equipamiento computacional, tesis de licenciatura, Universidad Católica de Chile 1987.

Martínez P. Rosa Alva , Mendoza Fernando; Facilidades de computo distribuido en el Instituto de Ingeniería: implementación y desarrollo de mecanismos de información, procesamiento y administración; tesis de licenciatura, Facultad de Ingeniería, UNAM 1995.

Direcciones Web

Proveedores:

3Com Corporation;
http://www.3com.com

Anixter Inc.;
http://www.anixter.com

Bay Networks Inc.;
http://www.baynetworks.com

Cabletron Systems Inc.;
http://www.cabletron.com

Cisco Systems Inc.;
http://www.cisco.com

IBM Corporation;
http://www.ibm.com

Hewlett-Packard Company;
http://www.hp.com

Network Peripherals Inc.;
http://www.npix.com

Xylan Corporation;
http://www.xylan.com

Organizaciones y Forums:

Forum ATM;
http://www.atmforum.com

InterOperability Lab at the University of New Hampshire;[238]
http://www.iol.unh.edu/training/index.html

[238] Contiene también ligas hacia otras paginas especializadas de las tecnologías, como son Forums, organizaciones e independientes.

Independientes:

Zahir Ebrahim; "A Brief Tutorial on ATM";
http://juggler.lanl.gov/lanp/atm.tutorial.html

Anthony Alles; "ATM Internetworking";
http://cell-relay.indiana.edu/cell-relay/docs/cisco.html

Charles Spurgeon; Fast Ethernet (100Base-TX,FX,T4) Reference Guide. By;
http://wwwhost.ots.utexas.edu/ethernet/descript-100quickref.html

Revistas:

LAN Times Magazine
http://www.lantime.com

Network Computing Magazine
http://techweb.cmp.com/nc/docs

Network Magazine
http://www.network-mag.com/

Anexo A. Comentarios finales

Modelo OSI como referencia para el desarrollo de redes de comunicaciones

Entre los aspectos importantes que cabe la pena resaltar, y que con frecuencia es un punto de conflicto para los diseñadores o administradores de redes, es la selección del esquema de organización a seguir para resolver proyectos de redes de comunicación. En la presente tesis se siguio el esquema planteado por el **Modelo OSI**, el cuál es un esquema bien estructurado que delimita bastante bien las diferentes funciones que debe tener una red de comunicaciones, ya que abarca al mismo tiempo desde las aplicaciones de los usuarios finales (capas superiores) hasta los métodos de comunicación entre los diferentes dispositivos electrónicos (capas inferiores). Estas características lo hacen la guia ideal para servir como modelo de referencia para el estudio e implantación de redes de computadoras, obteniéndose un punto de vista mas claro, estructurado y sencillo de como preparar, delimitar y desarrollar proyectos de redes de comunicaciones.

Una vez adoptado el Modelo OSI como referencia, se puede delimitar hasta que nivel es necesario abarcar en este proyecto para tener un resultado que cubriera las necesidades y expectativas de la red del Instituto de Ingeniería.

Por otro lado, se debe tener en cuenta que para realizar la implantación real de la red de datos del Instituto, se utilizaron principalmente dos sistemas o modelos, que de manera conjunta en buena medida cumplen con lo que establece el Modelo OSI. El primero, es el conjunto de protocolos **TCP/IP**, que abarca tanto las aplicaciones de usuarios como la comunicación lógica entre dispositivos. El segundo, es el conjunto de protocolos desarrollados por la **IEEE**, conocidos como los **estándares 800.X** (entre otros, que tan bien cumplen con los mismos objetivos que tienen los estándares de la IEEE); estas especificaciones de la IEEE definen la comunicación entre los dispositivos de redes, a un nivel mas bajo que los protocolos TCP/IP, es decir, en las capas inferiores.

Porqué seguir con el conjunto de protocolos TCP/IP

En el presente trabajo (capítulo 4) se habló de la importancia que tiene el escoger un sistema de comunicación abierto, es decir, que el esquema de comunicación fuera estándar, robusto, y sobre todo que estuviera soportado ampliamente por los fabricantes. Existían dos opciones a utilizar en la red del Instituto, la primera, era el

modelo de comunicación establecido por ISO (referido como el Modelo de Referencia OSI) y utilizar los protocolos que propone; ella segunda, era seguir trabajando con el conjunto de protocolos TCP/IP que actualmente se maneja en el Instituto.

Finalmente se decidió seguir trabajando con el conjunto TCP/IP ya que por una parte, la mayoría de las tecnologías de red actuales soportan ampliamente estos protocolos; también las aplicaciones de alto nivel utilizadas por los usuarios se encuentran basadas en estos mismos protocolos, y además, se tiene una gran base instalada de ellos en todo el mundo (las aplicaciones usadas en la red mundial Internet están basadas en estos). Por último, un punto importante, es que éste conjunto de protocolos, mantiene una continua evolución, para la cuál, toma en cuenta varias ideas y estándares propuestos en el Modelo de referencia OSI. Por todo lo anterior, el conjunto de protocolos TCP/IP sigue siendo el principal sistema abierto de comunicación en todo el mundo.

Internet como fuente de información para proyectos

Un aspecto relevante en cualquier proyecto, sobre todo en los que utilizan conocimientos referente a temas sobre tecnologías de computación y redes de comunicación, es la falta de información teórica y técnica actualizada entre otros puntos importantes. Esto es debido a que la mayoría de los libros y manuales contiene en cierta medida información atrasada a la fecha de su venta; al mismo tiempo la mayoría de los temas que abarcan, son tratados desde un punto de vista teórico.

Por otro lado, las revistas tratan temas actualizados, donde la mayoría de las veces abarcan a los proveedores y sus equipos, además de exponer los puntos de vista de personas especializadas en el tema. Sin embargo, la información es tratada de manera muy superficial, por lo que aveces es muy difícil de entender si no se tienen las suficientes bases sobre el tema.

Es por esto, que un aspecto muy importante y que cabe la pena resaltar, es que este trabajo, fue documentado y se basó en gran medida por información obtenida en la red Internet. Esta red ofrece una gran fuente de información tanto actualizada como diversa, ya que se obtuvieron pruebas realizadas por compañías independientes acerca del desempeño de varias tecnologías, asimismo pruebas de servicio y desempeño entre proveedores y sus equipos respectivamente; de igual forma se obtuvieron las especificaciones de los equipos por proveedor sin la necesidad de esperar a este, que nos proporcionara dicha información, por otro lado, se pudo tener contacto y recibir varios puntos de vista y experiencias tanto de grupos independientes, como de personal especializado en el tema a través de todo el mundo; se obtuvo mucha información teórica y técnica de todas las tecnologías

de red y otros temas relacionados a través de grupos de discusión, grupos de independientes, universidades, etc.; por último un detalle muy valioso y que solo fue posible a través de la Internet, fue la consulta de los forums y grupos de especialistas dedicados al desarrollo de las tecnologías tratadas, obteniendo información de dichas tecnologías, el estado de sus estándares y su planes a futuro. Como se puede observar mucha de la información que se utilizó tanto para la documentación de la tesis, como para llevar a cabo una buena selección de las tecnologías y el proveedor a contratar, fue posible gracias al apoyo que se tuvo al estar conectados. Asimismo, la información que se obtuvo, fue de manera casi inmediata y ahorra mucho tiempo y esfuerzo.

Concluyendo, la Internet es una fuente de información diversa y actualizada para todo tipo de temas y proyectos, con el cuál se ahorran muchos recursos y se obtienen muchos beneficios.

Perspectiva general aportada por la presente tesis

El Instituto de Ingeniería al ser uno de los mayores centros de investigación en varias áreas de la Ingeniería y tener contacto con otras instituciones tanto nacionales como extranjeras, es un modelo tecnológico a seguir. Es por esto que con la culminación de este trabajo, el Instituto mantiene su liderazgo tecnológico, además de proporcionar una estrategia a seguir a otras instituciones dentro de la UNAM y del país.

Asimismo el Instituto contará con los medios mas eficaces y eficientes, para la realizacion de sus funciones tanto de investigación como de administración. Además de una herramienta adecuada tanto para la difusión y publicación de todos sus trabajos, así como también para el intercambio de información con otras universidades e institutos en México y en el mundo.

Con este trabajo se ha dejado un documento que pueda servir a estudiantes e Instituciones como una guía y apoyo acerca de como llevar a cabo proyectos de esta misma naturaleza, la adecuación de una metodología costo efectivo, además de la base teórica completa de ciertos temas que comprenden la realización de una red de datos.

Finalmente, este trabajo ha servido de formación para saber desde como se prepara, hasta como se desarrolla un proyecto de estas características. De igual manera, nos ha formado una buena base teórica y práctica ya que descubrimos qué puntos se deben de tomar en cuenta y cuidar para la implantación de una red de datos. Por otro lado, como establecer los tratos tanto con proveedores como con los usuarios y personal de administración, y finalmente formarnos un criterio acerca del campo de trabajo en el área de redes de comunicaciones.

Anexo B. Tipos de Multiplexaje

Las compañías de telecomunicaciones han desarrollado tecnologías muy elaboradas para multiplexaje de varias conversaciones mediante un solo canal físico. Es decir, un multiplexor es un dispositivo que acepta datos procedentes de un conjunto de líneas de entrada, con una secuencia estática y predeterminada; y genera salidas de datos en una sola línea de salida con la misma secuencia.

Las tecnologías de multiplexaje pueden dividirse dentro de dos tipos básicos: **Multiplexaje por División de Frecuencia** (FDM: frecuency división multiplexing) y **Multiplexaje por División de Tiempo** (TDM: time division multiplexing).

Multiplexaje por División de Frecuencia

En la división por multiplexaje de frecuencia, el espectro de frecuencia se divide entre los canales lógicos, donde cada uno de los usuarios posee una banda de frecuencia de manera exclusiva. Por otro lado, en Multiplexión por División de Tiempo, los usuarios toman un turno de tiempo de manera cíclica (predeterminada), durante el cuál, cada uno, obtiene todo el ancho de banda durante un período de tiempo designado.

Multiplexaje por División de Tiempo

Un Multiplexor por División de Tiempo (TDM: Time Division Multiplexer) divide el ancho de banda dentro de ranuras de tiempo fijo y designa una ranura a la vez para cada uno de los canales de alimentación de entrada dentro del multiplexor. De esta manera, si un canal necesita 64 Kbps de ancho de banda, esta cantidad de ancho de banda es asignada y permanece fija. Ningún otro canal puede usar el ancho de banda no utilizado. Esto significa que una larga porción de ancho de banda puede estar frecuentemente en un estado ocioso. Además de que si los requerimientos de tráfico de datos son necesarios para otros canales, no existe manera para designar mas ancho de banda a otros canales individuales que lo requirieran y de esta manera no se puede mejorar el tiempo de respuesta.

Debido a que cada ranura de tiempo en la salida está dedicada a una línea especifica de entrada, no es necesario transmitir los números de las líneas de entrada (dirección de la línea de entrada del cual proviene). La gran desventaja de TDM como ya se había dicho, es que cuando no existe tráfico en un línea de entrada, se desperdicia una ranura de tiempo de salida. Es decir, las ranuras de salida se van llenando de información bajo un ciclo de las líneas de entrada, si no existen datos a transmitir, se utilizan unos caracteres de relleno. No es posible saltar u suprimir una ranura de tiempo, debido a que el extremo receptor mantiene un seguimiento estricto sobre qué carácter proviene de que terminal, mediante una posición en el flujo de salida. Por lo que los datos por sí mismos no

llevan una identificación indicativa de su origen. Si el multiplexor llegara a omitir una ranura de tiempo, suponiendo que no hubiera datos por transmitir procedentes de la línea de entrada, el receptor quedaría fuera de fase e interpretaría el origen de los caracteres siguientes de manera incorrecta.

Si cada línea de entrada tuviera información por transmitir durante una pequeña fracción de tiempo, el proceso de TDM haría un uso muy poco eficiente de la capacidad de la línea de salida. Ya que se estará desperdiciando la mayoría de las ranuras de tiempo de la línea de salida (con datos de relleno). Un mejor planteamiento consiste en que sólo se transmitan los datos reales, y no datos de relleno, esta estrategia introduce, sin embargo, el problema de decirle al receptor de donde provino (de que línea de entrada). Una solución a este problema consiste en enviar dos caracteres de salida por cada carácter de entrada: uno indicando el número de línea de entrada y el otro, el dato. A los dispositivos que utilizan este principio se les conoce comúnmente como **multiplexores estadísticos** o ATMD (Multiplexor Asíncrono por División de Tiempo), en contraste con los anteriores **multiplexores síncronos** o STDM (Multiplexor Síncrono por División en el Tiempo).

Multiplexaje estadístico

La Multiplexaje Estadístico por División de Tiempo o simplemente **multiplexaje estadístico**, es un esquema de designación de ancho de banda que forma la base para la conmutación de paquetes, frames y celdas, también conocida como **conmutación de paquete rápido** (fast packet switching). Esta intenta resolver el problema de las ranuras sin utilizar que tiene STDM. Como en el multiplexaje de tiempo (STDM), el ancho de banda es compartido entre múltiples estaciones al dividir este dentro de ranuras de tiempo para ser designadas a estaciones individuales de manera estática. A diferencia del STDM, en ATMD la designación no es estática en el tiempo, es decir, las estaciones individuales no son "propietarias" de las ranuras de tiempo. Cuando una estación tiene datos a enviar y el canal esta vacío, la estación obtiene todo el ancho de banda. Si el canal no esta vacío, la estación debe encolar los datos hasta que el ancho de banda del canal se encuentre vacío de nuevo.

Por lo anterior, se puede decir, que se lleva a cabo el multiplexaje de manera estadística, donde varias conexiones se llevan a cabo sobre el mismo enlace basándose en las características del tráfico, es decir, este toma ventaja de la naturaleza estadística de ráfagas de la mayoría del trafico de datos, de otra manera, si existe un gran número de conexiones con tráfico de ráfaga (bursty), entonces todos ellos pueden ser asignados a el mismo enlace en espera que estadísticamente todos ellos no lleguen a explotar al mismo tiempo, y si algunos de ellos explotan simultáneamente, que exista la suficiente elasticidad para que la explosión pueda ser almacenada y puesta en subsecuentes ranuras que se encuentren libres.

Este es la llamada **multiplexión estadística** y permite la suma del máximo ancho de banda requerido de todas las conexiones sobre un enlace hasta sobrepasar el ancho de banda disponible agregado del enlace bajo ciertas condiciones de disciplina. Esto es imposible sobre una red STDM y esta es la diferencia principal de una red ATM.

El multiplexaje estadístico en conclusión, provee esencialmente a la red con un ancho de banda sobre demanda, significando que la red puede obtener el ancho de banda que éste necesite cuando sea necesario sin tener que reservarlo por adelantado.

Anexo C. Conmutación

Los elementos de conmutación son dispositivos especializados que se utilizan para conectar dos o mas líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para enviarlos.

La conmutación de datos

La telefonía actual fue establecida para realizar comunicaciones entre seres humanos (voz) utilizando Multiplexaje por División de Tiempo (TDM) y Multiplexaje por División de Frecuencia (FDM), de las cuales ninguna es apropiada para el tráfico de datos. Por esta razón es necesario un tipo de conmutación totalmente diferente, las principales formas de conmutación son: Conmutación de Circuitos y la Conmutación de Paquetes. Explicadas en el anexo de redes de área amplia (WAN) conmutadas públicas.

Conmutación híbrida

Con los adelantos de la tecnología, se han hecho posibles nuevas estructuras híbridas. Dentro de la conmutación de paquetes existen las variantes como **Conmutación por División de Tiempo**, en la cual cada dispositivo conmutador examina sus líneas de entrada en un ciclo riguroso. Cada paquete se retransmite inmediatamente, a través de la línea de salida correcta, con frecuencia tan pronto como se llegue a leer la cabecera. Mediante el uso de paquetes de tamaño fijo y una sincronización perfecta, no es necesario tener un espacio para almacenamiento temporal por lo tanto los dispositivos conmutadores pueden reducir su complejidad. La gran ventaja de la Conmutación por División de Tiempo radica en que ofrece un rendimiento muy alto (> 100 Mbps).

Conmutación por división de tiempo

Con este tipo de conmutación, "n" líneas de entrada se muestrean en secuencia, para constituir una estructura (frame) de entrada con "n" ranuras en donde cada ranura tiene "k" bits (en ISDN el tamaño de cada ranura es de k=8 bits).
La parte esencial del conmutador por división de tiempo es el **intercambiador de ranura de tiempo**, que recibe y produce frames, en la entrada y salida respectivamente en las ranuras que se han re-ordenado. El intercambiador de ranura de tiempo trabaja de la siguiente manera: cuando un frame de entrada está listo para su procesamiento, cada ranura (es decir un octeto), se escribe en una memoria temporal RAM, localizada en el interior del intercambiador. Las ranuras se escriben ordenadamente, de tal forma que la palabra i, en la memoria temporal, contiene la ranura "i".

Después de que todas las ranuras del frame de entrada se han almacenado en la memoria temporal, se construye nuevamente el frame de salida por medio de la lectura de las palabras, pero en un orden diferente (El contenido de la tabla de transformación, por consiguiente determina que permutación de la trama de entrada se generará como trama de salida y también, que línea de entrada se conectará con que línea de salida.

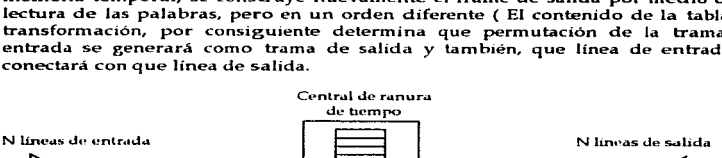


Figura C.1 Conmutación por división de el tiempo

La función consiste en establecer conexiones por medio de un ajuste del contenido de la tabla de transformación de ranuras, lo que permite una transmisión full dúplex.

Conmutación por División de Tiempo
La telefonía publica y las redes de telecomunicaciones están rápidamente evolucionando hacia un uso exclusivamente de tecnología digital

La digitalización de voz y técnicas de Multiplexaje por División de Tiempo síncrono (TDM), ambos voz y datos pueden ser transmitidos vía señales digitales. Esto ha permitido un cambio fundamental en el diseño de tecnología de sistemas de conmutación.

Actualmente todos los conmutadores de circuitos modernos utilizan técnicas de división de tiempo digital para el establecimiento y mantenimiento de circuitos. Conmutación de división de tiempo envuelve el particionamiento de un flujo de bit a baja velocidad dentro de piezas que comparten un flujo de bit de alta velocidad con otros flujos de bit . Las piezas individuales, o ranuras, son manipuladas por control lógico para enrutar los datos desde la entrada hasta la

salida. Tres conceptos comprenden la técnica de conmutación por división de tiempo.

- **TDM conmutación de bus (TDM bus switching)**
- **(TSI: Time-slot interchange)**
- **(TMS: Time-multiplex switching)**

Todas las técnicas de conmutación, están basadas en el uso de Multiplexaje por División de Tiempo síncrono (TDM). Este permite a múltiples flujos de bit de baja velocidad compartir una línea de alta velocidad. Un conjunto de entradas es un modelo en turno. Los modelos son organizados de manera serial dentro de ranuras (canales) para formar un frame recurrente de N ranuras. Una ranura puede ser de un bit , un byte, o un bloque un poco mas grande. Cabe hacer notar que con TDM el origen y el destino de los datos en cada ranura de tiempo son desconocidos. De aquí, que no existe la necesidad de bits de direccionamiento en cada ranura.

El mecanismo de TDM es muy simple, por ejemplo cada línea de entrada deposita sus datos en un almacén (buffer); el multiplexor explora los almacenes secuencialmente, tomando tamaños fijos de datos de cada almacén y los envía a fuera por la línea. Una exploración completa produce un frame de datos. Para las líneas de salida un procedimiento inverso es desarrollado, las líneas I/O de un multiplexor pueden ser síncronos o asíncronos, las líneas multiplexadas entre los dos multiplexores es síncrono. Las ranuras de tiempo son asignadas a las líneas I/O sobre una base fija, predeterminada. Si un dispositivo no tiene datos para enviar, el multiplexor debe enviar ranuras vacías o datos de relleno. Una gran desventaja del TDM, es que cuando no existe trafico en una terminal, se desperdicia una ranura de tiempo de salida. Las ranuras de salida se van rellenando de información bajo una estricta rotación, si no hay datos, se utilizan datos de relleno. No es posible saltar u omitir una ranura de tiempo, debido a que el extremo receptor mantiene un seguimiento sobre que caracter proviene de que terminal, esto mediante su posición en el frame de salida. Inicialmente, el multiplexor y el ordenador se sincronizan por si mismos.

Cada dispositivo se conecta al conmutador a través de dos líneas con almacenamiento (buffered lines), una para entrada y otra para la salida. Estas líneas son conectadas a través de compuertas controladas hacia un bus digital de alta velocidad. Cada línea de entrada se le asigna una ranura de tiempo. En el tiempo de duración de la ranura, la compuerta de la línea es habilitada , permitiendo una pequeña ráfaga (burst) de datos dentro del bus. Durante ese mismo tiempo de la ranura , una compuerta de salida es también habilitada. Durante ranuras de tiempo sucesivas, diferentes pares (entrada salida) son habilitados, permitiendo a un numero de conexiones ser llevadas sobre el bus compartido. Un dispositivo conectado lleva una operación full duplex al transmitir durante una ranura de tiempo asignada y recibiendo durante otro. En el otro final

de la conexión es un par para el cual esas mismas ranuras de tiempo tienen un manejo opuesto. Con este concepto se refiere como técnica de TDM de conmutación de bus.

Diferentes redes requieren diferentes velocidades de transmisión, prioritización de los datos y niveles de servicio. Ellos también tienen diferentes para conexiones de área amplia.

Anexo D. Redes de área amplia (WANs) conmutadas

Características de redes de datos públicas

Una red pública de datos (PDN : public data network) es una red establecida y operada por una autoridad de administración de red nacional específicamente para la transmisión de datos. Un requerimiento primario para una PDN es que deberá facilitar la interconexión de equipo de diferentes fabricantes, lo cual, requiere convenios de estándares para el acceso y uso de estas redes. Después de muchas discusiones y experimentación nacionales y después a nivel internacional, un conjunto de convenios estándares internacionales han sido aceptados por CCITT para uso con un rango de PDNs. Las recomendaciones referidas como las series-X y series-I incluyen estándares de velocidades de señalización de datos de usuario e interfaces de usuario con tales redes.

Existen dos tipos principales de Redes Públicas de Datos (PDN) : **Conmutación de Paquetes** (PSPDNs) y **Conmutación de Circuitos** (CSPDNs). En general, los estándares para estas redes se refieren a las tres capas inferiores del modelo de referencia OSI.

Conmutación de circuitos

Cada conexión establecida a través de una red de conmutación de circuitos resulta en un **canal de comunicación físico** siendo establecido a través de la red desde la llamada al equipo del subscriptor. Esta conexión es entonces usada exclusivamente por los dos subscriptores por la duración de la llamada (un ejemplo de este tipo de red es la red telefónica pública y las líneas privadas). En el contexto de la transmisión de datos, una característica de una conexión de conmutación de circuitos es que esta provee un canal de velocidad fija para la transmisión de datos y ambos subscriptores deberán operar a esta misma velocidad. Además, antes de que cualquier dato sea transmitido, es necesario establecer una conexión a través de la red.

El tener una trayectoria dedicada ofrece dos ventajas principales a la conmutación de circuitos. La primera, es que el tiempo total de propagación de la información del punto de origen al punto destino es constante e igual al tiempo que se tarda la información en recorrer la trayectoria física. La segunda es que como la línea es dedicada no puede congestionarse. Sin embargo, la conmutación de paquetes no se adapta de manera eficiente al tráfico intermitente (ráfagas) característico de las redes locales ya que en este tipo de trafico los circuitos físicos se encontrarían ociosos en un porcentaje alto de tiempo[239].

[239] La utilización promedio de las líneas privadas dedicadas es del orden del 25% al 30%.

En los primeros días de las redes telefónicas, el circuito que se establecía constituía una conexión ininterrumpida de cobre entre los dos aparatos telefónicos. En las redes telefónicas actuales ya no existe un circuito físico ininterrumpido entre los dos extremos de una conexión ya que se utiliza el Multiplexaje por División de Tiempo (TDM) en los enlaces de la red. Sin embargo, en las redes que utilizan TDM sigue conservándose la noción de un circuito dedicado, ya que a lo largo de la ruta por la que se transmite la información se reservan (durante todo el tiempo que dure la conexión) ranuras de tiempo en cada trama transmitida periódicamente en los enlaces. Por ejemplo, sobre un enlace E1 (a 2.048 Mbps) se multiplexan 30 circuitos E0 (a 64 Kbps) reservando una ranura específica de tiempo para cada circuito en las tramas que se transmiten cada 125 segundos.

Conmutación de paquetes

En las redes de conmutación de paquetes, es posible que la comunicación entre dos subscriptores se lleve a cabo en operaciones con diferentes velocidades de transmisión, esto es debido a que la tasa de transmisión a la cual son pasados los datos a las dos interfaces hacia la red es regulado de forma separada por cada equipo del subscriptor. Además, no se establecen conexiones físicas a través de la red. En lugar de esto, todos los datos a ser transferidos son primeramente ensamblados dentro de uno o mas unidades de mensaje llamados paquetes o frames, en el equipo de origen de la transferencia DTE (Equipo Terminal de Datos). Estos paquetes incluyen tanto la dirección origen como la destino. Estos paquetes son pasados bit por bit de manera serial por su DTE origen hacia su dispositivo de **intercambio conmutado de paquetes** local (PSE: packet-switching exchange). Cada PSE contiene un directorio de enrutamiento especificando él o los enlaces de salida a ser usados para cada dirección de red. En la recepción del paquete, el PSE envía el paquete sobre el enlace apropiado a la máxima velocidad de bit disponible. De manera similar como cada paquete es recibido (almacenado para su inspección de dirección) para cada PSE intermedio a lo largo de la ruta. La conmutación de paquetes soportan dos tipos de servicios: **servicios orientados a conexión (circuitos virtuales) y servicios sin conexión (datagramas).**

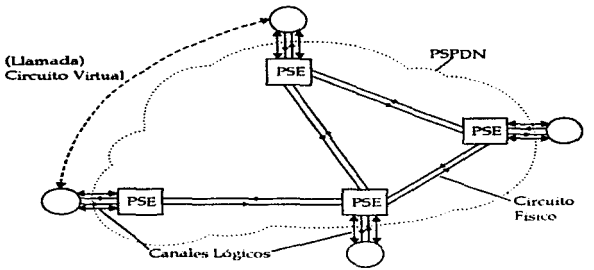


Figura D.1 Canales lógicos y llamas virtuales

Definición de servicios de red

Los servicios de red ofrecidos son definidos dentro de los **orientados a conexión** y **sin conexión** (conectionless). Los orientados a conexión definen un servicio el cual depende en establecer una conexión entre los puntos finales de manera lógica (circuitos virtuales) previa a la transferencia de datos. Servicios sin conexión, de otra manera, proveen conectividad fin-a-fin (lógica), pero sin la necesidad de establecer circuitos virtuales previos a la transferencia de datos. Los servicios orientados a conexión son generalmente utilizados en redes de área amplia (WANs) mientras que los servicios sin conexión principalmente en redes de área local (LANs).

Servicios orientados a conexión

Los circuitos virtuales son rutas establecidas de manera lógica a través de la red desde el origen hasta el destino. Estos circuitos virtuales permiten a un usuario tener múltiples conexiones de circuitos lógicos (varias conexiones punto a punto) sobre un mismo enlace de conexión física. El ancho de banda de acceso (56 Kbps/64 Kbps o 1.544 Mbps) puede ser asignado para cada una de estas rutas virtuales sobre una base de demanda (multiplexaje estadístico).

La principal característica de la técnica de circuitos virtuales es que una ruta entre estaciones es establecida de manera previa a la transferencia de datos, se debe notar que esta no es una ruta dedicada, como una conmutación de circuitos. Un paquete es aún almacenado en cada nodo y encolado para salir sobre la línea. La diferencia en cuanto al enfoque de datagrama, es que, con circuitos virtuales, el

nodo no necesita hacer decisiones de enrutamiento para cada paquete. Esto es hecho una ves para todos los paquetes que utilicen el circuito virtual.[240]

Direccionamiento

Cada interfaz física puede establecer uno o múltiples circuitos virtuales hacia interfaces físicas remotas. A cada uno de estos caminos virtuales se les ha asignado un número de identificación de canal lógico (similar a los números telefónicos). El número identificador de canal lógico tiene un significado de alcance local que indica la ruta del paquete hacia el próximo conmutador particular. Como el alcance es local, este número es actualizado en cada conmutador en la ruta por medio de tablas. Algunos ejemplos de identificadores de canales lógicos serían, el DLCI en frame relay y los VPI y VCI en ATM.

Una vez que son establecidos los circuitos virtuales, las comunicaciones de datos fin-a-fin son administradas a través de la conmutación de paquetes.

Existen diferentes tipos de circuitos virtuales: circuitos virtuales permanentes (PVC: permanent virtual circuit) y circuitos virtuales conmutados (SVC: switched virtual circuit).

Se provee al usuario hasta con 4095 canales virtuales, ya sea PVC o SVC.

Circuito virtual permanente

PVCs son circuitos virtuales establecidos de manera permanentemente entre un nodo origen y un nodo destino (punto-a-punto). Esto es similar a tener un enlace directo como si fuese una linea privada o alquilada todo el tiempo entre dos usuarios específicos por lo que garantizan una conexión entre dos puntos cuando sea demandado por el usuario[241]. El usuario siempre ve al circuito virtual como un circuito dedicado para su uso exclusivo todo el tiempo, mientras que la red provee el mismo circuito como un recurso compartido a múltiples usuarios sobre demanda. Estos circuitos permanecen definidos por un largo período de tiempo (semanas, meses o años).

Un PVC es establecido por medio de algún mecanismo externo (generalmente un administrador de la red), en el cual un conjunto de conmutadores (entre los sistemas origen y el destino) son programados con los valores de números identificadores apropiados[242].

---

[240] Stallings William.; ISDN and B-ISDN ; 4ª. Edición ; Macmillan; p. 74.

[241] Un PVC ahorra ancho de banda asociado con el establecimiento y eliminación del circuito, por lo tanto, es un ancho de banda dedicado que garantiza un nivel de servicio, para una estación particular

[242] Algún tipo de señalización puede facilitar el establecimiento de PVCs pero por definición, los PVCs siempre requerirán de alguna configuración manual.

Circuito virtual conmutado

Circuitos virtuales conmutados (SVCs) actúan de forma parecida como a las llamadas de conmutación de circuitos (teléfono), con la característica de ser conectados cuando es necesaria la conexión y desconectados después de que ha sido llevada a cabo la transferencia, es decir, los recursos son puestos en disposición solo por el período de duración de la transmisión (minutos u horas). Por lo tanto , un origen puede conectar a varios destinos en diferentes tiempos, opuesto a siempre estar conectado a un destino solamente. Se puede decir que la diferencia entre SVC y PVC es el tiempo de duración. Un SVC es una conexión que se establece de manera automática a través de un protocolo de señalización (es decir, no requieren la interacción manual necesaria para establecer los PVCs).

Servicio sin conexión

En la transmisión por datagramas se escoge para cada paquete la mejor ruta dependiendo de las condiciones de la red,

Anexo E. Redes telefónicas digitales

El uso de redes telefónicas conmutadas publicas (PSTN: Public switched telephone network) para la transmisión de datos ha sido considerada. Esta forma es solamente un método disponible para transmitir datos entre equipos de usuarios localizados en diferentes lugares, actualmente este, soporta solamente modestas velocidades de transmisión (generalmente desde 9600 bps hasta 28000 bps). Además de que las llamadas telefónicas tienen un cargo en base al tiempo y distancia de la llamada.

Por esta razón es que grandes organizaciones establecieron sus propias redes de datos privadas nacionales e internacionales. Generalmente, estas compañías usan alquiler de líneas dedicadas desde la compañía telefónica para interconectar un número de nodos conmutados particulares o multiplexados. Aunque las redes de este tipo ofrecen seguridad al usuario, flexibilidad y control, estas también envuelven grandes cantidades de inversión en compra o renta de equipo.

Servicios Digitales o líneas digitales

Los servicios digitales son frecuentemente utilizados para llevar voz, vídeo y datos. Los circuitos digitales pueden transmitir datos a velocidades mayores de 45Mbps. Usualmente, las líneas digitales son posibles al acondicionar líneas analógicas para manejar grandes velocidades de datos. Las líneas son generalmente alquiladas por un proveedor de intercambio local e instalados entre dos puntos para proveer un servicio dedicado. Son disponibles tanto como dedicadas o como servicios conmutados.

El estándar T1 es uno de los servicios de línea digital más ampliamente utilizados. T1 es una red digital de alta velocidad (1.544 Mbps) desarrollada por AT&T en 1957 e implantada en 1960 para soportar la modulación por impulsos codificados (PCM). La primera innovación de T1 fue introducir **digitalización** de voz y datos, de esta manera, se creó una red completamente capaz de representaciones digitalizadas.

Los circuitos que se enlazan, llevando múltiples llamadas de manera simultánea a través de una sola línea T1, se lleva a cabo en una forma digital por medio de **Multiplexaje por División de Tiempo** (TDM: time division multiplexing). Es decir, con TDM, las señales digitales provenientes de múltiples orígenes son cada una asignada a una ranura de tiempo especifico (time slot) en un enlace de alta velocidad, con lo que se produce una muestra de 8 bits cada 125 microsegundos[243].

[243] La capacidad de un circuito de voz, expresada digitalmente, es convertida de 4000 Hz a 64000 bits por segundo con lo que se tiene que un circuito de voz es equivalente en una forma digital, a un byte (8 bits) cada 125 microsegundos. 24 de estos canales compone 1.536Mbps además de que

La velocidad de bit del enlace, es por tanto, una función del número de canales de voz que este lleve. En Estados Unidos y Japón se agrupan 24 canales de voz mientras que en países que cumplen con las normas CCITT agrupan 30 canales. Teniendo una tasa de bits agregados en 1.544Mbps y 2.048 Mbps respectivamente

Los canales DS son canales digitales que llevan voz o datos de manera simultánea. Cada canal opera a 64Kbps (8bits por 125 microsegundos).

En la definición básica existe la discusión que hay un "mayor orden" o jerarquía de T1. Existe T1 el cual es, una red de 1.544Mbps de velocidad y fue diseñada para circuitos de voz o **canales** (24 canales por cada línea o tronco T1). En adición, existe T1-C el cual opera a 3.152 Mbps. Existe también un T-2, operando a 6.312 Mbps, también existe un T-3 operando a 44.736 Mbps y un T-4 operando a 274.176 Mbps. Los últimos tres son conocidos como **supergrupos** y sus velocidades de operación son generalmente referidas como 45Mbps y 274 Mbps respectivamente.

Estados Unidos				
Circuito Nivel de senal	VELOCIDAD (Mbps)	Número. T1s	Número canales de voz	acarreador
DS0	.064	1/24 de T-1	1 canal	--
DS1	1.544	1 T-1	24 canales	T1
DS1C	3.152	2 T-1	48 canales	T1C
DS2	6.312	4 T-1	96 canales	T2
DS3	44.736	28 T-1	672 canales	T3
DS3C	89.472	56 T-1	1344 canales	
DS4	274.176	168 T-1	4032 canales	T4

CCITT (CEPT) Europa		
Circuito	Velocidad (Mbps)	Canales voz/datos
E1	2.048	30
E2	8.448	120
E3	34.368	480
E4	139.264	1920
E5	565.148	7680

Jerarquía T-1 (DS: Señal digital y describe el nivel físico)

En los dos sistemas, la tasa de bits menor son conocidas como **fraccional T1/E1.**

Por razones matemáticas, un canal de voz fue seleccionado para ser de 64Kbps.

X.25	Frame Relay	SMDS	B-ISDN	Conmutados
DS-0		DS-1	DS-3	
0.064		1.544	44.736	Mbps

se tiene que enviar un bit extra de sincronización llamado bit de Frame, lo que forma (64x24+80=1.544) los 1.544Mbps.

T1 Fraccional

El fraccional T1 es para quienes necesitan canales de 64 Mbps área amplia pero de otra manera no necesitan un tubo T1 completamente. Un cliente puede empezar con un número de fraccional T1 y crecer hasta completar el servicio T1[244]. Las líneas son fraccionadas, lo que quiere decir que estas pueden ser divididas dentro de canales para voz o datos.

[244] Cuando un cliente contrata un servicio fraccional T1, el acarreador establece una interface T1 completa, pero solo hace el contrato de ancho de banda requerido.