58

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

"Migración de una Red de Cómputo a una Red de Alta Velocidad Mediante su Análisis y Rediseño. Caso: Instituto de Geofísica, Campus C.U. U.N.A.M."

T E S I S

Que para obtener el título de

Ingeniero en Computación

Presentan:

Juan Jacobo Lara Rodríguez
Juan Antonio Manjarrez Cuahunte
Raymundo Pichardo Muñoz

Director: Ing. Alfredo Hernández Mendoza
Co-Director: Ing. Noé Cruz Marín

Ciudad Universitaria **México 2002**

58

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

"Migración de una Red de Cómputo a una Red de Alta Velocidad Mediante su Análisis y Rediseño. Caso: Instituto de Geofísica, Campus C.U. U.N.A.M."

T E S I S

Que para obtener el título de

Ingeniero en Computación

Presentan:

Juan Jacobo Lara Rodríguez
Juan Antonio Manjarrez Cuahunte
Raymundo Pichardo Muñoz

Director: Ing. Alfredo Hernández Mendoza
Co-Director: Ing. Noé Cruz Marín

Ciudad Universitaria **México 2002**

Migración de una red de cómputo a una red de alta velocidad mediante su análisis y rediseño.

Caso:
Instituto de Geofísica campus C.U. - U.N.A.M.

ÍNDICE.

. . . . . .

TÍTULO DE LA TESIS:

"MIGRACIÓN DE UNA RED DE CÓMPUTO A UNA RED DE ALTA VELOCIDAD MEDIANTE SU ANÁLISIS Y REDISEÑO. CASO: INSTITUTO DE GEOFÍSICA – CAMPUS C.U.- UNAM"

ÍNDICE

INTRODUCCIÓN 1

i.- El Instituto de Geofísica 1
ii.- Departamentos del Instituto de Geofísica 2
iii.- Alcances y objetivos de la tesis 4

CAPITULO I. PLANTEAMIENTO Y ANÁLISIS DE LA PROBLEMÁTICA

I.1.- Antecedentes 6
Problemática presentada en años anteriores

I.2-. Estado actual de la red de cómputo del Instituto de Geofísica 13
Backbone de la Red-UNAM 13
Esquema general de la red de cómputo del Instituto de Geofísica 15

I.3.- Problemática actual 18
Estudio del diseño general 18
Servicios y servidores principales 19
Estadísticas del funcionamiento de la red 20

I.4.- Perspectivas a futuro 22
Plan de crecimiento de la red 22
Necesidades de equipamiento para las aplicaciones en Internet2 22

CAPÍTULO II. MARCO TEÓRICO

II.1.- Conceptos básicos de redes 24
Definición de redes de computadoras 24
Estructura de una red de computadoras 25
Clasificación de las redes de computadoras 26
Circuitos Multipunto y punto 28
Tipos de Transmisión 28

II.2.- Topologías 30
Topología estrella 30
Topología de bus 31
Topología de árbol 31
Topología anillo 32

II.3.- Modelo de referencia OSI 32

II.4-. Medios de transmisión 35
Cable coaxial 36
Cable par trenzado 37
Fibra óptica 39
Microondas 41

II.5.- Protocolos de comunicación 42

Protocolos de control de acceso al medio 42
TCP/IP Protocolos de la capa de red y de transporte 45
Protocolo de resolución de direcciones: ARP 47
Protocolo de réplica de resolución de direcciones: RARP 48
Servicios de Telnet, FTP,Mail 48
Principales Protocolos de Redes IBM y Microsoft 50
Principales protocolos de Netware 50

II.6.- Equipos de comunicación 51
Repetidor 51
Puentes (Bridges) 51
Concentradores (Hubs) 52
Conmutadores (Switches) 53
Ruteadores (Routers) 53
Compuertas (Gateway) 54

II.7.- Estándares y normas 54
Ethernet 54
Ethernet 802.3 55
Fast Ethernet 82
Gigabit Ethernet 86
FDDI 86
Frame Relay 87
ATM 88
II.8.- Internet 2 89
Ipv6 90

CAPÍTULO III.- DISEÑO DE REDES DE CÓMPUTO.

III.1.- Diseño de redes de cómputo 92
Consideraciones técnicas 92
Diseño de topología de red 95
Evaluación de servicios de Core 104
Evaluación de servicios de Distribución 110
Evaluación de servicios de acceso local 114
Identificando y seleccionando los dispositivos de red 119

III.2.- Cableado Estructurado 121

Evolución de sistemas de cableado 121
Cableado Horizontal 122
Cableado Vertical 125
Cuarto de Telecomunicaciones 126
Consideraciones de Diseño 127
Recomendaciones en cuanto a la documentación 134

III.3.- Tecnologías de alta velocidad 134
Estructura de la red Ethernet 134
100Base: Fast Ethernet a 100 Mbps 138
1000Base: Giganit Ethenet a 1000 Mbps 151
Otros estándares IEEE 159
FDDI. Interfaz de datos distribuida por fibra 163
ATM. 172
Configuración de redes para multisegmentación 185

CAPÍTULO IV.- REDISEÑO DE LA RED DE CÓMPUTO DEL INSTITUTO DE GEOFÍSICA

IV.1.- Metodologías de análisis 192
Metodología presentada por Teré Parnell 193
Metodología usada en DGSCA 201
Metodología propuesta 203
Análisis de la red de cómputo del Instituto de Geofísica 204

IV.2.- Rediseño de la red de cómputo del Instituto de Geofísica 223
Estudio del Edificio Principal 224
Estudio del Edificio II (Departamento de Física Espacial) 230
Estudio del edificio III 230
Estudio del Edificio IV 233

IV.3.- Deficiencias encontradas en la estructura actual de la red de cómputo del Instituto de Geofísica 233
Deficiencias encontradas en el estudio general del Instituto 233
Deficiencias encontradas en el estudio del Edificio Principal 234
Deficiencias encontradas en el estudio del Edificio II (Departamento de Física Espacial) 237
Deficiencias encontradas en el estudio del Edificio III (Biblioteca) 237
Deficiencias encontradas en el estudio del Edificio IV (Anexo) 237

IV.4.- Propuesta de rediseño del Backbone de Red-UNAM 237

IV.5.- Propuesta inmediata 240
Propuesta para el Edificio Principal 240
Propuesta para el Edificio II 241
Propuesta para el Edificio III (Biblioteca) 241
Propuesta para el Edificio IV (Anexo) 242

IV.6.- Propuesta óptima 242

IV.7.- Propuesta final 246

IV.8.- Propuesta económica 248

IV.9.- Relación costo beneficio 250

IV.10.- Justificación de la tecnología seleccionada 250

IV.11.- Justificación de la propuesta económica seleccionada 250

IV.12.- Presentación y análisis de los resultados obtenidos 251

CAPÍTULO V.- POLÍTICAS PARA LA ADMINISTRACIÓN DE LAS REDES DE CÓMPUTO

V.1.- Políticas para el Instituto de Geofísica 255

V.2.- Administración y Documentación de la Red 262
El lado administrativo de la gestión de red 262
Administración del la red 263
Seguridad de la red.- Panorama general 264
Factores Ambientales 265
Desempeño de la red 265
Administración del servidor 266

Resolución de problemas de la red 267
Monitoreo de la red 268

CONCLUSIONES 270

ANEXO A.- 272
CROQUIS DE LAS INSTALACIONES DEL INSTITUTO DE GEOFÍSICA.

ANEXO B.- 278
IMAGENES DEL EQUIPAMIENTO DE LA RED DE CÓMPUTO.

ANEXO C.- 292
NORMATIVIDAD DE TELECOMUNICACIONES. DGSCA-UNAM.

BIBLIOGRAFÍA 297

Introducción.

INTRODUCCIÓN

Con el desarrollo de esta tesis se pretende solucionar los problemas presentados en la Red de Cómputo del Instituto de Geofísica. Sin embargo, antes de empezar a realizar el estudio de la red de cómputo, es necesario involucrarse en la problemática misma de la red y aún más importante; implicarse en las necesidades presentes y futuras de cada uno de los usuarios de la red de cómputo con la finalidad de que el nuevo diseño de la red facilite y mejore su desempeño en el Instituto.

Para lograr un mejor trabajo y por consiguiente dar la mejor solución, es necesario el dividir este estudio en capítulos, de modo que las conclusiones de uno sirvan para de base para iniciar un buen estudio los subsecuentes capítulos.

Antes de comenzar el estudio de la problemática presentada en el Instituto, es necesario involucrarse en las tareas, objetivos y estudios que se hacen en el mismo, para así poder entender el por qué de la importancia de este trabajo y el por qué de la importancia de que la Red de Cómputo funcione apropiadamente.

i.- El Instituto de Geofísica

El Instituto de Geofísica de la Universidad Nacional Autónoma de México tiene gran relevancia no sólo en la Universidad si no también en el ámbito Nacional debido a las importantes investigaciones que se realizan dentro de esta dependencia.

El Instituto de Geofísica (IGEOF) es una dependencia del Subsistema de la Investigación Científica de la Universidad Nacional Autónoma de México (UNAM), que tiene entre sus objetivos fundamentales:

1. Realizar investigación en geofísica y en aspectos relacionados de carácter interdisciplinario con otras ciencias.

2. Formar y capacitar personal especializado.

3. Asesorar a otras dependencias de la Universidad y sectores gubernamentales y privados del país en aplicaciones de técnicas geofísicas.

4. Dar difusión de los resultados de las investigaciones del IGEOF y sobre el estado y avances científicos en Ciencias de la Tierra.

Las actividades del IGEOF abarcan un amplio espectro de las Ciencias de la Tierra y Espaciales, que incluyen estudios teóricos y experimentales en el contexto de las investigaciones y programas internacionales de geofísica y estudios básicos y aplicados de carácter regional y local, con particular énfasis en las características, recursos minerales y energéticos y fenómenos geológico-geofísicos del país.

El Instituto está actualmente constituido por cuatro departamentos, una sección, un conjunto de observatorios y laboratorios, tres servicios geofísicos nacionales, varios servicios de apoyo académico, una subsede en el Campus Juriquilla y el Posgrado en Ciencias de la Tierra. Los departamentos y secciones que integran el Instituto de Geofísica son: Departamento de Física Espacial, Departamento de Geomagnetismo y Exploración, Departamento de Recursos Naturales, Departamento de Sismología y Vulcanología y la Sección de Radiación Solar. Los observatorios y laboratorios incluyen: Observatorio de Teoloyucan, Observatorio de Radiación Cósmica, Laboratorio Universitario de Geoquímica Isotópica, Laboratorio de Química Analítica, Laboratorio de Espectrometría de Plasmas y Laboratorio de Paleomagnetismo y Geofísica Nuclear. Los servicios geofísicos están constituidos por el Servicio Sismológico Nacional, el Servicio Mareográfico y el Servicio Magnético. El Laboratorio Universitario de Geoquímica Isotópica es manejado conjuntamente con el Instituto de Geología. Adicionalmente, se cuenta con la Unidad de Investigación en Ciencias de la Tierra (UNICIT), la cual funciona como una unidad interdisciplinaria de los Institutos de Geología y Geofísica en el Campus Juriquilla, Querétaro.

Todas las investigaciones que se desarrollan en el Instituto de Geofísica son de gran importancia, ya que monitorean el comportamiento de la tierra mediante mediciones que son capaces de anticipar posibles movimientos telúricos y demás desastres naturales a causa del movimiento de las placas tectónicas y demás factores que afectan el comportamiento de la tierra. El aviso oportuno de estos posibles desastres corre a cargo del Centro Nacional de Prevención de Desastres (CENAPRED), que es quién se encarga de recabar la información generada por los departamentos de este Instituto.

ii.- Departamentos del Instituto de Geofísica

Cada uno de los Departamentos que componen este Instituto interactúa con los otros, de manera que la información de uno de ellos es relevante para los demás departamentos. A continuación se describen brevemente las tareas de Investigación que cada uno de los departamentos es encargado de realizar.

ii.i.- Departamento de Física Espacial

La Física Espacial se inicia como una disciplina independiente a raíz de las primeras exploraciones del espacio exterior por medio de satélites y sondas espaciales. El terreno de estudio de la Física Espacial es la heliosfera, esta es, la región del espacio interestelar controlada por el sol mediante el flujo del viento solar y de los cuerpos que se encuentran en ella.

Entre los objetivos principales de investigación en el Departamento de Física Espacial se encuentran las siguientes:

- El campo magnético y la activación del sol.
- El medio solar y el viento interplanetario.
- La ionosfera y la magnetosfera de la tierra.

- La interacción del viento solar con las magnetosferas y las ionosferas planetarias y con los comentas.
- Las perturbaciones interplanetarias y sus efectos sobre la tierra.
- La generación y propagación de partículas energéticas y rayos cósmicos en la heliosfera.
- Las relaciones entre la actividad solar y el clima.

Para realizar estas investigaciones se cuenta con el siguiente equipo:

- Una estación de rayos cósmicos, la cual tiene por objeto monitorear la cantidad de radiación solar que llega a la tierra desde el espacio.
- Un radio-interferómetro solar, que estudia la componente lentamente variable de la emisión de microondas del sol.
- Una estación de radio-sondeo que monitorea la ionosfera de México.
- Un Observatorio de Micropulsaciones Magnéticas en Teoloyucan, Estado de México, el cual permite estudiar el acoplamiento del viento solar con la magnetosfera terrestre.
- Un Observatorio de Centelleo Interplanetario que es sistema de alarma en caso de tormentas magnéticas.

ii-ii.- Departamento de Geomagnetismo y Exploración

El personal académico de este departamento produce información sobre ciencias básicas y aplicadas indispensables en el entendimiento de los fenómenos geofísicos y geoquímicos existentes tanto en las capas más internas de la tierra, núcleo y manto, como en la corteza de la misma. Las secciones de investigación en las que se ha dividido el departamento son:

- Geomagnetismo. Este grupo se encarga de caracterizar el comportamiento, origen e influencia interplanetaria del campo magnético actual de la tierra.

- Exploración. Grupo dedicado al desarrollo de métodos de exploración geofísica con aplicaciones a minería, geotermia, exploración petrolera y de cuencas sedimentarias, geofísica ambiental, geotecnia y arqueología.

- Paleomagnetismo. Los estudios se basan en la caracterización de las propiedades magnéticas de las rocas y minerales, con el fin de documentar los cambios del campo magnético terrestre en el pasado geológico.

- Geoquímica. Aquí se realizan trabajos de caracterización geoquímica e isotópica de diversas regiones geológicas de México.

- Paleoambientes e Impacto Ambiental. En esta área los estudios se enfocan a las fluctuaciones ambientales climáticas durante el cuaternario.

ii.iii.- Departamento de Recursos Naturales

Los estudios en este departamento se enfocan a la hidrogeología, geotermia, hidrogeoquímica, métodos geofísicos de exploración, modelación matemática y computacional de estructuras geológicas y de flujo y transporte de solutos en medios porosos, contaminación de sistemas acuíferos y la evaluación de impacto ambiental.

Dentro de las principales líneas de investigación se encuentran:

- Contaminación de acuíferos.
- Control óptimo de hidrogeología.
- Estructuras de impacto.
- Exploración y evaluación de aguas subterráneas, etc.

ii-iv.- Departamento de Sismología y Vulcanología

La sismicidad y actividad volcánica que ocurren en México está relacionada a la interacción entre placas tectónicas que conforman la litósfera de la tierra. Frente a este panorama, resulta de vital importancia el mantener una vigilancia constante de la actividad sísmica y volcánica de nuestro país, que permita obtener la información científica indispensable para la comprensión de tales fenómenos geológicos, y en un momento dado, poder estar prevenidos.

La sección de sismología se encarga del estudio y conocimiento de los procesos que gobiernan la mecánica, generación y efectos de los fenómenos sísmicos y volcánicos que afectan al territorio nacional y zonas circunvecinas, así como el estudio de la estructura cortical mexicana a partir de las ondas sísmicas. En esta sección opera el Servicio Sismológico Nacional (SSN), siendo la instancia responsable del reporte de los eventos sísmicos de importancia que ocurren en el país, así como de su compilación en boletines, catálogos y mapas. Dada la importancia que reviste el estudio de los sismos de potencial destructivo para otras instituciones, existen convenios de colaboración, principalmente con el Centro Nacional de Prevención de Desastres (CENAPRED) y el Instituto de Ingeniería.

La sección de vulcanología tiene como objetivo principal estudiar los volcanes activos de México bajo dos premisas: el estudio de la estratigrafía volcánica y la reconstrucción de la historia eruptiva de los volcanes mexicanos y la vigilancia geofísica y geoquímica de los volcanes activos.

iii.- Alcances y objetivos de la tesis.

Con la presente tesis se pretenden alcanzar los siguientes objetivos:

a) Elaborar el rediseño de la red de cómputo del Instituto de Geofísica de acuerdo a las necesidades presentes y futuras tomando en cuenta las tecnologías emergentes de alta velocidad que se están implantando en la actualidad.

b) Analizar el funcionamiento actual de la red de cómputo del Instituto de Geofísica para eliminar los problemas que se presentan.

c) Proponer una serie de políticas para la administración de la red del Instituto de Geofísica que permitan tener un mejor manejo de los recursos utilizados en la misma y, que a su vez cumplan con los lineamientos de DGSCA y se adecuen a las necesidades del Instituto.

Con el cumplimiento de los objetivos mencionados anteriormente se espera finalmente que:

- Los reportes y estudios generados por el Instituto de Geofísica que tienen gran importancia dentro del país e incluso para el extranjero se envíen oportuna y confiablemente, ya que de ellos depende la interpretación de los fenómenos que suceden en las capas internas de la tierra y a su vez dicha información es evaluada por el CENAPRED para dar aviso sobre las posibles zonas propensas a desastre, lo que significaría la salvación de muchas vidas humanas.

- Los tiempos de respuesta de las peticiones a la red estén en un rango de tiempo normal de acuerdo a los tiempos que se tenían en los instantes en que el problema estuvo en su apogeo. También se espera que el rediseño de la red de cómputo sea capaz de funcionar por lo menos 5 años después de su implantación, es decir, que dicho rediseño sea escalable a las nuevas tecnologías emergentes como Fast Ethernet, Gigabit Ethernet y ATM. Además se espera que con las nuevas Políticas de Administración para la red de cómputo se tenga un ordenado crecimiento de la misma, la pronta disposición de la información de los recursos con que se cuenta y un correcto uso de las herramientas por parte de los usuarios finales.

La solución a los problemas presentados en la red de cómputo de este Instituto significarán una pronta y segura adquisición de datos de los equipos que se encuentren monitoreando los principales puntos de actividad geofísica y geológica en nuestro país, estos datos servirán para generar los reportes necesarios en cada Departamento y a su vez poderlos intercambiar con los demás.

Capítulo I

Planteamiento y Análisis de la Problemática.

CAPÍTULO I:
PLANTEAMIENTO Y ANÁLISIS DE LA PROBLEMÁTICA

En este capítulo se expone el seguimiento que se le dio a una problemática en la red de cómputo del Instituto de Geofísica mostrada en años anteriores. Del mismo modo, se plantea una descripción de la configuración, estado y problemática actual presentada en la red de cómputo de este Instituto y finalmente, se trazan las perspectivas y necesidades que en un presente inmediato y a futuro tendrán los usuarios de esta red.

1.1.- Antecedentes

Una mayor complejidad en los entornos de red trae consigo un mayor potencial de problemas de conectividad y de rendimiento en las interredes, y el origen de dichos problemas con frecuencia es difícil de encontrar. Las fallas en la interredes se caracterizan por ciertos síntomas, éstos podrían ser generales o más específicos. Cada síntoma puede ser analizado, lo cual conducirá hacia los problemas o causas, empleando herramientas y técnicas específicas para la resolución de problemas. Las claves para mantener un entorno de red libre de problemas, así como para mantener la capacidad de aislar y corregir una falla con rapidez, son la comunicación, la documentación y la planeación.

La complejidad de la redes y de las aplicaciones que cada vez consumen más recursos hacen que las redes de cómputo deban estar migrándose hacia nuevas tecnologías. En los periodos donde se plantea esta migración es común que comiencen a surgir y/o a detectarse algunos problemas en las redes, tal es el caso de éste Instituto.

1.1.1.- Problemática presentada en años anteriores.

En febrero de 1997, el Departamento de Redes de la Dirección General de Servicios de Cómputo Académico (DGSCA) atendió un reporte de lentitud en la transferencia de datos interna y externamente en la red de cómputo del Instituto de Geofísica. Durante el análisis hecho a este Instituto, los resultados arrojados fueron los siguientes:

- Hubs conectados en cascada fuera del estándar establecido, en la *figura 1.1*, se puede observar que en la red del Instituto se tienen más de 4 Hubs (concentradores) conectados en cascada lo cual, no es válido, ya que se viola la norma de comunicaciones establecida por la IEEE para redes Ethernet 802.3, la cual a grandes rasgos dice que una red Ethernet puede tener conectados a lo más 4 concentradores en cascada. El conectar un mayor número de concentradores aumenta el índice de errores y de colisiones en la red, deteriorando así su desempeño.

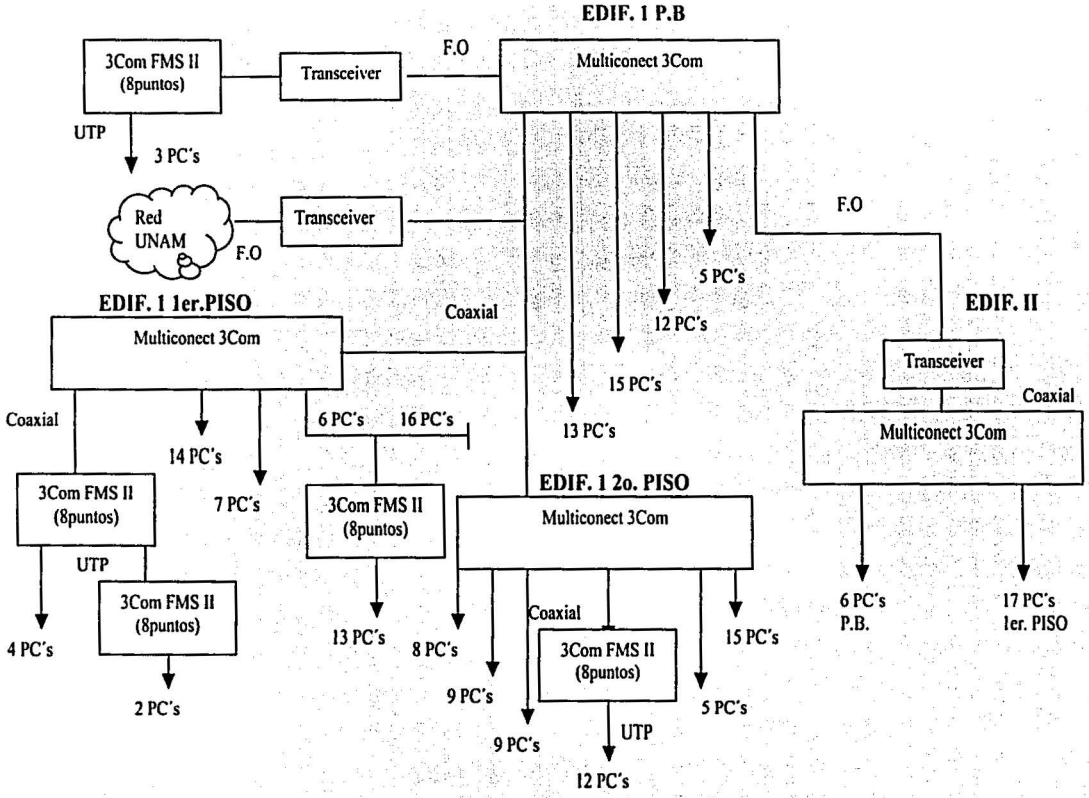


Figura 1.1.- Diagrama general de la red de cómputo en 1997

- Cableado de red propenso a fallas. La longitud máxima permitida de un segmento de cable coaxial delgado es de 185 m., sin embargo se pudo constatar que en este caso, no se rebasan los 185 m. establecidos por el estándar, pero el empleo excesivo de cableado coaxial delgado hace que la red del Instituto sea propensa a fallas propias en este tipo de cableados como falsos contactos o daños en los conectores.

Para solucionar estos problemas se realizó un análisis en donde se determinaron las soluciones más adecuadas, antes que nada se efectuaron 2 visitas al Instituto, en las cuales se tomaron una serie de datos sobre el comportamiento general de la red. En las *siguientes 2 tablas* aparecen los datos del primer análisis. Durante los primeros 35 min. del análisis en la red se presentó un índice de colisiones y errores aceptable, pero en el transcurso de la siguiente hora el número de colisiones y errores tuvo un aumento considerable mismo que deja ver la existencia de problemas en la red del Instituto.

PRIMEROS 35 MINUTOS	
ERRORES	COLISIONES
2895	2339

Tabla 1.1 Errores y colisiones en 35 minutos.

SIGUIENTE HORA	
ERRORES	COLISIONES
25349	15353

Tabla 1.2 Errores y colisiones en una hora.

En las siguientes tablas se muestran los datos correspondientes al segundo análisis efectuado en la red *tabla* 1.3, así como los correspondientes a una red con un número similar de nodos al de la red del Instituto, pero sin problemas de instalación, *tabla 1.4*. La diferencia en la cantidad de errores y colisiones mostraba que eran 1500% más errores y casi un 30% más de colisiones más que una red sin problemas.

SEGUNDO ANÁLISIS	
ERRORES	COLISIONES
40680	65520

Tabla 1.3 Segunda muestra de errores y colisiones

RED SIN PROBLEMAS	
ERRORES	COLISIONES
27	2371

Tabla 1.4 Red exenta de problemas.

Las soluciones presentadas en ese momento, fueron las siguientes:

Se revisó la *figura 1.2*, en donde se puede observar que el tráfico generado por la máquina A debe pasar por 5 concentradores antes de que la máquina B lo identifique. Dado que en una red tipo Ethernet todos los equipos comparten al ancho de banda y pueden hacer uso de la red en cualquier instante, la presencia de este tipo de conexiones provoca retardos que aumentan considerablemente el número de colisiones y errores en la red.

Por lo cual se vieron varias opciones para corregir el problema de cinco concentrados conectados en cascada.

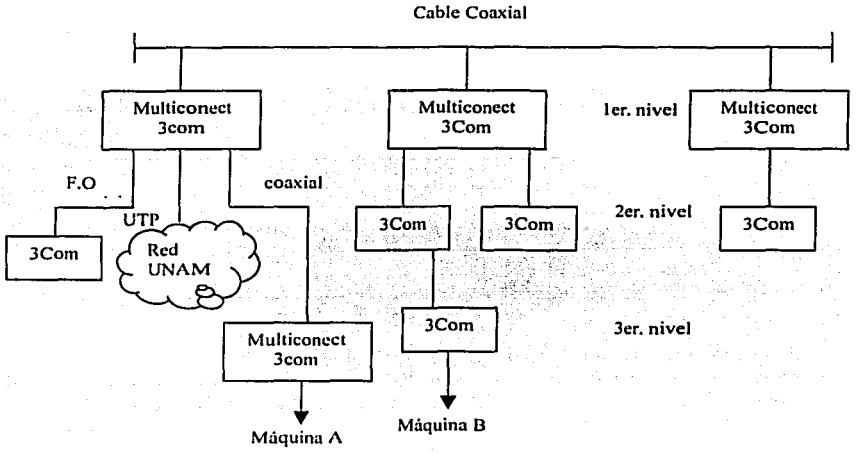


Figura 1.2. Segmento de la red en donde se encuentran más de 4 hubs entre 2 PC's.

La solución más simple, aunque se requería de analizar las posibilidades de efectuar un cambio, consistía en conectar el concentrador 3Com ubicado en el tercer nivel directamente a uno de los servicios del equipo Multiconect 3Com localizado en el edificio I, primer piso, como se muestra en la *figura 1.3*.

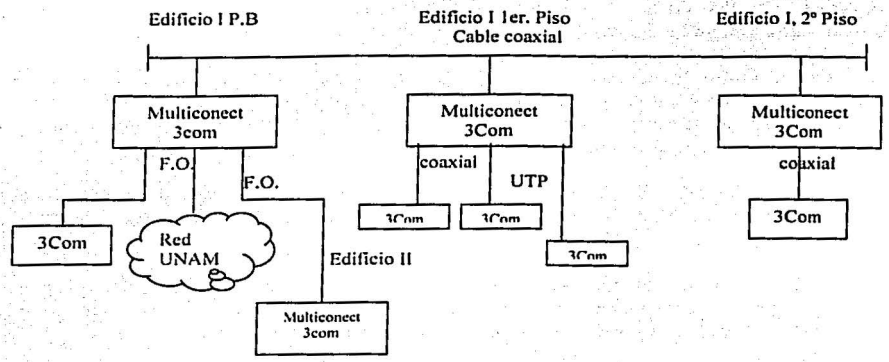


Figura 1.3 Hub conectado al multiconect.

Otra solución propuesta por parte de DGSCA fue la colocación de un puente (bridge) entre el edificio I y el primer piso como se indica en la *figura 1.4*.

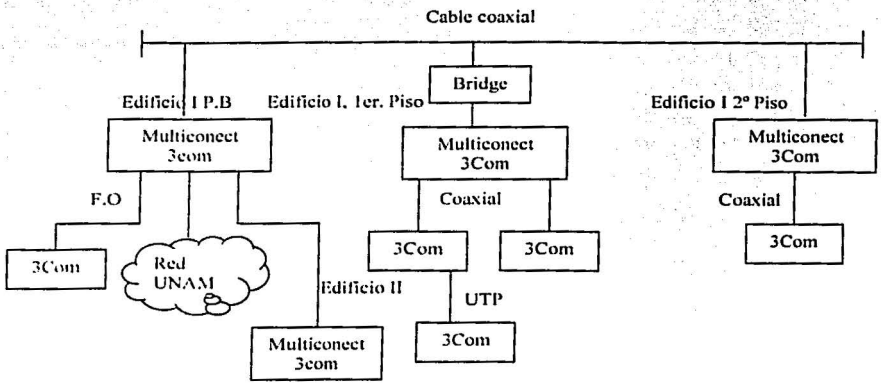


Figura 1.4 Puente colocado entre el edificio I y el primer piso.

La función del bridge es dividir la red en dos segmentos más pequeños A y B, cada uno de los cuales puede tener hasta cuatro concentradores en cascada sin afectar al otro. Adicionalmente, el puente filtra la información de cada uno de los segmentos en forma tal que el tráfico propio de cada uno de los segmentos no afecta al otro.

Con los análisis realizados se observó la ubicación de las PC´s que generaban la mayor cantidad de tráfico en la red del Instituto. Del primer análisis se hizo un recuento de los equipos que generaban la mayor cantidad de tráfico, obteniéndose en esa ocasión que el 32% del tráfico era generado por equipos localizados en el primer piso del edificio II y otro 23% del tráfico era producido por PC´s localizadas en el segundo piso del edificio I. El obtener este tipo de datos fue importante debido a que si el 32% del tráfico generado en la red era netamente local y al colocar el puente, dicho tráfico era aislado, aumentando con ello la eficiencia del otro segmento de la red.

En el segundo análisis que se realizó, se observó que el 70% del tráfico es generado por PC´s localizadas en el edificio I segundo piso y con la colocación del puente, dicho tráfico no afectaría a los equipos del primer piso del mismo edificio.

Este análisis, y sus soluciones se llevaron a cabo en marzo de 1997, se instaló el puente para corregir el problema de los 5 concentradores conectados en cascada y aumentar la velocidad de respuesta en dicha red como se muestra en la *figura 1.5.*

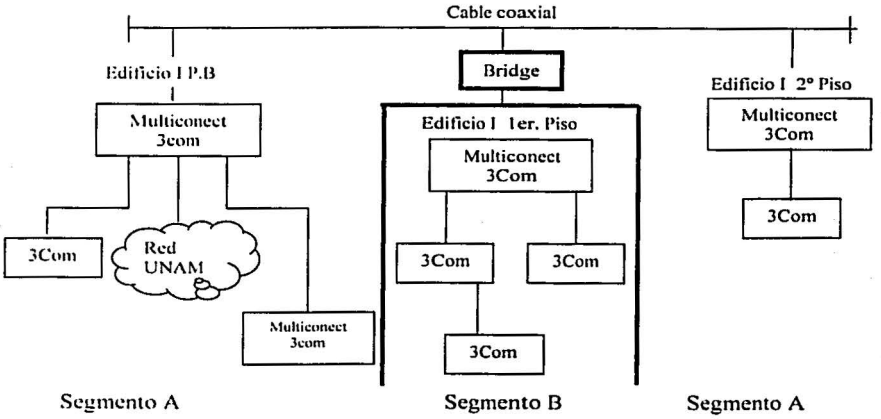


Figura 1.5 Segmentación de la red con el puente.

En la figura anterior se puede observar claramente como quedó segmentada la red (segmento A y segmento B) así como el punto en el cual se colocó el analizador para medir los errores y colisiones que se generan en el segmento B. Antes de instalar el puente se analizó la red del Instituto para observar el comportamiento de la red. Los datos obtenidos de dichos análisis se presentan a continuación, *tabla 1.5.*

SIN PUENTE	CON PUENTE
Errores: 4613	Errores: 8557
Colisiones: 10158	Colisiones: 21202

Tabla 1.5 Resultados antes y después del puente..

En las tablas anteriores se observa que el número de colisiones, presentan un aumento considerable a los obtenidos antes de la instalación del puente. El problema de 5 concentradores conectados en cascada se resuelve pero los resultados obtenidos con la segmentación de la red llevo a la suposición de que el problema también radicaba en la existencia de fallas en el cableado de la red del Instituto.

Para determinar cual o cuales eran los segmentos de cable coaxial presentaban alguna falla, se propuso analizar la red por segmentos. Dicha segmentación consistía en desconectar cada uno de los equipos Multiconec 3Com, uno a la vez, y analizar en forma aislada cual era el comportamiento del segmento de red que dependía de cada Multiconect, como se muestra en la *figura 1.6*.

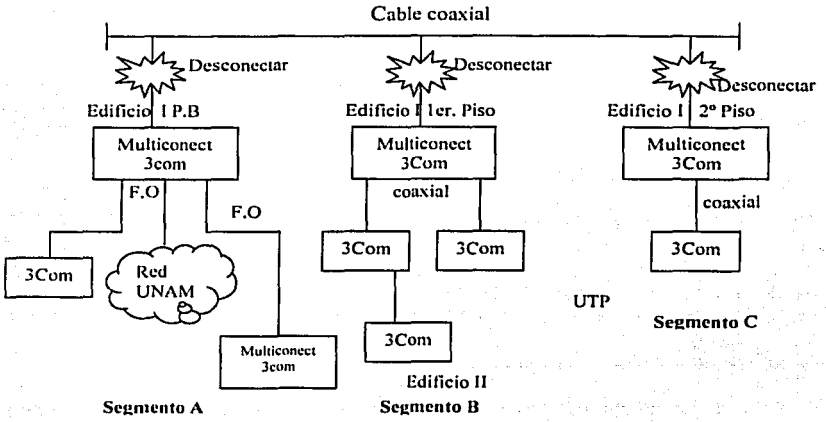


Figura 1.6 Análisis de la red por segmentos.

Una vez desconectado el segmento A, B o C sería necesario generar tráfico en forma local para determinar el número de colisiones que ocurrían en dichas secciones y poder identificar de esa forma en que parte de la red se encontraban las fallas en el cableado.

Después se determinó, que por motivos de pérdida de paquetes de información en la red, se realizaron las siguientes acciones:

- Se aisló la red del Instituto de RedUNAM, y se conectó directamente un equipo ruteador para verificar que la fibra óptica que comunica al Instituto con RedUNAM no presentaba ningún daño. La prueba que se realizó para comprobar eso fue la siguiente: se enviaron paquetes desde DGSCA al ruteador y viceversa, teniéndose como resultado que no había ningún problema, con lo que se determinó que no se debía a un asunto relacionado con la fibra óptica y en consecuencia se dedujo que era un problema interno de la red.

Las recomendaciones que se dieron en esa ocasión fueron las siguientes:

- Eliminar el cableado coaxial delgado de la red del Instituto de Geofísica
- Analizar el tipo de servicios de red que serían empleados a mediano y corto plazo para proponer una topología de red.
- Mantener la documentación de la red actualizada como hasta ese momento, para facilitar la solución de cualquier falla posterior.

1.2.- Estado actual de la Red de Cómputo del Instituto de Geofísica

Una vez presentada la problemática de los años anteriores de la red de cómputo de este Instituto, ahora es conveniente aclarar como esta conformado el backbone de Red-UNAM y a su vez, como es alimentado el Instituto de Geofísica a partir de él.

1.2.1.- Backbone de RedUNAM

La Universidad Nacional Autónoma de México en 1989 inicia nuevos proyectos enfocados al área de telecomunicaciones creándose así la Dirección de Telecomunicaciones, cuyo objetivo era establecer la Red Integral de Telecomunicaciones de la UNAM, red capaz de transmitir voz, datos, imágenes y posteriormente video entre las dependencias universitarias, ubicadas desde Ensenada, B.C. hasta Puerto Morelos, Q. Roo.

Los objetivos principales de esta red son:

- Integrar a sus alumnos, desde el bachillerato hasta el posgrado, a la cultura informática, entendida esta como la integración del cómputo y las telecomunicaciones.

- Incorporar la enseñanza de la informática a los planes formales de estudio de todas las disciplinas y actualizarla periódicamente.

- Proporcionar a su personal docente y de investigación todas las herramientas de la tecnología informática para el desarrollo de sus actividades.

- Dotar a la institución de una moderna infraestructura de telecomunicaciones y cómputo.

- Utilizar esta herramienta como un factor de transformación profundo en su modelo de enseñanza aprendizaje.

Al tiempo que se desarrolla la primera etapa, en el año 1989, se instala una red nacional privada satelital conformada por 7 estaciones terrenas para la transmisión de voz y datos. Paralelamente se sustituye el sistema telefónico en el campus de Ciudad Universitaria por una red de conmutadores telefónicos digitales que paulatinamente se incrementa para incorporar a los siete campus de las unidades multidisciplinarias distribuidas en el área metropolitana.

En el campus de Ciudad Universitaria inicia un proceso acelerado de crecimiento en su red de datos con una topología de anillo en el backbone de FDDI a 10 Mbps. En este momento la UNAM es la primera Institución latinoamericana en conectarse a Internet y es el principal protagonista del Internet en México.

A finales de 1992, esta red contaba ya con 31 nodos de cómputo y telecomunicaciones enlazados a través de fibra óptica, vía satélite o vía microondas y se destaca la incorporación de la Ciudad de la Investigación Científica en Cuernavaca, Morelos. El servicio de Internet es uno de los recursos más utilizados por los investigadores de la UNAM. Internet se ofrece también a universidades públicas y privadas en el país.

En junio de 1997 la infraestructura de telecomunicaciones tenía más de 15,000 computadoras conectadas a la Red de datos, más de 10,000 líneas del sistema telefónico digital, 20 salas de videoconferencia y 5 enlaces internacionales con capacidad de transmisión de 10 Mbps a los Estados Unidos de Norteamérica para la conexión a Internet. En esta fecha, el campus de Juriquilla, Qro. se integra a esta gran Red.

En agosto de 1997 la UNAM inicia operaciones con un backbone ATM que le permite consolidar con esta tecnología las redes de voz, datos y vídeo en una plataforma multimedia *figura 1.7.* En esta fecha se coloca la Institución como una de las redes más modernas y más grandes en el ámbito académico en Latinoamérica al contar con esta moderna tecnología y comparada incluso con redes de Universidades de Norteamérica.

En el año de 1998 se incorpora el campus Morelia en Michoacán. Actualmente, más del 96 % del total de las instalaciones de la Universidad están integradas a la Red con 21,500 computadoras conectadas, más de 13,000 líneas telefónicas en operación y 36 salas propias de videoconferencia que forman parte de la Red Nacional de Videoconferencia integrada por un total de 130 salas. Se tienen en operación 13 enlaces con capacidad de 25 Mbps para el tráfico de Internet y 1 Mbps para el tráfico de videoconferencia del tipo H.320.

Es importante destacar que la Red Integral de Telecomunicaciones es completamente privada y propiedad de la UNAM y es operada en su totalidad por personal de la Dirección de Telecomunicaciones.

Debido a la importancia que ha adquirido la Red Integral de Telecomunicaciones en la actualidad, como medio de comunicación indispensable en el trabajo universitario para el acceso e intercambio de información, se hace imprescindible contemplar la actualización de la tecnología bajo la idea de satisfacer las necesidades de crecimiento.

Asimismo, se emprenden actividades que sopesan la sofisticación y funcionamiento óptimo de la red, como es el migrar a la tecnología ATM (Asynchronous Transfer Mode) la red medular.

El diseño, la administración y la operación de la red se realizan bajo la supervisión de personal altamente calificado.

Así la Subdirección de Redes se encarga de la coordinación del mantenimiento y operación de la red universitaria de datos, Red-UNAM, abarcando los aspectos técnicos y administrativos. Analiza y en su caso dicta los lineamientos a seguir en la operación y evolución de la misma red.

Actualmente en la Universidad realiza un rediseño del backbone de Red-UNAM con el cual se obtendrán grandes beneficios para la comunidad universitaria y el país, así como para encontrarse a la vanguardia utilizando las tecnologías emergentes para esta época tal es el caso de Gigabit Ethernet, así como muchas otras. Además de la implantación de los proyectos IPv6 e Internet2, en los cuales se llevan grandes avances gracias a las pruebas realizadas por el Departamento de Operación de la Red de la Dirección de Telecomunicaciones.

1.2.2.- Esquema general de la Red de Cómputo del Instituto de Geofísica.

El enlace que llega del backbone de Red-UNAM al Instituto de Geofísica se da de la siguiente manera *figura 1.8.*

- Existe una delta redundante que es el backbone de Red-UNAM que interconecta equipos Passport de Nortel Networks con tecnología ATM. Cada uno de estos equipos se encuentran en los sites de DGSCA, IIMAS y Zona Cultural. El ancho de banda con la que se interconectan estos equipos son mediante enlaces tipo OC-3 (155 Mbps).

- Directamente conectado a cada uno de los Passport existe un equipo Cellplex 7000 de 3Com con protocolo LAN Emulation. La velocidad de interconexión es igualmente mediante enlaces OC-3 y estos equipos a su vez reparten el enlace hacia otros equipos mediante tecnología Ethernet a velocidades de 10 y 100 Mbps.

- Cada uno de los Cellplex alimenta a switches capa 2 y 3, algunos que alimentan directamente a algunas dependencias y otros que sirven de distribución. En el caso del Cellplex ubicado en IIMAS, este alimenta a un switch de capa 3 (Lanplex 2500 de 3Com) ubicado en el Instituto de Geografía mediante un enlace en 100 FX (100 Mbps en fibra óptica).

- El Lanplex 2500 del Instituto de Geografía cuenta con 4 slots de los cuales sólo 2 están ocupados. El primer slot tiene un puerto a 100 FX que es donde se recibe el enlace del Cellplex ubicado en IIMAS; el segundo slot cuenta con una tarjeta con 8 puertos en 10 FL (10 Mbps en fibra óptica). Dos de estos puertos son ocupados para alimentar la red de cómputo del Instituto de Geofísica, uno para el Edificio Principal y el segundo para el Edificio Anexo.

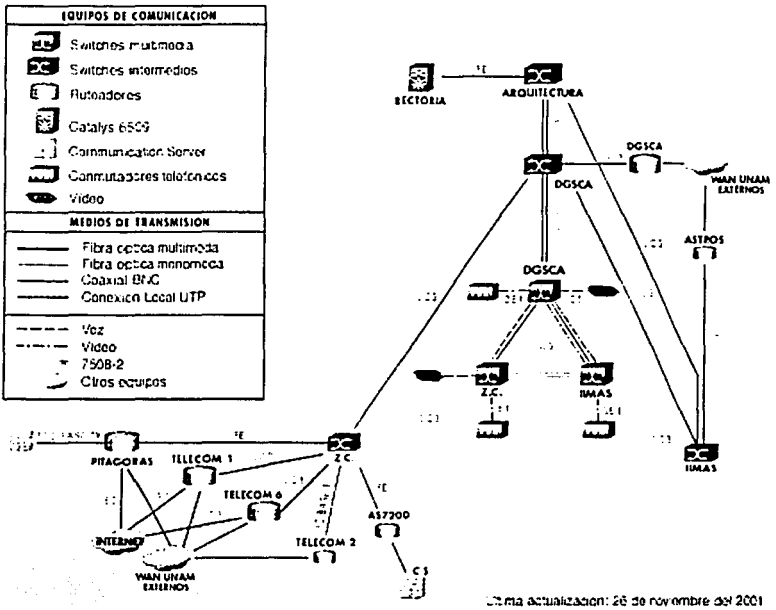


Figura 1.7. Backbone de Red-UNAM

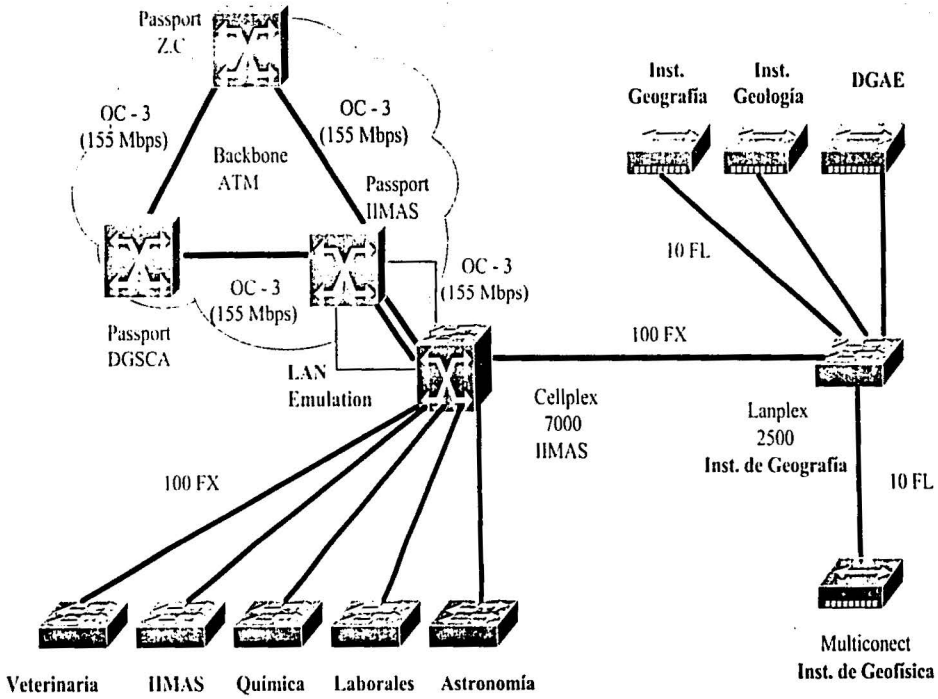


Figura 1.8.- Esquema general de la red de cómputo del Instituto de Geofísica.

1.3.- Problemática Actual

El Administrador general de la red de cómputo del Instituto de Geofísica de la Universidad Nacional Autónoma de México, solicitó a la Dirección General de Servicios de Cómputo Académico (DGSCA) un mayor ancho de banda debido a que esta dependencia tiene contemplado en un futuro realizar diversas aplicaciones en Internet 2; como efecto de esta solicitud se realizó una reunión en el Departamento de Operación de la Red de DGSCA, en la que se acordó llevar a cabo un análisis de su red, con el objeto de poder observar su comportamiento tomando en cuenta su diseño y ver si cumple con los requerimientos mínimos necesarios para poder soportar un enlace mayor.

El administrador del Instituto había reportado una disminución considerable en el rendimiento de su red, el cual incluía los siguientes datos:

- Demasiada lentitud en las velocidades de transferencia de información, esto se refleja en la comunicación entre sus equipos, así como en las aplicaciones que están compartidas entre usuarios, en comparación al rendimiento observado en meses anteriores.

- Demasiada lentitud en las velocidades de transferencia de información hacia el exterior, esto se observa en los enlaces internacionales, así como en los servicios de correo, en resumen un deficiente desempeño de la red.

Una vez expuesta la problemática detectada por el administrador de la red de cómputo del Instituto de Geofísica, entonces ahora es conveniente el comenzar a detallar la estructura de la red de cómputo de cada uno de los edificios que conforman al Instituto, para posteriormente identificar las deficiencias en su red de cómputo basándose en los conceptos, normatividad y teorías presentadas en los posteriores capítulos.

Para un mejor estudio de la red de cómputo del Instituto, se procederá a detallarlo por edificios, posteriormente por pisos y/o segmentos.

1.3.1.- Estudio del diseño general

En los momentos en que se comenzó a realizar el análisis del Instituto de Geofísica contaba con la siguiente infraestructura en su red de cómputo:

- Un enlace 10 FL hacia Red-UNAM a través de una Fibra Óptica Multimodo en el Edificio Nuevo

  - El enlace llega a un hub con un puerto en fibra óptica 10 FL y un puerto en cable par trenzado (UTP); en el segundo puerto sale un cable que se conecta a un switch marca 3Com, modelo 3900 con 36 puertos a 10/100 Mbps en UTP. En este switch sale un cable que alimenta a un hub con 2 puertos en Telco, que alimenta a 24 computadoras más.

- Un segundo enlace llega al Edificio Principal a través de un Fibra Óptica 10 FL que es recibida en un Transceiver, el cual esta a su vez conectado a un Multiconect (hub de cable Coaxial) marca 3Com con 6 puertos.

  - El primer puerto es quien recibe el enlace de Red-UNAM.
  - Un segundo puerto alimenta a un hub ubicado en la Secretaría Administrativa.
  - El tercer puerto alimenta a un segmento en cable coaxial que alimenta al Departamento de Geomagnetismo y Lugis.
  - Un cuarto puerto alimenta al Servicio Sismológico Nacional.
  - El quinto puerto alimenta a un transceiver de AUI a fibra óptica 10 FL, dicha fibra va hacia un tercer edificio al Departamento de Física Espacial, donde es recibida en un transceiver de fibra óptica (10 FL) a AUI que se conecta a un Multiconect.
  - El sexto puerto alimenta mediante cable coaxial a un hub con puertos a 10/100 Mbps, el cual alimenta a un switches con 2 puertos en Gigabit y 24 puertos a 10/100 Mbps, que a su vez alimenta a otro switch con 8 puertos en Gigabit. Este último distribuye la conexión hacia los otros pisos en el Edificio Principal. De un puerto del switch se alimenta al edificio donde se ubica la Biblioteca mediante un transceiver de UTP a fibra óptica 10 FL, la cual es recibida en un transceiver del mismo tipo, conectando el UTP a un conjunto de hubs.

1.3.2.- Servicios y servidores principales

El Instituto de Geofísica por ser una dependencia donde se concentran un gran número de investigadores y personal y por tener 4 edificios, concentra un gran número de servicios que satisfacen igual a un estudiante, a un investigador o a una secretaria. Este gran número de servicios tienen una diversidad de formas tales como:

- Impresión en red.
- Digitalización impresión en plotter.
- Digitalización de documentos e imágenes.
- Correo electrónico.
- Páginas WEB.
- Consulta de bases de datos.
- Almacenamiento y grabación de información.
- y naturalmente, servicios de monitoreo de las diversas aplicaciones que se ejecutan en el Instituto.

Dentro de los servidores que sirven de alojo para almacenar y/o dar el servicio de soporte de las aplicaciones anteriores, tenemos principalmente plataformas UNIX, LINUX y las diversas modalidades de Windows. A continuación se muestra una pequeña lista de la cantidad de servidores que existen por aplicación:

- 7 servidores acceso remoto (RAS).
- 12 servidores WEB.
- 11 servidores de correo electrónico.
- 4 servidores de impresión.
- 6 servidores de aplicación (consulta de bases de datos, FTP, etc).

1.3.7.- Estadísticas del funcionamiento de la red de cómputo

Como se comentó anteriormente el administrador del Instituto había reportado una disminución considerable en el rendimiento de su red, el cual incluía: demasiada lentitud en las velocidades de transferencia de información y demasiada lentitud en las velocidades de transferencia de información hacia el exterior, esto se observa en los enlaces internacionales, así como en los servicios de correo.

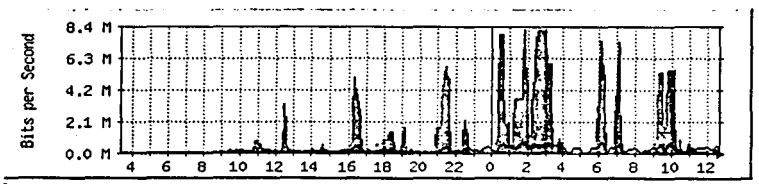
Con el fin de corroborar los informes del administrador de la red del Instituto, se procedió a analizar la red de cómputo del Instituto con una herramienta de monitoreo llamada MRTG (Multi Router Traffic Graphic), la cual arrojó los siguientes resultados:

Análisis de Tráfico

Segmentos:	132.248.6.0 y 132.248.182.0
Dependencia:	Instituto de Geofísica
Velocidad:	20 Mbits/seg (2 puertos de 10 Mbits/seg)
Administrador:	Centro de Asistencia Técnica
Equipo:	CoreBuilder 3com 2500. Módulo 3, Puertos Ethernet 1 y 5
IP:	132.248.254.230

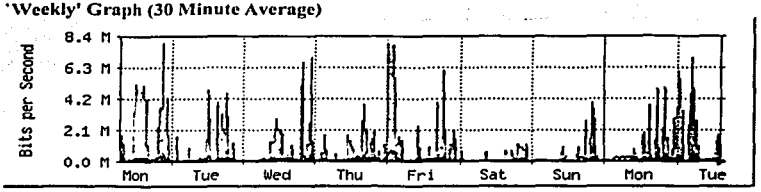
The statistics were last updated **Tuesday, 14 March 2000 at 14:31**

Daily' Graph (5 Minute Average)



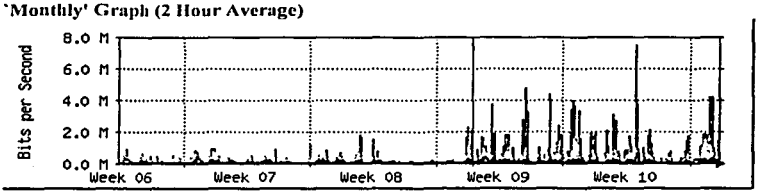
Max In:	7568.6 kb/s (75.7%)	Average In:	1315.1 kb/s (13.2%)	Current In:	256.7 kb/s (2.6%)
Max Out:	682.0 kb/s (6.8%)	Average Out:	171.6 kb/s (1.7%)	Current Out:	154.0 kb/s (1.5%)

'Weekly' Graph (30 Minute Average)



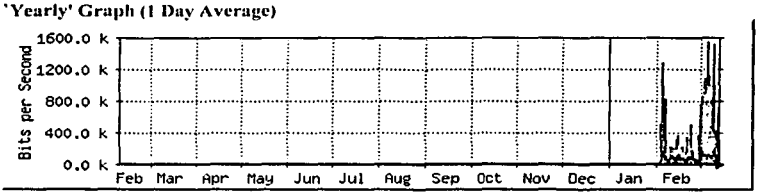
Max In:	8008.8 kb/s (80.1%)	Average In:	985.3 kb/s (9.9%)	Current In:	1812.0 kb/s (18.1%)
Max Out:	689.9 kb/s (6.9%)	Average Out:	112.5 kb/s (1.1%)	Current Out:	316.9 kb/s (3.2%)

'Monthly' Graph (2 Hour Average)



Max In:	7542.4 kb/s (75.4%)	Average In:	525.5 kb/s (5.3%)	Current In:	1454.8 kb/s (14.5%)
Max Out:	628.9 kb/s (6.3%)	Average Out:	92.6 kb/s (0.9%)	Current Out:	190.0 kb/s (1.9%)

'Yearly' Graph (1 Day Average)



Max In:	1561.3 kb/s (15.6%)	Average In:	509.2 kb/s (5.1%)	Current In:	721.4 kb/s (7.2%)
Max Out:	190.8 kb/s (1.9%)	Average Out:	88.0 kb/s (0.9%)	Current Out:	147.9 kb/s (1.5%)

Incoming Traffic in Bits per Second
BLUE ### Outgoing Traffic in Bits per Second

Como se puede observar en las gráficas anteriores, el porcentaje de utilización de la red de cómputo del Instituto de Geofísica rebasa el umbral entre el 30% y 40 % que es el recomendado para que una red tipo Ethernet funcione adecuadamente. Es decir, que la red no sea propensa a colisiones ni errores.

En la primera gráfica se muestra el comportamiento diario del 14 de marzo del 2000, se observa que hay un pico en el porcentaje de tráfico interno de un 75.7 % y un promedio diario de 2.6 %.

La gráfica semanal indica que durante los días hábiles de la semana las condiciones de la red fueron semejantes. En la tercera gráfica se observa que se esta en la tercera semana en la cual esta presente el mismo problema, es decir, un 75.4 % de utilización de la red; mismo problema que se muestra en la gráfica anual.

Una vez observado el reporte anterior se decidió realizar un análisis profundo y a conciencia del comportamiento y de la estructura de la red de cómputo del Instituto de Geofísica con el fin de solucionar los problemas presentados.

1.4.-Perspectivas a futuro.

Una vez tomada la decisión de realizar un análisis profundo del comportamiento de la red del Instituto y teniendo la información sobre la estructura de la misma, lo que sigue ahora es prever el crecimiento de la red, así como las necesidades de equipamiento para las aplicaciones que correrán bajo Internet 2.

1.4.1.-Plan de crecimiento de la red de cómputo

Actualmente en el Instituto se cuentan con 3 segmentos de red:

- Segmento 132.248.6.x con 254 direcciones disponibles y 254 utilizadas.
- Segmento 132.248.182.x con 254 direcciones disponibles y 190 utilizadas.
- Segmento 192.200.100.x con 10 direcciones disponibles y 10 utilizadas.

Esto nos da un total de alrededor de 454 PC's con dirección IP utilizadas, sin embargo según informes del administrador de la red, se cuentan con alrededor de por lo menos 600 PC's en total, distribuidas en los 4 edificios que conforman en Instituto.

Según los reportes del personal del Instituto, anualmente se adquieren 50 PC's entre nuevas adquisiciones y por sustitución; lo que nos hace prever que para los próximos 3 años (primer semestre del 2004), el Instituto contará con por lo menos 800 PC's distribuidas en los 4 edificios. Esto nos sirve para contemplar la estructura que se le dará al nuevo diseño de la red con el fin de que soporte el equipo actual y que a su vez sea capaz de crecer de acuerdo a las necesidades del Instituto.

1.4.2.-Necesidades de equipamiento para las aplicaciones en Internet 2

Internet 2 surge como una necesidad de Universidades e Instituciones dedicadas a la Investigación de crear una red paralela a Internet con el fin de no competir por el ancho de banda con las aplicaciones comunes. Dicha red tendría un mayor ancho de banda para correr las aplicaciones realizadas por estas Instituciones.

El ancho de banda necesario para esta nueva red requeriría de velocidades de transferencia mayores a 100 Mbps, por lo que Gigabit Ethernet representa una solución adecuada. Considerando lo anterior, las necesidades de equipamiento para soportar aplicaciones que corran bajo Internet 2 son:

- Switches con interfaces en gigabit ethernet.
- PC's con procesadores lo suficientemente rápidos para procesar las aplicaciones que se crearán.
- Tarjetas de red que serán las encargadas de comunicar las PC's con los equipos de interconexión y
- Un cableado estructurado que tendrá que tener enlaces en Gigabit para conectar los switches con las PC's.

Capítulo II

Marco Teórico.

CAPÍTULO II: MARCO TEÓRICO

Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras, así como a la puesta en órbita de los satélites de comunicación.

Durante los últimos años, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez.

A mediados de los ochenta, miles de empleados de oficinas dispersas en una amplia área geográfica empezaron a llevar sus propias computadoras personales al trabajo para ejecutar el nuevo software comercial escrito para PC, además esperaban tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. Cuando los empleados empezaron a intercambiar discos flexibles y a mantener sus propias bases de datos, las compañías empezaron a tener grandes problemas para conservar la integridad de sus datos. Las empresas también se dieron cuenta de que necesitaban idear sistemas más rápidos y flexibles para competir en el mercado. El costo y tamaño de las macrocomputadoras y minicomputadoras se convirtió en un problema en este ambiente. Las redes de computadoras ofrecen una solución a este problema.

2.1.-Conceptos básicos de red de computadoras

2.1.1.- Definición de red de computadoras

Es un conjunto de computadoras conectadas mediante una o más vías de transmisión. La red existe para cumplir un determinado objetivo: la transferencia e intercambio de datos entre computadoras y terminales. Permiten compartir recursos.[1]

Una red es un sistema de interconexión entre computadoras que permite compartir recursos e información. Para ello, es necesario contar, además de las computadoras correspondientes, con las tarjetas de red, los cables de conexión, los dispositivos periféricos y el software apropiado.[2]

Una red de computadoras es un sistema de comunicación de datos, que enlaza dos o más computadoras y dispositivos periféricos, con el fin de compartir información y recursos. Una red consta de tarjetas de interfaz de red, cables y software. En cada sistema se instala una tarjeta de interfaz de red y los sistemas se interconectan mediante cables.

[1] Ulyses Black, Redes de computadoras, protocolos, normas e interfaces, p.1

[2] José Luis Raya, Redes Locales y TCP/IP, p.1

Así mismo se instala software de comunicación de red, que permite que los usuarios y las aplicaciones accedan a la misma e intercambien información, con los demás sistemas conectados a ella.

2.1.1.1 Ventajas del uso de las redes

Las redes de computadoras ofrecen varias ventajas para la administración de una organización, que son importantes destacar:

- *Accesibilidad*: proporcionan acceso a los miembros de la organización a una Base de Datos Institucional, donde se registran los eventos y hechos importantes que ocurren a la empresa, no importando el lugar donde se realicen.

- *Seguridad*: en una red podrán participar solamente quienes tengan autorización para ello y el tipo de actividades que podrán hacer (consultar, registrar, modificar, borrar, etc.) podrá ser definido por la organización.

- *Eficiencia y Eficacia*: las redes podrán permitir eliminar operaciones repetitivas dentro de los procesos de una organización e, incluso, innovar los procesos mismos, generando valor agregado e incrementando la fuerza de la organización.

- *Ahorros*: una red podrá permitir a la organización disminuir sus inversiones en equipos periféricos y programas al permitir compartir el uso de impresoras, lectores de CD, grabadoras de CD y programas mediante el uso de licencias.

2.1.2 Estructura de una red de computadoras

La siguiente figura muestra un sencillo sistema de comunicación de datos. El proceso de aplicación es la aplicación que maneja el usuario final. Habitualmente es un programa de computadora. En la *figura 2.1* el nodo A podría ejecutar un programa de aplicación (AP_{A1}) en forma de programa para acceder al proceso de aplicación en el nodo B (que es en este caso, el programa [AP_{B1}] y una base de datos). La figura también muestra el programa en el nodo B (AP_{B2}) que accede a un archivo en el nodo A mediante un programa de aplicación (AP_{A2}).

La aplicación reside en el equipo terminal de datos o DTE. DTE es un término genérico para designar a la máquina de usuario final, habitualmente una computadora o una terminal.

La finalidad de las redes de computadoras es conectar DTE de tal forma que puedan compartir recursos, intercambiar datos, apoyarse entre sí y permitir a los usuarios realizar su trabajo desde lugares geográficamente remotos.

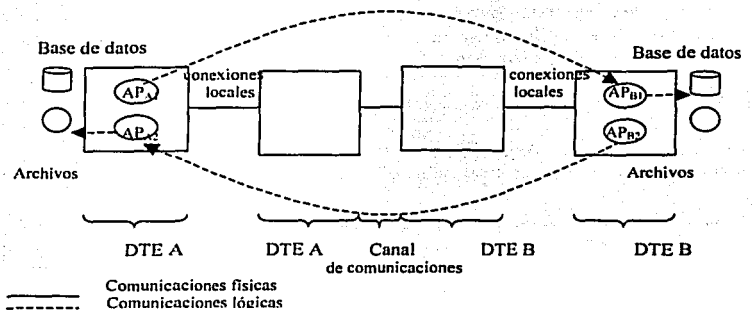


Figura 2.1 Esquema general del sistema de comunicación de datos.

En la *figura 2.1* podemos ver que una red proporciona comunicaciones lógicas y físicas entre las terminales y computadoras conectadas. Las aplicaciones y archivos emplean el canal físico para realizar comunicaciones lógicas. En este contexto, lógica significa que los DTE no necesitan saber nada de los aspectos físicos del proceso de la comunicación.

2.1.3 Clasificación de las redes de computadoras

2.1.3.1 Redes de Área Local (LAN)

Una red de área local LAN puede definirse como un sistema de comunicaciones que proporciona interconexión a una variedad de dispositivos en un área restringida (recinto, edificio, campus...) y que no utilizan medios de telecomunicaciones externos.[3]

En esta definición hay cuatro elementos significativos:

- Sistema de comunicaciones, es decir, conjunto de elementos cuyo objetivo es el intercambio de información entre dispositivos.
- Dispositivo, en sentido amplio, es decir, cualquier nodo de red, desde un gran procesador a un ordenador personal, pasando por estaciones de trabajo, clusters de terminales, impresoras, etc.
- El ámbito geográfico de una red de área local es reducido, generalmente se restringe a un único edificio o a un conjunto de ellos, como recinto industrial o campus.
- La propiedad de los medios de comunicación privada, lo que permite una flexibilidad en la fijación de las normas respecto a los medios y a los métodos de comunicación.

[3] Matt Hall, Aprendiendo Redes en 24 Hrs. , p 11

Una red de área local o LAN es la distinción organizacional menos compleja de las redes de computadoras. Una LAN no es más que un grupo de computadoras enlazadas a través de una que se encuentra en un solo lugar.[4]

Las LAN's tienen los siguientes parámetros:

- Ocupan tan sólo un lugar físico.
- Pueden ser redes punto a punto o redes cliente / servidor.

Una LAN es una red de datos, tolerante a fallas, que cubre un área geográficamente relativamente pequeña. Por lo general conecta estaciones de trabajo, computadoras personales, impresoras y otros dispositivos. Las LANs tienen muchas ventajas para los usuarios de computadoras, entre otras el acceso compartido a dispositivos y aplicaciones, el intercambio de archivos entre los usuarios conectados y la comunicación entre los usuarios.[5]

2.1.3.2 Redes de Área Metropolitana (MAN)

Una red de área metropolitana MAN es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos. Este tipo de redes se utiliza normalmente para interconectar redes de área local.

2.1.3.3 Redes de Área Extensa (WAN)

La interconexión de áreas extensas o amplias es la conexión de multiples LANs que se encuentran geográficamente separadas.

Esto se logra conectando las diferentes LANs utilizando servicios que incluyen líneas de teléfono dedicadas (punto a punto), o de discado tanto sincrónicas como asincrónicas, vínculos satelitales, y servicios de transporte de paquetes.

Una WAN es una red de comunicaciones de datos que tiene una cobertura geográfica relativamente grande y suele utilizar las instalaciones de transmisión que ofrecen compañías portadoras de servicios como las telefónicas. [6]

[4] Matt Hall, Aprendiendo Redes en 24 Hrs., p. 12
[5] Steve Spanier, Tecnologías de Interconectividad de Redes, p.38
[6] Steve Spanier, Tecnologías de Interconectividad de Redes, p.45

Distancia entre procesadores	Procesadores Localizados en el mismo:	Ejemplo:
0.1m	Tarjeta de Circuito	Flujo de datos en la Máquina
1m	Sistema	Multicomputadora
10m	Cuarto	
100m	Edificio	LAN
1km	Campus	
10km	Ciudad	MAN
100km	País	WAN
1000km	Continente	
10,000km	Planeta	Internet

Tabla 2.1 Clasificación de procesadores interconectados por distancia.

2.1.4 Circuitos Multipunto y punto a punto

Los equipos terminales de datos (DTE) y los equipos de terminación del circuito de datos (DCTE) pueden conectarse de dos formas. En la *figura 2.1*, los equipos están conectados en configuración "punto a punto", en la cual sólo existen dos dispositivos DTE por cada línea o canal de comunicación. En la *figura 2.2* aparece un método distinto, la configuración "multipunto", en la cual hay más de dos dispositivos conectados a un mismo canal.

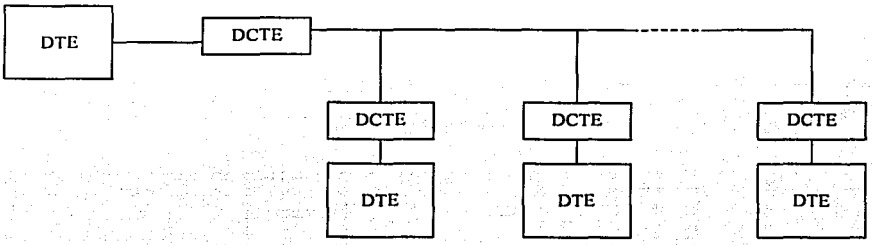


Figura 2.2 Conexión Multipunto.

2.1.5 Tipos de transmisión

2.1.5.1 Simplex

Este tipo de transmisión de emplea cuando los datos se van a transmitir sólo en una dirección, por ejemplo, en un sistema de asentamiento de datos en el que un dispositivo de vigilancia devuelve una lectura a intervalos regulares a la instalación de recolección de datos.

2.1.5.2 Semiduplex

Éste se da cuando los dos dispositivos interconectados desean intercambiar información (datos) en forma alternada; por ejemplo, si uno de los dispositivos devuelve datos sólo en respuesta a una solicitud del otro. Los dos dispositivos deben ser capaces de conmutar entre los modos de enviar y recibir después de cada transmisión.

2.1.5.3 Dúplex Integral

Transmisión en ambos sentidos a la vez (bidireccional simultánea). Hasta ahora se han empleado los términos dúplex y Semiduplex para describir el movimiento de los datos a través del circuito. En los siguientes diagramas vemos los circuitos físicos propiamente dicho, sin tomar en cuenta como se mueven los datos.

En comunicaciones telefónicas se utilizan con frecuencia los términos pares y cuadretes para describir el circuito que compone el canal. Los circuitos de pares se conocen como Semiduplex. Un hilo sirve para transmitir datos y el otro es línea de retorno eléctrico, como se ve en la *figura 2.3. Donde ETD es equipo terminal de datos y ETCD equipo de terminación de circuito de datos y ECD equipos de conmutación de datos.*

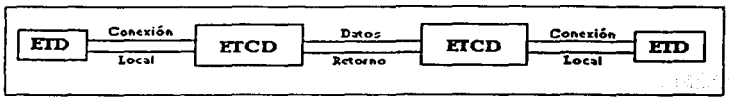


Figura 2.3 Circuito de dos hilos o Semiduplex.

Los circuitos de cuatro hilos se conocen como circuitos dúplex. Incluyen dos pares de hilos cada uno, dos de los hilos transmiten los datos y los otros dos cierran los correspondientes circuitos como se observa en la *figura 2.4.*

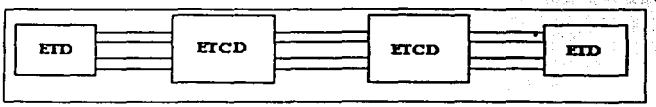


Figura 2.4 Circuito de cuatro hilos o dúplex.

Para las compañías telefónicas un enlace de dos hilos suele corresponder a un circuito telefónico conmutado normal, mientras que un circuito de 4 hilos suele ser una línea alquilada no conmutada. Las ventajas de las redes de comunicaciones que hemos visto hasta ahora, no podrían hacerse realidad sin un componente muy importante del sistema. Se trata de los equipos de conmutación de datos, cuya función principal es conmutar o encaminar los datos del usuario hasta su destino final a través de la red.

El ECD proporciona las funciones vitales de encaminamiento por la red, evitando los dispositivos y canales ocupados o fuera de servicio. Asimismo, el ECD puede dirigir los datos hacia su destino final a través de componentes intermedios, que pueden ser, a su vez, otros equipos de conmutación. En la *figura 2.5* se observa un sencillo esquema de organización de ECD, ETCD y ETD en una red.

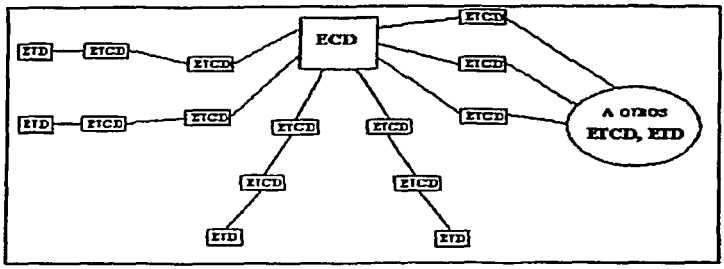


Figura 2.5 Organización de los ETD, ETCD y los ECD.

Éste se usa cuando los datos deben intercambiarse entre los dos dispositivos conectados en ambas direcciones al mismo tiempo; por ejemplo, cuando por razones de rendimiento los datos pueden fluir en ambas direcciones de manera independiente.

2.2 Topologías

Topología es el arreglo físico de los nodos y el medio de transmisión dentro de una estructura de red corporativa.[7]. La topología de una red de área local define la distribución de cada estación en la relación a la red y a las demás estaciones.

En términos de conectividad de redes, una topología no es más que la disposición de una red. La topología puede referirse a la disposición física de la red o la disposición lógica de la red. Las topologías lógicas establecen las reglas del camino para la transmisión datos. [8]

2.2.1 Topología Estrella

En la topología de estrella en todas las estaciones están conectadas mediante enlaces bi-direccionales a un nodo central, que asume las funciones de gestión (administración) y control de las comunicaciones proporcionando un camino entre dos dispositivos que deseen comunicarse *figura. 2.6.*

[7] Steve Spanier, Tecnologías de Interconectividad de Redes, p.657
[8] Matt Hall, Aprendiendo Redes en 24 Hrs., p.14

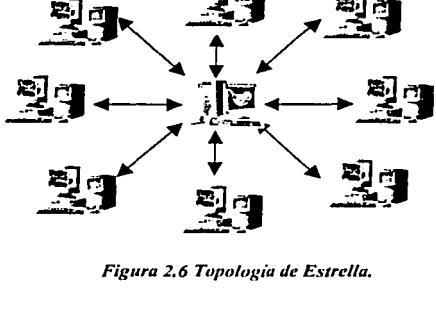


Figura 2.6 Topología de Estrella.

2.2.2 Topología en Bus

En esta topología las estaciones se conectan a un único medio bidireccional lineal o bus con puntos de terminación bien definidos. Cuando una estación transmite, la información se propaga a ambos lados del emisor hacia todas las estaciones conectadas al bus hasta llegar a los puntos de terminación donde la señal es absorbida; de aquí que el bus reciba también el nombre de canal de difusión, *figura 2.7.*

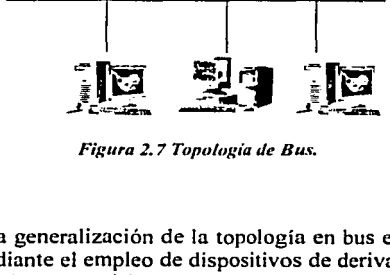


Figura 2.7 Topología de Bus.

2.2.3 Topología en Árbol

La topología en árbol es una generalización de la topología en bus en la que el cable se desdobla en varios ramales mediante el empleo de dispositivos de derivación, *figura 2.8* Al igual que la topología en Bus, las transmisiones se propagan por cada ramal de la red y llegan a todas las estaciones.

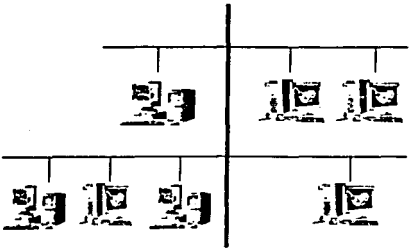


Figura 2.8 Topología de Árbol.

2.2.4 Topología en Anillo

El anillo consiste en una serie de repetidores conectados entre sí mediante un único enlace de transmisión unidireccional formando un camino cerrado.

Los datos se transfieren secuencialmente, bit a bit, de un repetidor al siguiente a lo largo del anillo. Cada repetidor regenera y retransmite cada bit, los repetidores constituyen un elemento activo de la red. Su principal función es contribuir al correcto funcionamiento del anillo, realizando los servicios de inserción, recepción y eliminación de información. Cuando una estación recibe información destinada a ella, la incorpora a la memoria; en caso contrario la hace circular hasta la próxima estación, *figura 2.9.*

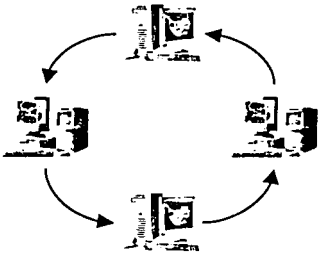


Figura 2.9 Topología de anillo.

2.3 Modelo de referencia OSI

La Organización Internacional de Estandarización (ISO: International Standard Organization) desarrolló un modelo de referencia para las arquitecturas de sistemas. Le llamó OSI: Open System Interconection. Este modelo es estratificado y en estructura de 7 capas.

En el concepto de OSI, un sistema es un conjunto de una o más computadoras, el software asociado, los periféricos, las terminales, los operadores humanos, los procesos físicos, los medios de transferencia de información, etc., que forman un ente autónomo con capacidad de realizar el procesamiento de la información. El modelo de referencia OSI constituye el marco de trabajo para el desarrollo de protocolos estándares para la comunicación entre dos capas homónimas ubicadas en equipos separados. Los formatos y protocolos para la comunicación de capas adyacentes *dentro de un sistema* no serían estandarizados.

A continuación se describen cada una de las capas que componen el modelo OSI:

1. *Capa de control de interconexión física.* Provee las características mecánicas, eléctricas, funcionales y de procedimiento, necesarias para establecer, mantener y liberar conexiones físicas entre el dispositivo terminal y el punto de conexión a la red, o entre dos dispositivos terminales.

2. *Capa de control de enlace de datos (DLC).* La capa DLC provee la conexión lógica a través de la línea, el direccionamiento, el secuenciamiento y la recuperación de errores.

   Existe una dirección de enlace que identifica una conexión de enlace en la capa DLC.

   En esta capa (DLC: Data Line Control), se determina el uso de una disciplina de comunicaciones conocida como HDLC (High – Level Data Link Control), éste es un protocolo de línea. Los datos se organizan en tramas. La trama es un encuadre de los datos según un formato.

   Por lo tanto, juntando las funciones de las capas 1 y 2, se tiene la forma de conectar físicamente dos nodos adyacentes y de transferir un mensaje de datos entre ellos, manejando direccionamiento, control de errores, etc., según se especifica en HDLC.

3. *Capa de control de red.* Esta capa provee el control entre dos nodos adyacentes. Dos conexiones se proveen: punto a punto o en red. Una o más conexiones de red pueden ser ubicadas en la misma conexión de enlace y se distinguen por sus direcciones.

4. *Capa de Transporte.* Las funciones proporcionadas por este estrato incluye el ruteo de los mensajes, las notificaciones de errores y opcionalmente la segmentación y el bloqueo. La utilidad de esta capa puede ser vista como de "dirección del control entre los puntos de conmutación", más que como una proveedora de ayuda para la transferencia de datos entre estos puntos.

5. *Capa de control de sesión.* Provee el soporte para interacciones entre entidades que cooperen en la Capa de Presentación. Las funciones de la capa de sesión se pueden dividir en dos categorías:

- Determinación y cancelación de contrato entre dos entidades de la Capa de Presentación (esto se llama Servicio de Administración de Sesión), y
- Control del intercambio de datos, entre esas dos entidades, comprendiendo sincronización, delimitación y recuperación de operaciones con los datos (esto se llama Servicios de Diálogo de Sesión).

Una sesión se identifica por "identificadores de destino final". Se han definido tres tipos de interacciones:

- Dos vías simultáneas,
- Dos vías alternadas, y
- Una vía.

6. *Capa de servicios de presentación.* Proporciona un conjunto de servicios de conversión y descifrado que la Capa de Aplicación (7) puede seleccionar, para poder interpretar el significado de los datos intercambiados. El modelo identifica tres ejemplos de protocolos en la capa 6:

   - Protocolos de terminal virtual,
   - Protocolos de archivo virtual y
   - Protocolos de transferencia de trabajos y manipulación.

   Otra de las cosas que puede incluirse en esta capa es la conversión de código.

7. *Capa de Aplicación.* Todas las otras capas existen en función de brindar soporte a ésta. Una aplicación se compone de procesos cooperantes que se intercomunican mediante el uso de los protocolos definidos en esta capa. Estos procesos de aplicación son la fuente y el destino último de los datos intercambiados.

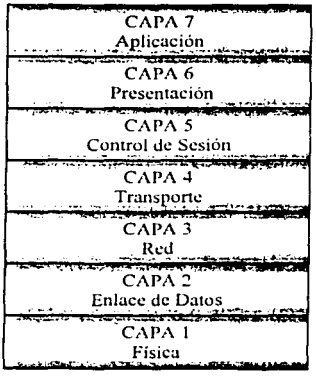


Figura 2.10: Modelo OSI.

2.4 Medios de transmisión

La transmisión es el mecanismo por el cual una red envía señales eléctricas. El método y la calidad de transmisión determinan si la estación de datos puede entender y procesar, o si recibe "basura electrónica" y debe solicitar una retransmisión.

Muchos de los métodos de transmisión más ampliamente utilizados hoy en día fueron desarrollados en sus orígenes para transmitir voz como parte de la red telefónica, utilizando incicialmente el tipo de transmisión analógica ("Transmisión Analógica: es el intercambio de un tipo de señal donde la información esta codificada en las diferencias de amplitud y frecuencia que ésta maneja, pudiendo ser periódica o no periódica"[9]). Conforme fue creciendo la demanda de conexiones, se fueron adaptando estos sistemas de transmisión de voz para transmitir datos. También se desarrollaron sistemas de transmisión especialmente para transmisión de información digital ("Transmisión Digital: en esta transmisión el intercambio de información está codificada entre dos niveles fijos de tensión, también llamados niveles lógicos y que son básicamente trenes de pulsos. Al igual que en la transmisión analógica las señales pueden ser periódicas o no periódicas"[10]).

El componente fundamental de cualquier sistema de transmisión es el medio de transmisión. "Este es el material a través del cual viajan las señales de datos"[11]. Existen 2 categorías generales de medios de transmisión, restringidos (medios guiados) y no restringidos (medios no guiados).

Par trenzado, cable coaxial y cable de fibra óptica son los medios restringidos (las señales viajan dentro de los límites del cable). Las transmisiones a través de microondas o vía satélite viajan a través del aire, el cual no tiene límite, es decir las señales se transmiten a través del aire o algún gas desde el emisor hasta el receptor; estos son los medios no restringidos.

Los medio de transmisión no restringidos son utilizados principalmente para transmisión de larga distancia entre edificios. A pesar de ello, la transmisión por infrarrojos y otros métodos de transmisión sin cables que utilizan medios de transmisión no restringidos (el aire) están empezando a ser más utilizados para transmisión de corta distancia dentro de los edificios.

Los medios de transmisión de cobre, como el par trenzado, son probablemente los medios de transmisión más comunes dentro de edificios (aunque el cableado de fibra óptica está empezando a ser más habitual). Es más, la interfaz entre medios de transmisión de corta distancia y medios de transmisión de larga distancia es normalmente cobre.

A continuación se describen los principales medios de transmisión tanto restringidos como no restringidos:

[9] Diccionario Técnico Larousse p. 621
[10] Diccionario Técnico Larousse p. 621
[11] Teré Parnell, Redes de Área Extensa Serie LAN Times, p.51

2.4.1 Cable Coaxial

Hay dos tipos de cable coaxial que se utiliza con frecuencia, uno de ellos es el cable de 50 ohms, que se utiliza para transmisión digital, en tanto que el otro tipo, el cable de 75 ohms se utiliza en la transmisión analógica.

2.4.1.1 Cable Coaxial de Banda Base (B. Angosta)

El cable coaxial de banda base (50 ohms) consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante al que, a su vez, lo rodea un blindaje de hoja de metal. Alrededor del blindaje de hoja de metal, hay un conductor tejido rodeado por otro blindaje de hoja de metal que, también, está cubierto por un conductor tejido. La parte externa del cable tiene una cubierta protectora (*Figura 2.11*). Entre sus principales características están:

- Transmiten una señal digital simple.
- No hay modulación de frecuencia.
- Diseñados primariamente para comunicaciones de datos, pero pueden correr aplicaciones de voz (no en tiempo real) y se transmite voz en forma digital.
- Es un medio pasivo donde la energía es provista por las estaciones del usuario.
- Uso de enchufes especiales para conexión física.
- Se conectan al transmisor - receptor: transceptor (transceiver).
- Se usa una unidad de interconexión a la red independiente o integrada, para conectar la estación del usuario a la red.
- Alcance de 1 a 10 km.
- Con el uso de repetidores, se largan las distancias de transmisión.
- Generalmente usado con topología de canal (bus) lineal; árbol y anillo.
- Una red típica contiene 200 a 1000 dispositivos.
- Ancho de banda de 10 Mbps.
- Poca inmunidad a los ruidos. Puede mejorarse con filtros.
- El ancho de banda puede transportar solamente un 40% de su carga para permanecer estable.

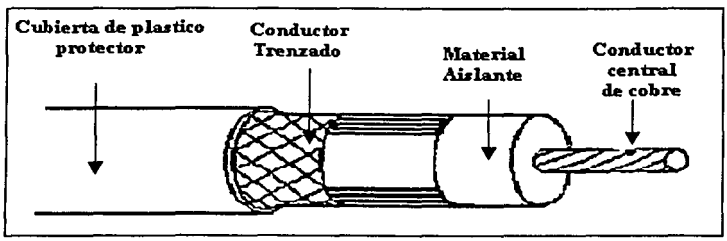


Figura 2.11 Estructura del Cable Coaxial.

2.4.1.2 Cable coaxial de banda ancha

El cable coaxial de banda ancha (75 ohms) emplea la transmisión analógica en el cableado que se utiliza comúnmente para el envío de la señal de televisión por cable. Aunque el término "banda Ancha" proviene del medio telefónico, en el cual se refiera a frecuencias superiores a los 4 Khz, el significado de este término en el medio de redes de computadoras se asocia a las redes de cables utilizados para la transmisión analógica. Físicamente ambos tipos de cables tienen la misma estructura. Otras características de este cable son:

- Se combina voz, dato y video simultáneamente.
- Se permite voz y video en tiempo real.
- Se considera un medio activo ya que la energía se obtiene de los componentes de soporte de la red y no de las estaciones de los usuarios conectados.
- Se usan amplificadores y no repetidores.
- Debido a los amplificadores y al alto número de canales, se pueden conectar hasta 25000 dispositivos con un alcance de 5 Km.
- Topologías: canal y árbol.
- Ancho de banda máximo: 400 MHz. Pueden transportar el 100% de su carga.
- Mejor inmunidad a los ruidos que la banda base.

2.4.2 Cable par trenzado

Este es el medio de transmisión más antiguo y aún el más utilizado. Este consistía en un principio en 2 alambres de cobre aislados, aunque ahora varía el número de pares por cable. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor.

Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre, entre otras cosas.

Actualmente casi todo el cable de cobre en redes Ethernet es el de pares trenzados sin apantallar (UTP, Unshielded Twisted Pair); más raramente se emplea el de pares trenzados apantallado (STP, Shielded Twisted Pair) o también cable coaxial. Esto no se debe a las virtudes del cable UTP, que es peor que el STP o el coaxial para transmitir datos debido a su elevada atenuación a altas frecuencias, sino a la necesidad de utilizar un cable de bajo costo que permita un cableado integral de voz y datos.

2.4.2.1 Categorías de cable par trenzado

Las normativas de cableado estructurado más conocidas son la TIA/EIA 568-A y la ISO/IEC 11801 *ver capitulo III*. Las dos coinciden en lo esencial, pero tienen pequeñas diferencias. Cuando se diseña un cableado es posible y conveniente cumplir ambas simultáneamente, ya que de esta forma se asegura la máxima compatibilidad con los

fabricantes. Una característica común a todos los sistemas de cableado estructurado es que la longitud máxima del enlace con cable UTP es de 100m.

La norma TIA/EIA 568-A clasifica los cables UTP en categorías de acuerdo con sus características para la transmisión de datos, las cuales vienen fijadas fundamentalmente por la densidad de trenzado del cable (número de vueltas por metro) y los materiales utilizados en el recubrimiento aislante. Conforme sube la categoría aumenta la densidad de trenzado, disminuye la atenuación y mejora la propagación de señales de alta frecuencia. Por otro lado, dado un cable cuanto mayor es la frecuencia mayor es la atenuación. Para cada categoría la norma especifica valores límite (máximos o mínimos, según el caso) de la atenuación y varios otros parámetros característicos del cable para un rango de frecuencias hasta una considerada la máxima utilizable para esa categoría. En la *tabla 2.2* aparecen las categorías actualmente especificadas o en curso de especificación, y las frecuencias máximas correspondientes:

Categoría	Frecuencia Máxima (Mhz)	Vueltas /Metro	Tipo Cable	Tipo Conector	Uso Ethernet (Mbps)
1	-	0	UTP	RJ-45	-
2	1	0	UTP	RJ-45	1
3	16	10-16	UTP	RJ-45	10-100
4	20	16-26	UTP	RJ-45	10-100
5	100	26-33	UTP	RJ-45	100
5e	100	-	UTP	RJ-45	1000
* 6	250	-	UTP	RJ-45	4000
* 7	600	-	STP	-	10000
Las categorías 6 y 7 aún no son normas oficiales.					

Tabla 2.2: Categorías de los cables de pares trenzados

Realmente las categorías 1 y 2 no forman parte de la norma, se han puesto por completar la tabla (se podría decir que son 'sub-normales'); de hecho no son UTP en sentido estricto, ya que carecen de trenzado. Actualmente están aprobadas las categorías 3, 4, 5 y 5e (Enhanced) que en realidad no es una categoría nueva sino una versión mejorada de la 5, puesto que no modifica la frecuencia máxima (aunque sí cambia los valores límite de los parámetros, e incluso añade otros nuevos).

Las normas evolucionan con el tiempo, y con ellas la especificación de las categorías, por lo que cuando se dice que una instalación está certificada categoría 5, por ejemplo, es importante saber la versión de la norma utilizada en la certificación. Las versiones actualmente vigentes de las normas TIA/EIA 568-A e ISO/IEC 11801 son de 1995. Una instalación certificada con referencia a una versión anterior podría no ser conforme con la norma actualmente vigente.

Hoy en día los cables más utilizados son categoría 5 y 5e; la diferencia de precio entre ambos es pequeña, y los costos de instalación similares, por lo que en instalaciones nuevas es aconsejable utilizar cable 5e.

Mientras que la especificación de la categoría 5e esta recién terminada, las categorías 6 y 7 se encuentran aun en discusión, y las últimas previsiones son de que su aprobación aun puede tardar varios años. Se estima que la categoría 6 llevará al límite las posibilidades del cableado UTP, por lo que será necesario utilizar cable STP para la categoría 7. Es de esperar que el cable categoría 6, cuando se produzca en grandes cantidades, sea sólo un poco más caro que el de categoría 5 ó 5e (como ocurre actualmente con la categoría 5e y 5 frente a las 3 y 4); en cambio el elevado costo de fabricación e instalación del cable categoría 7 STP, comparable ya al de la fibra óptica, lo hace poco atractivo para el usuario final, por lo que es previsible que cuando se aprueben las nuevas categorías el cable predominante sea el categoría 6.

La clasificación en categorías, además de aplicarse a cables aislados se aplica a instalaciones; a menudo sucede que una instalación hecha con cable categoría 5 no puede funcionar al máximo rendimiento debido a que la instalación no fue hecha con el suficiente cuidado: errores comunes son por ejemplo destrenzar una longitud excesiva en los conectores, apretar demasiado las bridas o doblar excesivamente el cable. En principio podría ser que una instalación categoría 5 cumpla sin más los requisitos de la categoría 5e. Para saberlo habría que recertificar toda la instalación de acuerdo con la norma 5e; alternativamente se puede aplicar una técnica de muestreo, por ejemplo probar un 10% de los cables (preferiblemente los más largos) y extrapolar los resultados, o certificar en particular aquellos cables en los que vayamos a conectar equipos Gigabit Ethernet. Se estima que entre un 5% y un 10% de las instalaciones categoría 5 no soportarán Gigabit Ethernet, debido fundamentalmente a problemas relacionados con los conectores

2.4.3 Fibra óptica

Este medio de transmisión se basa en la transmisión de información mediante pulsos de luz. Un pulso de luz puede utilizarse para indicar un bit de valor 1; la ausencia de un pulso indicará la existencia de un bit de valor 0. La luz visible tienen una frecuencia de alrededor de 10^8 Mhz, por lo que el ancho de banda de un sistema de transmisión óptica tiene un gran potencial.

Un sistema de transmisión óptica tiene 3 componentes: el medio de transmisión, la fuente de luz y el detector. El medio de transmisión es una fibra ultradelgada de vidrio o silicio fundido. La fuente de la luz puede ser un LED (Diodo Emisor de Luz), o un diodo láser; cualquiera de los dos emite pulsos de luz cuando se le aplica una corriente eléctrica. El detector es un fotodiodo que genera un pulso eléctrico en el momento en el que recibe un rayo de luz. Al colocar un LED o un diodo láser en el extremo de la fibra óptica, y un fotodiodo en el otro, se tiene una transmisión de datos unidireccional que acepta una señal eléctrica, la convierte y la transmite por medio de pulsos de luz y, después, reconvierte la salida en una señal eléctrica, en el extremo receptor.

Por propiedades propias de este medio de transmisión el haz de luz que viaja por este medio se refracta y queda atrapado en el interior de la fibra y puede propagarse a lo largo de varios kilómetros sin tener ninguna pérdida.

Hoy en día existen dos tipos de fibras ópticas, las que permiten la transmisión de más de un modo de ondas de luz, llamadas fibras Multimodo, y las que permiten la propagación de un sólo modo, fibras Monomodo.

2.4.3.1.- Fibra multimodo

Este tipo de fibra generalmente opera en las ventanas de 850 nm y 1300 nm, y es recomendada para usos en transmisión de datos, voz y video, en distancias no superiores a los tres kilómetros. Su alta apertura numérica y el diámetro de su núcleo, permiten una fácil conexión y el uso de emisores de luz de mayor ancho espectral, por lo cual, la fibra multimodo es una solución de bajo costo para transmisiones en cortas distancias.

Las fibras ópticas multimodo se dividen en:

Fibra óptica de índice escalonado (step index)

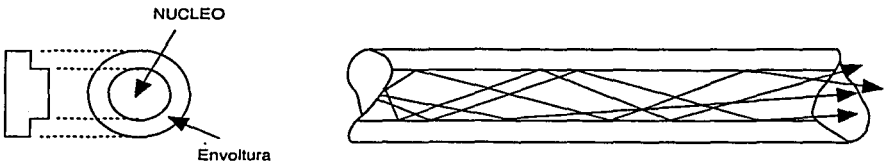


Figura 2.12 Fibra óptica de índice escalonado (step index).

En este tipo de fibra (*figura 2.*12), el núcleo tiene un índice de refracción constante, lo que produce que la distancia total recorrida por el rayo luminoso sea ligeramente diferente para cada modo, lo cual trae como consecuencia que estos lleguen al receptor con un desface en el tiempo, limitando así la frecuencia y la distancia a la cual es posible mandar estos impulsos.

Los diámetros usuales del núcleo de este tipo de fibra varía de 100 mm a1000 mm.

Fibra óptica de índice variable (graded index)

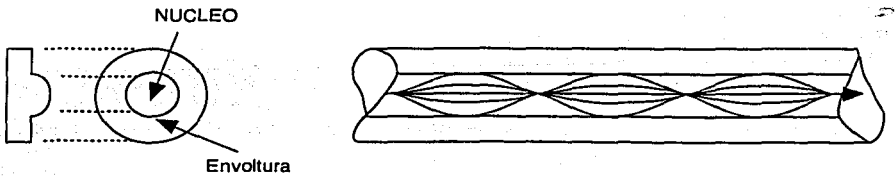


Figura 2.13 Fibra óptica de índice variable (graded index).

En esta familia de fibras (*figura 2.13*), el índice de refracción del núcleo disminuye en forma radial, produciendo que los modos que recorren una mayor distancia se aceleren a medida que se acercan a la envoltura del núcleo, mientras que los que viajan en forma mas recta, lo hacen a menor velocidad debido a la menor densidad, permitiendo así, que los tiempos de desplazamiento para las distintas formas de propagación tiendan a igualarse, disminuyendo la dispersión modal.

Los diámetros usuales del núcleo de este tipo de fibra son 50 mm, 62.5 mm y 100 mm.

2.4.3.2.- Fibra monomodo

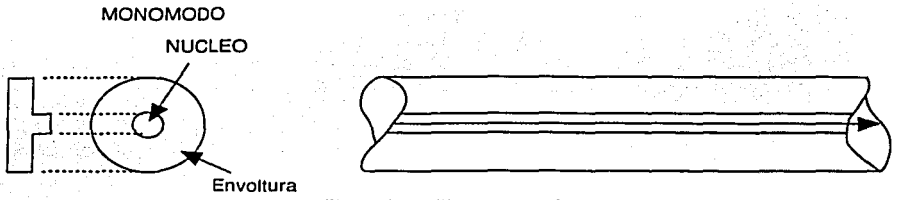


Figura 2.14 Fibra monomodo.

La fibra óptica monomodo (*figura 2.14*), se caracteriza por el pequeño diámetro de su núcleo, aproximadamente 8 micrones, el cual al ser muy cercano a la longitud de onda utilizada, permite que sólo un modo sea transmitido por la fibra, eliminándose así el problema de sobreposición modal.

Estas características, si bien hacen que la fibra óptica monomodo sea de alta capacidad de transmisión de datos y baja atenuación, haciéndola especialmente adecuada para transmisiones en sistemas de gran distancia, también traen como consecuencia una importante reducción en su apertura numérica, debiendo utilizarse fuentes emisoras de bajo ancho espectral, en general emisores láser.

2.4.4 Microondas

2.4.4.1 Microondas Terrestres

En un sistema de microondas se usa el espacio aéreo como medio físico de transmisión. La información se transmite en forma digital a través de ondas de radio de muy corta longitud. Pueden dirigir múltiples canales a múltiples estaciones dentro de un enlace dado, o pueden establecerse enlaces punto a punto.

Las estaciones consisten de una antena tipo plato y de circuitos que interconectan la antena con la terminal del usuario. La transmisión es en línea recta y por lo tanto se ve afectada por accidentes geográficos, edificios, bosques, mal tiempo, etc. El alcance promedio es de 40 km en la tierra.

Una de las ventajas importantes es la capacidad de poder transportar miles de canales de voz a grandes distancias a través de repetidores, a la vez que permite la transmisión de datos en su forma natural.

El uso de luz infrarroja se puede considerar muy similar a la transmisión digital con microondas. El haz infrarrojo puede ser producido por un láser o un LED. Los dispositivos emisores y receptores deben ser ubicados a la vista uno del otro. Velocidades de transmisión de hasta 100 Kbps pueden ser soportadas a distancias de hasta 16 kms. reduciendo la distancia a 106 km, se puede alcanzar 1.5 Mbps.

La conexión es punto a punto. El uso de esta técnica tiene ciertas desventajas. El haz infrarrojo es afectada por el clima, interferencia atmosférica y por obstáculos físicos. Como contrapartida, tienen inmunidad contra el ruido magnético o sea, la interferencia eléctrica.

2.4.4.2.- Microondas Satelitales

El satélite de comunicaciones es un dispositivo que actúa principalmente como reflector de las emisiones terrenas. Se podría decir, que es una extensión al espacio del concepto de torre de microondas. Al igual que éstas, los satélites reflejan un haz de microondas que transportan información codificada. Realmente, la función de reflexión se compone de un receptor y un emisor, que operan a diferentes frecuencias: recibe a 6 Ghz y envía (refleja) a 4 Ghz, por ejemplo.

Físicamente, los satélites giran alrededor de la Tierra en forma sincrónica con ésta a una altura de 35680 Km, en un arco directamente ubicado sobre el ecuador. Esta es la distancia requerida para que un satélite gire alrededor de la Tierra en 24 horas, coincidiendo entonces con la vuelta completa de un punto en el ecuador. Esta es la característica que en definitiva determina el objetivo geoestacionario que tienen los satélites de comunicaciones.

El espacio o separación entre 2 satélites de comunicaciones, es de 2880 kms equivalente a un ángulo de 4°, visto desde la Tierra. La consecuencia inmediata es que el número de satélites posibles a conectar de esta forma, es finito.

2.5 Protocolos de Comunicación

2.5.1 Protocolos de control de acceso al medio

2.5.1.1 Round Robin

Esta técnica es basada en la filosofía de darle a cada cual 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

2.5.1.2 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 periodo indefinido. La reservación de ranuras puede llevarse a cabo de una manera distribuida o centralizada.

2.5.1.3. Contención

Con esta técnica no se ejerce el control para determinar que estación tiene derecho a transmitir. Todas las estaciones contienen por el tiempo. Esta técnica es necesariamente distribuida. Las técnicas que han sido adoptadas para ser utilizadas en topologías de bus y árbol son:

- CSMA/CD Carrier Sense 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 topologías de anillo son:

- Token Ring (control token).
- Anillo ranurado (slotted ring).

2.5.1.4. CSMA/CD

CSMA/CD, es el acrónimo de Carrier Sense Multiple Access/Collision Detect. Esto quiere decir que Ethernet sensa el medio para saber cuando puede acceder, e igualmente detecta cuando sucede una colisión (por ej. cuando dos equipos trasmiten al mismo tiempo). Ethernet se soporta sobre una estructura física en BUS.

El sistema de detección de colisiones es una modificación del sistema ALOHA, usado por la Universidad de Hawai años atrás. En el sistema ALOHA, se intento comunicar múltiples estaciones ubicadas en diferentes islas a través de radio. Cuando dos estaciones trasmiten, y se sobreponen sus transmisiones, hay UNA COLISION y las estaciones deben de retransmitir la señal. Este principio lo retomo CSMA/CD. Aquí lo que se hace es sensar el medio físico(el cable) y "mirar" cuando puedo entrar(o sea cuando puedo transmitir). Esto es el Carrier Sense, o sea mirar si hay una portadora sobre el medio. Si no hay portadora puedo trasmitir, pero puede ocurrir que alguna estación ya halla trasmitido y por retardo en la red algún equipo(en un extremo por ejemplo) no se haya dado cuenta. Si el equipo que no se ha enterado trasmite, existirá una colisión.

Cuando la colisión es detectada, ambos equipos dejan de trasmitir, e intentaran trasmitir de nuevo en un tiempo aleatorio, que dependerá del tipo de Persistencia de CSMA/CD.

2.5.1.5. 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 al 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 una estructura 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 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 las estaciones activas conectadas al medio físico, proveen un fundamento para la inicialización y la recuperación de la conexión del anillo lógico y de la pérdida de la señal token.

Aunque las funciones de monitoreo son normalmente efectuadas entre todas las estaciones sobre el medio, solo una estación a la vez 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

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 de 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 transmitir. 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.

2.5.2. TCP/IP Protocolos de la capa de red y de transporte

La arquitectura del TCP/IP a menudo se llama la arquitectura del Internet, debido a que el TCP/IP e Internet están entrelazados de manera muy próxima. Las normas fueron desarrolladas por la Defense Advanced Research Projects Agency (DARPA); y finalmente pasada a la Internet Society.

Internet fue propuesta originalmente por la precursora de la DARPA, llamada Advanced Research Projects Agency (ARPA), como un método para probar la viabilidad de las redes de intercambio de paquetes. (Cuando el interés de la ARPA se volvió de naturaleza militar, se cambió el nombre). Durante su ocupación en el proyecto, ARPA previó una red de líneas arrendadas, conectadas por nodos interruptores. La llamó ARPANET y los nodos interruptores se llamaron Internet Message Processors (Procesadores de Mensajes entre Redes) o IMP.

El registro remoto y la transferencia de archivos remota fueron puestos en práctica en un protocolo llamado Network Control Program (NCP; Programa de Control de la Red). Más tarde, se agregó el correo electrónico por medio de File Transfer Protocol (FTP). Junto con los registros remotos y transferencia de archivo del NCP, conformaron los servicios básicos para ARPANET.

Para 1973, era claro que NCP era incapaz de manejar el volumen de tráfico y la funcionalidad nueva propuesta. Se comenzó un proyecto para desarrollar un nuevo protocolo. Las arquitecturas TCP/IP y gateway (equipo de compuerta de enlace) fueron propuestas por primera vez en 1974. El artículo publicado por Cerf y Kahn describía un sistema que proporcionaba un protocolo de aplicación estandarizada que además, usaba reconocimientos de extremo a extremo.

Cerf y Kahn sugirieron que el nuevo protocolo fuera independiente de la red y el hardware de computadoras subyacentes. Además, propusieron una conectividad universal a través de la red. Estas dos ideas fueron radicales en un mundo de hardware y software patentados, debido a que permitirían participar en la red a cualquier tipo de plataforma. El protocolo se elaboró y se conoció como TCP/IP.

En 1981 se estandarizó el TCP/IP versión 4 para ARPANET. En 1982, TCP/IP sustituyó al NCP como el protocolo dominante de la red creciente, la cual ahora estaba conectando máquinas a lo largo del continente.

2.5.2.1 IP: Protocolo de Internet (Protocolo de Interconexión de Redes)

El IP es un protocolo que pertenece al nivel de red, por lo tanto, es utilizado por los protocolos del nivel de transporte como TCP para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando.

Suponiendo que el protocolo TCP ha sido el encargado de manejar el datagrama antes de pasarlo al IP, la estructura del mensaje una vez tratado quedaría así *figura 2.15.*

Cabecera IP (20 byte)	*Cabecera TCP (20 byte)*	*Datos*

Figura 2.15 Estructura de un mensaje con protocolo TCP/IP.

La cabecera IP tiene un tamaño de 160 bit y está formada por varios campos de distinto significado. Estos campos son:

Versión: Número de versión del protocolo IP utilizado. Tendrá que tener el valor 4. Tamaño: 4 bit.

Longitud de la cabecera: (Internet Header Length, IHL) Especifica la longitud de la cabecera expresada en el número de grupos de 32 bit que contiene. Tamaño: 4 bit.

Tipo de servicio: El tipo o calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. Tamaño: 8 bit.

Longitud total: Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bit, el tamaño máximo del datagrama no podrá superar los 65.535 bytes, aunque en la práctica este valor será mucho más pequeño. Tamaño: 16 bit.

Identificación: Valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño: 16 bit.

Flags: Indicadores utilizados en la fragmentación. Tamaño: 3 bit.

Fragmentación: Contiene un valor (offset) para poder ensamblar los datagramas que se hayan fragmentado. Está expresado en número de grupos de 8 bytes (64 bit), comenzando con el valor cero para el primer fragmento. Tamaño: 16 bit.

Límite de existencia: Contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en una red correctamente diseñada, no debe descuidarse esta posibilidad. Tamaño: 8 bit.

Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bit.

Comprobación: El campo de comprobación (checksum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia. Tamaño: 16 bit.

Dirección de origen: Contiene la dirección del host que envía el paquete. Tamaño: 32 bit.

Dirección de destino: Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bit.

2.5.2.2 TCP: Protocolo de control de transmisión

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño, y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

La cabecera de un datagrama contiene al menos 160 bit que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. Para evitar todos estos problemas el TCP numera los datagramas antes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.

2.5.3 Protocolo de resolución de direcciones: ARP

El protocolo ARP (Address Resolution Protocol), es el encargado de convertir las direcciones IP en direcciones de la red física

El funcionamiento del protocolo ARP es bastante simple. Cuando una máquina desea enviar un mensaje a otra máquina que está conectada a través de una red ethernet se encuentra con un problema: la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP.

Este protocolo utiliza una tabla denominada *tabla de direcciones ARP*, que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Si la dirección solicitada se encuentra en esta tabla el proceso se termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la dirección física de la máquina destino.

Si la dirección buscada no esta en la tabla el protocolo ARP envia un mensaje a toda la red. Cuando un ordenador reconoce su dirección IP envía un mensaje de respuesta que contiene la dirección física. Cuando la máquina origen recibe este mensaje ya puede establecer la comunicación con la máquina destino, y esta dirección física se guarda en la Tabla de direcciones ARP.

2.5.4 Protocolo de réplica de resolución de direcciones: RARP

El protocolo RARP (Reverse Address Resolution Protocol) se utiliza cuando, al producirse el arranque inicial, los ordenadores no conocen su dirección IP.

Requiere que existan en la red, al menos, un servidor RARP. Cuando un ordenador desea conocer su dirección IP envía un paquete que contiene su propia dirección física.

El servidor RARP, al recibir el paquete, busca en su tabla RARP la dirección IP correspondiente a la dirección física inicial indicada en el paquete y envía un paquete al ordenador origen con esta información.

A diferencia del protocolo ARP que se incorpora normalmente en todos los productos TCP/IP, el protocolo RARP sólo se incorpora en unos pocos productos.

2.5.5 Servicios de Telnet, FTP, Mail

2.5.5.1 Telnet

Telnet es un servicio de conexión remota que nos permite la conexión a un ordenador remoto dentro de una red, y usarlo como si nuestro terminal estuviera directamente contectado con el mismo.

La conexión remota que se establece entre dos ordenadores vía telnet se efectúa gracias al protocolo telnet, que es uno de los protocolos del conjunto TCP/IP.

Telnet utiliza el sistema cliente-servidor. Para utilizar telnet debemos disponer de un programa telnet en nuestro ordenador (cliente), con el cual se accederá al ordenador remoto (servidor). Telnet convierte al ordenador cliente en un terminal del ordenador servidor, con lo que se permite utilizar los servicios que el ordenador remoto facilita a sus terminales. Con telnet el ordenador cliente se usa como un terminal (como si sólo fuera un teclado y una pantalla), por ello a los programas clientes telnet se les denomina programas de emulación de terminal.

Existen muchas terminales diferentes por lo que los programas telnet deben ser capaces de soportar las características de varios de ellos. En función del tipo de terminal que emule el programa telnet podemos hablar de dos variedades:

- Telnet. Para VT's de DEC, line-mode (VT100, VT220...). Es el más común. El URL de los servicios que emplean este sistema comenzará por telnet://

- tn3270. Versión especial de telnet con un emulador 327x de IBM, para sus aplicaciones full-screen. El URL de los servicios que emplean tn3270 será tn3270://

A través de telnet nos podemos conectar tanto a ordenadores en los cuales se tenga cuenta (login y password), es decir, de los que seamos usuarios, como a máquinas que ofrezcan servicios públicos disponibles para cualquier usuario (en los cuales sólo se requerirá un login que será público). Durante la conexión a la máquina remota deberemos expresar la dirección del ordenador remoto (su nombre de dominio o dirección IP), el login (nombre de usuario) y el password.

2.5.5.2 Protocolo de Transferencia de Archivos (FTP)

El Protocolo de Transferencia de Archivos (FTP) permite a un archivo de un sistema copiarse a otro sistema. En realidad el usuario no se registra como un usuario completo en la máquina a la que se desea tener acceso, como Telnet, en su lugar usa el programa FTP para permitir el acceso. Una vez más son necesarias las autorizaciones correctas para proporcionar acceso a los archivos. Para poder realizar esta operación es necesario conocer la dirección IP (o el "nombre") de la máquina a la que nos queremos conectar para realizar algún tipo de transferencia

Una vez que se ha establecido la conexión con una máquina remota, FTP permite copiar uno o más archivos a la máquina de uno. (El término *transferir* implica que el archivo se mueve de un sistema a otro, pero el original no se afecta. Los archivos se copian.) FTP es un servicio usado en forma amplia en Internet, así como en muchas LAN y WAN grandes.

2.5.5.3 Servicio de correo electrónico

El correo electrónico (electronic mail o email) es una utilidad que permite enviar (o recibir) mensajes a cualquiera de los usuarios de la Red en el mundo. Las ventajas del correo electrónico sobre el correo convencional o las llamadas telefónicas son enormes.

La inmediatez es una de ellas; a diferencia de una carta de papel que puede demorar varios días, un mensaje de correo electrónico enviado a través de Internet llega en pocos minutos.

El bajo costo es otro de sus atributos; en contraste con el elevado precio de las llamadas de larga distancia internacional, un usuario de Internet puede enviar todos los mensajes que quiera a cualquier lugar del mundo sin tener que pagar dinero adicional por ello (solo paga al proveedor de acceso a Internet por el tiempo que este conectado a la Red).

Una última cualidad del correo electrónico es la de ser un mecanismo asíncrono, es decir, que no requiere la intervención del emisor y el receptor al mismo tiempo; el primero lo envía cuando lo considere pertinente y el segundo lo lee cuando así lo quiera.

2.5.6 Principales Protocolos de Redes de IBM y Microsoft

2.5.6.1 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.

2.5.6.2 NetBIOS

Se utiliza para controlar las sesiones de usuario y gestionar partes de la LAN. Se ocupa de realizar muchas funciones asociadas con los niveles de red, de transporte y de sesión del modelo de referencia OSI. Se puede configurar como orientado o no orientado a conexión, y puede realizar operaciones de encaminamiento de fuente.

2.5.7 Principales protocolos de Netware

2.5.7.1 IPX: Capa de red

IPX (Intercambio de Paquetes de Red) es el protocolo original de la capa de red (Capa 3), utilizado para rutear paquetes por una red. IPX es un protocolo de red no orientado a la conexión que se basa en datagramas y, como tal, es semejante al Protocolo Internet que está en las redes TCP/IP.

IPX utiliza los servicios de un protocolo de ruteo vectorial de distancia dinámica (RIP [Protocolo de Información de Ruteo]) o un protocolo de ruteo basado en estado de enlaces (NLSP [Protocolo Basado en Estado de Enlaces de Netware]). El RIP de IPX envía actualizaciones de ruteo cada 60 segundos. A fin de realizar decisiones de ruteo de óptima trayectoria, el RIP de IPX utiliza un "pulso" como medida, que en un principio es el retardo esperado cuando se utiliza una longitud particular. Un pulso tiene una duración de 1/8 de segundo. En el caso de dos trayectorias cuyo conteo de pulso sea idéntico, el RIP de IPX utiliza el conteo de saltos para romper el empate. (Un salto se define como el paso de un paquete a través de un ruteador.) El RIP de IPX no es compatible con las implantaciones de RIP que se utilizan en otros ambientes de red.

Igual que en otras direcciones de red, las direcciones de IPX de Netware deben de ser únicas. Estas direcciones se representan en formato hexadecimal y constan de dos partes: un número de red y un número de nodo. El número de red de IPX, que es asignado por el administrador de red, tiene una longitud de 32 bits. El número de nodo, que en general es la dirección MAC (Control de Acceso a Medios) de una de las NICs (Tarjetas de Interfase de Red) del sistema, tiene una longitud de 48 bits.

El uso de una dirección MAC para el número de nodo por parte de IPX permite al sistema enviar nodos para predecir qué dirección MAC utilizar en un enlace de datos. (En contraste, puesto que la porción del anfitrión de una dirección de red en IP no tiene correlación con la dirección MAC, los nodos IP deben utilizar el Protocolo de Resolución de Direcciones [ARP] para determinar la dirección MAC destino.)

2.5.7.2 SPX: Capa de transporte

El SPX (Protocolo para el Intercambio de Paquetes en Secuencia) es el protocolo de Netware que permite que dos estaciones de trabajo se comuniquen mediante red. Este protocolo se asegura que los datos sean transferidos en secuencia y lleguen al destino pretendido. Se trata de un protocolo de la capa de transporte (Capa 4). SPX reside por encima de IPX en el conjunto de protocolos de Netware, y es un protocolo confiable, orientado a la conexión, que complementa el servicio de datagramas que ofrece el protocolo de la capa de red (Capa 3).

2.6 Equipos de comunicación

Los requisitos de longitud de cable no son limitantes para la mayor parte de las redes pequeñas. Sin embargo, si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada.

Lo bueno es que se dispone de varios dispositivos que extienden la longitud de la red. Cada uno de los dispositivos y de los métodos usados para expandir la red tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otros tipos de dispositivos para aumentar la flexibilidad y el valor. A continuación se presentan los principales equipos de comunicación entre redes:

2.6.1 Repetidor

Este es un dispositivo de la capa física (según el modelo OSI) que se utiliza para interconectar los segmentos de cable de una red extendida. En esencia, un repetidor hace posible que una serie de segmentos de cable se comporte como un solo cable. Los repetidores reciben señales de un segmento de red y amplifican, resincronizan y retransmiten esas señales hacia otro segmento de red. Estas acciones evitan el deterioro en la señal provocado por la presencia de tramos de cable de gran longitud y la gran cantidad de dispositivos conectados a la red. Los repetidores no pueden llevar a cabo un filtrado complejo ni otro tipo de procesamiento de tráfico. Además todas las señales eléctricas, incluyendo los disturbios eléctricos y demás errores, se repiten y amplifican. El total de repetidores y segmentos de red que se pueden conectar está limitado por la temporización y otros problemas.

2.6.2 Puente (Bridge)

Los puentes estuvieron disponibles en el mercado a principios de los años 80's. En ese entonces se usaban para conectar y habilitar el ruteo de paquetes entre redes homogéneas,

mas recientemente ya también el puenteo entre redes diferentes ha quedado definido y estandarizado.

Hay diferentes tipos de puenteo que han resultado ser importantes como dispositivos de interconectividad de redes. "El puenteo transparente se presenta principalmente en entornos Ethernet, en tanto que el puenteo origen ruta se utiliza sobre todo en entornos Token Ring"[12]

El puenteo de traducción da la traducción entre los formatos y los principios de tránsito de diferentes tipos de medios (generalmente, Ethernet y Token Ring). El puenteo transparente origen ruta combina los algoritmos del puenteo transparente para permitir la comunicación en entornos combinados Ethernet/Token Ring.

Los puentes pueden agruparse en categorías con base en diferentes características del producto. De acuerdo a un esquema de clasificación muy común, los puentes pueden se locales o remotos. Los puentes locales proveen una conexión directa entre múltiples segmentos de LAN en la misma área. Los puentes remotos conectan múltiples segmentos de LAN en áreas diferentes, en general, a través de líneas de telecomunicaciones.

El puenteo se presenta en el nivel de Enlace de Datos, que controla el flujo de datos, maneja los errores en la transmisión, proporciona el direccionamiento físico (a diferencia del lógico) y administra el acceso al medio físico de transmisión. Los puentes proporcionan estas funciones utilizando diferentes protocolos de la capa de Enlace de Datos que especifican algoritmos específicos para el control del flujo (los puentes revisan la dirección asociada con cada paquete de información, luego, si la dirección es la correspondiente al otro segmento de red, el puente pasará el paquete al segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del segmento de red actual, no pasará el paquete al otro lado), el manejo de errores, el direccionamiento y el acceso a medios, además de que son capaces de filtrar tramas con base en cualquiera de los campos de la Capa 2.

2.6.3 Concentrador (Hub)

El concentrador es un dispositivo de la capa Física que conecta varias estaciones de usuario por medio de un cable dedicado. Son un nodo central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella. Los concentradores son dispositivos que se encuentran físicamente alejados de cualquier nodo de la red, aunque algunos concentradores de hecho se conectan a un puerto de expansión en un nodo de red. El concentrador tiene varios puertos en su tarjeta, a los que se conecta el cable de otros nodos de red.

Pueden concentrarse varios concentradores (dependiendo de la tecnología) para permitir la conexión de nodos adicionales. Se utiliza un puerto de cada concentrador para conectarse con el siguiente. El cable empleado para conectar a los concentradores es el mismo que se usa entre el concentrador y los nodos de red, a excepción de que los alambres están traslapados entre los 2 conectores a cada extremo.

[12] . Merilee Ford, Tecnologías de Interconectividad de Redes, p 55

Muchos concentradores tienen conectores BNC en su tarjeta, además de los puertos normales RJ-45. El conector BNC permite que se enlacen concentradores por medio de un cable coaxial. Al disponer del conector BNC, no se desperdicia un puerto RJ-45 en cada concentrador para la conexión con otro concentrador. Por el contrario, ese puerto puede conectarse a un nodo de red adicional. Cada concentrador tiene al menos un puerto especial en la parte trasera para conectarse con otro concentrador mediante un cable especial; a esta forma de conexión se le conoce como apilado (stack.- donde este arreglo se ve como un solo equipo en la red). El número de concentradores que se pueden conectar varía de acuerdo al tipo de tecnología utilizada

2.6.4 Conmutador (Switch)

Los switches son dispositivos de la capa de enlace de datos que, como los puentes, permiten la interconexión de múltiples segmentos físicos de LAN en una sola red de gran tamaño. Los switches envían y distribuyen el tráfico con base en sus direcciones MAC (Control de Acceso a Medios). Sin embargo, a pesar de que la función de conmutación se lleva a cabo en hardware y no en software, es significativamente más rápida. Los switches utilizan tanto la conmutación almacenar y enviar como la conmutación rápida para reenviar el tráfico. Hay muchos tipos de switches entre los que se encuentran los switches ATM, LAN y varios tipos de switches WAN.

Los switches LAN se utilizan para interconectar segmentos múltiples de LAN. La conmutación en LAN representa una conmutación dedicada, libre de colisiones entre los dispositivos de red, que pueden soportar múltiples conversaciones simultáneas. Los switches LAN están diseñados para conmutar tramas de datos a altas velocidades.

2.6.5 Ruteadores (Routers)

Los ruteadores son semejantes a los puentes, sólo que operan a un nivel diferente. Los ruteadores requieren por lo general que cada red tenga el mismo Sistema Operativo de Red (NOS). Con un NOS común, el ruteador puede ejecutar funciones más avanzadas de las que podría permitir el puente, como conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring. Los ruteadores también suelen ser lo suficientemente inteligentes para determinar la ruta más eficiente para el envío de datos, en caso de haber más de una ruta.

La diferencia principal entre el ruteo y el puenteo es que el puenteo se presenta en la Capa 2 (Enlace de Datos) del modelo de referencia OSI, en tanto que el ruteo se presenta en la Capa 3 (Capa de Red). Esta diferencia significa que las funciones de ruteo y puenteo tendrán información diferente para utilizar durante el proceso de transferencia de información desde el origen hasta el destino; ambas funciones cumplen sus tareas en forma diferente.

La función de ruteo está formada por 2 actividades básicas: la determinación de las trayectorias óptimas de ruteo y el transporte de grupos de información (paquetes) a través de una red. En el contexto de los procesos de ruteo, a esto último se le conoce como conmutación.

2.6.6 Compuerta (Gateway)

Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de redes con otros dispositivos. Podría tenerse, por ejemplo, una LAN que consista en computadoras compatibles con IBM y otra que consista en computadoras Macintosh. En este caso, una compuerta permitiría que ambos tipos de computadoras compartieran archivos e impresoras.

2.7 Estándares y normas

Cuando la conmutación de paquetes estaba en su infancia, no trabajaba de manera muy eficiente. Las computadoras no sabían cómo evitar el envío de datos a través del cable mientras otros sistemas hacían lo mismo simultáneamente, por lo que la conectividad de redes en ese entonces era una tecnología muy ineficiente.

La red Ehernet, inventada en 1973 por Bob Metcalfe , fue una manera de solucionar las limitaciones de las redes anteriores. Se basaba en un estándar del IEEE llamado 802.3 CSMA/CD , y ofrecía formas de solucionar la situación que se presentaba cuando un gran número de computadoras trataba de transmitir a través de un solo cable de manera simultánea.

2.7.1 Ethernet

El estándar IEEE 802.3 define el protocolo de control de acceso al medio múltiple con detección de portadora y detección de colisión, CSMA/CD para la topología de Bus. Aunque la norma partió de la red Ethernet, IEEE 802.3 no son idénticos. La diferencia principal reside en la estructura de las tramas. Sin embargo si son compatibles con el medio físico.

La norma comprende, tanto el sub-nivel MAC: especificaciones de servicio y protocolo y unidades de datos, como el nivel físico: especificaciones de servicio, especificaciones independientes del medio y *especificaciones del medio físico.*

Ethernet es un sistema de hardware proporcionado para las capas de vínculos de datos y física del modelo OSI. *Como parte de los estándares de ethernet, se establecen los tipos de cable y las velocidades de difusión.*

Especificaciones dependientes del medio

En la norma IEEE 802.3 se han definido varios tipos de medios físicos de transmisión y distintas topologías para dar soluciones a las necesidades de diferentes aplicaciones. La notación utilizada para las distintas opciones es la siguiente:

<Velocidad de la red en Mbps> <Tipo de transmisión> <Máxima longitud del segmento en centares por metro>

Las opciones definidas dentro de la norma son:

2.7.2 Ethernet 802.3: Corriendo a 10 Mbps

2.7.2.1 10BASE5:Thick Ethernet

Es el estándar de cable coaxial "thick" Ethernet, durante los tempranos años 1970's. 10BASE5 deriva su nombre por contar la señalización de la MAC a 10Mbps ⇒10, transmisión en banda base ⇒10BASE, y un máximo de 500 metros de distancia entre las estaciones y un segmento ⇒10BASE5.

- 10BASE5 utiliza una topología de bus, todas las estaciones son conectadas vía un simple y continuo cable coaxial. La máxima longitud de un segmento de cable coaxial es de 500 metros, en función de la calidad del cable coaxial.
- El diámetro de una red 10BASE5 es limitada a 2500 metros, consistiendo esta de 5 segmentos de 500 metros con 4 repetidores.
- 10BASE5 utiliza una codificación Manchester para transmisión de datos.

2.7.2.1.1 Características del Cable Coaxial

El cable coaxial es de una impedancia constante. El cable es terminado en cada extremo por un adaptador ***ver 2.7.2.1.2 sección B*** y provee la ruta de transmisión para la conexión del dispositivo MAU. Los conectores del cable coaxial son usados para ser conexiones del cable a los adaptadores y entre las secciones del cable (si son necesarias). El cable tiene varios requisitos eléctricos y mecánicos que se han resuelto para asegurar una operación apropiada.

A. Parámetros eléctricos del cable coaxial

1) Características de Impedancia

La característica promedio (media) del cable coaxial es de 50 ± 2 Ω medidos en 10 MHz según IEC 60096-1:1986 y Amd.2:1993.

Las variaciones periódicas en impedancia a lo largo de una pieza única del cable pueden estar hasta ±3 Ω sinusoidal centrado alrededor del valor medio, con un periodo de menos de 2 m.

2) Atenuación

La atenuación de un segmento de cable de longitud de 500m no excederá 8.5 dB (17 dB/km) medido con una onda seno de 10 MHz, ni 6.0 dB (12 dB/km) medido con una onda seno de 5 MHz.

3) Velocidad de propagación

La velocidad mínima requerida de propagación es de 0.77C.

4) Impedancia de transferencia

El cable coaxial es capaz de proveer un suficiente blindaje para minimizar la susceptibilidad de un ruido externo y también para reducir al mínimo la generación de interferencia por medio de señales relacionadas. Mientras que la construcción del cable no se asigna por mandato, es necesario indicar una medida del funcionamiento esperada del componente del cable. El funcionamiento de los cables EMC son determinados en gran medida por la impedancia de transferencia valuada en el cable.

5) Loop

La suma de la resistencia de centro del conductor más la resistencia del blindaje, medida en 20 °C, no excederá 10 mΩ/m (*figura 2.16*)

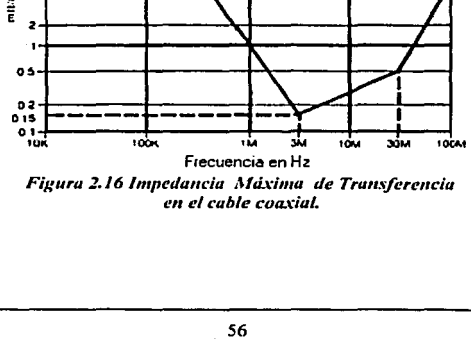


Figura 2.16 Impedancia Máxima de Transferencia en el cable coaxial.

B. Propiedades del cable coaxial

1) Requerimientos Mecánicos

El cable usado debe ser apropiado para encaminar varios ambientes, incluyéndolo, pero no limitándolo a techos caídos, a suelos levantados, y a través de un espacio abierto. El jack proveerá aislamiento entre el cable y cualquier edificio de estructura metálica .

También el cable será capaz de aceptar conectores para el cable coaxial descritos en *2.7.2.1.2.* El cable se conformará con los requisitos siguientes.

Construcción General

a) El cable coaxial consistirá en un conductor de centro, un dieléctrico, un sistema del blindaje, y jack aislador de polvo.

b) La concentricidad de los elementos del cable coaxial será mayor que 92% según lo medido de acuerdo con la configuración general siguiente:

$$\frac{\text{(jacket radius) - (center offset)}}{\text{(jacket radius}} \text{ X 100} \geq 92\ \%$$

Se asume que los valores del desplazamiento y del radio son el peor caso en cualquier punto dentro del sistema medido.

c) El jack del cable coaxial, el sistema de blindaje, y el material dieléctrico serán perforables por medio de cualquier tipo de conector especificado en ***2.7.2.1.2 sección C inciso 2*** o por una herramienta externa de la base.

d) La capacidad del sistema total de perforación del cable es un parámetro vital que afecta la confiabilidad de la conexión.

e) La habilidad para perforar el sistema del cable puede ser medido en términos de la carga de pruebas contra la firma de desplazamiento. Un cable perforable existe cuando el desplazamiento es mayor o igual 1.52 mm (0,06 in) entre la ruptura del sistema y del contacto del blindaje con centro del conductor.

f) El cable coaxial será suficientemente flexible para soportar un radio de curva de 254 milímetros (10 adentro).

2) El centro del conductor

El centro del conductor será de cobre sólido estañado o llano con un diámetro de 2.17mm ±0.013mm .

3) Material Dieléctrico

El material dieléctrico puede ser de cualquier tipo proveyendo las especificaciones anteriormente mencionadas.

4) Sistema de Blindaje

a) El sistema de blindaje puede contener ambos elementos, el trenzado y el de hoja suficientes para resolver las impedancias de transferencia. ***2.7.2.1.1 Sección A Inciso1***
b) El diámetro interior del blindaje será de 6.00 milímetros como mínimo (0.236 in).
c) El diámetro exterior del blindaje exterior será 8.00 milímetros ± 0.40 mm
d) El blindaje exterior será de una trenza de cobre estañado.

5) El Jack

a) Cualquier material del Jacket deberá ser utilizando las especificaciones 2.7.2.1.1 Secciones A y B.

b) Cualquiera de las dos dimensiones del Jacket se pueden utilizar para dos amplias clases de materiales especificadas en ***2.7.2.1.1 Sección B.***

- Cloruro de polivinyl (por ejemplo el PVC) o el equivalente a tener un OD de 10.3mm ±0.25 mm.

- Fluoropolymer (por ejemplo FEP,E-CTFE) o el equivalente a tener un OD 9.525 mm ± 0.254 mm.

El cable resolverá criterios aplicables de la inflamabilidad y del humo y los códigos locales y nacionales para la instalación.

6) Rotulado del Jack

El cable del jack se marcara con un color contrastante al color del jack. Las marcas se espaciarán a 2.5 m ± 5 cm regularmente a lo largo de la longitud entera del cable. Es permitido para los 2,5 m que espacian para ser interrumpido en las discontinuidades entre las secciones del cable unidas por los conectores. Se recomienda que el color de la base del jacket sea de un color brillante (por ejemplo el amarillo) con excepción del que es usado normalmente para la alimentación.

C. Resistencia Total

La suma total del centro del conductor, los conectores y la resistencia del blindaje no excederán de 5 Ω por segmento.

Cada par del conector en línea o el MAU no será no más de 10 m Ω. El uso de estos componentes reduce por consiguiente la longitud de segmento permisible total. Los valores antes mencionados se encuentran a una temperatura de 20°C.

2.7.2.1.2 Conectores del segmento del cable

El segmento de coaxial requiere de una terminación para poder ser extendido o particionado en secciones. Los dispositivos que se asociaran al medio como las MAU's requieren un medio de conexión para el medio. Hay dos tipos básicos del conector que proporcionan los medios necesarios de la conexión:

a) Los conectores N estandar (IEC 60169-16).
b) Conector coaxial "tap".

Todos los conectores tipo N tienen un tipo de impedancia constante de 50 Ω. Puesto que las frecuencias presentes en los datos transmitidos están debajo del rango de la banda UHV (siendo el limite de banda aproximadamente 20 MHz), las versiones de alta calidad de los conectores no se requiere, pero se recomiendan.

Todos los conectores tipo Tap deberán seguir las alineaciones del ***2.7.2.1.2 Sección C***

A. Conector coaxial en línea de extensión

Todos los cables coaxiales serán terminados con los conectores del enchufe (plugs) del tipo N. Los medios serán provistos para que se asegure que el conector no mantendrá contacto con ningún metal del edificio o algún otro conector.

Las extensiones coaxiales en línea entre dos secciones del cable coaxial serán hechas con un par de conectores del receptáculo del tipo "N" unidos en forma un barril. El aislante también se ensamblara en forma de barril.

B. Terminador del Cable Coaxial

1) Terminador (Adaptador)

Los terminadores del cable coaxial son usados para proveer una impedancia de terminación para que el cable iguale el valor de su impedancia característica, de tal modo minimizando la reflexión en los extremos del cable. La impedancia de terminación utilizada es de 50 Ω ±1 % medido desde 0 a 20 Mhz con la magnitud del ángulo de fase de la impedancia no sobre pase los 5° . El grado de potencia del terminador será de 1 W o mayor.

2) Tierra

La tierra del terminador del cable coaxial o de las extensiones del cable provee una conveniente ubicación para satisfacer los requerimientos de tierra en el punto.

Se recomienda una tierra terminal con un grado de corriente de por lo menos 1500 ampacity usados en uno de los dos terminadores o en un conector de extensión usado con un segmento de cable.

3) El poner a tierra del sistema del cable

El blindaje del conductor de cada segmento del cable coaxial hará el contacto eléctrico con una tierra de referencia eficaz en una punta y no hará contacto eléctrico con tierra otra parte de los objetos tales como una estructural metálica del edificio, los ductos, la base de la plomería, o el otro conductor involuntario. Los aisladores se pueden utilizar para cubrir cualquier conector coaxial usado para ensamblar secciones y los adaptadores del cable, para asegurarse de que este requisito está resuelto.

C. Conexión del MAU al cable coaxial

Los medios serán provistos para que permitan que se agregue un MAU al cable coaxial. La conexión no perturbará significativamente las características de la línea de transmisión del cable. Presentará una capacitancia fiable, baja en la desviación y por lo tanto una longitud corta insignificante del trozo. Esto es facilitado por el MAU ubicándolo lo más cerca posible de una conexión al cable. El MAU y el conector se consideran normalmente en un solo ensamblaje. Las conexiones largas entre el cable coaxial y la entrada de información del MAU comprometen este objetivo.

El funcionamiento del sistema total es dependiente en gran parte en la conexión de cable del MAU al coaxial siendo de una capacitancia de baja desviación.

Los conectores del tipo N seleccionados deben ser de alta calidad (es decir , resistencia de bajo contacto) para reducir al mínimo el impacto en el funcionamiento del sistema.

1) Requerimientos Eléctricos

Los requerimientos para el conector "tap" coaxial son los siguentes:

- Capacitancia : 2 pF conector nominal medido a 10 MHz.
- Resistencia de contacto : (se aplica a los contactos de centro del conductor y del blindaje) 50 mΩ para ambos , el blindaje y el centro del conductor sobre la vida útil del conector.
- Material de contacto : La superficie del material que es la punta de prueba o el suficiente blindaje , que satisfagan los requerimientos de resistencia de contacto en el ambiente y en cierto lapso.
- Grado de Voltaje : 600V de DC o el máximo rms de AC.

- Aislante : la resistencia de la salida de la C.C. de la cubierta "tap" será más alta de 1GΩ entre la trenza y los conductores en el ambiente para una operación normal.

- Grado de corriente probada : 0.1 A por contacto (prueba y blindaje).

- Grado de corriente Blindada: 1 A por segundo.

2) Requerimientos Mecánicos

Cubierta del conector

Características de blindaje : >40 dB a 50 MHz.

Confiabilidad del contacto

El funcionamiento total del sistema de la LAN depende de un fragmento grande de confiabilidad del medio del cable coaxial y de la conexión a este medio. Los sistemas de conexión "tap" deben ser considerados los parámetros eléctricos y mecánicos más relevantes , el punto de conexión eléctrico entre la prueba "tap" y el centro del conductor del cable para asegurarse que sea confiable el contacto eléctrico realizado y conservado a través de la vida útil de estos componentes.

Se recomienda que algunos medios esten provistos para asegurar una carga de confiabilidad constante de contacto en cierto plazo, con rastreo, con la temperatura y el ambiente típico. Típicamente las configuraciones del conector "tap" son las siguientes: *figura 2.17.a y 2.17b.*

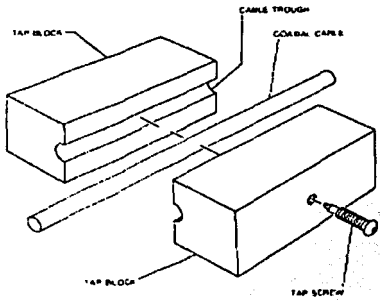


Figura 2.17.a Conector Tap.

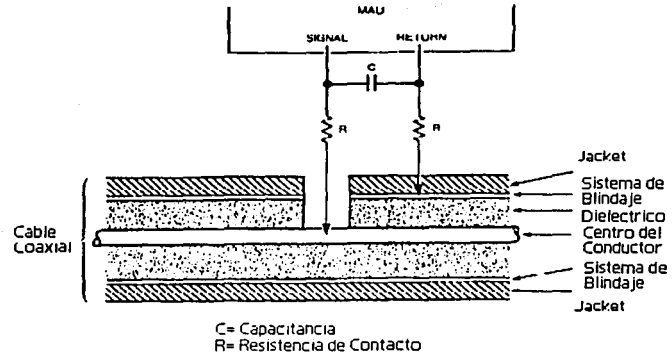


Figura 2.17b Conexión típica de un circuito "tap".

2.7.2.2 10Base2 : Thin ethernet

Se agregó en los 1980 y usa un cable coaxial más delgado. 10Base2 es muy similar a 10BASE5 y era inventado principalmente para reducir el costo y complejidad de la instalación de 10BASE5

- La máxima longitud de un segmento 10BASE2 es reducida a 185 metros, comparado a los 500 metros de 10BASE5.
- 10BASE2 permite solo 30 nodos por segmento contra de los 100 nodos de 10BASE5.
- 10BASE2 retiene la regla de los 5 segmentos y 4 repetidores, permitiendo un máximo diámetro de red de 5X 185metros =925metros. Si no se utiliza repetidores la máxima longitud de un simple segmento es de 185 metros.

2.7.2.2.1 Características del cable coaxial

El cable coaxial es de una impedancia constante. Es terminado en cada uno de los dos extremos por un adaptador *ver 2.7.2.2.2 Sección B* y provee la ruta de transmisión para la conexión del dispositivo MAU. Los conectores del cable coaxial se utilizan para hacer la conexión del cable a los adaptadores y entre las secciones del cable. El cable tiene varios requisitos eléctricos y mecánicos que sean resueltos para asegurar la operación apropiada.

A. Parámetros eléctricos del cable coaxial.

Los parámetros especificados en aquí son resueltos para los tipos de cable RG 58 A/U ó RG 58 C/U.

1) Características de impedancia

- La impedancia característica media del cable será 50 ± 2Ω.
- Las variaciones periódicas en impedancia a lo largo de una pieza única del cable pueden estar hasta ±3 Ω sinusoidal centrado alrededor del valor medio, con un período de menos de 2 m.

2) Atenuación

La atenuación de un segmento del cable de 185 m, no excederá 8.5 dB medidos en 10 Mhz ó 6.0 dB medidos en 5 Mhz.

3) Impedancia de Transferencia

El cable coaxial es capaz de proveer un suficiente blindaje para minimizar la susceptibilidad de un ruido externo y también para reducir al mínimo la generación de interferencia por medio de señales relacionadas. Mientras que la construcción del cable no se asigna por mandato, es necesario indicar una medida del funcionamiento esperada del componente del cable. El funcionamiento de los cables EMC son determinados en gran medida por la impedancia de transferencia valuada en el cable.

La impedancia de la transferencia del cable no excederá los valores mostrados en la *figura 2.18* en función de la frecuencia.

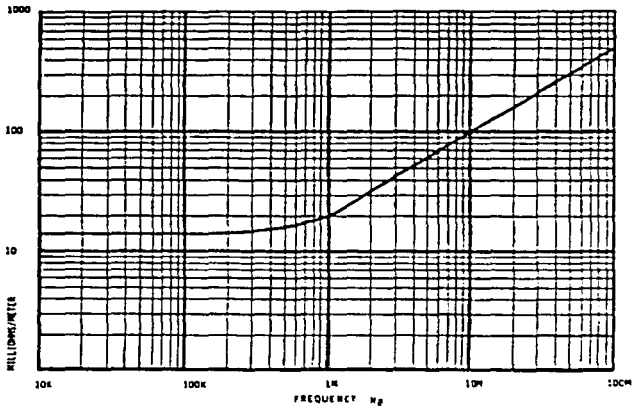


Figura 2.18 Máxima Impedancia de Transferencia para el cable coaxial.

4) Resistencia Total

La suma de la resistencia de centro del conductor más la resistencia del blindaje medida en 20 °C no excederá 50 mΩ/m.

B. Características Físicas del cable coaxial

1) Requerimientos Mecánicos

El cable usado debe ser apropiado para encaminar varios ambientes, incluyéndolo, pero no limitándolo a techos caídos, a suelos levantados, y a través de un espacio abierto. El jack proveerá aislamiento entre el cable y cualquier edificio de estructura metálica.

También el cable será capaz de aceptar conectores para el cable coaxial ***ver 2.7.2.2.2*** El cable se conformará con los requisitos siguientes.

1) Construcción General

- El cable coaxial consistirá en un conductor de centro, un dieléctrico, un sistema del blindaje, y un jack aislador del guardapolvo.
- El cable coaxial será suficientemente flexible para utilizar un radio de curvatura de 5 centímetros.

2) Conductor de Centro

El conductor de centro será trenzado, de cobre estañado con un diámetro total de 0.89 milímetros de ± 0.05 milímetros.

3) Material Dieléctrico

El material dieléctrico puede ser de cualquier tipo proveyendo las especificaciones ***ver 2.7.2.2.1 Sección A y B*** anteriormente mencionadas, sin embargo, se prefiere un dieléctrico sólido.

4) Sistema de Blindaje

El sistema que blindaje puede contener los elementos de la trenza y de la hoja suficientes para resolver la impedancia de la transferencia de punto ***2.7.2.2.1 Sección A Inciso 3*** y los especificaciones del EMC.

El diámetro interior del sistema que blinda será 2.95 milímetros de ± 0.15 milímetros

El sistema de blindaje será mayor de 95% de la cobertura. El uso de la trenza de cobre estañada se recomienda para resolver la resistencia del contacto y los requisitos en el blindaje.

5) El Jack

a) Cualquier material del Jacket deberá ser utilizando las especificaciones ***ver 2.7.2.2.1 Sección A y B.***

b) Cualquiera de las dos dimensiones del Jacket se pueden utilizar para dos amplias clases de materiales especificadas en ***2.7.2.2.1 Sección B Inciso 1***

- Cloruro de polivinyl (por ejemplo el PVC) o el equivalente a tener un OD de 4.9 mm ± 0.3 mm
- Fluoropolymer (por ejemplo FEP,E-CTFE) o el equivalente a tener un OD 4.8 mm ± 0.3 mm.

El cable resolverá criterios aplicables de la inflamabilidad y del humo y los códigos locales y nacionales para la instalación

5) Rotulado del Jack

Se recomienda que el cable del jack se encuentre rotulado por el fabricante y escribir el tipo de frecuencia nominal por lo menos cada metro a lo largo del cable.

C. Resistencia Total

La suma del conductor, de los conectores, y de la resistencia de centro del blindaje no deben exceder de 10 Ω por el segmento total. Cada par del conectores en línea o el MAU contribuirán no más de 10 mΩ

Un segmento de cable coaxial consiste de varias secciones de coaxial, todos los conectores y resistencias internas del blindaje y el centro del conductor serán incluidas en medida de la resistencia.

2.7.2.2.2 Conectores del Cable coaxial

El medio coaxial requiere de terminaciones y se reparte en secciones. Los dispositivos que se asociarán al medio requieren vías de conexión al medio. Este medio es provisto por un BNC adaptador "T", *figura 2.19* .

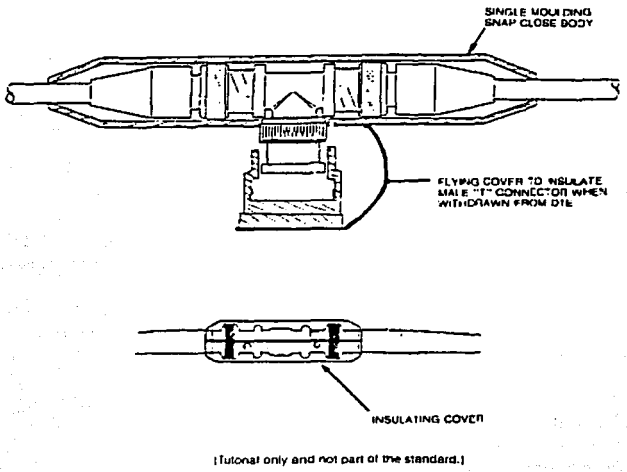


Figura 2.19 Conector cable coaxial.

Los conectores BNC serán de una impedancia constante de 50Ω.

A. Conector coaxial en línea de extensión

Todos los cables coaxiales serán terminados por un conector BNC. Los medios serán proporcionados de asegurarse de que la estructura del conector no realice contacto con ningún metal del edificio o el otro conductor involuntario.

El coaxial en la línea de extensión será hecha con conectores BNC de receptor a receptor, unidos en forma de barril. Un aislador también será provisto por un ensamblaje en forma de barril.

B. Terminador del cable coaxial

Los adaptadores del cable coaxial se utilizan para proporcionar a una impedancia de terminación para que el valor del cable sea igual a la impedancia característica, de tal modo reduciendo al mínimo la reflexión en los extremos de los cables. Los adaptadores serán empaquetados dentro de un conector macho o hembra. La impedancia de terminación será de 50Ω ± 1%. medida desde 0 a 20 Mhz. con una magnitud del ángulo de fase de la impedancia no excedida a 5° . El grado de potencia del terminador será de 0.5W o mayor. Los medios del aislante serán provistos por cada adaptador.

C. Conexión del cable del MAU al coaxial

Un adaptador BNC "T" (plug receptor plug) provee un medio para asociar el MAU con el cable coaxial. La conexión no perturbará significativamente las características de la transmisión del cable; presentará una capacitancia baja de la desviación y por lo tanto una insignificante longitud del pequeño trozo. Esto es posible por que el MAU esta localizado lo más cerca posible de una conexión. El MAU y el conector normalmente se consideran en un ensamblaje. El largo de la conexión (mayor a 4 cm) entre el cable coaxial y la entrada de la información del MAU comprometen este objetivo.

- El funcionamiento del sistema total es dependiente en gran parte de la conexión de cable coaxial al MAU siendo de baja capacitancia en la desviación.

- Los medios serán proporcionados para asegurarse de que el ensamblaje del conector no realice contacto con ningún metal del edificio o con ninguna otro conductor involuntario.

Se deberá colocar un aislador después de realizar la conexión. La cubierta del aislador tendrá las siguientes características:

- Debe proteger contra una tierra accidental del ensamblaje del conector.

- Debe permitir fácilmente conectar y desconectar el ensamblado del conector "T hacia el MAU, sin la necesidad de remover los conectores del cable.

- Debe ser un moldeado simple que asocie firmemente a un ensamblaje del conector.

2.7.2.3 10BASE-T : Par Trenzado

En 1990, el ethernet sobre el par trenzado sin blindaje, conocido como 10BASET, se estandarizó. La IEEE adopta el estándar 802.3i 10BASET, un completo estándar en una nueva capa física para ethernet.

- La topología es cambiada a estrella, y solo dos nodos por segmento son permitidos. (De estación a repetidor, o repetidor a repetidor, o estación a estación con un cable cruzado "crossover").

- 10BASET retiene la regla de 4 repetidores / 5 segmentos de 10BASE5, esto significa que una LAN de 10BASET puede tener un diámetro máximo de 500metros.

El sistema 10BASE-T es diseñado para soportar una transmisión de señales a 10Mbps sobre cableado de par trenzado categoría 3. Al menos la basta mayoría de sistema de cableado de par trenzado en uso hoy día está basado en cables de par trenzado categoría 5. Los cables de categoría 5 tienen alta calidad al llevar la señal y trabaja excelentemente con sistemas 10BASE-T.

A. Componentes de señalización 10BASE-T

Los siguientes componentes de señalización pueden ser usados en sistemas 10BASE-T para mandar y recibir señales concluyendo el sistema de medio.

- Interface Ethernet con un transceiver fijo 10BASE-T.
- Cable AUI transceiver.
- Un transceiver externo basado en AUI 10BASE-T, también llamado unidad agregada al medio MAU.
- Equipo repetidor, hub con puerto 10BASE-T.

1) Interfaz Ethernet

Una típica interface ethernet 10BASE-T incluye un transceiver fijo que es usado para realizar una directa conexión al segmento del cable par trenzado, ***figura 2.20.***

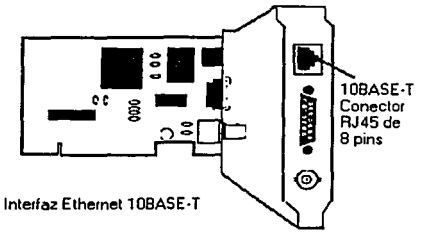


Figura 2.20 Interfaz Ethernet 10BASE-T.

Esta tarjeta en particular esta equipada con tres conectores que permiten agregar una gran variedad de sistemas de medio a 10 Mbps . La tarjeta es conectada al segmento 10BASE-T usando un transceiver fijo y la roseta RJ-45 que conecta hacia el cable par trenzado. Puede también conectarse a un segmento 10BASE-T utilizando el conector AUI de 15 pins y un transceiver externo 10BASE-T. En estos días, muchas NICs tienen solo conectores RJ-45, y usan transceivers internos para soportar funciones de múltiples velocidades. En tales interfaces multi-velocidad, el estándar de auto-negociación es típicamente utilizado para una configuración automática de la velocidad para su funcionamiento.

2) Cable Transceiver

Para equipos con tarjetas 10BASE-T con una interfaz de AUI , una cable tranceiver AUI puede utilizarse para hacer una conexión entre conector AUI en la interfaz y el conector AUI en un transceiver externo 10BASE-T. Un cable transceiver no es necesario cuando un transceiver fijo o empotrado 10BASE-T es utilizado.

3) Unidad Agregada al Medio MAU

El apartado define las características funcionales, eléctricas y mecánicas del MAU tipo 10BaseT y el medio específico para usar el MAU. El MAU y especificación medio está dirigido sobre todo a las aplicaciones de oficina donde el cable "par trenzado" está instalado a menudo. La simplicidad de la instalación y de la reconfiguración es permitida por el tipo de cable y de conectores usados. *Diagrama 2.1.*

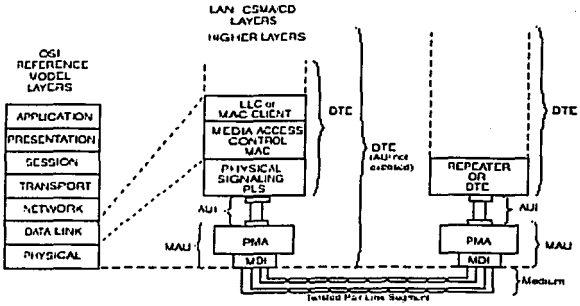


Diagrama 2.1 Lazo de 10BASE-T al modelo de la referencia (OSI) y al modelo del LAN de la IEEE 802.3 CSMA/CD.

En una interfaz de una estación que solo tiene un conector AUI de 15 pins puede conectarse a un segmento ethernet 10BASE-T usando un transceiver externo 10BASE-T, *figura 2.21.*

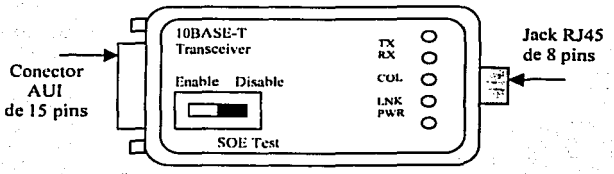


Figura 2.21 Transceiver Externo 10BASE-T.

Las características generales son las siguientes:

- Permite acoplar la Señalización Física de la subcapa de manera que la interfaz de la unidad de conexión (AUI) vaya a la conexión del conductor "par trenzado" definido en este apartado.
- Soporta un tráfico de mensajes en un índice de datos de 10 Mb/s.
- Provee una operación desde 0m hasta 100m de par trenzado sin el uso del repetidor.

- Permite que el equipo terminal de datos (DTE) o el repetidor confirme la operación del MAU y de la disponibilidad del medio.

- Soporta configuraciones de red usando el método de acceso de CSMA/CD definido en este estándar con señalización de banda base.

- Soporta interconexiones punto a punto entre MAU's y cuando este usando los repetidores tenga multiples accesos, utilizando una topología física (cableado) en estrella.

- Permite la incorporación del MAU dentro de los límites físicos de un DTE o de un repetidor.

- Permite cualquier operación en half duplex o full-duplex o ambas.

4) Modos de Operación

El MAU 10baseT es capaz de operar solo en modo normal. El MAU no funcionará en modo del monitor.

Cuando el modo normal está en la operación, el MAU funciona como una conexión directa entre el medio y el DTE o el repetidor. Los datos del DTE o del repetidor se hacen salir a uno de los segmentos de edición de conexiones a una cara del segmento y los datos recibidos en el otro segmento de edición de conexiones a la otra cara donde entra al DTE o al repetidor.

5) Unidad Repetidora

La unidad del repetidor se utiliza para ampliar la topología física del sistema y prevé el acoplamiento de dos o más segmentos. Los repetidores son una parte integral de todas las redes 10BASE-T con más de dos DTEs.

6) Codificación de la señal 10BASE-T

Las señales enviadas al medio 10BASE-T son codificadas con el sistema de codificación Manchester.

Señalización de la línea física.

La señalización de la línea física de 10BASE-T es enviar encima del cable par trenzado una diferencia balanceada de corrientes. En cada par del cable, un cable es utilizado para transportar una amplitud positiva de una señal diferencial (de 0 volts a 2.5 volts), y un cable lleva la amplitud negativa de la señal (de 0 volts a –2.5 volts). El pico de la señal transportada por cada uno de los cables es aproximadamente 2.5 volts, que provee un total de 5 volts pico a pico medido a través de ambos alambres en el par.

La señal diferencial provee su propia punta de referencia cero, alrededor de la cual las señales eléctricas hacen pivotar positivo o negativo. Esto no necesita la referencia de las señales en un segmento 10BASE-T hacia un nivel de tierra común compartido por el equipo en ambos extremos. Por tener una referencia de las señales a la tierra común, el sistema 10BASE-T es aislada de las variaciones en el voltaje de tierra que puede ocurrir en el par trenzado en el sistema de cableado. Esto elimina problemas con las corrientes a tierra y mejorar la confiabilidad en el sistema.

B. Medio: Componentes 10BASE-T

El siguiente conjunto de los componentes del medio, son utilizados para construir un segmento de par trenzado 10BASE-T:

- Cable par trenzado sin blindar, categoría 3 o mejor.
- Un conector modular RJ-45 de 8 pins.

1) Cable UTP

El sistema 10BASE-T opera encima de dos pares del cable UTP; un par recibe las señales de datos en la estación o un puerto del hub, y el otro par es ocupado para transmitir las señales de los datos desde la estación o el puerto del hub. La longitud en el estándar para un segmento basado en 10BASE-T en un cableado de grado de voz y componentes es de 100 metros.

El medio para 10BASE-T es alambre de conductor doble retorcido "par trenzado". Este cableado consiste en normalmente el alambre sin blindaje de 0,4 milímetros a de 0,6 milímetros de diámetro [AWG 26 a AWG 22] en un cable multipar. Las especificaciones del funcionamiento son generalmente 100 m de par-trenzado "twisted pair" del teléfono de 0,5 milímetros. Una longitud de 100 m, el objetivo de diseño, será utilizada para referirse a la longitud de un segmento en par trenzado, *figura 2.22.*

Objetivos:

- Proporcionar a los medios físicos para la comunicación entre las entidades de la capa de transmisión de datos del LAN.
- Asegurar la compatibilidad independientemente de las interfaces físicas y interfaces eléctricas.
- Proveer de un canal de comunicaciones con un "bit error rate", en la interfaz del servicio de la capa física de menos de una porción de 10^8.
- Preveer la facilidad de la instalación y servicio.
- Asegurar de que la imparcialidad del acceso del DTE no esté comprometida.

- Preveer redes de bajo costo, con respecto al equipo y cableado.

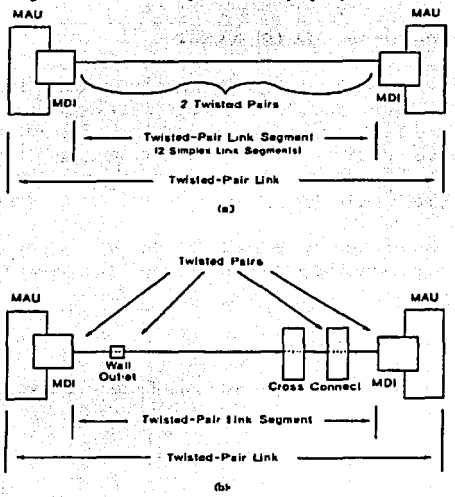


Figura 2.22 Conexión par trenzado

2) Consideraciones de Compatibilidad

Todas las implantaciones con el par-trenzado serán compatibles con el MDI (Interfaz Dependiente del Medio). Los MAU (Unidad Agregada al Medio) y el medio se definen para proporcionar una compatibilidad entre los dispositivos diseñados por diversos fabricantes.

Los diseñadores son libres de implantar circuitos dentro del MAU de una aplicación dependiente que provea satisfactoriamente las especificaciones del MDI y el AUI.

El mayor factor de limitación en un segmento 10BASE-T es la fuerza de la señal, o la atenuación de la señal. El circuito del receptor en un transmisor-receptor típico 10BASE-T tiene un nivel del silenciador de la señal fijado en 300 (mV), que ayuda a evitar que las señales débiles inducidas por interferencia de la señal entre los pares del alambre se conviertan en un problema, limitando el nivel en el cual se reciben las señales.

Una vez hundida la señal debajo de este nivel, no será recibido por un transmisor-receptor 10BASE-T. Con este acercamiento, las señales inducidas por interferencia debajo de 300mV no se les hace caso simplemente.

Sin embargo, esto también significa que cuando la atenuación de la señal encima del segmento del registro, baja el nivel verdadero de la señal debajo de 300mV, el segmento parará de trabajar.

3) Especificaciones de Atenuación 10BASE-T

La máxima atenuación en una señal permitida en las especificaciones para un segmento 10BASE-T es de 11.5 decibles (dB) medido desde un extremo del segmento a otro con un dispositivo de prueba del cable. Un cable típico de categoría 5 tiene una atenuación de 10db por 500 pies en una frecuencia de 10 Mhz. Por consiguiente, 500 pies de esta clase de cable par trenzado habría que utilizar encima de la mayoría de las pérdidas de la señal de 11.5db que se permite en un segmento 10BASE-T.

Se puede contar con que por lo menos 1.5dB del presupuesto de la pérdida sea utilizado para arriba por las pérdidas de la señal que ocurren en los conectores RJ-45, patch panel, y los cables de parcheo.

4) Impedancia en el par trenzado

Para mejores resultados se debe usar cable par trenzado con características de impedancia de 100Ω.

Sin embargo, el estándar observa que es posible construir segmentos usando el cable par trenzado como conductor con una impedancia característica de 120Ω, un tipo de cable usado comúnmente en ciertos países europeos.

5) Características diferenciales de la impedancia

La magnitud de la impedancia característica diferenciada de una longitud de 3 m de par trenzado, usada en un segmento de edición de conexiones esta entre 85Ω y 111Ω para todas las frecuencias entre 5.0 y 10 MHz.

Puesto que la impedancia característica tiende a disminuir con el aumento de frecuencia, el requisito antedicho es implicado, generalmente por la condición de la magnitud de la impedancia característica concluyendo que la banda de frecuencia de 1MHz a 16MHz es de 100Ω ± 15Ω. También, la magnitud de la impedancia de la entrada de información se realizó un promedio de bandas de frecuencias de 5.0MHz a 10MHz de un segmento de edición de conexiones terminando en 100Ω serán entre 85Ω y 111Ω.

6) Retardo

El retardo máximo de la propagación en el par trenzado será de 5.7ns/m. Y en un segmento de edición de conexiones no excederá de 1000ns.

7) Roseta, conector RJ45

El medio de 10BASE-T ocupa dos pares del cable, que son terminados en un conector RJ-45. Este significa que 4 pins del conector de 8 pins serán utilizados, *tabla 2.3.*

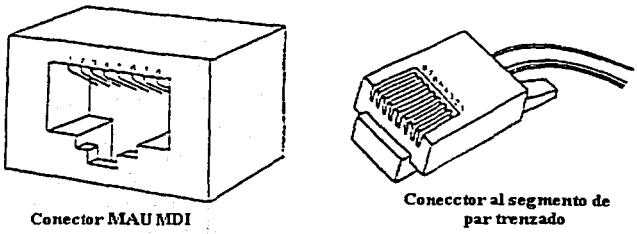
1	TD + (Transmitir Datos)
2	TD - (Transmitir Datos)
3	RD+ (Recibir Datos)
4	No usada por 10baseT
5	No usada por 10baseT
6	RD - (Recibir Datos)
7	No usada por 10baseT
8	No usada por 10baseT

Tabla 2.3 Señales en el conector de 8 pins 10BASE-T.

La TIA/EIA 568 A estándar de cableado estructurado recomienda la instalación de dos cables par trenzado para cada oficina. Uno para servicio de datos y otros para teléfonos u otro servicio. Un diseño conservador reserva un cable del cuarto-par para el servicio de los datos, utiliza un cable clasificado para resolver las especificaciones de la categoría 5, y conecta los ocho alambres del cable.

Los conectores MDI

Conectores del ocho-pins se usarán como la interfaz mecánica al eslabón del segmento par-trenzado. El plug del conector se usará en el segmento del par-trenzado y la roseta en los conectores de MAU. Estos conectores se observan (solo para el uso informativo) en *figura 2.23* La siguiente tabla muestra la asignación de las señales a los contactos del conector.



Conector MAU MDI **Conecctor al segmento de par trenzado**

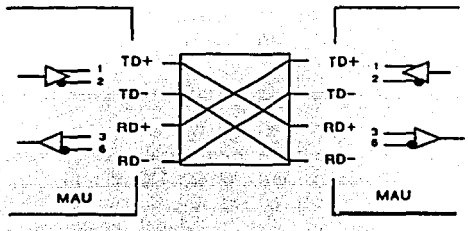
Figura 2.23 Conectores.

8) Función de Traspaso "CrossOver"

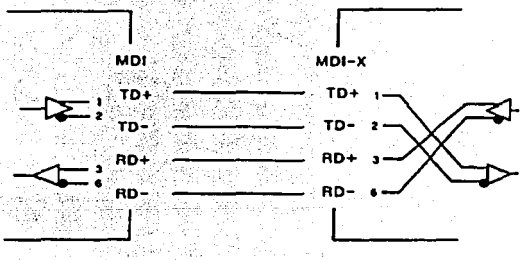
Una función del traspaso se llevará a cabo en cada conexión del par trenzado. La función del traspaso conecta el transmisor de un MAU al receptor del MAU al otro extremo de la conexión del par trenzado. Pueden llevarse a cabo las funciones del traspaso internamente a un MAU o en otra parte en la conexión del par trenzado.

Cuando un eslabón del par trenzado conecta un DTE a un repetidor, se recomienda que el traspaso se lleve a cabo en el MAU local al repetidor. Si ambos MAUs de un eslabón del par trenzado contienen internamente las funciones de traspaso, un traspaso externo adicional es necesario. Se recomienda que el traspaso sea visible a un instalador de uno del MAUs. Cuando ambos MAUs contienen los traspasos interiores, se recomiendo adicionalmente en redes en que la topología identifica un segmento central del backbone o un hub central el MAU se adicione al elemento central asignándole el traspaso externo para mantener la consistencia.

La implícita implantación de la función del traspaso dentro de un cable del par trenzado, o en un tablero de la instalación "patch panel", mientras no este expresamente prohibida, está más allá del alcance de esta norma ***figura 2.24***



a) Función de traspaso "crossover" externa



b) Función traspaso "crossover" interna en el MAU

Figura 2.24 Función de Traspaso.

2.7.2.4 10BASE-F: Fibra Óptica

10BASE-F se volvió un estándar oficial de la IEEE en 1993 , aunque los equipos de fibra ethernet habían estado disponibles durante varios años antes de esa fecha. 10BASEF es basada en un eslabón de fibra óptica del interepetidor (FOIRL) la especificación de 1987 que fue creada para interconectar repetidores que usan una distancia extendida a la conexión del cable de fibra óptica.

El 10BASE-F sistema de fibra óptica usa pulsos de luz para mandar señales ethernet. Este acercamiento tiene varias ventajas.

En primer lugar, un segmento del eslabón de fibra óptica puede llevar las señales del ethernet para las distancias considerablemente más largas que los medios de comunicación metálicos.

El medios de comunicación de fibra óptica se usa ampliamente en el cableado del backbone en un sistema de cableado estructurado. Le permite unir equipos locales en cada piso del edificio con un sistema que puede viajar a grandes distancia que los segmentos del par trenzado.

La fibra anterior y la nueva que une los segmentos

Hay dos tipos de eslabones de segmentos de fibra óptica en uso, el original eslabón de segmento de fibra óptica Inter-Repetidores (FOIRL) y él más nuevo segmento de 10BASE-FL. La especificación del FOIRL describe un segmento hasta de 1000 metros para ser usado sólo entre repetidores.

La nueva norma proporciona un juego de especificaciones de medios de comunicación de fibra incluso un nuevo segmento del eslabón que permitir las ataduras directas entre los puertos de los repetidores y estaciones. El estándar 10BASE-F incluye tres tipos de segmentos de fibra óptica.10BASE-FL, 10BASE-FP, y 10BASE-FB. 10BASE-FL (la L, como en el eslabón) la norma reemplaza las especificaciones de FOIRL más viejas y es hacia atrás compatible con el equipo existente basado en FOIRL. 10BASE-FL es el estándar de fibra universal de 10Mbps y puede usarse para conectar los DTEs, repetidores o switches. 10BASE-FL es la porción ampliamente usada del 10BASE-F de las especificaciones de fibra óptica, y el equipo está disponible por un sin número de vendedores. La norma 10BASE-F también incorpora los estándares 10BASE-FB (la B como en el backbone), y 10BASE-FP (P de pasivo). Éstos son sumamente raros, sin embargo la *tabla 2.4* proporciona una comparación de las opciones 10BASE-F diferentes. *tabla 2.5* resume las limitaciones de distancias de 10BASE-FL.

[illegible]			
FOIRL	Pre-estándar, solo repetidores	2	1000 metros
10BASE-FL	Nuevo estándar, universal, incluye repetidores, switches y nodos	4	400-2000 metros
10BASE-FB	Backbone repetidores con el AUI integrado		2000 metros
10BASE-FP	Repetidor central con fuente de poder AC	1 Estrella pasiva	500 metros o 300 metros

Tabla 2.4 Cuatro opciones de 10BASE-F.

Tipo de Conector	
Cualquier segmento de fibra de repetidor a DTE	400 metros
Con 4 repetidores y 5 segmentos	500 metros
Cualquier segmento de fibra entre repetidores	1000 metros
Sin repetidor (DTE a DTE o Switch a switch)	2000 metros

Tabla 2.5 Limitaciones de distancia para diferentes conexiones.

2.7.2.4.1 10BASE-FL

La norma del eslabón de fibra (FL) reemplaza los mas viejos eslabones de segmentos en FOIRL .La señalización del equipamiento de 10BASE-FL es diseñado para interoperar con equipo basado en FOIRL. 10BASE-FL provee un segmento de fibra óptica que puede ser hasta los 2000 metros de longitud, previniendo que el segmento solo use dispositivos 10BASE-FL.

Si se ocupan equipos mixtos de FOIRL y 10BASE-FL la longitud máxima del segmento será hasta 1000 metros. Un segmento 10BASE-FL puede ser usado para conectar dos computadoras o dos repetidores, o una computadora y un puerto del repetidor. 10BASE-FL es la porción más extensamente utilizada del conjunto de especificaciones de fibra óptica del 10BASE-F

A. Componentes de señalización 10BASE-FL

Los siguientes componentes de señalización pueden ser usados en el sistema 10BASE-FL para enviar y recibir señales sobre este medio:

- Interfaz ethernet equipada con un transceiver 10BASE-FL. Una conexión 10BASE-FL es más a menudo proporcionada por un transceiver externo que es agregada al conector de 15 pins AUI en la interfaz.
- Cable transceiver, también llamado unidad agregada a la interface (AUI).
- Un transceiver externo 10BASE-FL, también llamada unidad agregada al medio de fibra óptica (MAU).

1) Interface Ethernet 10BASE-FL

La basta mayoría de conexiones ethernet a los equipos de escritorio estan usando el medio de par trenzado. En consecuencia no hay una gran demanda para una intefaz ethernet en fibra óptica para 10Mbps.

2) Cable transceiver

En un sistema 10BASE-FL un cable transceiver puede ser usado para realizar una conexión entre la interfaz ethernet y un transceiver externo 10BASE-FL. Si el transceiver 10BASE-FL es bastante pequeño, cabe directamente sobre el conector de 15 pins AUI en el interfaz de Ethernet, entonces el cable tranceiver no será necesario.

3) Transceiver 10BASE-FL

Una conexión típica hacia el segmento de fibra óptica es hecha con una interfaz ethernet que conecta a un transceiver externo 10BASE-FL usando un conector AUI de 15 pins, ***figura 2.25.***

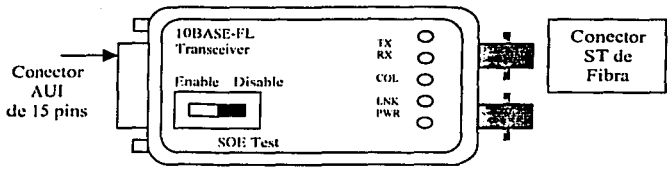


Figura 2.25 Transceiver 10BASE-FL.

Unidad agregada al medio MAU 10Base-FL

La MAU de 10BASE-FL tiene las características generales siguientes:

- Permite el acoplamiento del PLS por la vía del AUI al eslabón de fibra de banda base.
- Soporta el tráfico del mensaje de datos de 10 Mbps.
- Mantiene operando por encima de 0 a por lo menos 2000 metros del cable fibra óptica especificada anteriormente sin el uso del repetidor.
- Permite al DTE o a repetidor confirmar funcionamiento del MAU y disponibilidad del medio.
- Soporta configuraciones de la red que usan el metodo de acceso CSMA/CD definido en ISO/IEC 8802-3 con la señalización de la banda de base.
- Soporta una interconexión de punto a punto entre MAUs y, cuando se usan con repetidores de puertos múltiples, soportan un cableado de topología de estrella.
- Permite incorporación del MAU dentro de los límites físicos de un DTE o repetidor.

4) Unidad repetidora

La unidad del repetidor se usa para extender la topología del sistema físico y mantiene acoplando dos o más segmentos. Los repetidores son una parte íntegra de todo el 10BASE-FL conectando una red de computadoras con más de dos DTE. Se permiten las unidades del repetidor Múltiples dentro de un solo dominio de la colisión para proporcionar la longitud del camino óptico de conexión máxima especificadas.

5) Codificación de la señal 10BASE-FL

Las señales enviadas sobre el medio de 10BASE-FL, utilizan un sistema de codificación Manchester.

6) Señalización en la línea física

El transceiver 10BASE-FL envía y recibe señales en pulsos de luz sobre el segmento de fibra óptica que consiste en dos cables de fibra óptica: Un cable para transmitir datos y otro para recibirlos. Esto se hace usando un esquema de señalización de línea muy simple llamado Non-Return-to-Zero(NRZ). NRZ produce un pulso de luz para transmitirse un uno lógico (1) y ningún pulso de luz para el cero lógico (0). Las señales son enviadas sobre un segmento 10BASE-FL turnando el haz de luz por intervalos para indicar las señales de código Manchester que representan unos y ceros.

2.7.2.4.2 10BASE-FB

Las especificaciones del 10BASE-FB describe una señalización zirconio en el segmento de fibra del backbone (FB). Este sistema permite varios repetidores ethernet para ser conectados en serie, excediendo el límite usual en el número total de repetidores que permite el sistema ethernet a 10 Mbps. Las conexiones 10BASE-FB – típicamente asociada a los repetidores (hubs) es usada para conectar repetidores síncronos 10BASE-FB junto a un sistema de repetidores Backbone que puede atravesar largas distancias. Las conexiones individuales de 10BASE-FB pueden ser hasta 2000 metros de longitud. El sistema 10BASE-FB no fue extensamente adoptado. Durante los primeros años después de que la norma fue desarrollada, el equipo estaba disponible con muy pocos vendedores.

Unidad agregada al medio

El 10BASE-FB MAU tiene las características generales siguientes:

- Habilita acoplamiento de la Señalización de la Capa Física (PLS) los mensajes a la banda base de la conexión de fibra óptica definidas.
- Soporta el tráfico del mensaje de datos de 10 Mb/s.
- Mantiene operando por encima de 0 a por lo menos 2000 metros de cable de fibra óptica.

- Transmite datos y los señales síncronamente con el reloj de bit y recibe los datos sin resincronizandos en cada paquete.
- Conecta un repetidor a un segmento de fibra óptica del backbone.
- Proporciona señalización del punto a punto del estado de la vía de la señalización síncrona.
- Transmite señales síncronas.
- Soporta configuraciones de la red que usan el método de acceso CSMA/CD definidas en la IEEE 802.3 con la señalización de la banda de base.
- Soporta una interconexión de punto a punto entre los repetidores, y cuando se use con repetidores con múltiples puertos, soporta un cableado de una topología de estrella.

2.7.2.4.3 10BASE-FP

El estándar de fibra pasiva (FP) provee un conjunto de especificaciones para una mezcla de segmentos de fibra óptica pasiva. Esto era basado en un dispositivos que no tienen una fuente de poder que actuaban como acoplador óptico de la señal de la fibra, conectándose múltiples computadoras en un sistema de fibra óptica.

Según la norma, 10BASE-FP los segmentos pueden ser hasta 500 metros de largo; un solo acoplador de 10BASE-FP de señalización pasiva de fibra óptica puede unirse hasta 33 computadoras. El equipo basado en este estándar no existe.

Unidad agregada al medio

La unidad agregada al medio de 10BASE-FP tiene las características generales siguientes:

- Soporta totalmente una topología pasivo-estrella de interconexión medios.
- Conecta un DTE o repetidor a un segmento 10BASE-FP de fibra óptica.
- Soporta un tráfico de mensaje de datos de 10 Mb/s.
- Permite arriba de 500 metros de cable de fibra óptica, entre los MAU de 10BASE-FP y un 10BASE-FP Estrella.
- Permite al DTE o a repetidor confirmar funcionamiento del MAU y disponibilidad del medio.
- Permite al DTE probar la circuitería de detección de colisión del MAU.

- Transmite codificado el "jam" durante la colisión para determinar la detección del fin de colisión.

- Soporta configuraciones de la red que usan el CSMA/CD mecanismo de acceso definido en esta norma.

A. Componentes del Medio 10BASE-FL

Los siguientes componentes del medio son usados para segmentos en fibra óptica:

- Cable de fibra óptica.
- Conectores de fibra óptica.

1) Cable de fibra óptica

Las especificaciones del cable de la fibra óptica en el estándar para una conexión al segmento consiste de una clasificación, cable fibra multi-modo (MMF) con un centro de 62.5 micron (μm) de la fibra óptica y un revestimiento exterior de 125μm. La designación para este tipo de fibra es de 62.5/125μm. Cada conexión de fibra óptica requiere de dos cuerdas de fibra, una que transmite los datos y la otra que los reciba.

Para salvaguardar el fiable funcionamiento del sistema ethernet, el aislamiento eléctrico proporcionado por segmentos de fibras ópticas es esencial cuando se instalan los segmentos ethernet entre los edificios. Los medios de comunicación de fibra óptica también es útil en los ambientes como los suelos industriales, además los segmentos de fibra óptica no son afectados por los niveles altos de ruido eléctrico que puede generarse por los motores pesados, soldadores, u otros tipos de equipos.

2) Atenuación

Esta norma se desarrolló en base, a un valor de atenuación igual o menor a 3.75 dB/km, midiendo en una longitud de onda de 850 nm.

3) Modelo de ancho de Banda

Cada fibra óptica tendrá un producto del modelo de longitud de ancho de banda de no menos de 160 MHz-km a una longitud de onda de 850 nm.

4) Retraso de la Propagación

El retraso de la propagación será 5 μs/km. (Esto es equivalente a una velocidad de propagación de 0.67c.).

B. Conectores de fibra óptica

Los conectores de fibra óptica usados en las conexiones de segmentos 10BASE-FL generalmente son conocidos como conector ST. El nombre formal de este conector en el estándar internacional ISO/IEC es BFOC/2.5 *figura 2.26*

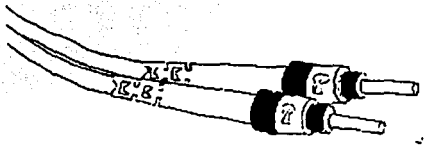


Figura 2.26 Conector ST.

La norma del ethernet contiene las pautas para un solo segmento 10BASE-FL de fibra óptica, así como las pautas por unirse a segmentos múltiples en un sistema half-duplex, *tabla 2.6.*

[illegible]	[illegible]	[illegible]
10BASE-FL	2000m	2
FOIRL	1000m	2

Tabla 2.6 10BASE-FL.

2.7.3.- Fast Ethernet

Una de las opciones más simples para obtener alta velocidad en redes de área local consiste en adaptar el estándar IEEE 802.3 para CSMA/CD a la velocidad de 100Mbps. La idea básica es conservar el método de acceso, MAC, con el objeto de mantener la máxima compatibilidad con la extensa base instalada de redes ethernet e IEEE 802.3 / ISO 8802-3. Pueden destacarse las siguientes características:

- Costo reducido, en línea con la norma Ethernet/IEEE802.3
- Mantener la MAC, para simplificar la interoperabilidad con las redes existentes y poder utilizar el mismo software.
- Utilización de cable UTP (par trenzado sin apantallar), por ser el más extendido y económico.
- Fácil coexistencia y migración con los estándares existentes. La situación ideal es poseer tarjetas de red que operen 10/100 Mbps.

El nivel físico de IEEE 802.3 se ha modificado para obtener la velocidad de 100 Mbps.

100Base-T Fast Ethernet es una mejora en velocidad del sistema original Ethernet, conservando el mecanismo inicial de acceso al medio CSMA/CD (Carrier Sense Multiple Access / Collision Detect). Por ser sólo una actualización de 10Base-T la IEEE decidió hacerlo parte del estándar 802.3 y es conocido como 802.3u (Junio de 1995).

100Base-T Fast Ethernet fue desarrollado para facilitar el trabajo en redes de alta velocidad y su dominio de colisiones a un radio de acción de 205 metros. Fast Ethernet usa cables basados en los dos principales estándares internacionales de construcción de cableados ISO/IEC (International Organization for Standardization / International Electromechanical Commission) 11801 y ANSI-EIA/TIA 568A.

Hay 3 variedades de Ethernet que han sido especificados para transmisión de señales a 100Mbps : 100Base-TX, 100Base-T4, 100Base-FX, *ver tabla 2.7.*

Nombre	Cable	Segmento Máximo
100BaseT4	Par Trenzado	100m
100BaseTX	Par Trenzado	100m
100BaseFX	Fibra Óptica	2km

Tabla 2.7 Cableado para Fast Ethernet.

2.7.3.1. 100Base TX

El sistema 100Base-TX esta diseñado para permitir segmentos de hasta 100 metros de longitud cuando usamos cable UTP que tiene una impedancia característica de 100 ohmios y sigue las especificaciones EIA/TIA de cable categoría 5. Los segmentos de 100Base-TX están limitados a un máximo de 100 metros para asegurar que las especificaciones *del "round trip timing"* sean cumplidas. El estándar de cableado EIA/TIA recomienda una longitud de 90 metros entre el equipo terminal en el cuarto de cableado y el "wall plate" en la oficina. Esto provee 10 metros de cable para acomodar remiendos de cable en cada punto final del enlace, perdidas de señales en las terminaciones intermedias de cable sobre el enlace, etc. *figura 2.27.*

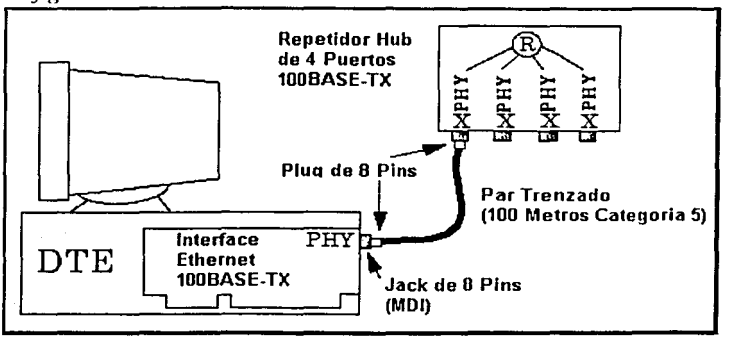


Figura 2.27 100base TX.

2.7.3.2. 100BaseT4

100BaseT4 esta diseñado para correr 100Mbps sobre 4 pares de cable categoría 3, 4 ó 5. Al igual que 100Base-TX en 100BASE-T4 los segmentos están limitados a un máximo de 100 metros para las cumplir especificaciones del "round trip timing". También se recomienda una longitud maxima de 90 metros entre el equipo terminal en el centro de cableado y el "wall plate" en la oficina, *figura 2.28.*

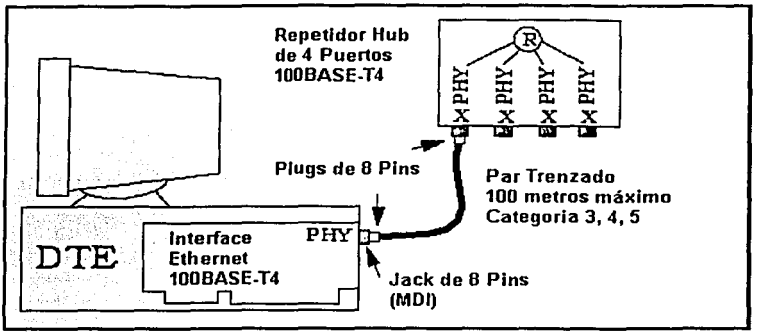


Figura 2.28 100BaseT4.

2.7.3.3. 100BaseFX

100Base-FX define 100Mbps sobre dos hilos de fibra óptica de 62.5/125 micrómetros y usa un esquema de señalización similar al de 100Base-TX. La más grande ventaja de 100Base-FX es su habilidad para transmitir datos sobre distancias más largas que el cable UTP. Este es usado particularmente para conexiones entre bridges, routers y switches en los backbones de las redes.

100Base-FX usa conectores de fibra MIC, ST ó SC, los mismos definidos por FDDI.

El sistema media 100Base-FX esta diseñado para permitir segmentos de hasta 412 metros de longitud. Aunque es posible enviar señales sobre fibra para distancias mucho más largas, el limite de los 412 metros para segmentos de fibra en Fast Ethernet se tiene para asegurar que las especificaciones del "round trip timing" sean cumplidas.

Las especificaciones de 100Base-FX dicen que se requieren dos hilos de cable de fibra óptica multimodo (MMF, del ingles MultiMode Fiber), por enlace, uno para transmisión de datos, y otro para recibir datos, *figura 2.29.*

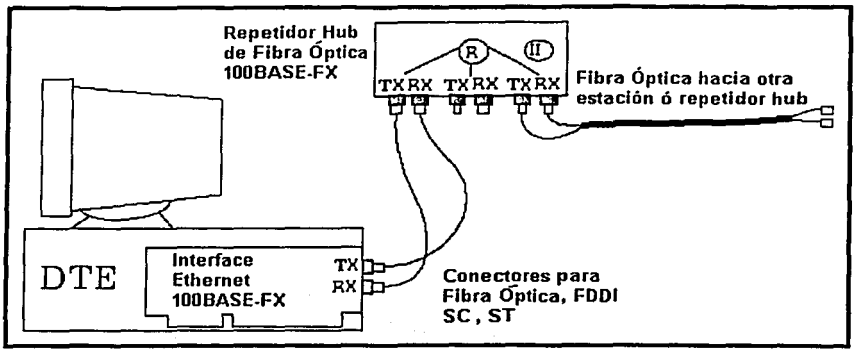


Figura 2.29 100BaseTX.

Round Trip Timing

Para que el sistema de control de acceso al medio actúe adecuadamente, todas la interfaces Ethernet deben ser capaces de responder a otras señales dentro de una cantidad de tiempo especificada. La cantidad de tiempo que le toma a la señal ir desde un punto final del dominio de colisión hasta otro punto extremo y volver es conocido como "round trip time". El máximo "round trip time" de las señales sobre el canal Ethernet esta estrictamente limitado para asegurar que cada interfaz Ethernet pueda escuchar todas las señales de la red en una cantidad de tiempo especificada provista por el sistema de control de acceso al medio Ethernet. Entre más largo sea un segmento de red, más tiempo le tomara a la señal viajar sobre él. Existen unas guías de configuración cuya intención es que estemos seguros que los limites del "round trip timing" sean conocidos, sin importar que tipo de medio de segmentos sea usado en el sistema. Las guías de configuración proveen reglas para combinar segmentos con repetidores de tal forma que el tiempo correcto de señal sea mantenido en la LAN entera. Si las especificaciones para las longitudes de cada segmento y las reglas de configuración para combinación de segmentos no son seguidas, entonces las computadoras pueden no escuchar señales de otras computadoras dentro del tiempo límite requerido, y podrían interferir generando colisiones. La operación correcta de un LAN Ethernet depende de que los segmentos hayan sido construidos de acuerdo a las reglas publicadas para cada tipo de medio (100Base-TX, 100Base-T4 o 100Base-FX).

2.7.3.4 100VG-AnyLAN

La tecnología 100VG-AnyLAN fue desarrollada por Hewlett Packard (HP) como alternativa de CSMA/CD para aplicaciones novedosas sensibles al tiempo, como multimedia. El método de acceso se basa en demanda de las estaciones y se diseño como un método mejorado para redes ethernet y token ring a 16 Mbps, La tecnología 100VG-AnyLan funciona con los siguientes tipos de cable:

- UTP categoría 3 de 4 pares.
- UTP categoría 4 ó 5 de 2 pares.
- STP.
- Fibra óptica.

El estándar del IEEE 802.12 100VG-AnyLan especifica las limitaciones en cuanto a la longitud de enlace, configuraciones del concentrador y distancia máxima de la red. Las longitudes de enlace del nodo al concentrador son de 100 m en categoría 3 del UTP o de 150 m en categoría 5.

Las limitaciones en cuanto a la longitud de extremo a extremo de la red son de 600m en UTP categoría 3 o de 900m en la categoría 5.

La tecnología 100VG-AnyLAN utiliza el método de acceso de prioridad por demanda con el que se eliminan las colisiones y permite tener una carga de tráfico mayor que 100BaseT. El método de acceso de prioridad por demanda es más determinista que CSMA/CD, debido a que el concentrador controla el acceso a la red.

2.7.4. Gigabit Ethernet

Gigabit Ethernet es una extensión a las normas de 10-Mbps y 100-Mbps IEEE 802.3. Ofreciendo un ancho de banda de 1000 Mbps, Gigabit Ethernet mantiene compatibilidad completa con la base instalada de nodos Ethernet.

Sus características principales son:

- Velocidad de proceso de datos de 1000 Mbps.
- Compatibilidad con 10BaseT y 100BaseT.
- Transmisiones *half* (para conexiones compartidas que usan repetidores y los métodos de acceso CSMA/CD) y *full-duplex* (para conexiones conmutador - conmutador y conexiones conmutador - estación) a 1000 Mbps.

Los medios portadores y distancias que soportarán este tipo de tecnología son:

- 500 metros con fibra óptica multimodo.
- 2000 metros con fibra óptica monomodo.
- 25 metros con Coaxial.
- 100 con UTP Categoría 5.

2.7.5. Fiber Distributed Data Interface (FDDI)

Basado en un medio de transmisión de fibra óptica, el protocolo FDDI define una interconexión de propósito general para todo tipo de ordenadores y periféricos a una velocidad de transmisión de 100 Mbps.

El estándar FDDI fue desarrollado por el grupo de trabajo ANSI X3T9.5. Se describió una red que proporcionara una interconexión de propósito general, con alto ancho de banda, entre ordenadores de alta velocidad y periféricos de todas las clases. Las características principales de una red FDDI son:

- Utilización de un esquema MAC de paso de testigo basado en el estándar IEEE 802.5 (Token Ring).
- Compatibilidad con las redes de área local IEEE 802 mediante el uso del nivel LLC (logical link control) del 802.2.
- Capacidad de utilizar fibra óptica, así como par trenzado.
- Una topología de doble anillo para soportar la tolerancia a fallos.
- Velocidad de transmisión de 100 Mbps.
- Conexión física de hasta 500 estaciones (ó 1000 accesos MAC, teniendo en cuenta la topología de doble anillo).
- Un cableado de fibra óptica de hasta 100 Km por anillo (200 Km en total considerando dos anillos).
- La capacidad de asignar dinámicamente ancho de banda, de manera que se pueden proporcionar simultáneamente tanto servicios de datos síncronos como asíncronos.

2.7.6. Frame Relay

Frame Relay es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.

Frame Relay ha evolucionado, proporcionando la integración en una única línea de los distintos tipos de tráfico de datos y voz y su transporte por una única red que responde a las siguientes necesidades:

- Alta velocidad y bajo retardo.
- Soporte eficiente para tráficos a ráfagas.
- Flexibilidad.
- Eficiencia.
- Buena relación costo – beneficio.
- Transporte integrado de distintos protocolos de voz y datos.
- Conectividad "todos con todos".
- Simplicidad en la gestión.
- Interfaces estándares y acuerdos de implantación.

En 1988, el ITU-T (antiguo CCITT, Comité de Consulta Internacional de Telefonía y Telegrafía) estableció un estándar (I.122), que describía la multiplexación de circuitos virtuales en el nivel 2, conocido como el nivel de "frame" (trama). Esta recomendación fue denominada Frame Relay.

ANSI tomó lo anterior como punto de partida y comenzó a definir estándares que iban siendo también adoptados por el ITU-TSS (CCITT). *Ver tabla 2.8.*

Estándares

ITU/T	ANSI
Descripción del Servicio	1.233 T1.606
Transferencia de Datos	0.922 T1.618
Señalización	0.933 T1.617
Congestión	I.370 T1.606
Interworking	I.555

Tabla 2.8 Estándares para Frame Relay.

2.7.7. Asynchronous Transfer Mode (ATM)

Es la tecnología que administra el ancho de banda asignado a cada una de las señales que circulan por la red, sean estas voz, datos o imágenes, de manera que el usuario final la reciba en forma integrada.

En términos técnicos, ATM consiste en un protocolo en el cual la información a transmitir es almacenada en celdas de 53 bytes de largo, de los cuales cinco se usan en el control de la transmisión y los 48 restantes para el envío de información útil.

Este fue seleccionado por la CCITT. Como base para Broadband ISDN(B-ISDN) en 1988. Desde entonces se ha continuado con el trabajo en las especificaciones de los detalles de ATM en sí mismo(Estandarizado en 1991), y en las interfaces ATM a diferencia de los requerimientos de servicios B-ISDN (Parcialmente estandarizado en 1991).

ATM debe ser capaz de llevar servicios de banda ancha alta, tales como Televisión de alta definición (HDTV High Definition Television) así como los servicios más convencionales de Banda ancha baja tales como la voz.

ATM debe de ser capaz de proveer transporte en redes de banda ancha alta, enlazando oficinas centrales en ambientes de redes públicas. En redes privadas, la banda ancha alta es también requerida para incorporarse a un sitio y entre sitios. En estas situaciones los anchos de banda altos se deben a los servicios de Banda ancha o alternativamente resultará de la multiplexión de grandes volúmenes de servicios de banda ancho bajos. La interfaz especificada por la CCITT para B-ISDN son de 155 Mbps y 622 Mbps. En Norte América, ANSI (American National Standards Institute Organization), también tienen aprobada una interfaz de 45 Mbps.

El mayor atractivo de ATM desde el punto de vista de un operador de redes públicas, no es el ancho de banda alto en sí, sino la habilidad de integrarse a una variedad de servicios diferentes dentro de una sola red usando un sólo método de transmisión y conmutación.

Los beneficios de integración son ahorros en términos de:

- Que reduce los costos en el equipo.
- Que reduce costos de operación.
- Que reduce costos de mantenimiento

2.8. Internet 2

Internet, como lo conocemos hoy en día, tiene sus orígenes en un proyecto del Departamento de Defensa de los Estados Unidos en 1969. El proyecto consistía en lo siguiente: "Comunicaciones digitales en tiempo de guerra". Lo que se quería lograr era una red digital de comunicaciones que en tiempo de guerra siempre estuviera funcionando.

Para 1985 las redes locales en computadoras personales ya estaban madurando y esto ayudó a completar la idea de Internet. Ya podíamos tener redes y sub-redes, podíamos conectar redes de área ancha con redes locales.

Internet2 (también conocida como I2) es un proyecto colectivo que reunió en sus inicios a más de 100 universidades de los Estados Unidos de América. Un objetivo básico de Internet2 es desarrollar la próxima generación de aplicaciones telemáticas para facilitar las misiones de investigación y educación de las universidades En cada una de las universidades que participan en el proyecto existe un equipo de desarrolladores e ingenieros que trabaja para desarrollar y hacer posibles las aplicaciones de Internet2. El proyecto Internet2 lo inició en el otoño de 1996 un grupo de universidades que se unieron a socios empresariales y gubernamentales para acelerar conjuntamente la próxima etapa del desarrollo de Internet.

Internet2 no substituirá a la Internet actual ni tiene como objetivo construir una red nueva que compita con la anterior. Inicialmente, Internet2 hará uso de la redes nacionales norteamericanas existentes tales como la *vBNS National Science Foundation's very high speed Backbone Network Service).*

En último término, I2 utilizará otras redes de alta velocidad para conectar a todos sus miembros entre sí y con otras organizaciones de investigación. Parte de la misión de Internet2 es asegurar que tanto la tecnología hardware como software se basan en estándares abiertos y puede ser adoptada por otros, incluidas las redes comerciales y los proveedores de servicios Internet (ISP's por sus siglas en inglés).

Fundamental para el diseño de la infraestructura de la Internet2 es el mantenimiento de un "servicio portador común" para la comunicación entre las aplicaciones de red. El "servicio portador" es la interfaz básica de transporte de información para las comunicaciones de área extensa, de forma análoga a la capa 3 (capa de red) en el modelo de red *ISO*. Una de las características más potentes de la Internet actual es la capacidad de un nodo de comunicarse con cualquier otro en un formato de transporte compatible. Este debe conservar esta misma potencia en Internet2.

El servicio portador común hoy en día es el Protocolo Internet (*IP* o *Internet Protocol*) versión 4. I2 desplegará IP versión 6 (*IPv6*) tan pronto como sea posible. Pero todas las implantaciones deberán ser compatibles con la anterior versión *IPv4*.

Además de implementar *IPv6*, I2 debe permitir a las aplicaciones especificar una "calidad de servicio" (*QoS* o *Quality of Service*) de red en cuestiones tales como la velocidad de transmisión, el retardo limitado y los límites de variación del mismo, el rendimiento y la planificación.

El nuevo elemento clave en esta arquitectura es el gigapop (de gigabit capacity point of presence o "punto de presencia con capacidad de gigabits") - un punto de interconexión de tecnología avanzada y alta capacidad donde los participantes de I2 pueden intercambiar tráfico de servicios avanzados con otros participantes del proyecto. Las universidades de una determinada región geográfica se unirán en un gigapop regional para conseguir una variedad de servicios Internet.

2.8.1 Ipv6

Entre las principales características de la versión 6 de IP destaca que introduce más capacidad de direccionamiento, gracias a que sus direcciones son de 128 bits, en lugar de los 32 bits que contienen las habituales direcciones Ipv4 a las que se esta acostumbrado en Internet. Esta mayor capacidad soluciona la problemática presentada del agotamiento de las direcciones, y permite cubrir la necesidad que en la actualidad se empieza a presentar de dar cabida para conectar un gran número de nuevos equipos a Internet.

La notación con la versión 6 de IP varía a la usada por su antecesor. Si con el IPv4 las direcciones IP se representaban de la siguiente forma: 192.172.34.3, con el nuevo IPv6 se amplía el número de direcciones quedando así: FF02::AC:D:F, donde el símbolo"::" representa tantos grupos de ceros para llegar a los 8, en lugar de los 4 de la versión IPv4.

Esta gran capacidad de direccionamiento permite efectuar una división muy jerárquica del espacio de direcciones para facilitar el enrutado. De esta forma se solventa la problemática del desbordamiento del límite de las tablas de enrutado de los sistemas. La estructura jerárquica de las direcciones IPv6 disponibles ha sido muy bien definida, quedando incluidas dentro de esta estructura de direcciones las direcciones actuales de IPv4.

El aspecto de la seguridad ha sido otro de los puntales en la mejora del protocolo IP, ya que se incluye autentificación, integridad de los datos y, opcionalmente, la confidencialidad de la información. De esta forma se solucionan los aspectos de seguridad que no se cubrían en la versión 4 de IP ya que el diseño inicial de la arquitectura Internet era para una red reducida con una cierta confianza, características que desaparecen con el aumento de tamaño de usuarios de Internet y del creciente número de operaciones comerciales que se realizan a través de ella.

Capítulo III

Diseño de Redes de Cómputo.

CAPÍTULO III:
DISEÑO DE REDES DE CÓMPUTO

Este capítulo provee reglas para analizar las necesidades técnicas de los clientes para un diseño de redes de la empresa. Analizando las metas técnicas del cliente se pueden recomendar tecnologías que podrían cubrir por completo las necesidades. Además se tocarán las tecnologías de alta velocidad que se utilizan frecuentemente en la operación de las redes área local por su gran versatilidad. En el capítulo anterior se dio un panorama general, ahora se tratarán con mayor detalle para finalizar con un cuadro comparativo donde se definirá la tecnología a utilizar en la implantación del diseño.

3.1 Diseño de redes de cómputo

3.1.1 Consideraciones técnicas

Las típicas metas técnicas en el diseño de redes de cómputo incluyen: escalabilidad, disponibilidad, rendimiento, administración, utilización, flexibilidad y relación costo-beneficio.

Escalabilidad

Se refiere a como va a crecer el diseño de la red. La escalabilidad es en la mayoría de las empresas una de las primeras metas ya que diariamente en las compañías se están adhiriendo usuarios, aplicaciones, sitios y conexiones externas a la red. El propósito del diseño de una red es adaptarse al incremento y adhesión de usuarios.

Planeando la expansión.

Para planear el crecimiento de la red, es necesario indagar con el cliente su visión del crecimiento de su red en el siguiente año y como lo proyecta a 5 años más. Las siguientes preguntas pueden ser útiles para tener una idea clara sobre la visión de los clientes:

- ¿Cuántos nodos serán adheridos en el siguiente año?.
- ¿Cómo se podría extender la red a cada uno de esos nodos?.
- ¿Cuántos usuarios podrían ingresar a la intranet de la organización?.
- ¿Cuántos servidores podrían adherirse en el siguiente año?, entre otras.

Expandiendo la información disponible a los usuarios.

La información en las empresas es tradicionalmente alojada en los servidores centralizados, sin embargo, ya en los 90's las compañías han colaborado entre sí para organizar las extranets (sitios alojados en una empresa, pero que otras empresas pueden acceder a esa información), con el fin de cooperar en el desarrollo de las mismas. Junto con lo anterior, las nuevas metas en los negocios hacen necesario que la información este disponible de manera inmediata haciendo que el rendimiento de las redes se base en los siguientes puntos:

- Conectar rápidamente los departamentos dentro de la red de la empresa.
- Eliminar los problemas de cuellos de botella causados por el incremento del tráfico de la red y por la mala planeación de la misma.
- Colocar servidores centralizados que residan en granjas de servidores de la intranet.
- Agregar nuevos sitios que funcionen como cuartos de comunicaciones.

Finalmente, una vez tomando en cuenta los puntos anteriores, se debe tener cuidado al seleccionar la tecnología para la red, ya que ésta debe ser capaz de manejar un gran número de usuarios y aplicaciones de manera que la cantidad no afecte el rendimiento de la red.

Disponibilidad

Se refiere a la cantidad de tiempo que la red esta disponible para satisfacer las necesidades de los usuarios. La disponibilidad puede ser expresada como un porcentaje de un periodo, ya sea años, meses, semanas, días u horas.

La disponibilidad es en si, el tiempo en que la red esta en un estado operacional.

A menudo se confunden disponibilidad con la redundancia, sin embargo la segunda es una técnica o solución para llegar a la primera. Otro aspecto de la disponibilidad es la prevención de desastres. Un plan de prevención de desastres incluye un proceso para mantener la información a salvo o poder acceder a ella desde algún sitio alterno.

Algo más que considerar respecto a la disponibilidad son los costos que se tendrán que absorber por el tiempo que la red no este operando adecuadamente y por lo tanto la información no este disponible; de igual manera se debe considerar el costo que involucra el tiempo en que el equipo presenta fallas y el tiempo en que se resuelve este problema. Observando lo anterior, se puede estar seguro de que cualquier falla en la red representa una gran pérdida de recursos y tiempo.

Rendimiento de la red

Cuando se analizan los requerimientos técnicos en el diseño de la red, se debería introducir el concepto de rendimiento de los equipos al criterio del cliente, es decir, los conceptos de tolerancia a fallas, eficiencia, respuesta en el tiempo, etc., características propias de los dispositivos.

Un buen comienzo para analizar el rendimiento de la red, es el analizar el rendimiento de la red existente y determinar en que se esta acertado y en que hay fallas.

El rendimiento se puede medir en capacidad (ancho de Banda- BW), utilización de la red, tolerancia a fallas de los equipos, eficiencia de los mismos, retardo y respuesta en el tiempo.

Seguridad

Este aspecto es uno de los principales a contemplar en el diseño de redes, esto debido a que cada vez son más las compañías que se conectan a Internet y que comparten información con otras empresas mediante una Extranet, por lo cual necesitan que su información tenga la mayor seguridad posible.

El paso esencial para tener una red segura, es la planeación. Mediante esta se analizan los riesgos y requerimientos de la red.

Es de suma importancia el mantener la red fuera del alcance de los hackers, estos individuos pueden desde urgar en la información hasta hacer mal uso de ella. Mucha de la seguridad en la red depende no sólo de los dispositivos y software implementados, si no de la políticas de seguridad que se sigan internamente en la empresa.

Administración

Para cada cliente el concepto de administración difiere enormemente. Para algunos solo es necesario contar en sus equipos con el protocolo SNMP (Simple Network Managment Protocol – Protocolo Simple de Administración de Red) para monitorear los dispositivos de la red, mientras que para otros es necesario la definición de un plan.

Cuando no se tiene un plan para la administración, se puede considerar el tomar como base para la definición del plan la terminología utilizada por la ISO (International Organization for Standarization – Organización Internacional de Estandarización):

- Administración de rendimiento: Para ello es necesario analizar el tráfico y el rendimiento antes de optimizar la red.
- Administración de fallas. Aquí se debe detectar, aislar y corregir los problemas reportados por los usuarios finales.
- Administración de la configuración. Se debe controlar, operar, identificar y colectar los datos de los dispositivos principales que componen la red.
- Administración de la seguridad. Finalmente, es necesario monitorear y probar las políticas de seguridad.

La mayoría de la veces, estas tareas de administración de rendimiento, de fallas, de configuración y seguridad recaen en el personal de la empresa cliente, por lo que también se vuelve necesario la capacitación en la administración de la red.

Facilidad de uso

Se refiere a la sencilla manera en que los usuarios pueden acceder a la red o a sus recursos. Este punto es importante ya que una mala administración o estrictas políticas de seguridad pueden provocar que el usuario se sienta incómodo al utilizar los recursos de la red y optar por no usar ésta.

Flexibilidad

Durante el diseño de la red es importante considerar que los equipos que se tomen en cuenta puedan adaptarse a nuevas tecnologías o bien, conectarse con equipos diseñados para esas tecnologías.

Así mismo, es importante la flexibilidad de los dispositivos al manejo o convivencia con los diferentes protocolos y o tecnologías existentes, la capacidad de adaptarse al tráfico cambiante y a los requerimientos de calidad de servicio (QoS), en suma, la capacidad de estar preparado para soportar nuevas tecnologías en un futuro inmediato.

Relación costo vs beneficio

Este es un aspecto muy importante para el cliente ya que se refiere al costo – beneficio que tendrá el equipamiento del nuevo diseño de la red. Parte importante de esta meta es el no requerir a dispositivos costosos ni baratos, si no a recurrir a una red operacional.

Un aspecto adicional que se debe tomar en cuenta para instalar, mantener y administrar la red son los costos que se tendrán que hacer para la capacitación del personal que se hará cargo de la red, gastos que muchas empresas no ven como algo redituable.

3.1.2 Diseño de topología de red

Una topología es un mapa de una red que indica los segmentos de red, puntos de interconexión y los grupos de usuarios. El principal propósito es el mostrar la geografía de la red. El mapa muestra por donde corre la red, su localización y el tamaño de las oficinas, pero no muestran los materiales con que estas están construidas.

Durante la fase de diseño, se deben identificar los puntos de interconexión, el tamaño y alcance de la red y los tipos de dispositivos que podrían ser requeridos, pero ya no se toma en cuenta la estructura actual de la red. Si alguna de las rutas actuales nos sirve para nuestro propósito, entonces es válido tomarla en cuenta.

Dentro del diseño de topologías de red se contemplan 3 modelos básicos: Modelo Jerárquico, Modelo de Redundancia y Modelo de Seguridad. A continuación se describen cada uno de ellos, de acuerdo a documentación publicada por Cisco Sytems[13].

[13] Dirección de Internet de Cisco Systems http://www.cisco.com

3.1.2.1 Diseño Jerárquico

Cuando se habla de una red de más de 50 nodos, se esta hablando de diseñar una topología consistente en componentes interrelacionados. Esta topología se puede facilitar tomando la filosofía de "divide y vencerás".

Se ha creado un modelo de red llamado jerárquico que ayuda a desarrollar una topología en capas. Cada capa puede tener una función específica, dependiendo de las aplicaciones que se quiera que ejecute cada una.

Una típica topología jerárquica consta de 3 capas:

- Capa de Core. Es la parte final superior (puede ser un ruteador o un switch) que optimiza la disponibilidad y el rendimiento de la red. En ella hay un intercambio de información a gran velocidad para intercambiar los paquetes tan rápido como sea posible. Esta capa no debe realizar ninguna manipulación de la información;

- Capa de distribución. En ella principalmente se implementan políticas. Su propósito es definir el límite entre las otras capas y es el lugar donde la manipulación de la información tienen lugar;

- Capa de Acceso. En esta capa se conectan los usuarios finales locales a los dispositivos (ruteadores o switches).

Las redes que están creciendo sin un plan a seguir tienden a convertirse en un formato desestructurado. Cuando los dispositivos de red tienen que comunicarse con varios dispositivos más, el intercambio de información entre ellos provoca un mayor retardo en la información. Un paquete de broadcast al ser procesado consume tiempo del procesador en cada uno de los dispositivos del dominio de broadcast. Estos dispositivos incluyen: ruteadores, estaciones de trabajo y otros servidores.

Un diseño de red jerárquico es una topología modular que limita el número de peticiones entre los dispositivos de la red. Usando el modelo jerárquico se pueden reducir los costos y se pueden conseguir los dispositivos apropiados para cada capa. La modularidad del modelo garantiza un crecimiento ordenado y reducción del uso del ancho de banda. La responsabilidad de la administración de la red y los sistemas de administración pueden ser distribuidos en las diferentes capas de la arquitectura modular.

El diseño jerárquico facilita los cambios de los dispositivos y/o tecnologías ya que tarde o temprano por la evolución misma de la red los cambios tienen que darse; de la misma manera, esta modularidad hace que el costo de una actualización este implícita en una pequeña partida del total de la red. En una arquitectura de malla, los cambios tienen un gran impacto en la red debido a lo complejo de ésta, lo que no sucede con el modelo jerárquico.

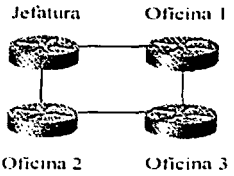
Cuando la escalabilidad es una de las principales metas, la topología jerárquica es recomendada por su modularidad y sencillo crecimiento e implantación.

Topología Plana vs Jerárquica

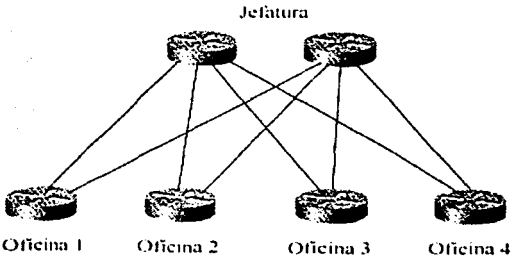
Una topología plana es adecuada para redes pequeñas. En esta topología cada dispositivo realiza esencialmente el mismo trabajo y la red no esta dividida en capas o módulos. Una topología plana es fácil de diseñar e implantar, pero ésta se complica cuando se tienen la necesidad de crecer.

Una pequeña Red de Área Amplia (WAN), consiste en pocos sitios conectados entre si creando un lazo cerrado, comúnmente un loop. Cada dispositivo es conectado a otros 2 dispositivos punto a punto. Una topología plana no es recomendable para redes con varios dispositivos.

Un loop en la topología puede significar que hay muchos saltos entre los dispositivos, resultando un significante retardo y una alta probabilidad de fallas. En un análisis de tráfico, el flujo indica que los ruteadores en lados opuestos en una topología con loop intercambian mucho tráfico, por lo que se debe recomendar una topología jerárquica en lugar de la anterior. Para evitar cualquier punto de falla, los dispositivos redundantes pueden ser situados en las capas superiores del modelo jerárquico, *figura 3.1.*



Topología plana de loop



Topología jerárquica redundante

Fig. 3.1 Topología plana de loop y Jerárquica redundante.

El clásico modelo Jerárquico de 3 capas.

El modelo de 3 capas permite balancear y filtrar tráfico por 3 sucesivas capas de ruteadores y/o switches. Esta característica hace que el modelo escalable jerárquico de 3 capas sea el modelo más utilizado internacionalmente. Aunque el modelo fue desarrollado originalmente solo para ruteadores, hoy es aplicable a otros dispositivos como los switches. A continuación se muestra la clásica topología de 3 capas.

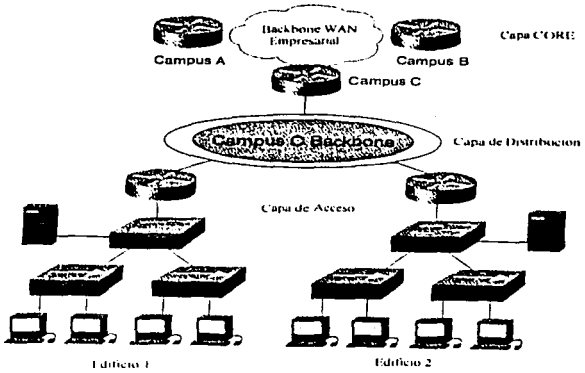


Fig. 3.2 Una clásica topología jerárquica.

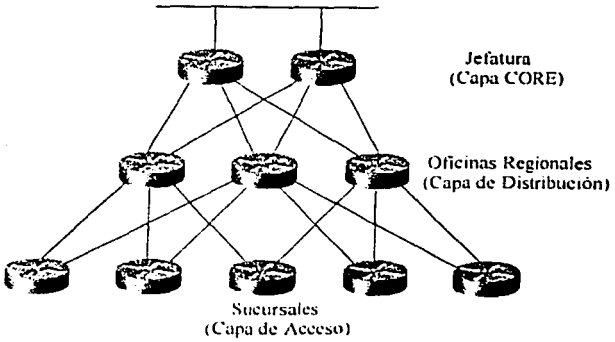


Fig. 3.3.- Acoplamiento parcial del diseño Jerárquico.

En el modelo cada capa tiene un papel específico. La capa de core provee un óptimo transporte de la información entre los diferentes sitios. La capa de distribución conecta los servicios de red a la capa de acceso e implementa las políticas referentes a la seguridad, lectura de tráfico y ruteo. En el diseño de una WAN, la capa de acceso consiste de ruteadores en cada límite de las redes de campus; en una red de campo, la capa de acceso provee acceso a los usuarios finales mediante switches.

Capa de Core

Como ya se mencionó, en este capa es donde se da un intercambio de información a gran velocidad. Debido a que la capa de core es crítica en la interconectividad, se debe diseñar esta capa con dispositivos redundantes. La capa de core debe ser altamente fiable y debería adaptarse a los cambios rápidamente.

Cuando se configuran ruteadores para esta capa, se deben usar dispositivos que optimicen el procesamiento de los paquetes. Se recomienda evitar el filtrado de paquetes ya que disminuye el procesamiento de la información, además se debe optimizar el core para disminuir la latencia (demora natural de una señal al viajar de un extremo a otro) y tener una buena manipulación.

Esta capa debe estar bien delimitada y ser consistente en su diámetro. Los dispositivos en la capa de distribución y los clientes de la LAN pueden ser agregados en el modelo sin incrementar el diámetro del core. La limitante del diámetro en el core provee un rendimiento previsible y una sencilla resolución de problemas.

Para los cliente que necesitan conectarse con otras empresas vía Extranet o por Internet, esta topología debe incluir uno o más enlaces hacia la red externa. Los administradores de redes corporativas deben analizar a conciencia el crecimiento a nivel regional para su conexión entre las sucursales y/o hacia Internet. Centralizar estas funciones en la capa de core reduce la complejidad y los problemas de ruteo y/o switcheo potenciales y es esencialmente la primera medida de seguridad.

Capa de Distribución

La capa de distribución es el punto de demarcación entre la capa de acceso y la de core. Esta capa tiene muchos roles, incluyendo el control de acceso a los recursos por razones de seguridad y el control del tráfico en la red por razones de rendimiento. La capa de distribución es a menudo la capa de delimita el dominio de broadcast (aunque también puede ser la capa de acceso). Si el plan es implementar VLAN (Virtual LAN – LAN's virtuales), la capa de distribución puede ser configurada para rutear entre VLAN's.

La capa de distribución permite a la capa de core conectar diversos sitios mientras mantengan un alto rendimiento. Para mantener un aceptable rendimiento en el core, la capa de distribución puede distribuir su carga entre el ruteo de protocolos en la capa de acceso y la optimización de los mismos en la capa de core.

Para mejorar el rendimiento del ruteo de protocolos, la capa de distribución puede simplificar el ruteo para la capa de acceso. Para algunas redes, la capa de distribución ofrece ruteo por default a los ruteadores de la capa de acceso y sólo corre protocolos de ruteo dinámico cuando se comunican con dispositivos de la capa de core.

Otra función que puede ocurrir en la capa de distribución es la traducción de direcciones. La traducción de direcciones funciona convirtiendo las IP's de una red privada en legítimas direcciónes de Internet para que sea reconocida por el resto de la organización y/o individuos que acceden al Internet.

Capa de Acceso

La capa de acceso provee a usuarios y/o segmentos locales de acceso a la interredes. La capa de acceso puede incluir ruteadores, switches y hubs. Regularmente los switches son implementados en esta capa en las redes de campus para dividir dominios de ancho de banda que contienen la demanda necesaria de BW para aplicaciones que no pueden tener un rendimiento variable ni compartir dicho BW.

Para redes que incluyen pequeñas oficinas por toda la ciudad, la capa de acceso provee acceso dentro de la red corporativa usando tecnologías WAN como ISDN, Frame Relay, renta de líneas digitales y líneas de modems análogos. Se pueden implementar algunas propiedades de ruteo para controlare la utilización del BW y minimizar el costo del acceso remoto.

Guías para el diseño de Redes Jerárquico

Las siguientes 2 técnicas describen algunos pasos para el diseño de redes jerárquicas. Siguiendo esta simple guía se podrá ayudar a diseñar redes tomando las ventajas y beneficios del diseño jerárquico.

En la primera guía se debe controlar el diámetro de la topología de red jerárquica. En muchos de los casos las 3 capas parecen ser suficientes.

Controlar el diámetro de la red produce una baja y predecible latencia. Esto es algo que ayuda a predecir patrones de ruteo, flujo de tráfico y requerimientos de capacidad. Un diámetro de red controlado provocará una sencilla identificación de problemas y administración de la red.

Un estricto control en la capa de acceso de esta topología debe ser mantenido, ya que esta capa de acceso es más susceptible a violaciones en el diseño de redes jerárquico. Los usuarios en la capa de acceso tienden a agregar segmentos de red de una manera inapropiada. Por ejemplo, un administrador de red de una oficina externa podría conectar esta red a un dispositivo en nuestra capa de acceso, agregando entonces una cuarta capa (este es un error conocido como "agregando eslabones - Chain").

Para evitar lo anterior, hay que eludir las puertas traseras (backdoors). Un backdoor es una conexión entre dispositivos en la misma capa *figura 3.4*. Un backdoor puede ser un ruteador o un switch que conecta 2 redes. Las backdoor deben evitarse debido a que muchas veces causan problemas de ruteo y hacen más difícil la documentación y la identificación de los problemas en la red.

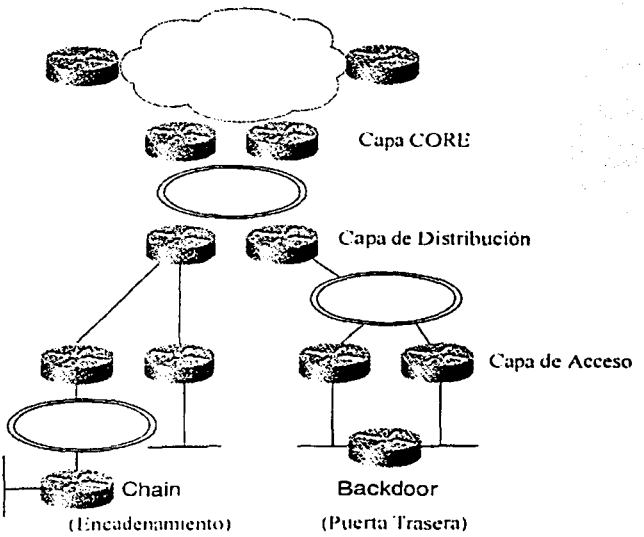


Fig. 3.4.- Eslabones y puertas traseras en la Capa de Acceso.

Algunas veces es válido agregar eslabones o backdoor. Por ejemplo, en una red internacional podría necesitarse un eslabón para conectar otra ciudad. Un backdoor a veces incrementa el rendimiento y redundancia entre 2 dispositivos paralelos en una capa. Pero, en general, otras opciones de diseño pueden ser usadas para no perder la estructura jerárquica. Para maximizar los beneficios del modelo jerárquico, los eslabones y backdoor deben ser evitados.

Finalmente, la otra guía para redes jerárquicas se basa en que se debe diseñar primero la capa de acceso, siguiendo la de distribución y terminando con la capa de core. Para comenzar con la capa de acceso, se debería tener una mayor capacidad de planeación para las capas de distribución y core. Se puede reorganizar las técnicas de optimización necesarias para las siguientes capas.

En general, se debe diseñar cada capa usando técnicas modulares y jerárquicas y entonces planear, las inteconexiones entre capas basándose en análisis de tráfico, flujo y comportamiento.

3.1.2.2 Diseño Redundante

El diseño de red redundante permite mantener la disponibilidad de la red duplicando la conectividad de la red y los dispositivos de interconexión. La redundancia elimina la posibilidad de tener un punto de interconexión propenso a falla en la red. La meta es duplicar algún componente requerido que tenga alguna aplicación o funcionamiento crítico. El dispositivo podría ser un ruteador, una fuente de poder, la conexión hacia la WAN, la conexión hacia el proveedor de Internet, etc.

La redundancia puede ser implementada en ambos extremos de un campus de una red corporativa. Implementar redundancia en redes de campus ayuda a mantener las metas de disponibilidad para el acceso de usuarios en la red local. Implementar redundancia en redes WAN puede ayudar a mantener las metas generales de disponibilidad y rendimiento.

Debido a que la redundancia es costosa de mantener e implementar, se debe tener cuidado al implementar esta topología, además se debe seleccionar que nivel de redundancia apropiado que requieren los clientes para disponer de su información.

Antes de seleccionar un diseño redundante, se debería primero analizar la organización y las metas técnicas del cliente. Se deben identificar las aplicaciones críticas, sistemas, dispositivos de interconexión y conexiones. La no implantación de redundancia podría significar una baja tolerancia de riesgos. Se habrá de discutir con lo clientes las ventajas de la redundancia contra el costo, y la simplicidad contra la complejidad. La redundancia agrega complejidad a la topología de red y agrega además direccionamiento y ruteo.

3.1.2.3 Diseño de Seguridad

Cuando se desarrolla la topología lógica de una red se debe empezar por ver donde el equipamiento podrá ser instalado. Se debe comenzar a trabajar con el cliente para que considere cual sería el equipamiento crítico que debería ser instalado en los cuartos de comunicaciones y que tengan acceso restringido, previendo robo, actos de vandalismo y desastres naturales como fuego, inundaciones, temblores, etc. La seguridad física no es realmente un aspecto de diseño lógico, pero es mencionado aquí porque la planeación de la seguridad física debería empezar por el camino correcto, en este caso darse el tiempo de construir e instalar los mecanismos de seguridad.

Dentro de la seguridad a nivel lógico, existen herramientas llamadas "firewalls" (pared de fuego) que pueden ser encontradas a nivel software y hardware. De acuerdo a la NCSA (National Computer Security Association) en Estados Unidos, un firewall es "un sistema o combinación de sistemas que forzan a un camino entre 2 o más redes". Un firewall puede ser un ruteador con control de acceso a listas (ACL's), un dispositivo dedicado o un software corriendo en una PC o un sistema UNIX. Un firewall debería ser puesto en una topología de red de modo que todo el tráfico externo tenga que pasar por este firewall.

Las políticas de seguridad de la empresa especificarán que tipo de tráfico es autorizado a pasar por el firewall.

Los firewalls son especialmente importantes en el direccionamiento entre redes empresariales y el Internet. Una topología básica de firewall es simplemente un ruteador de una WAN conectado a Internet, una conexión LAN de la red empresarial y software que tiene características de seguridad. Esta elemental topología es apropiada si el cliente tiene políticas de seguridad sencillas. Estas políticas pueden ser implementadas en un ruteador con listas de acceso. El ruteador puede también traducir el direccionamiento de la red para esconder las direcciones de la red de los hackers de Internet.

Para clientes que necesitan publicar datos y proteger algunos de esos datos, el firewall puede incluir una LAN pública con servidores WEB, FTP, DNS y SMNP. La literatura sobre seguridad hace referencia a LAN's publicas como zonas desmilitarizadas. Esta literatura se refiere a un host de una zona desmilitarizada como un sistema seguro que soporta un número límite de aplicaciones para usuarios externos. Los hosts (servidores) a los que los usuarios externos puedan conectarse, como páginas WEB, son extremadamente protegidos de usuarios externos con el fin de que no manipulen la información.

Para grandes clientes, es recomendable usar firewall dedicados en adición con ruteadores entre Internet y la red empresarial. Para maximizar la seguridad, se pueden habilitar características de seguridad en los ruteadores y en el firewall dedicado, sin embargo el habilitar estas políticas en el ruteador disminuye el rendimiento de la red. A continuación se muestra un esquema para esta propuesta:

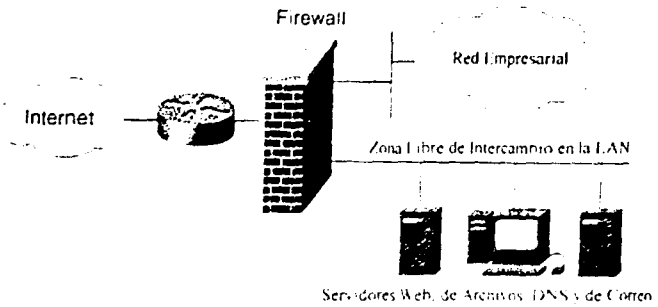


Fig. 3.5.- Zona Libre de intercambio de información dentro del Firewall

Una topología alterna es el usar 2 ruteadores como firewall y crear entre ellos una zona desmilitarizada donde residan los servidores de la red pública *figura 3.6*. El clásico firewall compuesto por 3 partes provee una excelente protección, la única desventaja es que la configuración de los ruteadores podría ser demasiado compleja, consistente en muchas listas de acceso para el control del tráfico dentro y fuera de la red privada y la zona libre.

Las políticas de seguridad de la empresa especificarán que tipo de tráfico es autorizado a pasar por el firewall.

Los firewalls son especialmente importantes en el direccionamiento entre redes empresariales y el Internet. Una topología básica de firewall es simplemente un ruteador de una WAN conectado a Internet, una conexión LAN de la red empresarial y software que tiene características de seguridad. Esta elemental topología es apropiada si el cliente tiene políticas de seguridad sencillas. Estas políticas pueden ser implementadas en un ruteador con listas de acceso. El ruteador puede también traducir el direccionamiento de la red para esconder las direcciones de la red de los hackers de Internet.

Para clientes que necesitan publicar datos y proteger algunos de esos datos, el firewall puede incluir una LAN pública con servidores WEB, FTP, DNS y SMNP. La literatura sobre seguridad hace referencia a LAN's publicas como zonas desmilitarizadas. Esta literatura se refiere a un host de una zona desmilitarizada como un sistema seguro que soporta un número límite de aplicaciones para usuarios externos. Los hosts (servidores) a los que los usuarios externos puedan conectarse, como páginas WEB, son extremadamente protegidos de usuarios externos con el fin de que no manipulen la información.

Para grandes clientes, es recomendable usar firewall dedicados en adición con ruteadores entre Internet y la red empresarial. Para maximizar la seguridad, se pueden habilitar características de seguridad en los ruteadores y en el firewall dedicado, sin embargo el habilitar estas políticas en el ruteador disminuye el rendimiento de la red. A continuación se muestra un esquema para esta propuesta:

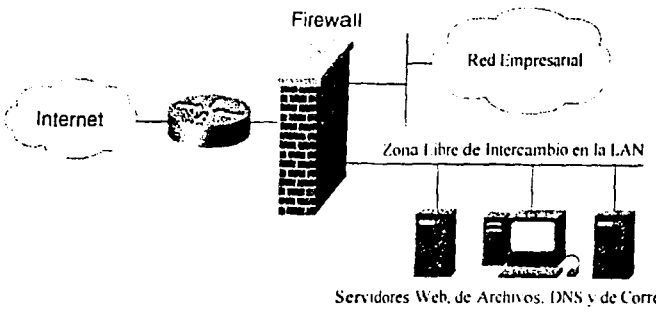


Fig. 3.5.- Zona Libre de intercambio de información dentro del Firewall

Una topología alterna es el usar 2 ruteadores como firewall y crear entre ellos una zona desmilitarizada donde residan los servidores de la red pública *figura 3.6*. El clásico firewall compuesto por 3 partes provee una excelente protección, la única desventaja es que la configuración de los ruteadores podría ser demasiado compleja, consistente en muchas listas de acceso para el control del tráfico dentro y fuera de la red privada y la zona libre.

Usualmente los firewalls dedicados tienen una interfaz gráfica que facilita las políticas de seguridad y su administración.

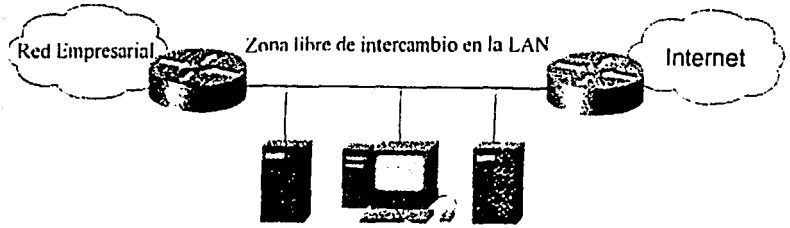


Fig. 3.6.- Topología en 3 partes con Firewall.

3.1.3.- Evaluación de los servicios de core

A continuación se describen características que soportan los servicios de CORE. Los puntos a tratar son los siguientes:

- Optimización del camino.
- Priorización del tráfico.
- Balanceo de cargas.
- Caminos alternativos.
- Acceso switcheado.
- Encapsulamiento.

Optimización de los caminos

Una de las ventajas de un ruteador, es su capacidad para ayudar a implementar un medio ambiente lógico con caminos óptimos para que el tráfico lo seleccione automáticamente. Los ruteadores cuentan con protocolos de ruteo que son asociados con varios niveles de protocolos de red para lograr la automatización de la optimización de los caminos.

Dependiendo de los protocolos de red implementados, los ruteadores permiten llevar a cabo ambientes de asignación de rutas que satisfacen los requerimientos de esa red. Por ejemplo, en una red IP, los ruteadores CISCO pueden soportar todos los protocolos de ruteo implementados incluyendo OSPF, RIP, IGRP, BGP, EGP y Hello. La llave que permite la capacidad de optimizar los caminos incluye la rápida y controlable convergencia de ruteo, métricas y tiempos de ruteo.

La convergencia es el proceso en el cual todos los ruteadores están en las rutas óptimas. Cuando un evento de la red provoca detener la operación de algunas rutas o poner disponibles otras, los ruteadores distribuyen los mensajes de actualización de asignación de rutas. Los mensajes de actualización penetran en las redes, estimulando el cálculo de las nuevas rutas y actualizando a los ruteadores para que se aprendan las nuevas rutas. Los algoritmos de ruteo que convergen suavemente pueden causar loops o paros de la red.

Diferentes y múltiples métricas son usadas por los algoritmos de ruteo. Algunos sofisticados algoritmos de ruteo basan la selección de la ruta en la combinación de diferentes métricas, resultando una métrica híbrida. La combinación de valores como ancho de banda (BW), tráfico y retardos crean una métrica compleja. Los protocolos de ruteo emplean una métrica que representa el costo asociado a la ruta.

Priorización de tráfico

Aunque algunos protocolos de red pueden priorizar tráfico homogéneo interno, el ruteador prioriza el flujo de tráfico heterogéneo. Dicha priorización de tráfico habilita políticas basadas en ruteo y asegura que protocolos transporta los datos de la misión crítica y que toman precedencia sobre tráfico menos importante.

Colas de prioridad.

Las colas de prioridad permiten al administrador de red prioriza el tráfico. El tráfico puede ser clasificado de acuerdo a varios criterios, incluyendo tipos de protocolo y subprotocolos, entonces el tráfico puede quedar en una de las 4 colas: alta, media, normal y baja (la mayoría de los equipos soportar ya hasta 8 colas de priorización). Para el tráfico IP, es posible una adicional priorización. Las colas de prorización son usadas normalmente en conexiones seriales de baja velocidad. La *figura 3.7* muestra como las colas de prioridad pueden ser usadas para segregar tráfico por nivel de prioridad y rápidamente el transito de ciertos paquetes va pasando por la red.

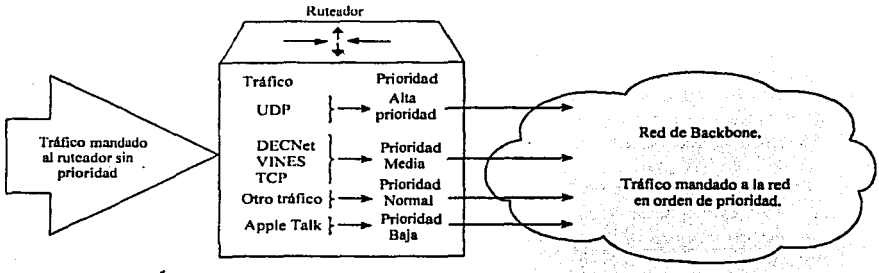


Figura 3.7.- Colas de priorizaciòn.

Finalmente muchos de los protocolos ruteables (AppleTalk, IPX, DECnet, etc) emplean un protocolo de ruteo basado en el costo y valor que tienen las diferentes rutas al destino. Optimizando los parámetros asociados, se pueden forzar a tipos particulares de tráfico a tomar rutas particulares, mientras tanto se realizará una priorización manual del tráfico.

La costumbre de hacer colas.

Las colas de priorización introducen un problema de equidad en los paquetes clasificados con baja priorización, que por ello no podría dar el servicio de un modo adecuado a esos paquetes o a todos. Las colas de priorización fueron diseñadas para direccionar estos problemas. La costumbre de hacer colas permite conocer el orden más adecuado para hacer la cola de priorización. De hecho, esta característica es común en el ambiente de redes en donde multiples protocolos de las capas superiores son soportados. Las colas de priorización reservan BW para protocolos específicos, esto permite a aplicaciones críticas tener un mínimo BW garantizado en cualquier momento.

La priorización trabaja con tráfico multiprotocolo. Un máximo de 16 colas pueden construirse bajo este esquema de priorización. Cada cola es secuencialmente mantenida hasta que el número de bytes mandados excede la cuenta de bytes configurados o la cola es vaciada. Si para una cola se reserva el 40% del BW de la red y el protocolo que corre en ella sólo usa el 50% de este total, el 20% restante puede ser compartido con el tráfico de otra aplicación.

Las colas son diseñadas para medios ambientes que quieren asegurar un mínimo nivel de servicio para todos los protocolos de red. Hoy el medio ambiente de los protocolos de red más importantes tienen características que permiten compartir el medio con otros.

Justa inclinación hacia las colas de priorización.

La inclinación hacia las colas de priorización es debido a un algoritmo que administra la prioridad del tráfico que usa Multiplexación por División de Tiempo (TDM – Time Division Multiplexing), módulo que divide el BW disponible entre los clientes que comparten la misma interfaz. En TDM, a cada cliente se le asigna una porción de tiempo. El BW es distribuido eventualmente entre clientes para que ellos consigan una porción justa en el caso de que tengan el mismo peso. Se puede asignar un peso diferente a cada cliente, por ejemplo, a través de tipos de servicios, para que más BW se asigne.

Si a cada cliente le es permitido un mismo BW independientemente de la velocidad de llegada, el volumen bajo de tráfico tiene prioridad sobre el volumen de tráfico más alto. El uso del peso permite el tráfico por retraso de tiempo sensible (time –delay-sensitive) para obtener BW adicional, así que hay una respuesta constante en el tiempo que es garantizada bajo el tráfico pesado. Hay diferentes tipos de datos que convergen en un medio, como se muestra en la *figura 3.8*.

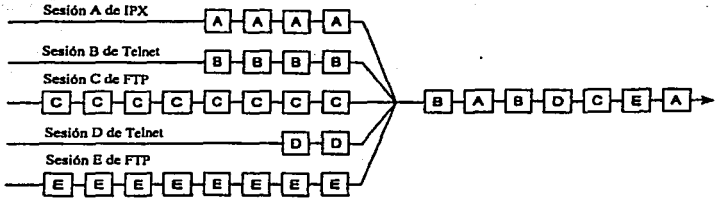


Figura 3.8.- Justa inclinación hacia las colas de priorización.

La sesión C y E son de FTP y tienen un alto volumen de tráfico. A, B y D son sesiones interactivas y tienen un bajo volumen de tráfico. En cada sesión es terminada la comunicación para este caso. Si cada conversación es atendida en modo cíclico y obtiene un turno sin tener en cuenta su velocidad de llegada, las sesiones FTP no monopolizan el BW. Los retrasos por el viaje cíclico de las sesiones del tráfico interactivo, por lo tanto, se vuelven predecibles.

La formación de colas provee un algoritmo para identificar los datos dinámicamente usando una interfaz y los separa en una cola de manera lógica. El algoritmo usa varios discriminadores basado en cualquier información de protocolos de la capa de red que están disponibles. Por ejemplo, para tráfico IP, los discriminadores son la dirección origen y destino, tipo de protocolo, número de socket, etc. Esto es como las 2 sesiones de Telnet (sesión B y D) que son asignadas a diferentes colas, como se muestra en la *figura 3.8.*

Idealmente, el algoritmo debería clasificar cada conversación que comparte el medio, así cada conversación recibiría esta justa distribución del BW. Desgraciadamente hay protocolos que no pueden distinguir entre dos sesiones suyas. El algoritmo de la formación justa de colas, trata estas sesiones como una sola conversación. Si se tienen muchas sesiones TCP, estas sesiones obtienen la mayoría del BW y el tráfico restante obtiene el resto del BW.

La formación justa de colas, sin embargo, tiene muchas ventajas sobre la priorización y las clásicas colas. Estas últimas dos requieren de la instalación de listas de acceso, el BW tiene que ser previamente asignado, la prioridad tiene que ser predefinida y algunas veces el administrador de red no puede identificar y priorizar el tráfico de red en tiempo real.

Balanceo de cargas

Este sencillo camino para agregar tráfico en el backbone de la red se realiza mediante la implantación de conexiones adicionales. Los ruteadores proveen formación de balanceo de carga para múltiples conexiones y caminos. Se pueden usar 4 caminos para llegar al destino en la red; en algunos casos, los caminos necesitan tener un mismo peso.

Dentro de IP, los ruteadores proveen balanceo de carga sobre la base de por paquete y por destino. Para el balanceo de carga por destino, cada ruteador usa su cache para determinar la interfaz de salida. Los ruteadores usan métricas para determinar cada camino que el paquete podría tomar; la cantidad de carga a balancear puede ser ajustado por el usuario.

El balanceo de tráfico puenteado sobre líneas seriales es también soportado. Las líneas seriales pueden ser asignadas a un grupo de circuitos, si una de las conexiones seriales en el grupo de circuitos esta en el árbol de expansión de la red (spanning tree), alguna de las conexiones seriales en el grupo de circuitos puede ser usada para balancear cargas. El problema de ordenar datos es evitado asignando cada destino a una conexión serial. La reasignación se hace dinámicamente si las interfaces suben o bajan.

Caminos alternativos

Muchos backbones de interredes llevan información crítica para la organización. Las organizaciones están usualmente interesadas en proteger la información de su backbone a cualquier costo. Los ruteadores ofrecen suficiente confiabilidad, así que ellos no son una conexión débil en la cadena de la interred. La clave es proveer caminos alternativos que puede seguir una línea de conexiones cuando llegan a ocurrir fallas en la red.

La fiabilidad extremo a extremo no esta asegurada, solo la tolerancia del backbone. Si la comunicación de un segmento local de un edificio es destruida por alguna razón, la información podría no alcanzar el backbone. La fiabilidad extremo a extremo solo es posible cuando la redundancia es empleada en la red. Ya que la redundancia es usualmente prohibida debido al alto costo que representa, muchas compañías prefieren emplear caminos redundantes solo en segmentos que tienen información crítica.

¿Qué hace al backbone confiable?. Los ruteadores son la llave de la fiabilidad de las interredes. Dependiendo de la definición de fiabilidad, este medio puede duplicar todos los sistemas en cada ruteador y posiblemente en cada componente. Sin embargo, la duplicación de componentes de hardware no es una compleja solución porque la circuitería extra es necesaria para unir los componentes duplicados para permitir la comunicación entre ellos. Esta solución es usualmente muy costosa, pero lo más importante, no es completamente direccionable el problema. Incluso suponiendo que todos los ruteadores en la red son completamente confiables, los problemas de conexión entre nodos dentro del backbone pueden todavía ganarle a la solución con hardware redundante.

Para realmente direccionar el problema de la fiabilidad de la red, la conexión deberá ser redundante. Sin embargo, esto no es suficiente para duplicar todas las conexiones. Las conexiones duales deben terminar en los ruteadores, excepto los ruteadores del backbone que son tolerantes a fallas (no puntos de fallas individuales). De otro modo, los ruteadores del backbone que no son tolerantes a fallas pueden llegar a ser puntos de fallas. La inevitable conclusión es que un ruteador completamente redundante no es una solución efectiva para el problema de la fiabilidad porque es costoso y todavía no hay fiabilidad en la conexión de direccionamiento.

Muchos diseñadores no implantan completamente una red redundante. En cambio, los diseñadores de redes implantan redes parcialmente redundantes.

Acceso Switcheado

El acceso switcheado provee la capacidad de habilitar una conexión WAN vía la configuración de los ruteadores. Un modelo más fiable de backbone consiste en redundancia, conexiones dedicadas y conexiones switcheadas para terminar con el tiempo ocioso. Bajo condiciones de operación normales, se puede balancear tráfico sobre conexiones duales, pero en conexiones switcheadas no es operacional hasta que una conexión dedicada falle.

Tradicionalmente, las conexiones WAN usan líneas dedicadas. Esto puede ser muy caro cuando una aplicación requiere solo un volumen bajo de conexiones periódicas. Para reducir las necesidades de circuitos dedicados, esta disponible una característica llamada "ruteo bajo llamada en demanda" (dial on demand routing –DDR). La *figura 3.9* ilustra una conexión DDR.

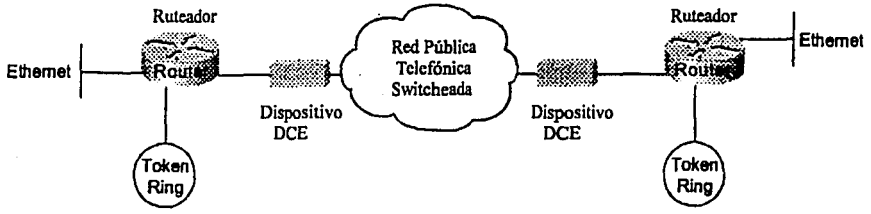


Figura 3.9.- ruteo bajo llamada en demanda.

Usando DDR de bajo volumen, una conexión periódica de red puede hacerse sobre una red pública telefónica. Un ruteador activa el DDR cuando este recibe un paquete switcheado o ruteado que es destinado a una localización del otro lado de la línea telefónica. Después que el ruteador marca el número telefónico de destino y establece la conexión, los paquetes de los protocolos pueden se transmitidos. Cuando la transmisión es completada, la línea es automáticamente terminada. Este tipo de conexión reduce el costo de la transmisión.

Encapsulamiento (Tunneling)

El encapsulamiento toma paquetes de un sistema de la red y los pone dentro de los límites de otra red, este método se llama tuneleo. El tuneleo provee un medio para encapsular paquetes dentro de un protocolo ruteable mediante interfaces virtuales. El transporte del SDLC (Synchronous Data Link Control – Control Síncrono de Conexiones de Datos) es también un encapsulado en paquetes en un protocolo ruteable.

3.1.4.-Evaluación de los servicios de distribución

En esta sección se describen las características que soportan los servicios de distribución. Los siguientes puntos son descritos:

- Administración del BW del backbone.
- Áreas y servicios de filtrado.
- Políticas basadas en distribución.
- Servicios de Gateway.
- Interprotocolo de distribución de ruteo.
- Traducción del Medio.

Administración del BW del backbone

Para optimizar el BW en la operaciones de la red, los ruteadores ofrecen varias características de rendimiento. Por ejemplo, la priorización, métricas de protocolo de ruteo y terminación de sesiones locales.

Se puede ajustar la longitud de las colas en la priorización. Si una cola de priorización de desborda, el exceso de paquetes se descarta y envía mensajes que detienen el flujo del paquete (si es lo apropiado) para el protocolo. Se puede ajustar las métricas de ruteo para incrementar el control sobre los caminos que el tráfico toma a través de la red.

La terminación de la sesión local permite a los ruteadores actuar como "apoderados" del sistema remoto que representa la sesión de punto final (un proxy es un dispositivo que actúa como parte de otro dispositivo). La *figura 3.10* representa un ejemplo de terminaciónn de una sesión local de un dispositivo IBM.

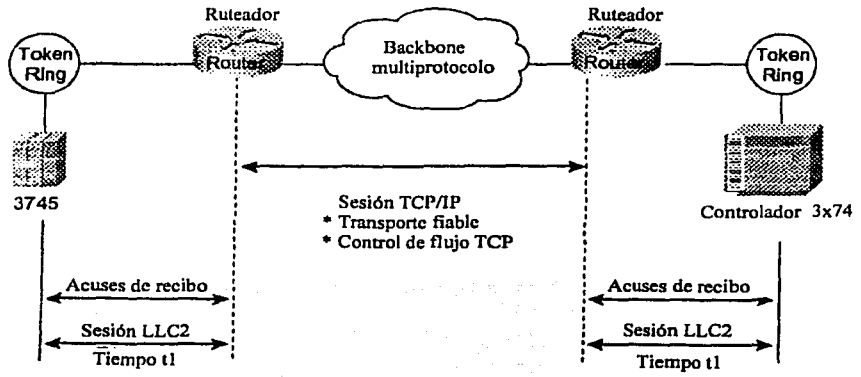


Figura 3.10.- Terminación de una sesión local sobre multiprotocolos de backbone.

En la *figura 3.10*, los ruteadores terminan localmente el control lógico de la conexión (Logical Link Control – LLC) de las sesiones. Después de terminar una sesión, durante la cual todas las sesiones de control de información pasan sobre el multiprotocolo del backbone, los ruteadores toman la responsabilidad y reconocimiento de paquetes que vienen de los hosts directamente conectados a las LAN's. El reconocimiento local ahorra el BW de la WAN (por lo tanto, los costos de utilización de la WAN), resuelve los problemas de interrupciones en las conexiones y provee una rápida respuesta a los usuarios.

Áreas y servicios de filtrado

Los filtros de tráfico basados en áreas o tipos de servicio son primariamente herramientas de servicio distribuidas usadas que proveen políticas basadas en control de acceso dentro de los servicios de backbone. Las áreas y servicios de filtrado son implementados usando listas de acceso. Una lista de acceso es una secuencia de declaraciones, cada una de las cuales permite o niega ciertas condiciones o direcciones. Las listas de acceso pueden permitir o denegar mensajes para algún nodo de la red en particular y el envío de mensajes de protocolos y servicios particulares.

Un área o filtro de acceso al red son usados para dar fuerza a transmisiones selectivas de tráfico basado en la dirección de la red. Se puede aplicar esto en los puertos de entrada o salida. El servicio de filtros usa listas de acceso aplicados a los protocolos, aplicaciones como SMTP (Simple Mail Transfer Protocol – Protocolo Simple De Transferencia de Correo) y protocolos específicos.

Suponiendo que se tienen una red conectada a Internet, y se requiere de un hosts en la red Ethernet para estar disponible para conexiones TCP para muchos de los hosts en Internet; sin embargo, no se requiere que los hosts en Internet estén disponibles para conexiones de hosts en la red Ethernet, excepto para el puerto dedicado de SMTP del host en turno.

SMTP usa el puerto 25 del protocolo TCP en el extremo de la conexión y un número de puerto aleatorio en el otro extremo. Los mismos 2 puertos son usados a lo largo de la conexión. Los paquetes de correo son mandados por Internet y tienen como destino el puerto 25. Los paquetes que salen pueden tener el número de puerto invertido, el hecho es que el sistema seguro detrás del ruteador siempre acepta conexiones de correo en el puerto 25 que es lo que hace posible controlar separadamente los servicios entrantes y salientes.

Políticas basadas en distribución

Estas políticas se basan en la premisa de que diferentes departamentos de una misma organización podrían tener diferentes políticas referentes a la distribución de tráfico en la organización. Las políticas basadas en distribución tienen como objetivo mantener los diferentes requerimientos sin comprometer el rendimiento y la integridad de la información.

Una política dentro del contexto de interredes es una regla o conjunto de reglas que gobiernan la distribución extremo a extremo del tráfico y a través de él, en el backbone de la red. Un departamento podría mandar tráfico representado por 3 diferentes protocolos en el backbone, pero podría querer apresurar el tránsito de un protocolo en particular a través del backbone porque lleva información de aplicaciones críticas. Para minimizar el tráfico interno excesivo, otro departamento podría excluir todo su tráfico del backbone excepto el correo electrónico y alguna aplicación de suma importancia para la organización.

Este ejemplo refleja las políticas específicas de un departamento. Sin embargo, las políticas reflejan las metas de la organización. Por ejemplo, una organización podría querer regular el tráfico del backbone en una máximo de 10% del BW durante un día de trabajo y un pico de 30% durante un minuto. Otra política de la coorporación podría ser asegurar la comunicación entre 2 departamentos remotos independientemente de la tecnología que utiliza cada uno de ellos.

Diferentes políticas frecuentemente requieren diferentes grupos de trabajo y tecnologías por departamento. Por consiguiente, el soporte para las políticas basadas en distribución, implica soporte para un amplio rango de tecnologías actuales usadas para implementar estas políticas. Esto permite implementar soluciones que soportan un amplio rango de políticas, lo cual ayuda a incrementar la flexibilidad y disponibilidad de aplicaciones en la organización.

Para apoyar las tecnologías de interredes, debe haber un medio que mantenga separadas e integradas estas tecnologías apropiadamente. Las diferentes tecnologías deberían coexistir o combinarse inteligentemente.

Considerando la situación descrita en la *figura 3.11*, se asume que la política coorporativa limita el tráfico de backbone innecesario. Una manera pata hacer esto es restringir la transmisión de mensajes SAP (Service Advertisement Protocol – Protocolo de Servicio de Anuncios). Los mensajes SAP permiten a los servidores NetWare anunciar servicios de los clientes. La organización podría tener otra política que declara que todo el tráfico de NetWare debería proveerse localmente. Si este fuese el caso, no debe haber razón para que los servicios sean anunciados remotamente. Los filtros SAP impiden que el tráfico SAP se mantenga en la interfaz del ruteador, cumpliéndose así esta política.

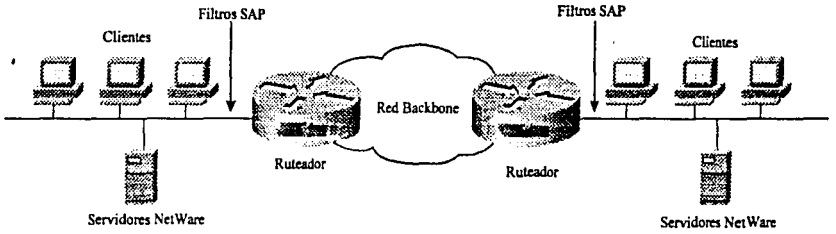


Figura 3.11.- Políticas basadas en distribución: SAP-Protocolo de Servicio de Anuncios.

Servicio de Gateway (Puerta de Enlace)

Las capacidades de los protocolos de gateway son parte de cada software estándar de los ruteadores. Por ejemplo, DECnet en su versión V, maneja las direcciones de diferente manera comparada con la versión IV. Para esos casos se requiere que ambos tipos de protocolos coexistan en la red, la manera es conformar una guía específica para la comunicación entre ambas versiones. Los ruteadores interoperan con ruteadores digitales y hosts digitales que no diferencian entre los diferentes dispositivos.

AppleTalk es otro protocolo con múltiples versiones, cada uno tiene diferentes características de direccionamiento. Normalmente la versión A no puede entenderse con la versión B. Sin embargo, los ruteadores permiten el ruteo entre ambas versiones por el mismo cable usando rutas de transición.

Se puede lograr un ruteo de transición conectando 2 puertos del ruteador con el mismo cable, configurando un puerto para soportar la versión A y otro para el B. Ambos puertos deberían tener un número único de red. Los paquetes son entonces traducidos y mandados fuera del otro puerto como sea necesario.

Redistribución de los protocolos de ruteo

Los servicios de gateway permiten que 2 nodos finales con diferentes aplicaciones, puedan comunicarse mediante el ruteo de protocolos de gateway. Los ruteadores también pueden actuar como gateway para rutear protocolos. La información derivada de un protocolo de ruteo como IGRP, puede pasar a ser, y usado por, otro protocolo de ruteo como RIP. Esto es útil cuando múltiples protocolos de ruteo corren en la misma interred.

La información de ruteo puede ser intercambiada entre cualquier protocolo de ruteo IP, estos incluyen RIP, IGRP, OSPF, Hello, EGP, BGP, etc. La información de rutas definidas (estáticas) también puede distribuirse, es decir, se pueden asignar valores por defecto para que un protocolo pueda usar la misma métrica para todas sus rutas redistribuidas, por ello se simplifican los mecanismos de redistribución de ruteo.

Traducción de medios

Las técnicas de traducción de los medios de comunicación traducen los paquetes (frames) de un sistema de redes dentro de paquetes de otro. Tal traducción es difícilmente eficaz al 100% porque un sistema podría tener atributos sin el corolario de otro. Por ejemplo, las redes Token Ring soportan un sistema de prioridad y reservación, mientras Ethernet no lo hace.

Para estos casos en el cual las comunicaciones entre las estaciones finales en diferentes medios es requerida, los ruteadores pueden traducir mediante diversas técnicas entre los paquetes Ethernet y Token Ring, entre otros.

3.1.5.-Evaluación de los servicios de acceso local

Los siguientes puntos discuten las características de la interred que soporta los servicios de acceso local. Los tópicos que se incluyen dentro de estos servicios son los siguientes:

- Direccionamiento de red de valor agregado.
- Segmentación de la red.
- Capacidades de Broadcast y Multicast.
- Capacidades de cache local, nombrado y proxy.
- Seguridad de acceso al medio.
- Descubrimiento de rutas.

Direccionamiento de red de valor agregado

Los esquemas de direccionamiento para redes LAN con NetWare y otras, no siempre se adaptan perfectamente para usarse como multisegmentación LAN o WAN; esta es una herramienta que implementan los ruteadores para asegurar que cada protocolo es el protocolo específico de direccionamiento de ayuda. El direccionamiento de ayuda es un mecanismo para asisitir el movimiento de tráfico específico a través de la red cuando el tráfico podría transitar de otro modo a través de la red.

El uso del direccionamiento de ayuda se ilustra mejor en el siguiente ejemplo. Considerando el uso de direccionamiento de ayuda en interredes Novell IPX, los clientes Novell mandan mensajes de broadcast cuando buscan un servidor. Si el servidor no es local, el tráfico de broadcast podría ser mandado a través de los ruteadores. El direccionamiento de ayuda y las listas de acceso pueden ser usadas conjuntamente para permitir broadcast para ciertos nodos en una red para ser específicamente direccionado a determinados servidores en otra red. Múltiples direccionamientos de ayuda en cada interfaz son soportados, así que los paquetes de broadcast pueden ser enviados a múltiples hosts. La *figura 3.12* ilustra el uso de direccionamiento de ayuda en redes NetWare.

A los clientes NetWare en la red AA se les permite transmitir por broadcast hacia algún servidor en la red B. Una lista de acceso aplicable debería especificar qué tipos de broadcast podrían ser permitidos para [illegible] nodos en la red AA. Una configuración específica del direccionamiento de ayu[illegible] direccionamiento en la red BB para la cual el broadcast es dirigi[illegible] la red BB recibe broadcast y ningún otro broadcast fuera de los 10 tipos permi[illegible] ruteado.

A cualquier red más allá de la red AA no se le permite la transmisión de broadcast a la red BB a través del ruteador C1, a menos que tanto la red AA y las posteriores a ella (por ejemplo AA1) sean configuradas en el ruteador para la transmisión de broadcast. Estas entradas deberían ser aplicadas a las interfaces de entrada y para la transmisión de broadcast entre las redes directamente conectadas. De esta manera, el tráfico pasa directamente a lo largo de las redes.

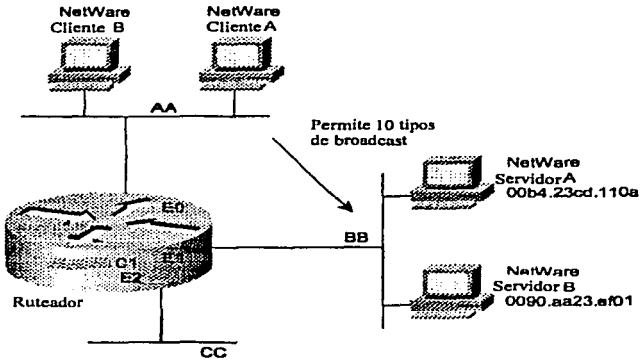


Figura 3.12.- Mapeo de red que ilustra el control de direccionamiento de ayuda de broadcast.

Segmentación de la red

La segmentación de la red dentro de las piezas más manejables es una regla esencial para los ruteadores de acceso local. En particular, los ruteadores de acceso local implantan políticas particulares y limitan el tráfico innecesario. Ejemplos de capacidades que permiten a los diseñadores de red el uso de ruteadores de acceso local para segmentar redes incluye las subredes IP, el direccionamiento de área DECnet y las zonas AppleTalk.

Se pueden usar los ruteadores de acceso local para implantar políticas locales colocando ruteadores en lugares estratégicos y configurándolos con políticas especiales de segmentación. Por ejemplo, se pueden preparar una serie de segmentos LAN con diferentes direccionamientos de subredes; los ruteadores podrían ser configurados con las máscaras de subredes e interfaces convenientes. En general, el tráfico en un segmento dado es limitado al broadcast local, al tráfico pretendido para una estación del extremo específico en ese segmento, o al tráfico pretendido para un ruteador específico. Para la distribución cuidadosa de hosts y clientes, se puede usar un método simple para dividir (segmentar) la red para reducir la congestión en la red.

Capacidades de Broadcast y Multicast

Muchos protocolos hacen las capacidades de broadcast y multicast. El broadcast son mensajes que se mandan hacia todos los destinos de la red. Multicast son mensajes que se mandan a un conjunto específico de destinos en la red. Sin embargo, los ruteadores pueden ser configurados para transmitir tráfico de broadcast de ser necesario. Bajo ciertas circunstancias, la transmisión de información por broadcast es deseable y posiblemente necesario. El control de estos tráficos de broadcast y multicast se da a través de ruteadores.

En el mundo IP, como con otras muchas otras tecnologías, las peticiones de broadcast son muy comunes. A menos que el broadcast sea controlado, el BW de la red puede ser seriamente reducido. Los ruteadores ofrecen varias funciones que limitan el tráfico broadcast. Por ejemplo, el broadcast dirigido permite la transmisión a una red o una serie de redes específicas en lugar de a toda la interred. Cuando la saturación de la red por broadcast es necesaria, la mayoría de los ruteadores soportan una técnica en la cual el broadcast es mandado sobre spanning tree en la red. El spanning tree asegura una completa cobertura sin el tráfico excesivo, porque solo un paquete es enviado a cada segmento de red.

Las características de multicast, permite al tráfico IP propagarse de un origen a varios destinos. En lugar de enviar un paquete a cada destino, un paquete es mandado a un grupo de multicast identificado por una sola dirección IP de grupo. El multicast IP provee un excelente soporte para aplicaciones como vídeo y audioconferencia, descubriendo recursos, y dando confianza a la distribución de tráfico.

Para todo el soporte de multicast IP, los hosts IP deben correr el Protocolo de Administración de Grupo de Internet (IGMP – Internet Group Managment Protocol). IGMP es usado por hosts IP para informar que pertenece a un grupo de multicast e inmediatamente ir al ruteador de multicast vecino. La cantidad de miembros del grupo de multicast es variable. Los ruteadores multicast mandan mensajes de peticiones IGMP a otras redes cercanas, los miembros del grupo de multicast responden a las peticiones hechas por el otro grupo de IGMP al que ambos pertenecen. Los reportes son mandados por el primer hosts en el grupo de multicast, eliminan los mensajes idénticos que son mandados como respuesta por los otros grupos.

El ruteador de multicast cercano a la red local toma la responsabilidad para enviar datagramas de multicast para un grupo de multicast de todas las redes que tienen miembros en el grupo. Los ruteadores construyen árboles de grupos de multicast (tablas de ruteo), así que los paquetes de multicast tienen caminos libres redundantes para todos los grupos de multicast, así que los paquetes no son duplicados. Si los reportes no son recibidos por el grupo de multicast después de un número de peticiones IGMP, los ruteadores de multicast asumen que el grupo no tienen miembros y detiene el envío de información e intenta con otro grupo.

Capacidades de Cache local, Nombrado y Proxy

Son 3 las capacidades del ruteador que ayudan a reducir el tráfico en la red y promueve una eficiente operación de la interred; soporte de servicio de nombres, servicios de proxy y cache de información en la red.

Las aplicaciones de red y los servicios de conexión proporcionados sobre segmentos de interredes requieren un camino racional para resolver (traducir) los nombres y direcciones. Varios dispositivos brindan estas ventajas; cualquier ruteador que se selecciones debe soportar el servicio de nombres implementados para diferentes dispositivos de sistema final. Ejemplos de servicios soportados incluyen NetBIOS, DNS (Domain Name System – Sistema de Nombres de Dominios IP's) y NBP (AppleTalk Name Binding Protocol – Protocolo de Conexión de Nombres AppleTalk).

Un ruteador también puede actuar como un proxy para un servidor de nombres. El soporte del ruteador de cache de nombres NetBIOs es un ejemplo de este tipo de capacidad. El cache de nombre NetBIOs permite al ruteador mantener un cache de nombres NetBIOs, el cual evita la sobre transmisión de todo el broadcast entre los clientes y servidores de las PC's con NetBIOs. Cuando el cache de nombres NetBIOs es habilitado, el ruteador hace lo siguiente:

- Cuando hay avisos de hosts que mandan información duplicada se limita la retransmisión a un frame por periodo. El lapso de tiempo por periodo es un parámetro de la configuración.

- El cache mantiene un mapeo entre el servidor NetBIOs y los clientes de nombres y otras direcciones MAC. Como resultado, el envío de peticiones de broadcast por clientes para encontrar el servidor (y los servidores responden a los clientes) pueden enviarse directamente a sus destinos, en vez de iniciar la transmisión de broadcast sobre toda la red switcheada.

Cuando el cache de nombres NetBIOS es habilitado y los parámetros predefinidos son fijados en el ruteador, aproximadamente 20 paquetes de broadcast son mantenidos en el anillo local en donde han sido generados.

El ruteador puede también administrar BW usando una variedad de recursos y proxys. Usando los ruteadores para actuar en nombre de otros dispositivos para hacer varias funciones, logrando escalar más fácilmente las redes. En lugar de forzar o agregar más BW cuando un nuevo grupo es adicionado a la situación, se puede usar el ruteador para administrar la resolución de direcciones y el control de servicios de mensajes.

Algunas veces los segmentos de redes no pueden participar en actividades de ruteo o no pueden implantar software que conforman a los protocolos que generalmente se implementan para la resolución de direcciones. La implantación de proxys en los ruteadores permite a los diseñadores de red soportar estas redes o hosts sin configurar las interredes. Ejemplos de este tipo de capacidades incluye el ARP (Addres Resolution Protocol – Protocolo de Resolución de Direcciones) para IP y proxy NBP para AppleTalk.

Los caches locales previamente aprenden información acerca de la red así que las nuevas solicitudes de información no necesitan ser transmitidas nuevamente. Un ruteador de cache ARP almacena direcciones físicas y mapeo de redes, así que no es necesaria la transmisión de las mismas direcciones por broadcast durante un lapso de tiempo determinado.

Seguridad de Acceso al Medio

Si toda la información esta disponible para todos los usuarios en la organización, las violaciones de seguridad y el acceso inapropiado a archivos pueden ocurrir. Para prevenir esto, los ruteadores deben hacer lo siguiente:

- Impedir que el tráfico local alcance el backbone.
- Impedir que el tráfico del backbone termine en un departamento o grupo de trabajo inapropiado.

Estas 2 funciones requieren del filtrado de paquetes. La capacidad de filtrado de paquetes deberían ser medidos para soportar un variedad de políticas corporativas. Los métodos de filtrado de paquetes pueden reducir los niveles de tráfico en una red, por eso se permite a las compañías el continuar usando estas estrategias actuales en vez de invertir en más hardware de red. En suma, el filtrado de paquetes puede mejorar la seguridad impidiendo el acceso a usuarios no autorizados y pueden minimizar los problemas de la red causados por la excesiva congestión.

Los ruteadores soportan múltiples esquemas de filtrado diseñados para proveer el control sobre el tráfico de la red que alcanza al backbone. Quizá el más poderoso de estos mecanismos de filtrado son la listas de acceso. Cada uno de los siguientes servicios de acceso local pueden proporcionarse a través de las listas de acceso.

- Se tiene una red de ruteo Ethernet para Internet y se requiere que cualquier hosts en Ethernet pueda mantener conexiones con Internet. Sin embargo, se requiere que no todos los hosts en Internet puedan mantener conexiones TCP dentro de nuestra red Ethernet, excepto el puerto SMTP para el puerto de correo.

- Se requiere anunciar sólo una red a través del ruteo RIP.

- Se requiere impedir que los paquetes que se originaron en cualquier estación SUN se están switcheando en un segmento de red Ethernet en particular.

- Se requiere mantener un protocolo particular basado en IPX de Novell para establecer una conexión entre una red origen y una combinación de puertos orígenes y una red destino o una combinación de puertos destino.

Las listas de acceso impiden el paso de ciertos paquetes para atravesar una interfaz del ruteador en particular, por eso se provee una herramienta general para implantar seguridad en la red. En suma, para este método existen varios sistemas de seguridad específica para ayudar a incrementar la seguridad en la red. Por ejemplo, el gobierno de los Estados Unidos ha especificado el uso de un campo optativo en los paquetes IP para colocar un paquete de seguridad en los sistemas llamado: Protocolo Opcional de Seguridad en Internet (Internet Protocol Security Option – IPSO).

Algunos otros sistemas de seguridad se diseñan para impedir a los usuarios remotos acceder a la red a modo que estos tengan la autorización adecuada. Esto se logra mediante mecanismos de asignación de contraseñas.

Descubrimiento de Rutas

Los hosts deben poder localizar los ruteadores cuando ellos necesitan accesar a los dispositivos externos a la red local. Cuando más de un ruteador esta cercano a un hosts local, el hosts debe localizar el ruteador que represente el camino óptimo hacia su destino. Este proceso de encontrar ruteadores es llamado descubrimiento de rutas. Los siguientes son protocolos de descubrimientos de rutas:

- Sistema Intermedio a Sistema Final (End System to Intermediate System – ES-IS). Este protocolo es definido por el modelo OSI de la ISO. Es dedicado al intercambio de información entre sistemas intermedios (ruteadores) y sistemas finales (hosts). ES manda un mensaje a todos los IS en la subred local. De vuelta, el mensaje de los IS son mandados de todos los IS a todos los ES en la subred local. Ambos tipos de mensajes son transmitidos en la subred y la dirección de capa de red del sistema que los generó. Usando este protocolo, los sistemas finales e intermedios pueden localizar un ruteador.

- ICMP Protocolo de descubrimiento de rutas (ICMP Router Discovery Protocol – IRDP). Aunque esta actualmente bajo estudio, no hay manera única y estandarizada la manera en que los hosts localizan los ruteadores en el mundo IP. En ambos casos, las estaciones son configuradas manualmente con la dirección de un ruteador local.

- Protocolo Proxy de Resolución de Direcciones (Proxy Address Resolution Protocol - ARP). ARP usa mensajes de broadcast para determinar la dirección MAC que corresponde a una red en particular. ARP es suficientemente genérico para permitir el uso de IP, con virtualmente cualquier tipo de mecanismo de acceso al medio. Un ruteador que tiene habilitado el proxy ARP responde a peticiones ARP de los hosts quienes tienen un ruteador, lo cual permite asumir a los hosts que todos los demás hosts están actualmente en otra red.

- RIP (Router Internet Protocol – Protocolo de Ruteo Internet). Es un protocolo de ruteo que está disponible en los hosts IP. Muchos hosts usan RIP para encontrar la dirección de los ruteadores en la LAN o cuando hay múltiples ruteadores se pueden escoger la mejor ruta para llegar al destino determinado.

Cada administrador puede escoger el mecanismo de descubrimiento de rutas que trabajen mejor en un dispositivo en particular.

3.1.6.- Identificando y seleccionando los dispositivos de red

Los diseñadores de red tienen 4 tipos básicos de dispositivos de red disponibles para el diseño de la misma:

- Hubs y Puentes.
- Switches y Ruteadores.

Los expertos en comunicaciones de datos generalmente están de acuerdo que el diseño de redes se encamine hacia el uso primariamente de switches y ruteadores en la construcción de redes. Como consecuencia, se discuten las reglas para el empleo de switches o ruteadores en el diseño de redes.

Los switches pueden ser divididos funcionalmente dentro de 2 grupos: los switches capa 2 y los switches multicapa que proveen las capacidades de capa 2 y 3. Hoy, los diseñadores de red, están reemplazando los hubs en los closets de telecomunicaciones con switches para incrementar el rendimiento de la red y proteger sus instalaciones existentes.

Los ruteadores segmentan tráfico en la red basado en el direccionamiento de la redes (capa 3) en lugar de hacer las conexiones basadas en la dirección MAC. Por consiguiente, son dependientes del protocolo.

Beneficios de los Switches (Servicios de capa 2)

Un solo switch de capa 2 podría ofrecer algunos de los siguientes beneficios:

- BW. Una LAN switcheada provee un excelente rendimiento para los usuarios permitiendo un BW dedicado en cada puerto. Cada puerto del switch representa un segmento de red diferente. Está técnica es conocida como microsegmentación.

- VLAN's. Los switches LAN pueden agrupar un conjunto de puertos dentro de un grupo de trabajo lógico llamado VLAN (Virtual LAN), por eso las restricciones del dominio de broadcast están designadas a miembros de VLAN por puertos. Las VLAN's también son conocidas como dominios switcheados y dominios de switcheo autónomo. La comunicación entre VLAN's requiere de un ruteador.

- Traducción y reconocimiento automático de paquetes. Esta característica permite a los switches traducir formatos de paquetes automáticamente como una MAC Ethernet.

Beneficios de los Ruteadores (Servicios de capa 3)

Porque los ruteadores usan las direcciones de capa 3, cuando típicamente tienen estructura para usar técnicas para construir redes que mantengan el rendimiento y ser sensibles al crecimiento. Por imposición de la estructura, generalmente jerárquica, en una red, los ruteadores pueden usar caminos redundantes y determinar las rutas óptimas incluso en una red que cambia dinámicamente.

Los ruteadores son necesarios para asegurar la escalabilidad en una red que crece y se expande. Los ruteadores proveen las siguientes capacidades que son vitales en el diseño de redes:

- Control de broadcast y multicast.
- Segmentación de broadcast.
- Seguridad.
- Calidad de servicio (Quality of Service – QoS).
- Servicios Multimedia.

3.2 Cableado Estructurado

Un sistema de cableado estructurado consiste de una infraestructura flexible de cables que puede aceptar y soportar múltiples sistemas de computación y de teléfono, independientemente de quién fabricó los componentes del mismo. En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella, facilitando la interconexión y la administración del sistema. Esta disposición permite la comunicación con virtualmente cualquier dispositivo, en cualquier lugar y en cualquier momento. Un plan de cableado bien diseñado puede incluir distintas soluciones de cableado independiente, utilizando diferentes tipos de medios, e instalados en cada estación de trabajo para acomodar los requerimientos de funcionamiento del sistema.

3.2.1 Evolución de los Sistemas de Cableado

Los sistemas de cableado de lugares utilizados para servicios de telecomunicaciones, han experimentado una constante evolución con el correr de los años. Los sistemas de cableado para teléfonos fueron en una oportunidad especificados e instalados por las compañías de teléfonos, mientras que el cableado para datos estaba determinado por los proveedores del equipo de computación. Después de la división de la compañía AT&T en los Estados Unidos, se hicieron intentos para simplificar el cableado, mediante la introducción de un enfoque más universal. A pesar de que estos sistemas ayudaron a definir las pautas relacionadas con el cableado, no fue sino hasta la publicación de la norma sobre tendido de cables en edificios ANSI/EIA/TIA-568 en 1991, que estuvieron disponibles las especificaciones completas para guiar en la selección e instalación de los sistemas de cableado.

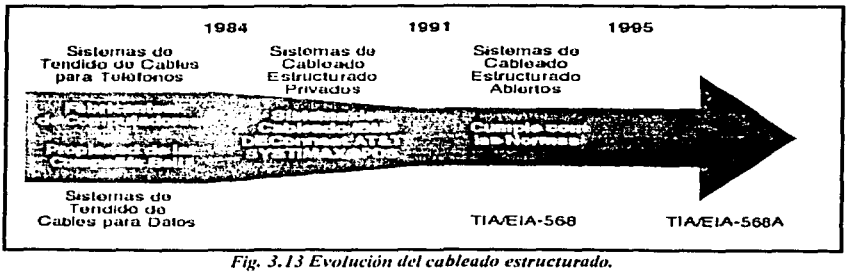


Fig. 3.13 Evolución del cableado estructurado.

Un sistema de cableado estructurado permite realizar el cableado sin conocer de antemano los equipos de comunicación de datos que lo utilizarán (cualquier ambiente).

El tendido de los cables es sencillo de administrar (cambios, adiciones, etc).

Las fallas son menores y más fáciles de localizar que en los sistemas POTS (Plain Old Telephone System).

3.2.2 Cableado horizontal

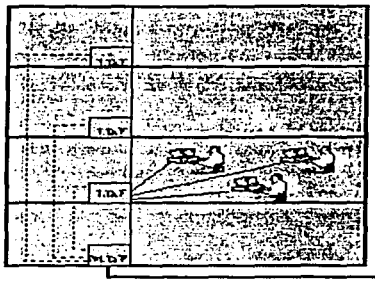


Figura 3.14 Cableado horizontal.

El cableado horizontal es la porción del sistema de cableado que se extiende desde el closet de telecomunicaciones (rack) hasta el usuario final en su estación de trabajo y consta de:

Cable horizontal y hardware de conexión

Aquí se deben proporcionar los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales. Este incluye:

Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo. En inglés: Work Area Outlets (WAO).

Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.

Páneles de empate (patch panel) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Rutas y Espacios Horizontales. Sistemas de distribución horizontal

Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado horizontal.

El término horizontal es utilizado debido a que típicamente el sistema de cableado se instala horizontalmente a través del piso o del techo del edificio.

El cableado horizontal consta de cable par trenzado de cobre, aunque si se requiere un alto rendimiento se puede utilizar fibra óptica.

El cableado horizontal se debe implementar en una topología de estrella. Cada punto terminal de conexión de datos y/o voz debe estar conectado al pánel de empate.

Se debe tener en cuenta que:

- No se permiten empates (múltiples apariciones del mismo par de cables en diversos puntos de distribución) en cableados de distribución horizontal.
- Algunos equipos requieren componentes en la salida del área de telecomunicaciones.
- Estos componentes deben instalarse externos a la salida del área de telecomunicaciones. Esto garantiza la utilización del sistema de cableado estructurado para otros usos.
- Si la línea es de datos, se establece una conexión adicional entre el pánel de empate y el concentrador (hub), para que el equipo quede conectado a la red.

Consideraciones para el cableado horizontal

Distancias Horizontales

- La máxima distancia horizontal permitida es de 90 metros (295 ft) independiente del tipo de medio.
- Esta es la distancia máxima entre el pánel de empate y la terminal de conexión.
- La longitud máxima del punto terminal hasta la estación de trabajo es de 3 metros (9.8 ft).

Tipos de Cables

Existen tres tipos de cables que pueden ser utilizados en los sistemas de cableado horizontal:

- Cable UTP (Unshielded Twisted Pair) de 4 pares a 100 ohms .
- Cable STP (Shielded Twisted Pair) de 2 pares a 150 ohms.
- Fibra Optica 62.5/125 mm de 2 pares.

El cable a utilizar por excelencia es el par trenzado sin blindaje UTP de cuatro pares categoría 5e. El cable coaxial de 50[Ω] se acepta, pero no se recomienda en instalaciones nuevas.

Salidas de área de trabajo

Los ductos a las salidas de área de trabajo WAO deben prever la capacidad de manejar tres cables. Las salidas de área de trabajo deben contar con un mínimo de dos conectores.

Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableado T568A ó T568B.

Algunos equipos requieren componentes adicionales en la salida del área de trabajo. Estos componentes no deben instalarse como parte del cableado horizontal, deben instalarse externos a la salida del área de trabajo. Esto garantiza la utilización del sistema de cableado estructurado para otros usos.

Adaptaciones comunes en el área de trabajo son, pero no se limitan a:

- Un cable especial para adaptar el conector del equipo (computadora, terminal, teléfono) al conector de la salida de telecomunicaciones.
- Un adaptador en "Y" para proporcionar dos servicios en un solo cable multipar (por ejemplo el teléfono con dos extensiones).
- Un adaptador pasivo utilizado para convertir del tipo de cable del equipo al tipo de cable del cableado horizontal.
- Un adaptador activo para conectar dispositivos que utilicen diferentes esquemas de señalización.

Un cable con pares transpuestos

Manejo del cable

El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm. para cables UTP categoría 5 y 5e.

El radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable. Para par trenzado de cuatro pares categoría 5 y 5e, el radio mínimo de doblado es de 2.5 cm.

Evitando la Interferencia Electromagnética

A la hora de establecer la ruta del cableado de los clósets de alambrado a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos:

- Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
- Cables de corriente alterna.
- Mínimo 13 cm. para cables con 2KVA o menos.
- Mínimo 30 cm. para cables de 2KVA a 5KVA.
- Mínimo 91cm. para cables con mas de 5KVA.
- Luces fluorescentes y balastros (mínimo 12 centímetros).
- El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimo 12 cm.).
- Equipo de soldadura.
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

3.2.3 Cableado vertical *(backbone)*

El cableado vertical (backbone) provee interconexión entre el cuarto de telecomunicaciones, cuarto de equipos y la entrada al edificio. Este consiste del cableado vertical, de la conexión cruzada intermedia y principal, de las terminaciones mecánicas y de los patch cords. El closet de telecomunicaciones, el cuarto de equipos y los puntos demarcados pueden estar localizados en diferentes edificios; el cableado vertical incluye los medio de transmisión entre diferentes edificios.

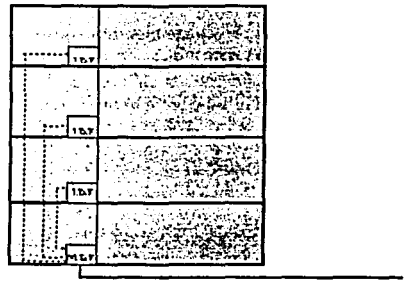


Figura 3.15 Cableado vertical o backbone.

El cableado vertical debe soportar todos los dispositivos que están dentro del clóset de telecomunicaciones y a menudo todas las impresoras, terminales y servidores de archivo de un piso de un edificio. Si más clientes o servidores son agregados a un piso, ellos compiten por el ancho de banda disponible en el cableado vertical. Sin embargo existe una ventaja, y esta es la poca cantidad de canales verticales en un edificio y por ello se pueden usar equipos más costosos para proveer un mayor ancho de banda.

Este es el área donde la fibra óptica se ha convertido en el medio más apropiado. El cableado vertical se presenta en diferentes topologías, la más usada es la topología en estrella.

Consideraciones al instalar el cableado vertical:

Cables Reconocidos y Distancias Máximas

Cable UTP 100Ω	800 m	Voz *
Cable STP 150 Ω	90 m	Datos *
Cable Monomodo de Fibra Optica de 62.5/125 µm	3000 m	Datos *
Cable Multimodo de Fibra Optica de 8.3/125 µm	2000 m	Datos *

***Tabla 3.1** *Nota: Las distancias del backbone, son dependientes de la aplicación. Las distancias máximas especificadas arriba son basadas en transmisión de voz para UTP y en transmisión de datos para STP y fibra óptica.*

Selección del Medio de Transmisión

Con cualquiera de los estándares existentes se puede construir un cableado vertical; pero debe tenerse en cuenta los siguientes factores:

- Flexibilidad con respecto a los servicios soportados.
- Vida útil requerida para el cableado vertical.
- Tamaño del sitio y la población de usuarios.
- No se pueden colocar más de dos niveles jerárquicos de cross-connects.
- No se pueden utilizar puentes.
- La longitud del patch-cord del cross-connect principal e intermedio no puede ser mayor a 20 m.
- El polo a tierra debe cumplir con los requerimientos de definidos en la norma EIA/TIA 607.

3.2.4 Cuarto de telecomunicaciones

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que puedan haber en un edificio.

3.2.5 Consideraciones de diseño

El diseño de un cuarto de telecomunicaciones depende de:

- El tamaño del edificio, *tabla 3.2.*
- El espacio de piso a servir.
- Las necesidades de los ocupantes.
- Los servicios de telecomunicaciones a utilizarse.

a) Cantidad de cuartos de telecomunicaciones: Debe de haber un mínimo de un cuarto de telecomunicaciones por edificio, mínimo uno por piso, no hay máximo.

b) Altura: La altura mínima recomendada del cielo raso es de 2.6 metros.

c) Ductos: El número y tamaño de los ductos utilizados para acceder, al cuarto de telecomunicaciones varía con respecto a la cantidad de áreas de trabajo, sin embargo se recomienda por lo menos tres ductos de 100 milímetros (4 pulgadas) para la distribución del cable del cableado vertical. Los ductos de entrada deben de contar con elementos de retardo de propagación de incendio "firestops". Entre Cuartos de Telecomunicaciones de un mismo piso debe haber mínimo un conduit de 75 mm.

d) Puertas: La(s) puerta(s) de acceso debe(n) ser de apertura completa, con llave y de al menos 91 centímetros de ancho y 2 metros de alto. La puerta debe ser removible y abrir hacia afuera (o lado a lado). La puerta debe abrir al ras del piso y no debe tener postes centrales.

e) Polvo y electricidad estática: Se debe el evitar polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento especial a las paredes pisos y cielos para minimizar el polvo y la electricidad estática.

f) Control ambiental: En cuartos que no tienen equipo electrónico la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente (24 horas, 365 días al año) entre 10 y 35 grados centígrados. La humedad relativa debe mantenerse menor a 85%. Debe de haber un cambio de aire por hora.

En cuartos que tienen equipo electrónico la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente (24 horas al día, 365 días al año) entre 18 y 24 grados centígrados. La humedad relativa debe mantenerse entre 30% y 55%. Debe de haber un cambio de aire por hora.

g) Plafón falso: Se debe evitar el uso de plafón falso en los cuartos de telecomunicaciones.

h) Prevención de inundaciones: Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso. De haber regaderas contra incendio, se debe instalar una canaleta para drenar un goteo potencial de las regaderas.

i) Pisos: Los pisos de los cuartos de telecomunicaciones deben soportar una carga de 2.4 KPa.

j) Iluminación: Se debe proporcionar un mínimo equivalente a 540 lux medido a un metro del piso terminado. La iluminación debe estar a un mínimo de 2.6 metros del piso terminado. Las paredes deben estar pintadas en un color claro para mejorar la iluminación. Se recomienda el uso de luces de emergencia.

k) Localización: Con el propósito de mantener la distancia horizontal de cable promedio en 46 metros o menos (con un máximo de 90 metros), se recomienda localizar el cuarto de telecomunicaciones lo más cerca posible del centro del área a servir.

l) Potencia: Deben haber tomacorrientes suficientes para alimentar los dispositivos a instalarse en los andenes. El estándar establece que debe haber un mínimo de dos tomacorrientes dobles de 110V C.A. dedicados de tres hilos. Deben ser circuitos separados de 15 a 20 amperios. Estos dos tomacorrientes podrían estar dispuestos a 1.8 metros de distancia uno de otro. Considerar alimentación eléctrica de emergencia con activación automática. En muchos casos es deseable instalar un pánel de control eléctrico dedicado al cuarto de telecomunicaciones. La alimentación específica de los dispositivos electrónicos se podrá hacer con UPS y regletas montadas en los andenes.

Separado de estos tomas deben haber tomacorrientes dobles para herramientas, equipo de prueba, etc. Estos tomacorrientes deben estar a 15 cm. del nivel del piso y dispuestos en intervalos de 1.8 metros alrededor del perímetro de las paredes.

El cuarto de telecomunicaciones debe contar con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable de mínimo 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA-607.

m) Seguridad: Se debe mantener el cuarto de telecomunicaciones con llave en todo momento. Se debe asignar llaves a personal que esté en el edificio durante las horas de operación.

Se debe mantener el cuarto de telecomunicaciones limpio y ordenado.

n) Requisitos de tamaño: Debe haber al menos un cuarto de telecomunicaciones o cuarto de equipo por piso y por áreas que no excedan los 1000 metros cuadrados. Instalaciones pequeñas podrán utilizar un solo cuarto de telecomunicaciones si la distancia máxima de 90 metros no se excede.

Área de Servicio Edificio Normal	
500 m^2 o menos	3.0 m. x 2.2 m.
Mayor a 500 m^2, menor a 800 m^2	3.0 m. x 2.8 m.
Mayor a 800 m^2, menor a 1000 m^2	3.0 m. x 3.4 m.
Área de Servicio Edificio Pequeño	
100 m^2 o menos	Montante de pared o gabinete encerrado.
Mayor a 500 m^2, menor a 800 m^2	Cuarto de 1.3 m. x 1.3 m. o Closet angosto de 0.6 m. x 2.6 m.
* Algunos equipos requieren un fondo de al menos 0.75 m.	

Tabla 3.2 Requisitos de tamaño para un cuarto de telecomunicaciones.

o) Especificaciones de equipos: Los andenes (racks) deben de contar con al menos 82 cm. de espacio de trabajo libre (al frente) de los equipos y páneles de empate. La distancia de 82 cm. Se debe medir a partir de la superficie más salida del andén.

De acuerdo al NEC, NFPA-70 Articulo 110-16, debe haber un mínimo de 1 metro de espacio libre para trabajar de equipo con partes expuestas sin aislamiento.

p) Paredes: Al menos dos de las paredes del cuarto deben tener láminas de plywood A-C de 20 milímetros de 2.4 metros de alto. Las paredes deben ser rígidas para soportar equipo. Las paredes deben ser pintadas con pintura resistente al fuego, lavable, mate y de color claro.

q) Cuarto de equipos. El cuarto de equipos es un espacio centralizado para los equipos de comunicaciones (p.ej. PBX, equipos de cómputo, switch), que sirven a los ocupantes del edificio. Este cuarto, debe guardar equipos directamente relacionados con el sistema de comunicaciones y sus sistemas de soporte. La norma que estandariza este subsistema es la EIA/TIA 569.

Se deben tener en cuenta las siguientes especificaciones al momento de diseñar el cuarto de equipos:

Selección del Sitio.

Cuando se seleccione el cuarto de equipos se deben evitar sitios que estén restringidos por componentes del edificio que limiten la comunicación tales como: elevadores,

escaleras, etc. El cuarto debe tener suficiente espacio para la entrada de grandes equipos y el acceso a este cuarto debe ser restringido al personal autorizado.

La capacidad de resistencia del piso debe ser tal que soporte la carga distribuida y concentrada de los equipos instalados. La carga distribuida debe ser mayor a 12.0 kpa (250 lbf/ft2) y la carga concentrada debe ser mayor a 4.4 kN (1000 lbf) sobre el área de mayor de los equipos.

El cuarto de equipos no debe estar localizado debajo de niveles de agua a menos que medidas preventivas se hallan tomado en contra de la filtración de agua. Un drenaje debe ser colocado en el cuarto en caso de que exista el ingreso de agua. El cuarto de equipos debe tener un acceso directo al HVAC (Heating, Ventilating and Air-Conditioning System)

El cuarto debe estar localizado lejos de fuentes de interferencias electromagnéticas, a una distancia que reduzca la interferencia a 3.0 V/m a través del espectro de frecuencia. Se debe tener especial cuidado con transformadores eléctricos, motores, generadores, equipos de rayos X, radios o radares de transmisión. Es deseable colocar el cuarto de equipos cerca de la ruta del cableado vertical.

Tamaño.

El cuarto de equipos debe tener un tamaño suficiente para satisfacer los requerimientos de los equipos. Para definir el tamaño debe tener en cuenta tanto los requerimientos actuales, como los proyectos futuros.

Cuando las especificaciones de tamaño de los equipos no son conocidas se deben tener en cuenta los siguientes puntos:

Guia para Voz y Datos. La práctica consiste en proveer 0.70 m^2 de espacio en el cuarto por cada 10m^2 de una estación de trabajo. El cuarto de equipos debe ser diseñado para un mínimo de 14m^2. Basándose en el número de estaciones de trabajo, el tamaño del cuarto debe ser según la siguiente *tabla 3.3*:

Número de Estaciones de Trabajo	
Hasta 100	14
Desde 101 hasta 400	37
Desde 401 hasta 800	74
Desde 801 hasta 1200	111

Tabla 3.3 Tamaño del cuarto según el número de estaciones de trabajo.

Guia Para Otros Equipos. Los equipos de Control Ambiental, tales como distribuidores de energía, aires acondicionados y UPS hasta 100 kVA se deben instalar en el cuarto de equipos. UPS mayores a 100 kVA debe estar localizadas en cuartos separados.

Provisionamiento

La altura mínima de un cuarto de equipos debe ser de 2.44 metros (8 pies) sin obstrucciones.

El cuarto de equipos debe estar protegido de contaminación y polución que pueda afectar la operación y el material de los equipos instalados. Cuando la contaminación presente es superior al indicado en la siguiente *tabla 3.4*, barreras de vapor o filtros deben ser instalados en el cuarto.

Cloro	0.01 ppm
Sulfato de Hidrógeno	0.05 ppm
Oxido de Nitrógeno	0.01 ppm
Dioxido de Sulfuro	0.3 ppm
Polvo	100 ug/m3/24h
Hidrocarburo	4 ug/m3/24h

Tabla 3.4 Valores máximos para concentración de contaminantes

El cuarto de equipos debe estar conectado a la ruta del cableado vertical. En caso de necesitarse detectores de humo, estos deben estar dentro de su caja para evitar que se vayan a activar accidentalmente. Se debe colocar un drenaje debajo de los detectores de humo para evitar inundaciones en el cuarto.

Equipos de Calefacción, Ventilación y Aire Acondicionado (HVAC)

Estos equipos deben ser proveídos para funcionar 24 horas por día y 365 días por año. Si el sistema del edificio no asegura una operación continua, una unidad independiente (Stand Alone) debe ser instalada para el cuarto de equipos.

La temperatura y la humedad deben ser controladas entre unos rangos de 18 °C a 24 °C, con una humedad del 30% al 55%. Equipos de humedificación y deshumedificación pueden ser requeridos dependiendo de las condiciones ambientales del lugar. La temperatura ambiente y la humedad deben ser medidas a una distancia de 1.5 metros sobre el nivel del piso y después de que los equipos estén en operación.

Si se utilizan baterías para backup, se deben instalar equipos adecuados de ventilación.

Acabados Interiores

El piso, las paredes y el techo deben ser sellados para reducir el polvo. Los acabados deben ser de colores luminosos para aumentar la iluminación del cuarto. El material del piso debe tener propiedades antiestáticas.

Iluminación

La iluminación debe tener un mínimo de 540 luxes, medida 1 metro sobre el piso en un lugar libre de equipos. La iluminación debe ser controlada por uno o más switches, localizados cerca de la puerta de entrada al cuarto.

Energía

Se debe instalar un circuito separado para suplir de energía al cuarto de equipos y debe terminar en su propio panel eléctrico. La energía eléctrica que llegue al cuarto no se especifica ya que depende de los equipos instalados.

Puerta

La puerta debe tener un mínimo de 91 cm de ancho y 2 m de alto y contener una cerradura. Si se estima que van a llegar equipos muy grandes, se debe instalar una puerta doble de 1.820 m de ancho por 2.28 m de alto.

Polo a Tierra

Se debe instalar un conducto de 1-1/2 desde el cuarto de equipos hasta electrodo a tierra del edificio.

Extinguidores de Fuego

Se deben proveer extinguidores de fuego portátiles y hacerles mantenimiento periódicamente. Estos, deben ser instalados tan cerca a la puerta como sea posible.

Cuarto de entrada de servicios

La entrada de servicios provee el punto en el cual el cableado externo se une con el cableado vertical (backbone) interno del edificio. Este consiste en una entrada de servicios de telecomunicaciones al edificio, la cual incluye el punto de entrada a través de la pared del edificio y continuando al cuarto o área de entrada. La entrada al edificio debe contener la ruta del cableado vertical que interconecta con los otros edificios del campus. En caso de una comunicación a través de una antena, esta también pertenece a la entrada al edificio.

Requerimientos de Funcionamiento y de Ancho de Banda

Los diferentes sistemas de cableado ofrecen distintas características de funcionamiento. La variedad de velocidad de transmisión de los datos que un sistema de cableado puede acomodar, se conoce como el ancho de banda utilizable. La capacidad del ancho de banda está dictada por las características de comportamiento eléctrico que los componentes del sistema de cableado tengan. Ésto viene a ser especialmente importante cuando se están planeando futuras aplicaciones que impondrán mayores demandas sobre el sistema de cableado.

El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se está apoyando las necesidades actuales sino también cuando se anticipan las necesidades

del mañana. Hacer esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del sistema de cableado.

Existen tres opciones típicas de sistemas de cableado estructurado, cada una posee características de producto y de funcionamiento particulares.

Recomendaciones en cuanto a canalizaciones y ductos

- Los cables UTP no deben circular junto a cables de energía dentro de la misma cañería por más corto que sea el trayecto.
- Debe evitarse el cruce de cables UTP con cables de energía. De ser necesario, estos deben realizarse a 90°.
- Los cables UTP pueden circular por bandeja compartida con cables de energía respetando el paralelismo a una distancia mínima de 10 cm. En el caso de existir una división metálica puesta a tierra, esta distancia se reduce a 7 cm.
- En el caso de pisoductos o caños metálicos, la circulación puede ser en conductos contiguos.
- Si es inevitable cruzar un gabinete de distribución con energía, no debe circularse paralelamente a más de un lateral.
- De usarse cañerías plásticas, lubricar los cables (talco industrial, vaselina, etc) para reducir la fricción entre los cables y las paredes de los caños ya que esta genera un incremento de la temperatura que aumenta la adherencia.
- El radio de las curvas no debe ser inferior a 2".
- Las canalizaciones no deben superar los 20 metros o tener más de 2 cambios de dirección sin 18 cajas de paso.
- En tendidos verticales se deben fijar los cables a intervalos regulares para evitar el efecto del peso en el acceso superior.
- Al utilizar fijaciones (grapas, precintos o zinchos) no excederse en la presión aplicada (no arrugar la cubierta), pues puede afectar a los conductores internos.

3.2.6 Recomendaciones en cuanto a la documentación

La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, cruzadas, páneles de empate, armarios de telecomunicaciones y otros espacios ocupados por los sistemas de telecomunicaciones.

La documentación es un componente de la máxima importancia para la operación y el mantenimiento de los sistemas de telecomunicaciones.

Resulta importante poder disponer, en todo momento, de la documentación actualizada, y fácilmente actualizable, dada la gran variabilidad de las instalaciones debido a mudanzas, incorporación de nuevos servicios, expansión de los existentes, etc.

En particular, es muy importante proveerlos de planos de todos los pisos, en los que se detallan:

- Ubicación de los gabinetes de telecomunicaciones.
- Ubicación de ductos a utilizar para cableado vertical.
- Disposición de tallada de los puestos eléctricos en caso de ser requeridos.
- Ubicación de pseudoductos si existen y pueden ser utilizados.

3.3 Tecnologías de Alta velocidad

Ethernet es la capa física más popular de la tecnología de LAN usada actualmente; es conocido porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes combinados con la amplia aceptación del mercado y la habilidad de soportar virtualmente todos los protocolos de red más populares, hacen a ethernet la tecnología ideal para la red de la mayoría de usuarios de la informática de hoy. La norma de Ethernet fue definida por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) como el estándar 802.3. Adhiriéndose a la norma de la IEEE, los equipos y protocolos de red pueden interoperar eficazmente.

Estándares Ethernet

3.3.1 Estructura del Ethernet

3.3.1.1 Pasos para transmitir del Ethernet

CSMA/CD consiste a grandes rasgos de siete pasos diferentes que constituyen una transmisión del ethernet, *figura 3.16.*

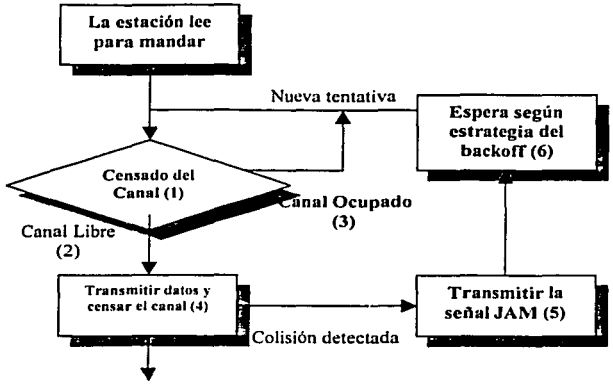


Figura 3.16 Pasos para transmisión de Ethernet.

Una estación que quiere transmitir un marco de información tiene que asegurar que ningún otro nodo o estaciones están usando los medios de comunicación compartidos actualmente, para que la estación escuche primero al medio. (Ésta es la parte de sentido del portador, también conocido como "escuche antes de hablar.")

1. Si el medio está callado para un cierto periodo mínimo de tiempo, llamando el interframe del hueco (IFG), la estación puede comenzar una transmisión ("hablar si el medio esta libre").

2. Si el medio está ocupado, se supervisa continuamente hasta que se ponga libre para el lapso de tiempo de mínimo de IFG. A estas alturas, la transmisión empieza (conocido como el acceso múltiple, o "esperar antes de hablar").

3. Una colisión (dos estaciones que transmiten en el cable al mismo tiempo) puede ocurrir cuando dos o más estaciones escuchan mientras que esperan transmitir, simultáneamente determinan que ese "canal" es libre, y empieza transmitiendo casi al mismo momento. Este evento llevaría a una colisión y destruiría ambos frames "marcos" de datos. Ethernet continuamente monitorea el medio durante la transmisión para descubrir las colisiones (el descubrimiento de la colisión, o "escuchar mientras se habla").

4. Si una estación descubre una colisión durante la transmisión, la transmisión inmediatamente se detiene. Una señal "jam" se envía al medio para garantizar que todas las otras estaciones descubran la colisión y rechazan cualquier marco de datos corrompidos que ellos pueden haber estado recibiendo (llamada también la parte del descubrimiento de la colisión, o "uno habla a la vez").

5. Después de un período de espera (llamado un backoff) las estaciones que desean transmitir intentan hacer una nueva transmisión. Un algoritmo del "backoff" aleatorio especial (llamado el backoff exponencial binario, o BEB) determina un tiempo de retrazo en que las estaciones diferentes tendrán que esperar antes de intentar enviar de nuevo sus datos. Claro, otra colisión podría ocurrir después de la primera, sobre todo cuando muchos nodos están intentando obtener el acceso al mismo tiempo. Después de 16 colisiones consecutivas para volver intentar una transmisión, el paquete se desechará. Esto puede y pasa si el medio de Ethernet es sobre utilizado. Ésta también es parte del método de acceso múltiple.

6. La secuencia regresa al primer paso.

3.3.1.2 El frame de Ethernet

Ethernet utiliza marcos de datos para transmitir la actual información, también conocido como la carga útil "payload", de la fuente al destino. Como otras más redes de área local en la existencia hoy día, Ethernet transmite un marco de longitud variable. La longitud del marco cambia porque la carga útil o el campo de datos pueden variar.

El original frame de Ethernet especificado por Digital, Intel, y Xerox es conocido como el "el frame DEC-Intel-Xerox Ethernet V2.0", o sólo DIX o "frame Ethernet II ". El oficial frame ethernet de la IEEE como consecuencia lo reemplazan *tabla 3.5*. La única diferencia está en el 2 byte del frame tipo / longitud del campo.

Hueco entre tramas	(12)
Preámbulo	7
Delimitador inicio de trama	1
Dirección de destino	6
Dirección de origen	6
Protocolo/Longitud	2
Datos	0-1500
Relleno	0-46
Secuencia de comprobación(CRC)	4

Tabla 3.5 Estructura de la trama Ethernet.

El hueco entre tramas es un período de tiempo en que no se transmite nada, de longitud equivalente a 12 bytes (96 ns a 10 Mb/s) que sirve para separar las tramas. Este hueco entre tramas es el mecanismo empleado en Ethernet para detectar cuando termina la trama anterior, ya que el campo longitud puede no existir y aunque exista no se utilizará en tiempo de captura para averiguar el fin de la trama. El hueco también permite al receptor tomarse un respiro para realizar diversas tareas de mantenimiento antes de volver a la escucha para capturar la trama siguiente.

Para asegurar que se respeta el hueco cuando una estación que va a transmitir detecta el medio libre espera el tiempo equivalente a 12 bytes antes de empezar a transmitir el preámbulo[14]

El preámbulo está formado por la secuencia 10101010 repetida siete veces, y el delimitador de inicio por la secuencia 10101011. Al ser transmitidos con codificación Manchester a 10Mb/s estos ocho bytes generan una onda cuadrada de 5 MHz durante 6,4 ms, lo cual permite a las demás computadoras sincronizar sus relojes con el emisor. El último bit del delimitador de inicio de trama marca el final del preámbulo y el comienzo de ésta.

Los campos dirección de destino y origen contienen la conocida dirección MAC IEEE de 6 bytes.

El campo protocolo/longitud se interpreta como protocolo cuando el valor es superior a 1536, y como longitud en caso contrario. El primer caso corresponde al antiguo formato DIX, y el segundo al formato 802.3 (actualmente el estándar 802.3 acepta ambos significados).

El campo datos puede tener una longitud entre 0 y 1500 bytes. Cuando su longitud es menor de 46 bytes se añade un relleno para asegurar que la longitud de la trama no es menor de 64 bytes (la trama propiamente dicha abarca desde el campo dirección de destino al CRC, ambos inclusive).

La secuencia de comprobación es un CRC de 32 bits basado en un generador polinómico de grado 32.

Como ya hemos comentado la longitud mínima de trama y la velocidad de la red fijan el diámetro de una Ethernet[15]. De haber mantenido la trama mínima de 64 bytes en Gigabit Ethernet el diámetro máximo habría sido de unos 45 m, inaceptable en la mayoría de situaciones. Para evitar esto la trama Gigabit Ethernet incorpora un segundo relleno denominado -extensión de portadora- que se añade al final de la trama para garantizar que la longitud mínima nunca sea inferior a 512 bytes (4096 bits). Así el tiempo de ida y vuelta puede ser de hasta 4.096 m s (en vez de 0,512 ms) y el diámetro puede llegar a 330 m. La extensión de portadora no es formalmente parte de la trama Ethernet, por lo que solo existirá mientras ésta viaje por Gigabit Ethernet. En el caso de que una trama con extensión de portadora sea transmitida a una red de 100 o 10 Mb/s la extensión de portadora se eliminará, e inversamente, si una trama menor de 512 bytes llega a una red Gigabit Ethernet

[14] En 1993 un investigador del centro de investigación de Xerox en Palo Alto detectó que muchas interfaces de red no respetaban en determinadas circunstancias el hueco entre tramas. Esto provocaba que se perdieran tramas, ya que algunas estaciones no estaban a la escucha, confiadas de que nadie transmitiría en ese momento. Esto ocurría en equipos de AMD, Cisco, HP, Intel, Network General y Silicon Graphics. Como el fallo afectaba a analizadores (HP y Network General) el problema solo podía detectarse con un osciloscopio.

[15] Definimos diámetro de la red como la distancia máxima entre dos estaciones.

desde Fast Ethernet o Ethernet el conmutador correspondiente añadirá la extensión de portadora necesaria para que la longitud sea de 512 bytes.

El uso de extensión de portadora supone una pérdida de eficiencia en el caso de tramas pequeñas, y un mayor riesgo de colisiones. Para reducir en lo posible estos problemas se prevé la posibilidad de que una estación que quiera enviar varias tramas pequeñas seguidas lo haga como una ráfaga sin necesidad de 'envolver' cada una en una extensión de portadora independiente (sin embargo si aún así la ráfaga es menor de 512 bytes seguirá generándose una extensión de portadora).

La longitud máxima de una trama Ethernet es de 1518 bytes (1500 bytes de datos más cabeceras). Un tamaño mayor permitiría mejorar la eficiencia, ya que se transmitirían menos tramas y se enviarían menos cabeceras; también se reduciría el tiempo de CPU empleado en procesar las tramas (en la mayoría de las implementaciones actuales el procesado de cada trama provoca una interrupción en la CPU). Por contra supondría que una estación pudiera monopolizar la red por más tiempo (1518 bytes suponen 1,214 ms a 10 Mb/s) y requeriría mayor cantidad de memoria para buffers en la interfaz de red; cuando se diseñaba Ethernet a finales de los 70's 1500 bytes se consideró un compromiso razonable entre costo y eficiencia. Actualmente, con precios mucho menores de la memoria y redes más rápidas sería interesante utilizar tramas mayores, por lo que de vez en cuando surge la propuesta de ampliar el tamaño máximo de trama de Ethernet implementando lo que se conoce como 'jumbo-frames'. Pero no parece factible que esta idea prospere en un futuro próximo, ya que requiere importantes modificaciones al estándar. Por otro lado según los expertos buena parte de la mejora en eficiencia que podría obtenerse con tramas mayores (la relativa al tiempo de proceso e interrupciones a la CPU) puede conseguirse con el tamaño de trama actual, con pequeñas mejoras en los controladores de red (poniendo algunas puertas lógicas más, es decir un poco más de silicio en la tarjeta), con lo que los beneficios de utilizar tramas mayores serían menores de lo que a primera vista podría pensarse.

3.3.2 Tecnologías Ethernet de alta velocidad

3.3.3 100BASE-T Fast Ethernet

100BASE-T es la versión del clásico estándar de Ethernet a 100Mbps. La IEEE oficialmente adopta la nueva especificación IEEE 802.3u Fast Ethernet 100BASE-T en mayo de 1995. Las características de 100BASE-T son las siguientes:

La MAC de 100BASE-T usa originalmente la MAC de Ethernet operando a 10 veces la velocidad.

El estándar 100BASE-T es diseñado para incluir múltiples capas físicas. Tres diferentes capas físicas de 100BASE-T son parte del estándar 802.3u: Dos para UTP y una para fibra multi-modo. EL PHY de UTP después se agregó a la especificación 802.3y.

Como 10BASE-T y 10BASE-F, 100BASE-T requiere una configuración de cableado en estrella con un hub central.

100BASE-T también incluye una especificación para una MII, la versión de 100Mbps de hoy es AUI. La capa de MII es una interfaz digital conectando la MAC y la PHY y permite transceiver externos.

Las diferencias entre 10BASE-T y 100BASE-T son en los estándares de la PHY y el diseño de las áreas de red. Porque las nuevas especificaciones del IEEE 802.3u contienen nuevas reglas para los repetidores y la topología de red. *figura 3.17* provee una apreciación global del nuevo estándar IEEE 802.3u

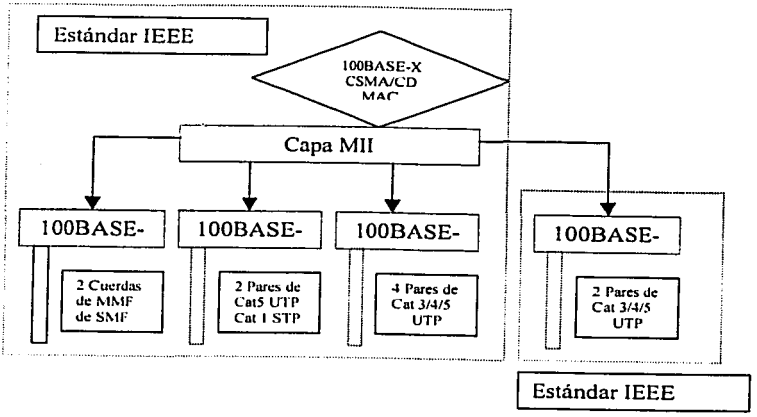


Figura 3.17 802.3u 802.3x.

3.3.3.1 La MAC de CSMA/CD de Fast Ethernet

La MAC de 100BASE-T es casi idéntica a la clásica MAC de ethernet de 10Mbps.

Según lo mencionado antes, la MAC del 802.3 CSMA/CD es intrínsecamente escalable, esto significa que puede ejecutarse en diversas velocidades y ser interconectada a diversas capas físicas. StartLAN/1BASE5 se aprovechó de esta escalabilidad para ejecutar el ethernet a 1Mbps. La *tabla 3.6* compara los estándares de la MAC a 10Mbps y el nuevo ethernet a 100Mbps. Nota la MAC de ethernet a 100Mbps retiene todos los parámetros de la MAC ethernet a 10Mbps excepto por el Inter.-FrameGap, que se ha disminuido a un décimo de su valor original, de 9.6μs a 0.96μs. Una frame de Fast Ethernet tiene el mismo formato de la construcción como un ethernet a 10Mbps, sólo que se transmite por el cable a 10 veces más de velocidad.

Slottime	512 bit times	Igual
Minimun InterFrameGap	96 bit times (9.6µs)	Igual (=0.96µs)
Attempt Limit	16 (tries)	Igual
BackoffLimit	10 (exponential number)	Igual
JamSize	32 bits	Igual
MaxFrameSize	1518 bytes	Igual
MinFrameSize	64 bytes (512bits)	Igual
AddressSize	48 bits	Igual

Tabla 3.6 Comparación de estándares.

Se puede calcular el tiempo de bit de 100BASE-T como sigue:

1 bit-time = 1 bit / 100Mhz= 10 ns

El 100BASE-T acopla la MAC de IEEE 802.3 de CSMA/CD con una familia de 100 Mbps de capas físicas. Mientras el MAC puede descascararse prontamente a los niveles de la diseño superiores, el nuevo estándar requiere de la capa física para operar a 100Mb/s.

Las relaciones entre 100BASE-T,the IEEE 802.3 existentes (CSMA/CD MAC), y el ISO/IEC del OSI se muestra en el siguiente *Diagrama 3.1*

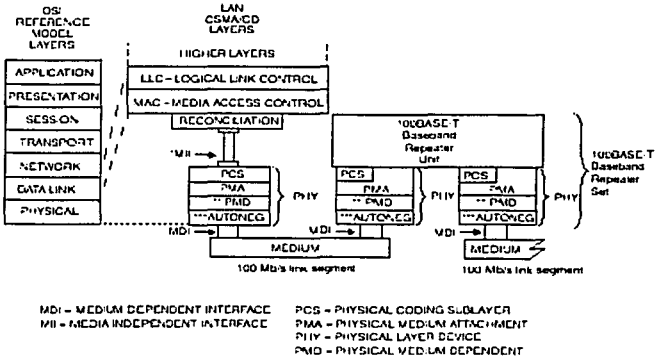


Diagrama 3.1 Arquitectura 100BASE-T.

El 100BASE-T usa la existente interfaz de capa de MAC del IEEE 802.3, conectado a través de la interfaz física independiente a la entidad de la Capa Física (PHY) subcapa como 100BASE-T4, 100BASE-TX, o 100BASE-FX.

El 100BASE-T extiende la MAC de IEEE 802.3 a 100 Mbps. El bit es más rápido, tiempos del bit son más cortos, tiempos de transmisión de paquete están reducidos, y los presupuestos de retraso en cable son menores —todo en proporción al cambio del ancho de banda. Esto significa que esta relación de duración del paquete para la propagación del retardo en la red para el 100BASE-T es igual al de 10BASE-T.

3.3.3.2 Las PHYs de fast Ethernet

Como en el 10BASE-T, el 100BASE-T combina el CSMA/CD con las especificaciones de la capa físicas diferentes. La especificación de la IEEE 802.3u contiene tres nuevas capas físicas para 100Mbps Ethernet.

El sistema 100BASE-TX de par trenzado es un tipo de medio de comunicación ampliamente usado. El estándar 100BASE-TX es basado en especificaciones de par trenzado primeramente diseñado para el estándar FDDI TP-PMD (Medio físico dependiente par trenzado). El sistema funciona bajo dos pares del cable par trenzado, uno para recibir señales de datos y el otro para transmitir señales de datos.

A. 100BASE-TX Componentes de señalización

Los siguientes componentes de señalización pueden ser usados en el sistema 100BASE-TX para enviar y recibir señales:

- Interfaz Ethernet incluido el tranceiver 100BASE-TX
- Interface Independiente del Medio (MII)
- Transceiver externo 100BASE-TX, también llamado PHY dispositivo de capa física.

1) Interfaz Ethernet 100BASE-TX.

Una interfaz 100BASE-TX puede equiparse con un tranceiver 100BASE-TX utilizado para hacer una conexión directa hacia el segmento de par trenzado. Si la interfaz esta equipada con un conector MII de 40 pins, pueden usarse los tranceiver externos *figura 3.18*

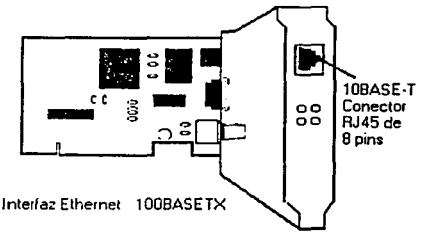


Figura 3.18 Interfaz Ethernet 100BASE-TX

La tarjeta es equipada con un conector RJ-45 que realiza una conexión al cable par trenzado. Típicamente la mayoría de las NIC's tienen solo un conector RJ-45. Tales NIC's pueden usar tranceivers internos para soportar la operación de múltiples velocidades. En tal, una interfaz de velocidades múltiples, el estándar de auto-negociación es típicamente utilizado para configurar automáticamente la velocidad de operación.

2) Interfaz Independiente del Medio (MII)

La MII es un conector de 40 pins que permite un transceiver externo 100BASE-TX para conectarse a la interfaz ethernet. Un transceiver externo es típicamente directamente conectado al conector de la MII en la interfaz.

3) Transceiver 100BASE-TX

Una interfaz 100BASE-TX que tiene fijo un transceiver que es conectado directamente al segmento ethernet de par trenzado. No hay la necesidad por un transceiver externo desde que el transceiver se incluye en la interfaz de la tarjeta. Sin embargo , si el dispositivo ethernet esta equipado con un conector MII de 40 pins , esta puede ser conectada al segmento de par trenzado ocupando un transceiver externo ethernet 100BASE-TX, *figura 3.19.*

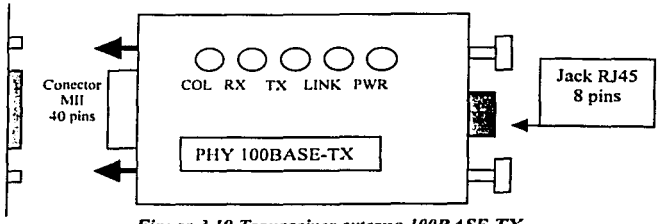


Figura 3.19 Transceiver externo 100BASE-TX.

4) Codificación de las señales 100BASE-TX

El sistema 100BASE-TX es basado en un codificación original diseñada para el estándar de FDDI X3T9.5, la cual incluye a ambos medios, la fibra óptica y al par trenzado. La codificación de la señal usada en FDDI y 100BASE-TX es el sistema de 4B/5B.

Línea de señalización física.

La señalización física utilizada para transmitir los símbolos de 5bits sobre cables de par trenzado esta fundado en un sistema llamado multi-nivel de umbral de 3 tiempos (MLT-3) . Esto significa que cada transición señalada de las señal pueden tener uno de tres niveles. Durante cada tiempo de transición , un cambio desde un nivel hacia el siguiente marca un uno lógico (1), donde hay una señal constante indica el cero lógico (0). Desde que el nivel señalado no cambia, cuando el cero se transmite, esto reduce el tarifaje de la señalización total en el alambre.

De las $2^5 = 32$ combinaciones posibles solo se utilizan 16, lo cual permite evitar las combinaciones con todo ceros o todo unos, que serían nefastas desde el punto de vista del sincronismo, y da una cierta capacidad de detección de errores. Con 4B/5B la señalización para 100 Mb/s es de 125 Mbaudios, con lo que la frecuencia fundamental es de 62,5 MHz. Esto permite utilizar cable categoría 5 (especificado hasta 100 MHz).

5) Componentes de 100BASE-TX

El siguiente conjunto de componentes son usados para un segmento de 100BASE-TX:

- Cable par trenzado blindado o sin blindar.
- Conectores RJ-45 de 8 posiciones que reúnan las especificaciones de categoría 5.

a) Cable par trenzado sin blindar.

El sistema 100BASE-TX opera sobre 2 pares de cable par trenzado sin blindaje (UTP); un par recibe las señales de los datos , mientras el otro par transmite señales de datos. La longitud máxima de un segmento es de 100 metros de cable par trenzado sin blindar que permite una característica de grado impedancia de 100 Ω y que reúne o excede las especificaciones de categoría 5 de la TIA/EIA.

b) Cable Par trenzado blindado.

El estándar TP-PMD soporta la opción de enviar señales FDDI sobre cable par trenzado blindado. Subsecuentemente el estándar 100BASE-TX es basado en TP-PMD, también provee esta opción de soporte de cableado en STP unas características de impedancia de 150Ω.

c) Roseta RJ-45

La versión del cable par trenzado sin blindaje del medio 100BASE-TX es la más usada. En este sistema de cables son terminados en un conector de 8 posiciones (RJ-45).

Las señales empleadas en 100BASE-TX en el conector de 8 pins son las mismas del 10BASE-T. *Capitulo2 tabla 2.3.*

Los números de pins utilizados en el conector de 8 pins para 100BASE-TX fueron cambiados de los que está definidos en el estándar del ANSI TP-PMD, para conformarse con el esquema del cableado ya en uso, el estándar 10BASE-T. El estándar del ANSI utiliza los contactos 7 y 8 para reciben datos. La manera, de que un adaptador de Ethernet 100BASE-TX puede substituir un adaptador 10BASE-T en una estación y este en el mismo sistema del cable de la categoría 5, es no cambiar los alambres.

Según el estándar de cableado estructurado, la categoría 5 de segmento del par-trenzado construido tendrá ocho alambres conectados al conector de RJ-45, incluso 100BASE-TX sólo usa cuatro de los ocho alambres. Los otros alambres no deben usarse para apoyar cualquier otro servicio, cuando el sistema de 100BASE-TX no se diseña para tolerar la diafonía (ruido eléctrico que se origina en señales de otros hilos del cable).

B. 100BASE-FX

El sistema de fibra óptica 100BASE-FX provee todas las ventajas de una conexión en un segmento de fibra óptica en 10BASE-FL, donde el funcionamiento es diez veces más rápido. La distancia de 2km sobre cables de fibra multi-modo es cuando se opera el segmento de 100BASE-FX en full-duplex. Las distancias considerablemente más largas son posibles al usar solo segmentos de fibra de mono-modo. Esto es porque el medio de 100BASE-FX es una opción popular para la red del backbone de ethernet.

Componentes de señalización 100BASE-FX

Los siguientes componentes de señalización pueden ser usados en el sistema 100BASE-FX para enviar y recibir señales sobre el medio:

- Interfaz Ethernet incluido el tranceiver de fibra óptica en 100BASE-FX
- Interfaz Independiente del Medio (MII)
- Transceiver externo 100BASE-FX, también llamado PHY dispositivo de capa física.

1) Interfaz ethernet 100BASE-FX

Una interfaz 100BASE-FX puede estar equipada con un tranceiver fijo 100BASE-FX, el cual se usa para hacer una conexión directa al segmento de fibra óptica. Si la interfaz es equipada con un conector de 40 pins MII , entonces pueden usarse los transceivers externos, *figura 3.20*

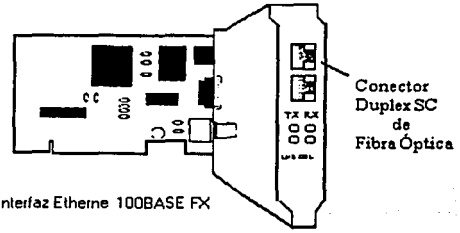


Figura 3.20 Interfaz Ethernet 100BASE-FX.

2) Interfaz Independiente del Medio

La MII is un conector de 40pins que permite un transceiver externo 100BASE-FX para poder conectar la interfaz ethernet. El transceiver típico es conectado directamente al conector MII en la interfaz ethernet.

3) Transceiver 100BASE-FX

Una interfaz 100BASE-FX con un transceiver fijo es conectado directamente hacia el segmento ethernet de fibra óptica; no hay necesidad por un transceiver externo desde que existe un transceiver en la interfaz de la tarjeta.

Sin embargo, si un dispositivo del ethernet está provisto con un conector de 40-pins MII, el puede conectarse a un segmento ethernet de fibra óptica con un transceiver externo de 100BASE-FX, *figura 3.21.*

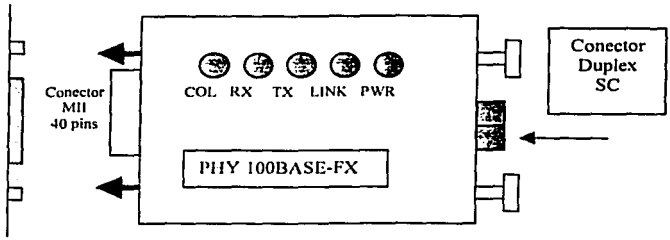


Figura 3.21 Transceiver Externo 100BASE-FX.

4) Codificación de la señal 100BASE-FX

El sistema 100BASE-FX es basado en una codificación original diseñada para el estándar de FDDI X3T9.5, la cual incluye a ambos medios, la fibra óptica y al par trenzado. La codificación de la señal usada en FDDI y 100BASE-FX es el sistema de 4B/5B.

5) Señalización de la línea física

La señalización física usada para transmitir señales de 100BASE-FX es lograda por enviar pulsos de luz sobre cables de fibra óptica. El sistema 100BASE-FX usa una variante del esquema no regreso a cero NRZ, que se llama Non-Return-to Zero, Invert-on-ones (NRZI). El sistema no realiza ningún cambio en el nivel de la señal al enviar un lógico cero (0), e invierte la señal desde un estado previo para un uno lógico (1).

El poder de la máxima transmisión óptica de un transceiver 100BASE-FX está entre 200 y 400(μW) microwats. Dado un número aproximadamente igual de unos y de ceros enviados sobre el segmento, la potencia media enviada sobre una conexión óptica de la fibra está entre 100 y 200(μW).

Estas figuras son para la luz que es juntada en una fibra estándar de 62.5/125 micrones. Puesto que no hay emisiones electromagnéticas en una conexión de fibra óptica, no hay necesidad de revolver los datos, según lo hecho con los sistemas 100BASE-TX para limitarse al nivel de emisiones electromagnéticas.

6) Componentes 100BASE-FX

El siguiente conjunto de componentes del medio son usados para un segmento de fibra óptica:

- Cable de fibra óptica.
- Conectores de fibra óptica.

a) Cable de fibra óptica

Las especificaciones de 100BASE-FX requiere de dos cuerdas de fibra multi-modo (MMF) por cada conexión, una para transmitir datos y otra para recibir datos.

Hay muchas clases de cables de fibra óptica disponibles, extendiéndose de los cables simples del puente del dos-hilo con el plástico del PVC para el material externo del jack hasta los cables grandes para edificios que llevan muchas fibras en conjunto.

El cable típicamente usado de fibra óptica para una conexión al segmento de 100BASE-FX consiste en un cable de MMF. Estas fibras ópticas tienen un corazón de 62.5µm y un revestimiento externo de 125 µm (62.5/125).

La longitud de onda de la luz usada en una conexión a un segmento de la fibra 100BASE-FX es de 1350 nanómetros (nm).

Las señales enviadas en esa longitud de onda sobre la fibra MMF pueden proporcionar longitudes de segmento de hasta 2000 metros cuando el modo de operación de la conexión es en modo full-duplex.

b) Conector de Fibra Óptica.

La interfaz dependiente del medio (MDI) para una conexión de 100BASE-FX puede ser una de tres tipos de conectores de fibra óptica. De los tres, el conector duplex SC (*ver figura 3.22*) es el recomendado como una alternativa en el estándar y es el más ampliamente usado por los vendedores. El conector SC es diseñado por la facilidad de uso; el conector se empuja en lugar y se encaja a presión automáticamente hacia el conector que contiene para terminar la conexión.

Figura 3.22 Conector Duplex SC.

El conector ST puede también ser utilizado. Este es el mismo conector usado para una conexión 10BASE-FL.

Según el estándar, el conector óptico del interfaz de los media de la fibra del FDDI (MIC) se puede también utilizar en el equipo 100BASE-FX; sin embargo, este conector opcional no ha sido adoptado por los vendedores del equipo.

La norma contiene las pautas para construir un solo segmento 100BASE-FX de fibra óptica, así como las pautas para unirse a los múltiples segmentos en un gran sistema, ***tabla 3.7.***

Fibra óptica 100BASE-FX	412m (1351 pies)[16]	2

Tabla 3.7 Segmento más largos de fibra.

Los segmentos más largo de fibra son posibles cuando la conexión es operada en modo full-duplex. El modo full-duplex en una conexión de un segmento de edición de conexiones significa que la longitud de segmento ya no se restringe por los límites de tiempo del round-trip de un canal compartido de Ethernet. En cambio, la longitud del segmento está limitada por la pérdida de poder óptico (la atenuación señal) y la dispersión de señal encima del cable de fibra óptica. Típicamente los transceiver de fibra óptica pueden alcanzar distancias de 2km. Sobre segmento de 100BASE-FX usando cables de fibra multi-modo. Las distancias más largas pueden ser alcanzadas cuando se utiliza una fibra simple-modo para un segmento full-duplex.

Mientras que las conexiones unimodales 100BASE-FX pueden alcanzar distancias de 20 kilómetros o más, este tipo de fibra es más costoso y difícil de utilizar ya que cuenta con varios modos de funcionamiento. La base unimodal de la fibra puede típicamente ser 8 o 9 um en el diámetro, comparado a la base de 62.5 um en con varios modos de funcionamiento. Juntar una fuente de luz en la base pequeña de la fibra unimodal requiere una fuente de luz laser más costosa y conectores muy exactos.

C. 100BASE-T2

100BASE-T2 es virtualmente desconocido. Es un estándar, pero no es un producto que se hizo comercial. La tecnología de 100BASE-T2 reaparecerá con el PHY de 1000BASE-T.

[16] Esta longitud máxima del segmento es para una conexión del segmento en half –duplex entre dos estaciones. Si un repetidor se usa para unirse dos segmentos de fibra óptica, la distancia máxima permitida será menos de 412 metros. No hay longitud mínima especificada para este tipo del segmento. Dos estaciones 100BASE-FX se pueden conectar a un cable de la corrección que sea tan corto como practicable.

Los ingenieros de IEEE propusieron 100BASE-T2 porque ellos pensaron que 100BASE-T4 tenían dos limitaciones que ellos podrían mejorar. Primera T4 requiere 4 pares de categoría 3, pero algunas instalaciones solo tienen 2 pares presentes o usables. El otro problema con T4 es no full-duplex. Cuando 100BASE-T4 era diseñado, fue pensado en que se exigirían cuatro pares para transferir 100Mbps.

Debido a los adelantos en el proceso de señalado digital (DSP) y tecnología de astilla de circuito integrado, se ha puesto posible transferir 100Mbps encima de sólo dos pares de categoría 3 UTP. El IEEE trabajó durante aproximadamente dos años en 100BASE-T2 normal. Cuando la norma estaba completa, al menos,100BASE-TX ya dominaba el mercado a tal una magnitud que ningún producto de T2 fue construido en la vida. Lo siguiente es los rasgos principales de 100BASE-T2:

Utiliza dos pares de voz o datos del cable par trenzado categoría 3, 4 ó 5 sin blindaje.

Usa ambos pares para transmitir y recibir simultáneamente, también conocido como dual-doble.

Utiliza un esquema de la codificación cinco-nivelado más complicado llamado PAM5X5. (PAM representa la modulación por amplitud del pulso), *tabla 3.8.*

Parámetro	100BASE-...	100BASE-...	100BASE-...	100BASE-...	100BASE-...
Origen de la Tecnología		CDDI TP PMD (ANSI X3T9.5	Desarrolada desde 1995 a 1996	FDDI PMD (ANSI X3T9.5)	Desarrollada desde 1994 a1995
Estándar IEEE	802.3i 1990	802.3u 1995	802.3u 1995	802.3u 1995	802.3y 1996
Codificación	Manchester	4B/5B	8B/6T	4B/5B	PAM5X5
Cableado Requerido	UTP Categoría 3,4,5	UTP Categoría 5 o STP	UTP Categoría 3,4,5	Multimodo o Simplemodo	UTP Categoría 3,4,5
Frecuencia de la señal	20MHz	125MHz	25MHz	125MHz	25MHz
Número de pares Requeridos	2	2	4	2	2
Distancia	100 m	100m	100m	150/412/2000 m	100m
Full Duplex	Si	Si	No	Si	Si
Número de pares para transmitir	1	1	3	1	2

Tabla 3.8 Comparación de 100BASE-T con las 4 especificaciones de las capas físicas del 100BASE-T.

D. 100BASE-T4

Subcapa de código físico (PCS), la subcapa del anexo al medio físico (PMA) y el medio de banda base, tipo 100BASE-T4.

Las especificaciones de PCS 100BASE-T4, PMA y el medio banda base se apuntan a los usuarios que requieren 100 Mb/s de desempeño, pero reteniendo los beneficios de usar el grado de señalización del cable par-trenzado. 100BASE-T4 requiere cuatro pares de categoría 3 o bien un cable mejor.

100BASE-T4 no transmiten una señal continua entre paquetes que lo hacen útil en la batería de energía en las aplicaciones. El PHY de 100BASE-T4 es uno de la familia de redes 100BASE-T de CSMA/CD de alta velocidad.

Juntas, las capas PCS y PMA comprenden una capa física 100BASE-T4 (PHY). A continuación se proveen las característica técnicas funcionales, eléctricas, y mecánicas para el tipo 100BASE-T4 PCS, PMA, y MDI. Estas cláusulas también especifica el medio de la banda de base usado con 100BASE-T4.

Objetivos

Los objetivos de 100BASE-T4 son:

- Soportar la MAC de CSMA/CD en el modo half duplex para su funcionamiento.
- Soportar el MII de 100BASE-T, el repetidor y la autonegociación.
- Proporcionar 100 Mb/s de datos al MII.
- Proporcionar funcionamiento sobre el cable de pares trenzado sin blindaje de Categoría 3, 4, o 5, en instalaciones, como se especifica en ***3.3.3.2 inciso D sección 1***, a las distancias arriba de 100 metros (328 pies).
- Permitir una magnitud de la red nominal de 200 metros, incluyendo,:

  - Los eslabones de par-trenzado sin blindaje de 100 metros.
  - Dos repetidores de red de aproximadamente 200 metros de palmo.
  - Proporcionar un canal de comunicación con un significativo símbolo ternario valor de error a la interfaz de servicio PMA.

Características del segmento de eslabón

1) Cableado

Generalmente la apropiada practica de cableado e instalación para el uso con esta norma aparece en el ISO/IEC11801:1995. Las excepciones, notas, y los requisitos adicionales mencionadas debajo.

100BASE-T4 usa una topología de estrella. El cableado horizontal se usa para conectar las entidades de PHY.

100BASE-T4 es una aplicación clase C (ISO/IEC 11801:1995). La frecuencia fundamental más alta transmitida por el código 8B/6T es de 12.5 MHz. Los datos agregados clasifican para tres de pares que usan 8B/6T codificando es 100 Mbps.

100BASE-T4 usarán cuatro pares del cableado balanceado, categoría 3 o bien, con una impedancia característica nominal de 100 Ω

El uso de cable blindado está fuera del alcance de esta norma.

2) Impedancia característica diferencial

La magnitud de la impedancia característica diferencial de 1 a 3 metros de par trenzado usado en un eslabón estará entre 85 Ω y 115 Ω para todo las frecuencias entre 2 MHz y 12.5 MHz.

3) Retraso Máximo del eslabón

El retraso de la propagación de un segmento del eslabón simplex no excederá 570 ns en todas la las frecuencias entre 2.0 MHz y 12.5 MHz.

Retraso máximo del eslabón por el metro

El retraso de la propagación por el metro de un segmento del eslabón simplex no excederá 5.7 ns/m en todas las frecuencias entre 2.0 MHz y 12.5 MHz.

4) Diferencia en los retrasos del eslabón

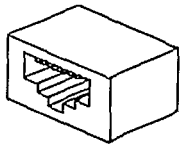
La diferencia en el retraso de la propagación, o sesgo, en todas las condiciones, entre el más rápido y el más lento en un segmento del eslabón no excederán de 50 ns todas las frecuencias en entre 2.0 MHz y 12.5 MHz. Es un requisito funcional adicional, una vez instándolo, la inclinación entre todo las combinaciones del par debido a las condiciones ambientales no variará más de ± 10 ns, dentro del requisito anterior.

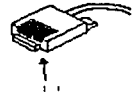
5) Especificaciones del MDI

Esta cláusula define al MDI. La topología del eslabón requiere una función del traspaso entre PMAs. También se definen la aplicación y situación de este traspaso en esta cláusula.

a) Conectores de MDI

Los conectores de ocho-pins que reúnen los requisitos de sección 3 y figura 1 a través de 5 de IEC 60603-7:1990 se usará como la interfaz mecánica al balanceo del cableado. El conector "plug" se usará en el balanceo del cableado y el jack en el PHY. Estos conectores se pintan (sólo para el uso informativo) en las *figuras 3.23a y 3.23b*. La *Figura 3.23c* muestras la asignación de signos de PMA a los contactos del conector para PHYs con y sin un traspaso interior "crossover".





Conector MDI Conector Balanceado

Contact	PHY without internal crossover recommended for DTE internal PMA signals	PHY with internal crossover recommended for repeater internal PMA signals	MDI labeling requirement
1	TX [+]	TX [+]	TX [+]
2	TX [-]	RX [+]	TX [-]
3	RX [+]	TX [-]	RX [+]
4	[-]	[-]	[-]
5	[-]	[-]	[-]
6	RX [-]	RX [-]	RX [-]
7	[-]	[-]	[-]
8	[-]	[-]	[-]

Figura 3.23 a)Superior izquierda, b)superior derecha, c)inferior

3.3.4. 1000BASE: Gigabit Ethernet, a 1000 Mbps

3.3.4.1 1000BASE-T

Las especificaciones para el medio de 1000BASE-T están diseñadas en suplemento del estándar de la IEEE 802.3ab, que fue formalmente adoptado en Julio de 1999. Soportando 1 billón de bits por segundo sobre cable par trenzado sin blindar (UTP), siendo un logro notable.

Para realizar el proyecto, el sistema de 1000BASE-T utiliza una mezcla de las técnicas de señalización y de codificación que fueron desarrolladas originalmente para los estándares 100BASE-TX, 100BASE-T2 y 100BASE-T4. Mientras que 100BASE-T2 y 100BASE-T4 no fueron adoptados extensamente en el mercado, su tecnología fue utilizada en desarrollar el estándar 1000BASE-T.

El estándar 100BASE-T2 Fast Ethernet esta basado en un sistema complejo de codificación de la señal usada para enviar señales a 100Mbps encima de dos pares del cable de categoría 3. Las técnicas fueron adoptadas y extendidas para el estándar 1000BASE-T para usarse sobre 4 pares del cable par trenzado categoría 5.

Del sistema 100BASE-T4, el estándar 1000BASE-T adoptó la técnica de enviar y de recibir señales simultáneamente sobre los mismos pares del alambre. El sistema 1000BASE-T también adoptó la línea de señalización del sistema popular Fast Ethernet

100BASE-TX. Manteniendo la misma línea de señalización que permite que 1000BASE-T trabaje sobre el mismo cableado de categoría 5 que soporta una conexión 100BASE-TX.

A. Componentes de señalización 1000BASE-T

A diferencia de otros sistemas ethernet que proporcionan un conector AUI o una MII que utilizan un transceiver externo y un cable para el transceiver, el sistema de 1000Base-T requiere una interfaz ethernet con un transceiver Giga Ethernet incorporado "empotrado" . No hay ningún conector del transceiver en el sistema Gigabit Ethernet , y por lo tanto no existe un soporte para un transceiver externo.

La interfaz 1000BASE-T viene equipada con un transceiver fijo usado para realizar una conexión directa hacia el segmento de par trenzado 1000BASE-T (la interfaz electrónica).

El elemento electrónico de la interfaz se puede construir en la computadora de fábrica, o puede ser una tarjeta del adaptador que está instalada en una de las ranuras de expansión en las computadoras. Una interfaz Ethernet también se encuentra en cada acceso al puerto del hub, *figura 3.24.*

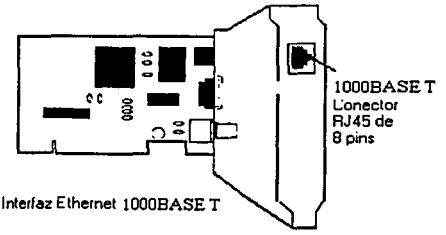


Figura 3.24 Interfaz Ethernet 1000BASE-T.

Esta tarjeta en particular es equipada con un jack RJ45 que realiza una directa conexión al segmento de par trenzado. Muchas de las tarjetas típicas tienen un solo conector RJ-45 en ellos. Tales tarjetas pueden usar una combinación de transceiver interno de GII o MII para soportar múltiples velocidades para su funcionamiento. En tal interfaz múltiple, el estándar de auto negociación es típicamente utilizado para una configuración automática de la velocidad de operación.

1) Codificación de la señal 1000BASE-T

Las técnicas de señalización inicialmente diseñadas para los estándares 100BASE-T2, T4 y TX han sido adoptadas y extendidas para Gigabit ethernet. A este conjunto pre-existente de tecnologías, el sistema 1000BASE-T agrega su propio conjunto de técnicas para el proceso de la señalización digital.

La codificación de la señal en una conexión 1000BASE-T esta basada en un complejo esquema de bloque de codificación llamado 4D-PAM5.

Las señales codificadas son transmitidas usando un símbolo de 5° nivel que lleva dos bits de datos en cada símbolo.

Los cuatro símbolos codificados representan un octeto de 8 dígitos binarios de datos en la porción de la codificación llamada 4d. El esquema de codificación y el conjunto completo de símbolos codificados usados son absolutamente complejos, y de interés primario solamente a los diseñadores del chip del transceiver.

Los símbolos codificados se transmiten sobre los pares del alambre usando una modulación PAM5 llamado sistema de la amplitud de pulso de cinco niveles. El sistema que señala 5-nivel de línea incluye señales de corrección de error para mejorar la relación de transformación de la señal/interferencia en el cable. Los voltajes diferenciados usados en el par del alambre hacen pivotar de aproximadamente cero a +1 voltios en el alambre positivo y a partir de 0 a 1 voltios en el alambre negativo.

2) Señalización y razón de datos

Un enlace 1000BASE-T transmite y recibe datos en todos los 4 pares simultáneamente. En los transceiver 1000BASE-T a cada final de la conexión contiene cuatro secciones idénticas para transmitir y cuatro secciones idénticas para recibir. Cada 4 pares del cable en la conexión del segmento están conectados ambos circuitos de transmisión y recepción en el transceiver. Un circuito especial conocido como híbrido hace posible que el transmisor-receptor se ocupe de la tarea de transmitir y recibir simultáneamente señales en cada par del alambre *figura 3.25.*

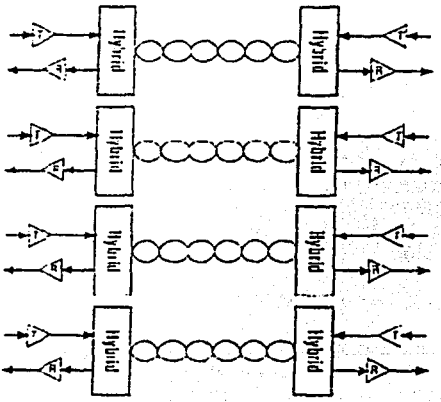


Figura 3.25 Transmisión de la señal 1000BASE-T.

Este gráfico muestra los caminos de datos básicos a través de los circuitos híbridos en cada transmisor-receptor. Dos dígitos binarios de los datos de Ethernet se codifican y se envían por la transición de señal en cada par del alambre y todos los cuatro pares del alambre se utilizan simultáneamente para enviar y recibir datos. El resultado es total de ocho dígitos binarios de información enviados a través de los cuatro pares para cada transición de señal. La transición a razón de 125Mbaud alcanza un total de los datos de 1000Mbps. Usando un sistema de señalización de la línea de cinco niveles que mantiene aproximadamente la misma tarifa de la señalización en el cable que 100BASE-TX Fast Ethernet.

La continua señalización en ambas direcciones en todos los 4 cables, genera una señal de eco y diafonía, que el sistema 1000BASE-T debe manejar. El sistema 1000BASE-T utiliza un conjunto de técnicas de proceso de la señal digital (DSP) para solucionar estos problemas. Esto incluye la cancelación del eco y la cancelación de la diafonía. Otra técnica es la equalización de la señal, para ayudar a compensar la distorsión de la señal sobre el canal.

B. Requerimiento de Cableado 1000BASE-T

La señalización para un sistema 1000BASE-T opera al misma razón de la señalización encima del cable como el sistema de 100BASE-TX. Sin embargo, las técnicas de la señalización complejas usadas en el 1000BASE-T son más sensibles a ciertos problemas del funcionamiento de la señal en segmentos de la categoría 5. Por consiguiente, es importante que todos los cables del par-trenzado y otros componentes usados en un segmento 1000BASE-T excedan las especificaciones de transporte de la señal de la categoría 5, se puede adquirir el cable de categoría 5e que ha mejorado las capacidades de transporte de señal. También se puede encontrar cables con valuaciones de calidad señaladas aun superiores, que se venden por vendedores del cable.

La operación confiable de Gigabit-Ethenet requiere que todas las cuerdas del patch estén ensambladas correctamente usando componentes de la alta calidad. Los pares trenzados deben mantener sus torceduras lo mas posiblemente cerca a los conectores RJ45, y los conectores deben ser de alta calidad para tener la capacidad para llevar la mejor señal. Puede realmente ser absolutamente difícil construir las cuerdas del patch hechas en casa que resuelvan estos requisitos. Los cables hechos en casa no reunen las especificaciones de la categoría 5e y pueden causar problemas en un segmento 1000BASE-T.

1) Componentes 1000BASE-T

Los siguientes componentes son usados para un segmento de par trenzado de 1000BASE-T

- Cable categoría 5e UTP
- Conectores RJ45 de 8 posiciones que reúnan o excedan las especificaciones de la categoría 5e.

a) Cable UTP

El sistema 1000BASE-T opera sobre cuatro pares de cables de categoría 5e. La máxima longitud de un segmento es de 100 metros de cable UTP con una característica de impedancia de 100Ω y que reúnan o excedan las especificaciones de la TIA/EIA de categoría 5e.

b) Jack de 8 posiciones RJ-45

El sistema 1000BASE-T utiliza 4 pares de cable que son terminados en un "jack" conector de 8 posiciones, subsecuentemente el sistema usa 4 pares del cable, todos los pins del conector son ocupados, *tabla 3.9*.

1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

Tabla 3.9 Pins del conector.

En la tabla anterior, los 4 pares del cable son usados para llevar 4 señales bidireccionales de datos (BI_D). Las 4 señales bidireccionales de datos son llamadas BI_DA, BI_DB, BI_DC, BI_DD. Las señales de datos en cada par del segmento 1000BASE-T esta polarizado, con un alambre de cada par señalado que lleva el signo positivo (+), y el otro llevando el negativo (-). El signo se conecta para que ambos alambres se asocien con un signo dado siendo miembros de un solo par del cable.

Los transceiver típicos incluyen circuitos que pueden detectar señales con polaridad incorrecta en el alambre del par (polaridad de reversa). Estos circuitos pueden corregir la polaridad de reversa automáticamente moviendo las señales hacia un circuito correcto dentro del transceiver.

Sin embargo, no todos los dispositivos Ethernet pueden ser capaces de corregir la polaridad de inversión , y no es una buena idea depender de estas habilidades. Insertando, todos los cables deben ser alambrados para que la polaridad correcta se observe.

3.3.4.2 1000BASE-X

Las especificaciones para el sistema 1000BASE-X fueron diseñadas en el suplemento 802.3z del estándar de la IEEE. 1000BASE-X es un identificador colectivo para 3 medios de segmentos: dos segmentos para fibra óptica y un puente de cobre. De estas tres, los segmentos de fibra óptica son extensamente utilizados, mientras que el puente de cobre corto no ha sido adoptado por el mercado. Los dos segmentos de fibra óptica consisten de

un segmento de 1000BASE-SX (corta longitud de onda) y un segmento de 1000BASE-LX (Larga longitud de onda). El tercer tipo de segmento es el llamado 1000BASE-CX corto puente de cobre.

El medio 1000BASE-X es basado en especificaciones primeramente publicadas en el estándar de canal de fibra ANSI X3T11. El canal de fibra es una tecnología de red de alta velocidad que fue diseñada para soportar aplicaciones a granel de datos como servidores de archivos y proporcionando al transporte una alta velocidad de la imagen para editar video. El estándar 1000BASE-X adopta la codificación de la señal y señalización del medio físico del estándar canal de fibra "Fiber Channel", con el único cambio en el aumento de la razón de datos a partir de 800 Mbps a 1000Mbps.

A. Componentes de señalización 1000BASE-X

Como con el sistema 1000BASE-T, el sistema de Ethernet del gigabit 1000BASE-X requiere un interfaz de Ethernet con transceiver incorporado de Giga-Ethernet. La interfaz 1000base-X se equipa de un transceiver incorporado, para realizar una conexión directa a uno de los segmentos del medio 1000BASE-X, *figura 3.26*

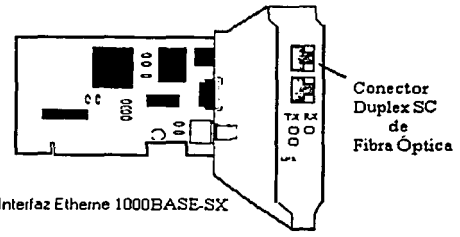


Figura 3.26 Interfaz Ethernet 1000BASE-SX.

Las NIC's disponibles de 1000BASE-X se diseñan lo más extensamente posible para la conexión a un segmento 1000BASE-SX, y solamente utilizan el modo full-duplex.

El sistema 1000BASE-SX usa un diseño de láser de corta distancia que es menos costoso para una conexión de longitudes relativamente cortas a segmentos de fibra óptica multi-modo. Por consiguiente, el sistema 1000BASE-SX se usa a menudo dentro de los edificios, y para las conexiones a los servidores de alto desempeño (estaciones de trabajo).

Una interfaz 1000BASE-X en un puerto del hub o switch puede soportar segmentos 1000BASE-SX o 1000BASE-LX, dependiendo del diseño hub para cada segmento. El alto funcioamiento del backbone en el switch o hub soporta a ambos tipos de medios 1000BASE-SX y 1000BASE-LX, siendo el resultado una máxima flexibilidad. Generalmente en un edificio se equipa con 1000BASE-SX. El 1000BASE-CX fue incluido en el estándar para conexiones tales el cuarto de cableado. Sin embargo no es asi ya que no existe equipo 1000BASE-CX disponible hoy día.

2) Componentes 1000BASE-X

Los segmentos de fibra óptica para Gigabit ethernet utiliza pulsos de láser en lugar de las corrientes eléctricas para enviar las señales ethernet. Tal situación tiene grandes ventajas. La primera, una conexión al segmento de fibra óptica puede llevar señales Gigabit ethernet a grandes distancias que el par trenzado. La especificación del estándar en un segmento 1000BASE-LX en modo full-duplex puede alcanzar hasta los 5000 metros .

Sin embargo, muchos vendedores ofrecen "longer haul" versiones de equipo 1000BASE-LX diseñado para distancias de 10 km. En fibra simple modo.

B. Componentes 100BASE-SX y 1000BASE-LX

El siguiente conjunto de componentes son usados en segmentos de fibra 1000BASE-SX como en 1000BASE-LX

- Cable de fibra multi-modo o simple-modo.
- Conectores de fibra óptica.

1) Cable de fibra óptica

Ambos segmentos de fibra 1000BASE-SX y 1000BASE-LX requiere de dos cuerdas de fibra óptica ; una para transmitir y otra para recibir datos. Se requiere el traspaso de la señal, la transmisión (TX) en uno de los extremos se conecta al (RX) del otro extremo.

2) Conectores de Fibra Óptica

El estándar recomienda que se utilicen un conector duplex SC de fibra óptica para ambos segmentos 1000BASE-SX y 1000BASE-LX *figura 3.27.*

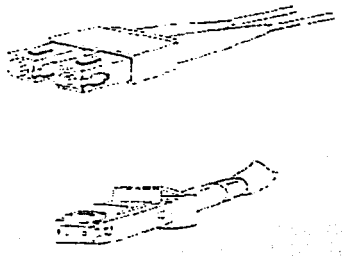


Figura 3.27 Conectores de fibra óptica (tipo SC y LC).

3) Convertidor de interfaz Gigabit

Algunos vendedores utilizan el convertidor de interfaz del gigabit (GBIC), que permite que el cliente utilice los tipos de media 1000BASE-SX o 1000BASE-LX en un solo acceso.

C. Componentes 1000BASE-CX

Un segmento 1000BASE-CX consiste de un cable corto "jumper" basado en un cable blindado de par trenzado de alta calidad. El cable puede tener una longitud de 25 metros de largo. El jumper es pensado para conectar equipos en pequeñas áreas , tales como los closets de los switch y la sala de computadoras . Este estándar no ha sido adoptado en el mercado.

El tipo de segmento 1000BASE-CX es basado en un cable blindado balanceando, los pares del cable tienen características de impedancia de 150Ω. Un cable jumper CX requiere una red pasiva de componentes (capacitores, resistencias, inductores) para un mejoramiento de la portador de la señal en el cable.

1) Conectores 1000BASE-CX

Hay dos conectores definidos en el estándar para usarse en los extremos de cable CX. El conector preferido es un conector serial de 8 pins de alta velocidad. (SHCD o Fiber Channel 2), *figura 3.28.*

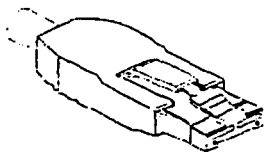


Figura 3.28 Conector HSSDC.

Proporcionando buenas características eléctricas y un tamaño menor al conector alternativo.

Las señales 1000BASE-CX en el conector SHCD 2 son conectados como sigue:

- Transmisión + en el 1 pin.
- Transmisión – en el 3 pin.
- Recepción - en el 6 pin.
- Recepción + en el 8 pin.

El conector alternativo es un conector blindado de 9 pins D-Subminiature. Este es un conector DB9 usado en token Ring con 150 Ω de impedancia en el cable.

Las señales 1000BASE-CX en el conector de 9 pins son conectadas como sigue:

- Transmisión + en el 1 pin.
- Transmisión – en el 6 pin.
- Recepción + en el 5 pin.
- Recepción - en el 9 pin.

1000BASE-SX ,1000BASE-LX

En la *tabla 3.10* se listan las distancias características para segmento 1000BASE-SX y 1000BASE-LX . Múltiples segmentos de 1000 Mbps pueden ser conectados en modo half-duplex con un repetidor, proveyendo una red con un máximo diámetro del cable de 200 metros entre estaciones.

1000 Base-SX	2 m	220 m	MMF	Full-duplex	2
1000 Base-LX	2 m	550 m	MMF	Full-duplex	2
1000 Base-LX	2 m	5,000 m	SMF	Full-duplex	2

Tabla 3.10 Distancias caracteristicas de 1000Base-SX y LX.

3.3.6 Otros estándares IEEE

802.1Q.- Especificaciones de VLAN's

Si sé esta confundido a cerca de que tipo de VLAN's implementar en la red, habría que revisar el estándar 802.1Q; en este estándar, una etiqueta (tag) especial es agregada en el paquete Ethernet. El frame de etiquetado (tagged) tiene un campo llamado VLAN ID (identificador) que indica al frame a cual VLAN pertenece. La *figura 3.29* muestra la VLAN ID.

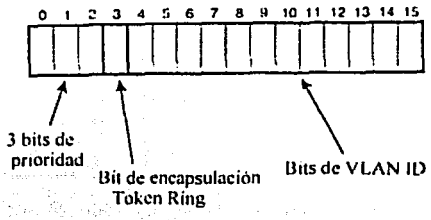


Figura 3.29 Localización y contenido de VLAN ID.

Los primeros 3 bits del VLAN ID son los bits prioritarios. Estos bits permiten a cada frame tener un paquete entre las colas 1 y 8, dependiendo de la importancia que tenga el frame. El siguiente bit es el de encapsulación Token Ring, este indica si el frame de encapsulación Token Ring tiene actualmente un formato de frame Ethernet.

Los siguientes 12 bits representan el VLAN ID, el cual asigna al frame una VLAN, en particular en la red. Todos los switches en la red conocen la VLAN ID ya que los switches son los responsables de la comunicación entre miembros de la VLAN.

¿Quién identifica que VLAN ID pertenece a cada frame?. En teoría, cada estación final identifica la VLAN ID cuando el frame es inicialmente creado. Si cada frame pertenece a un switch sin VLAN ID, el switch puede optar por insertar el VLAN ID y enviar el frame.

Aunque las VLAN's prometen muchas cosas, se puede mantener el rendimiento y necesidades de segmentación en la red con el simple desarrollo de los switches capa 3. Los switches capa 3 despliegan la influencia existente de ruteadores usando los protocolos estándar de ruteo. El despliegue de VLAN's mantiene un nuevo conjunto de herramientas administrativas y esquemas propietarios de comunicación inter-switch. Con esta intención, se podría usar las VLAN's solo en los grupos donde se puede justificar las necesidades. La *tabla 3.11* muestra algunos ejemplos comunes de los usos lógicos de las VLAN's.

Basada en puerto	Baja
Basada en MAC	Alta
Basada en dirección de capa 3	Media
Basada en Protocolo	Baja
Basada en IP Multicast	Alta
Tagged (etiquetado)	Alta

Tabla 3.11.- Usos prácticos de las VLAN's.

802.1 D.- Algoritmo Spanning Tree (Árbol de expansión)

Últimamente, el broadcast sencillo puede perderse dentro de una tormenta de broadcast, lo cual podría saturar por completo la red y tirar la misma. El algoritmo spanning tree (STA – Spanning Tree Algorithm) fue inventado por Radia Perlam of Digital Equipment Corporation para tratar este problema. Los siguientes son puntos importantes acerca del algoritmo Spanning tree:

- Los puentes construyen una estructura lógica de conexión en árbol para intercambiar información acerca de la topología completa de la red. Todos los puentes mandan hacia fuera frames específicos, llamados Protocolo de Densidad de Datos del Puente (BPDU – Bridge Protocol Data Units), para construir el árbol.

- El STA siempre esta activo. Durante el tiempo de encendido, los puentes individuales se comunican vía BPDU's para construir el árbol inicial, lo que toma entre 15 y 50 segundos. La base del árbol, o la raíz, es determinado en un camino

semejante como proveer solo un posible camino de datos entre algunos de los 2 diferentes puentes dentro de el puenteo de fábrica. En este tiempo, el STA también elimina los caminos redundantes (loops) temporalmente desconectando todas las conexiones paralelas. Estas conexiones paralelas son en efecto inactivas, la reactivación se hace necesaria más tarde. Para eliminar conexiones paralelas, el STA, tiene en efecto, la construcción de una estructura que parece un árbol, con la raíz o el puente maestro localizado en la base.

- El STA permite redundancia o soporte para conexiones paralelas. La naturaleza dinámica de STA significa que si una conexión existente entre 2 puentes se rompe, el STA podría reactivar una conexión inactiva en menos de un minuto. Esto provee redes puenteadas con un elemento con capacidad de recuperación.

- El STA se convirtió en un estándar IEEE en 1990 y es conocido como 802.1D. El STA es usado para ser una característica opcional con puenteo prematuro. En estos días, todos los puentes y switches incorporan esta característica. El STA puede ser eliminado con más puentes.

- A diferencia de los puentes, los ruteadores permiten activar múltiples caminos. De hecho, los ruteadores tienen suficiente inteligencia para tomar ventaja de múltiples caminos, tanto para la redundancia como para el costo de optimización. Los ruteadores usan algoritmos similares al STA para determinar el óptimo camino entre 2 estaciones conectadas en una WAN.

La *figura 3.30* muestra una topología de puente con múltiples caminos.

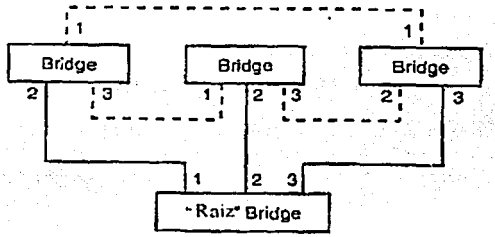


Figura 3.30 Una red con caminos paralelos puenteados muestra como STA crea la configuración de árbol. Las líneas punteadas indican las conexiones paralelas deshabilitadas por el STA.

El puenteo es importante ya que este introduce el concepto de spanning tree. Esto consiste básicamente en 2 ideas: la prevención de loops y configuración de conexiones redundantes. La prevención de loops es necesaria porque una serie de puentes o switches puede colocar sobre cada camino un paquete que debería ser transmitido de un switch a otro, con el último switch mandando el paquete de regreso al primero y así sucesivamente repitiendo el ciclo. Spanning tree identifica esta situación y previene que las conexiones se caigan.

802.3x.- Full Duplex / Estándares de Control de flujo

El estándar usa el método de control full-duplex con 2 mejoras. La primera, el estándar podría permitir un senseo automático de capacidades full-duplex mediante la autonegociación. Segundo, el estándar incluye una nueva característica, llamada control de flujo, quien previene la congestión y sobrecarga. Mientras full-duplex y el control de flujo son tecnologías separadas, se podría entender lo racional para esta unión debido a que cada una de estas tecnologías es complementaria de la otra.

802.1p.- Prioridad de switcheo

Uno de los pilares de ATM es la capacidad de priorizar tráfico dentro de diferentes clases. Ethernet, ha sido criticado por esa falta de capacidad de diferenciar datos con tiempos críticos para tráfico de baja importancia. Esto porque Ethernet tiene en sí mismo la tecnología de transmisión al mejor esfuerzo, lo cual no da servicios garantizados. En los últimos años, muchas tecnologías como 100 VG AnyLAN y 802.3x han tenido que garantizar las mejoras sobre el método de acceso al medio CSMA/CD para mejorar la transmisión digital de voz y video, pero no ha satisfecho la transmisión de datos. Con el surgimiento de Fast y Gigabit Ethernet, las crecientes capacidades del BW de Ethernet tiene amplias ventajas. Algunas personas argumentan que full-duplex switcheado a 10, 100 y 1000 Mbps Ethernet proveen algunos tipos de QoS. Esto no es verdad. En efecto, full-duplex y el switcheo incrementan las capacidades del BW en Ethernet. Por lo tanto, Ethernet aún no tiene QoS garantizado y no ofrece capacidades de priorizar tráfico.

El nuevo IEEE 802.1Q contiene campos que permiten priorizar tráfico Ethernet. El tercer bit del campo permite tener 2^3=8 diferentes niveles de prioridad (colas de priorización) para la información crítica.

802.3ad.- Conexiones agregadas (Link Aggregation)

El algoritmo de spanning tree 802.1D permite conexiones paralelas redundantes entre 2 switches. STA podría deshabilitar las conexiones paralelas, solo reactivándolas para propósitos de soporte. Si las conexiones activas están dadas de baja, STA podría habilitar una conexión de soporte después de algunos segundos. La *figura 3.31* muestra esto.

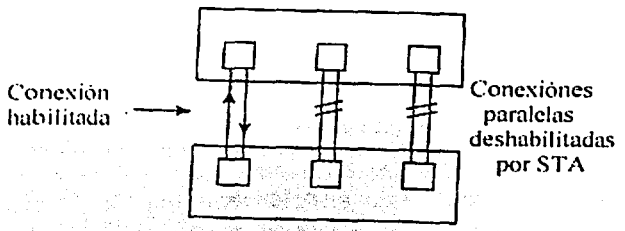


Figura 3.31.- El algoritmo spanning tree deshabilita temporalmente las conexiones paralelas puenteadas.

El algoritmo spanning tree 802.1D desafortunadamente no permite agregar conexiones (link aggregation) porque este fue diseñado para puertos individuales hace más de una década. A pesar de estos beneficios, la tecnología EtherChannel es propietaria. Los otros vendedores tienen esquemas semejantes, pero el problema es que no pueden agregar ambas tecnología (spanning tree y link aggregation) en el mismo switch. El grupo de trabajo 802.3ad esta constantemente trabajando en el estándar, lo que podría llevar a convertir a la tecnología EtherChannel en un estándar. Las conexiones switch a switch, switch a servidor, switch a cliente y switch a ruteador podrían entonces ser posibles. El trunking ocurre en la capa 2 del modelo OSI.

3.3.7 FDDI.- Interfaz de datos distribuida por fibra

FDDI (Fiber Distribuied Data Interface) es una norma de cable de fibra óptica desarrollado por el comité X3T9.5 del Instituto Americano de Normalización (ANSI, American National Standards Institute). Trabaja a 100 Mbps y utiliza una topología de anillo doble que admite 500 nodos sobre una distancia máxima de 100Kilometros. Es posible establecer las conexiones mediante cable de cobre, pero en este caso las distancias se reducen considerablemente.

Los anillos dobles ofrecen redundancia (tolerancia a fallos). Si se produce el fallo de un enlace o se corta el cable, el anillo se re-configura por si solo, como se muestra en la *figura 3.32* de modo que se puede continuar con la transmisión de tráfico en la red.

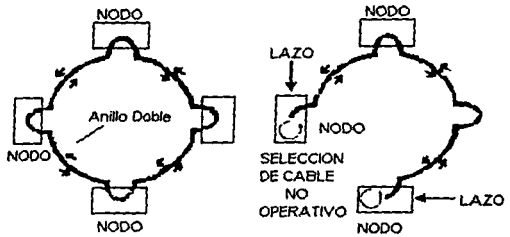


Figura 3.32 Anillos dobles.

FDDI constituye un excelente medio de construcción de redes soporte *figura 3.33.* Los segmentos de las redes locales se conectan a la red soporte, al igual que las computadoras centrales y otros sistemas. Las redes pequeñas que constan de un número escaso de segmentos de LAN probablemente tendrán más beneficios mediante una red soporte ethernet. Las redes más extensas, que poseen numerosos segmentos LAN, generadoras de grandes cantidades de tráfico debido a las estaciones de trabajo de altas prestaciones o a la transferencia de archivos gráficos o a otro tipo de tráfico se beneficiaran más con FDDI.

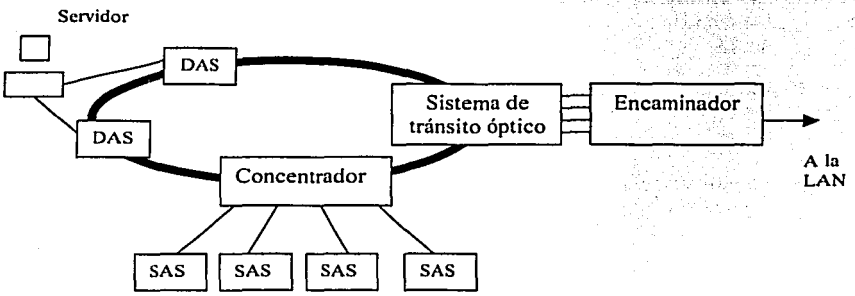


Figura 3.33 Configuración de una red para soporte FDDI.

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 transmisión y otro de seguridad. Algunas estaciones, las denominadas estaciones de acoplamiento doble (DAS, Dual Attached Stations) se conectan a los dos anillos. Las estaciones de acoplamiento único (SAS, Single Attached Stations) se conectan a través de un concentrador que proporciona las conexiones oportunas a muchas SAS. Una ventaja de esta configuración es que una SAS que falle no puede romper el anillo. Además la mayoría de las SAS son estaciones de trabajo de usuario que se apagan a menudo, lo que podría interrumpir el anillo si su conexión se realizara de forma directa.

El sistema óptico proporciona la circuitería que mantiene al anillo intacto si se produce un fallo en un ruteador. Puede utilizarse una conexión redundante para dispositivos de cierta importancia, como los servidores que necesiten mantener una conexión continua. Si una de las estaciones falla, se establece la otra mediante dos conexiones DAS de un servidor, *figura 3.33.*

Algo que se debe mantener en una red compartida como FDDI es que el ancho de banda puede llegar a saturarse. Se debe evaluarse los requisitos de trafico de la red soporte. Un switch de alta velocidad podría proporcionar una mejor solución.

A. Método de acceso a FDDI

FDDI utiliza un método de acceso de paso de testigo. Se pasa una trama testigo de estación a estación a través de la red; si una estación necesita transmitir, captura la trama. La estación transmite los datos y sitúa el testigo de vuelta en el anillo al finalizar. Se utiliza un mecanismo de regulación para evitar que una estaciones mantenga el testigo durante demasiado tiempo. Para acomodarse a aquellas estaciones que generan un alto volumen de tráfico, el administrador de la red puede dar prioridad a dichas estaciones, generalmente concediéndole un periodo mayor de tiempo de transmisión a antes de liberar el testigo. Teniéndose en cuenta las siguientes características:

- Las estaciones directamente conectadas a FDDI trabajan como repetidores. Reciben los paquetes de un vecino y los envía al otro, siguiendo el sentido correcto. Cuando un nodo detecta su dirección en un paquete, lo copia en su memoria.

- Pueden existir multiples tramas en la red. Si una estación renuncia al testigo mientras sus tramas todavía se encuentra en transito, las otras estaciones pueden comenzar a transmitir.

- Se utiliza 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 tráfico en ruta.

- La norma FDDI especifica los niveles físicos y MAC de un bucle basado en el concepto de testigo sobre fibra óptica, consiste a nivel MAC en un protocolo de acceso que permite que fuentes síncronas y asíncronas compartan el soporte.

B. La norma FDDI se descompone en:

- Un nivel físico, PL (Physical Layer), dividido en dos subniveles: el PMD (Physical Medium Dependent) y el PHY (PHYsical Layer Protocol);

- Un nivel de enlace de datos, DLL (Data Link Layer), dividido en dos subniveles: el MAC (Medium Access Control) y el LLC (Logical Link Control);

- Un estándar de gestión de estación, SMT (Station Management), que suministra el control necesario, a nivel de la estación, para gestionar los procesos situados en los diversos niveles de FDDI.

1) Nivel Físico

El nivel físico PL (Physical Layer) está constituido por dos subniveles:

La subnivel PMD (Physical Medium Dependent), que ofrece todos los servicios necesarios para las comunicaciones digitales punto a punto entre las estaciones de una red FDDI, es decir, para la transmisión de oleadas de bits codificadas de una estación a otra. El PMD define y caracteriza los emisores y receptores ópticos, los inconvenientes de código impuestos por el soporte, los cables, los conectores, el balance energético, los repetidores ópticos y otras características físicas. El subnivel PMD es objeto de una norma: la ISO 9314.3. En esta norma están definidos:

El soporte, para el cual hay dos posibilidades: la fibra óptica multimodo de 62.5/125 µm m de diámetro y el balance óptico de 11 dB, o bien la fibra óptica monomodo. La utilización de la fibra óptica monomodo. La utilización de la fibra óptica monomodo permite establecer enlaces de una treintena de kilómetros entre las estaciones, enlaces limitados a 2 kilómetros con las fibras multimodo.

- La longitud de onda: 1,300 nm.
- El emisor: LED.
- El conector: doble conector ST.

El subnivel PHY (PHYsical Layer Protocol), que es objeto de la norma ISO 9313.1. Permite la conexión entre el PMD y el DDL. El nivel PHY es responsable de la sincronización y de la codificación y descodificación. Se utilizan dos niveles de codificación: el PHY convierte los símbolos procedentes del MAC en bits codificados en NRZ, el código utilizado es un código de grupo de tipo 4B/5B, un grupo de 4 bits de datos está codificado en un grupo de 5 bits codificados en NRZ, que a su vez están codificados en una secuencia de 5 bits codificados en NRZI.

2) El subnivel MAC (ISO 9314.2)

Este subnivel está destinado a ser utilizado sobre una red de altas prestaciones. Este protocolo está pensado para ser operativo a 100 Mbits/s sobre un bucle en anillo basado en testigo y un soporte de fibra óptica, pudiendo cubrir distancias de varias decenas de kilómetros. El acceso al soporte está controlado por un testigo; una estación que haya capturado el testigo lo retransmite inmediatamente por el soporte una vez que haya terminado su transmisión. Se han diferenciado dos clases de servicios sobre una red FDDI.

- Servicio síncrono.
- Servicio asíncrono.

La clase de servicio síncrono responde a aplicaciones que necesitan una banda de paso de alta capacidad y/o un tiempo de propagación en el encaminamiento determinado, con problemas si varían estos tiempos.

La clase de servicio asíncrono satisface los inconvenientes de tráfico de tipo asíncrono, presentando cierta cantidad de banda de paso compartida por todas las estaciones que utilicen este método.

Con el fin de ofrecer un servicio satisfactorio al tráfico síncrono, el tiempo de rotación del testigo está controlado. Es decir, que el tiempo total utilizado por el testigo para recorrer toda la red debe resultar inferior a un umbral determinado por las aplicaciones que utilicen la red. Un valor determina el tiempo de rotación del testigo: el TTRT (Target Token Rotation Time), que se establece durante la inicialización de la red. El valor TTRT se carga en un temporizador, llamado TRT (Token Rotation Timer) que controla la adquisición del testigo para la transmisión de las tramas en espera. El testigo puede ser capturado para transmitir una trama síncrona independientemente del valor del TRT, mientras que sólo será código para transmitir una trama asíncrona si el tiempo del TRT no ha expirado. Opcionalmente, pueden distinguirse varios niveles de prioridad dentro del tráfico asíncrono de una estación, lo que permite controlar la banda de paso ofrecida a estas diferentes fuentes asíncronas. Cuanto más elevada sea la prioridad de una estación, mayor es la banda de paso disponible para las fuentes asíncronas de esa prioridad.

Tipos de FDDI

Las nuevas aplicaciones de multimedia y vídeo en tiempo real representan 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. 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 distintas maneras, se mencionan a continuación:

FDDI dispone de tres modos de transmisión. Los dos pioneros, asíncrono y síncrono, ya aparecen en la norma FDDI original. El tercero, basado en circuitos, puede proporcionar circuitos dedicados. Este modo se encuentra disponible en la nueva norma FDDI-II, que requiere nuevas tarjetas de adaptación.

a) Servicios Asíncronos.

El modo de anillo asíncrono se base 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 trafico, lo que perjudica al tráfico 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 videoconferencia interactiva, en la cual las personas establecen conversaciones, aunque sí es aceptable si se trata de una simple visualización de una secuencia almacenada de vídeo.

b) 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 ofrecen capacidad síncrona conceden a los gestores de la red la posibilidad de reservar parte del ancho de banda para tráfico sensible al tiempo. Las estaciones de trabajo asíncronas luchan por el resto. Las capacidades síncronas deben añadirse a través de actualizaciones de software en la mayoría de las tarjetas FDDI existentes. El comité de ANSI trabaja actualmente en una nueva norma, de modo que esta utilidad estará disponible como opción estándar en la mayoría de las nuevas tarjetas.

c) Servicios Basados en Circuitos.

El modo basado en circuito (unicamente 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 isocrona.

3) El subnivel SMT

Este subnivel todavía no está normalizado. Proporciona servicios tales como el control de inicialización del sistema, la gestión de la configuración, la desconexión del nuevo elemento asociado, así como los procedimientos de planificación.

C. Cable de fibra

Existe cable de fibra monomodo y multimodo. El primero propaga la transmisión de una única frecuencia de luz, mientras que el segundo propaga varias frecuencias. Hay que tener en cuenta que la versión de FDDI con cable par trenzado de cobre se han normalizado.

El grupo normalizador de FDDI ha elegido el cable multimodo de fibra óptica como soporte físico, con una longitud de onda normalizada de 1.300 nm. El estándar especifica el uso de la fibra multimodo 62.5/125 μ de índice gradual. Sin embargo, pueden emplearse otros tipos de fibra (p.ej:50/125, 85/125, 100/140 μ).

El cable multimodo puede utilizarse si la especificación FDDI lo consiente. Estas especificaciones se encuentran disponibles a través de cualquier fabricante de FDDI. Algunos prefieren cables de un gran ancho de banda, anticipándose a los requisitos futuros.

El cable de fibra óptica multimodo se recomienda debido a que es más adaptable a los productos futuros.
Para todos estos tipos de fibra se especifica un ancho de banda de al menos 500 MHz x km y una atenuación no mayor de 2.5 dB/km. Recientemente se han empezado trabajos sobre una variante FDDI que utiliza fibra monomodo (PMD-SMF), a 100 Mbit/s, para enlaces a distancias mayores a 2 km, y especifica el empleo de diodos láser para transmisión, obteniéndose enlaces de 60 a 100 km. La especificación aún está incompleta, pero se vienen empleando conversores multimodo/monomodo (no contemplados en el estándar) para instalaciones donde ya existe fibra monomodo.

La fibra óptica ofrece las ventajas de una anchura de banda prácticamente ilimitada, inmunidad al ruido, un alto nivel de seguridad y opera a una velocidad diez veces mayor que una red de área local convencional.

1) Distancia entre nodos

Para minimizar costos (dispositivos ópticos y cable), la norma FDDI especifica la utilización de transmisores tipo LED y fibra multimodo. Con esta tecnología "barata", por el empleo de dispositivos económicos en emisión y recepción, la distancia máxima de los enlaces es de 2 km. (limitada por la dispersión modal y cromática).

Extensión

Con estas elecciones técnicas, se pueden configurar redes de hasta 50 km. de diámetro, en donde la distancia máxima entre nodos de conexión es de 2 km. Pueden conectarse a la red hasta 500 nodos; puesto que estos nodos pueden ser puentes de acceso hacia redes *Ethernet* y *Token Ring*, el número de ordenadores usuarios de una red FDDI puede alcanzar varios miles de unidades *figura 3.34.*

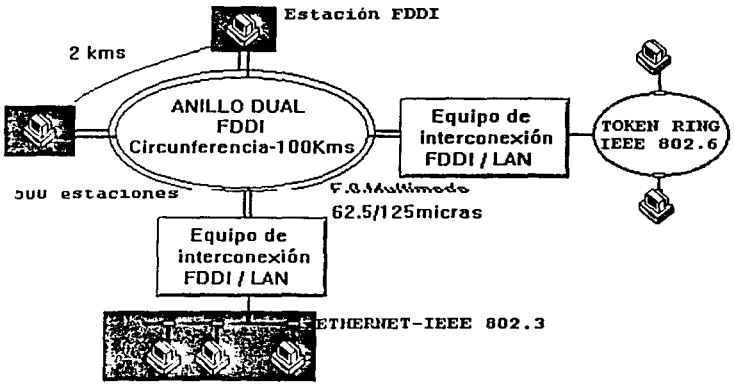


Figura 3.34 Distancia entre los nodos FDDI.

2) Seguridad y Privacidad

La utilización de fibra óptica en una red FDDI permite alcanzar grados de seguridad óptimos y detectar cualquier tipo de intrusión en el medio de transmisión.

Aunque la privacia de los datos no es una característica funcional que se requiera en un entorno de red privada, siempre es posible utilizar técnicas de cifrado de datos que permiten obtener un mayor grado de privacidad.

D. Arquitectura de red

A continuación se incluye una clasificación de las distintas configuraciones al nivel funcional que soportan las redes de área metropolitana:

- Redes Terminales (*back-end):* Permiten la transferencia rápida de información entre la Unidad Central de Proceso (CPU) y dispositivos de almacenamiento masivo (discos ópticos, unidades de cintas) y periféricos de alta velocidad (impresoras, trazadores).

- Redes Dorsales (*backbone):* Conectan redes de área local de velocidades menores. La velocidad de transmisión de la red de área metropolitana permite manejar una carga agregada de múltiples redes conectadas sin establecer cuellos de botella ni degradar sus respectivas prestaciones. Las redes de área local compatibles IEEE 802.X (*Ethernet* 802.3, *Token Bus* 802.4 y *Token Ring* 802.5) se interconectan mediante puentes o encaminadores con salida al nodo de red MAN. La red dorsal permite establecer enlaces con las redes pública de área extensa (X.25 *frame relay*) o con redes privadas del tipo SNA mediante pasarelas específicas.

- Redes Frontales (*front-end):* Conectan grandes ordenadores, minis y ordenadores personales, estaciones de trabajo, terminales gráficos de alta resolución CAD/ CAM, impresoras láser, etc. Esta configuración se asemeja al entorno de red local, pero con unas prestaciones muy superiores comparada con *Ethernet* o *Token Ring. figura 3.35.*

Servicios ofrecidos

La tecnología FDDI permite utilizar servicios no orientados a conexión, puesto que el método de acceso por paso de testigo temporizado posibilita el envío de datos a la red sin la necesidad de reservar previamente el medio para efectuar la transmisión. Dentro de los servicios prestados se encuentran aplicaciones para tráfico síncrono y asíncrono.

Para el tráfico síncrono, los datos son enviados en modo paquete, indicándose las direcciones de los nodos origen y destino. El retardo máximo de los paquetes es función de los parámetros de temporización del testigo y por tanto se puede cuantificar.

El servicio para aplicaciones que requieren tráfico asíncrono permite el uso de diferentes niveles de prioridad a nivel de paquetes de datos.

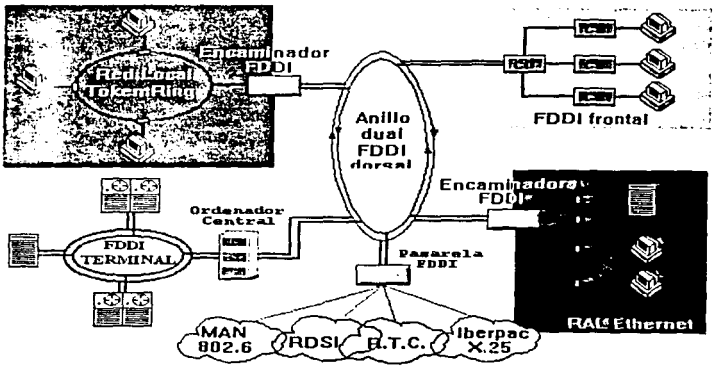


Figura 3.35 Redes frontales.

El desarrollo de circuitos integrados VSLI que incorporan los diferentes niveles de la norma FDDI, han permitido la rápida introducción de este estándar en el campo de la comunicaciones entre redes de área local. Hoy en día se encuentran productos comerciales (puentes, ruteadores y pasarelas) que permiten dicha interconexión. Así mismo, numerosos fabricantes de ordenadores, están comercializando sus productos con interfaz de conexión hacia redes FDDI.

A pesar de que la tecnología FDDI representa un gran avance en las comunicaciones de área local, algunas de las aplicaciones que se piensa podrá soportar la ISDN (Red Digital de Servicios Integrados) de banda ancha no son susceptibles de circular por redes FDDI. Por ejemplo, la TV de alta definición requerirá un ancho de banda de 150 Mbit/s por canal, lo cual supera el máximo permitido en FDDI.

E. FDDI-II

En 1985 surgió la necesidad de una red local capaz de soportar simultáneamente voz y datos. El protocolo FDDI-I se reveló inadecuadamente para este tipo de aplicación, principalmente en redes con gran número de nodos. Así, pues, se propuso una nueva versión del bucle FDDI, principalmente a iniciativa de especialistas en telecomunicaciones, como la British Telecom y AT&T, también basada sobre bucles de fibra óptica. A fin de ofrecer una calidad de servicio adecuada para la voz, el protocolo FDDI-II utiliza una técnica de conmutación híbrida. De esta forma, la norma FDDI-II ofrece procedimientos de conmutación de circuitos para tráficos de voz y vídeo y, de conmutación de paquetes, para los datos.

FDDI-II es una propuesta de norma americana de la ANSI (Comité X3T9.5) para una red local de 100 Mbits/s de capacidad con una longitud de más de 50 km. Se trata de un doble bucle, con control de acceso por testigo. FDDI-II es una extensión de la norma FDDI-I, que añade una trama síncrona. La banda de paso está constituida por la trama asíncrona y 16 canales síncronos que contienen 96 "cyclic groups" de 16 bytes cada uno. El flujo síncrono alcanza, por consiguiente, 16x96x8/125 ?s=98.304 Mbits.

La norma FDDI ha sido ideada hace más de diez años para ser utilizada exclusivamente con fibra óptica; sin embargo, sus principios pueden aplicarse a pares trenzados.

La utilización de la FDDI sobre pares trenzados: TPDDI (Twisted PAir Distributed Data Interface), llamada incluso CDDI (Copper Distributed Data Interface), permite reducir considerablemente el coste de las conexiones. Las distancias son claramente más cortas: de una treintena a un centenar de metros, dependiendo de la calidad de los pares metálicos.

F. TPDDI puede descomponerse en dos subclases:

TPDDI sobre STP (Shielded Twisted Pair), para la utilización de FDDI sobre pares trenzados blindados. Algunas sociedades, como Cabletron, Chipcom y Synoptics especialmente, ya se han inclinado hacia la realización de tarjetas de este tipo. Estas tarjetas permiten la comunicación a 100 Mbits/s sobre un cable de par trenzado blindado.

TPDDI sobre UTP (Unshielded Twisted Pair), para la utilización de FDDI sobre pares trenzados sin blindar. Se han hecho algunos pronunciamientos referentes a la realización de una red FDDI sobre este tipo de pares. AT&T, Apple Computer, Cabletron, Fibronics y Ungermann-Bass -que incluso se han asociado en un grupo llamado UTPF (Unshielded Twisted Pair Foundation)-, con el fin de potenciar los productos FDDI sobre UTP.

De esta forma, cabría esperar al menos dos normas ANSI relativas a la FDDI sobre pares trenzados: la primera para la utilización del par trenzado blindado (tipo 1 y 2 de IBM); la segunda para el par trenzado sin blindar, previsto para distancias inferiores a 100m.

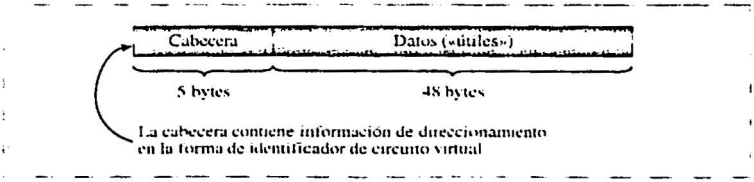
3.3.8 ATM

ATM es un protocolo punto a punto, full-dúplex, orientado a conexión y basado en conmutación de células que dedica ancho de banda a cada estación. Utiliza multiplexación por división en el tiempo asíncrona (TDM) para controlar el flujo de información en la red. ATM opera en un ancho de banda que varía desde 25 Mbps hasta 522 Mbps, aunque la mayoría del esfuerzo de desarrollo se orienta hacia ATM a 155 Mps.

Entre los beneficios ofrecido por ATM se hallan:

- Excelente escalabilidad .
- Integración con las redes existentes.
- Ancho de banda bajo demanda.
- Posibilidad de gestionar la totalidad del rango de tráfico de la red (voz, datos, imagen, video, gráficos y multimedia).
- Adaptabilidad tanto a los entornos LAN como a los WAN.

La conmutación de paquetes, que utiliza el ancho de banda solo cuando hay tráfico de datos, se desarrollo para gestionar el tráfico a ráfagas de datos. Sin embargo, los sistemas de conmutación de paquetes no se comportan de manera adecuada en caso de tráfico bidireccional en tiempo real, como el video interactivo. ATM supera esta limitación gracias a la utilización de células, que son paquetes de longitud fija, en vez de emplear paquetes de longitud variable. Cada célula ATM está compuesta por un campo de datos de 48 bytes y una cabecera de 5 bytes como se muestra en la *figura 3.36.*



Estructura de la célula ATM.

Figura 3.36 Estructura de la célula ATM

Las células ATM de longitud fija ofrecen muchas ventajas con respecto de los paquetes de longitud variable:

- Posibilidad de conmutación mediante hardware. Puesto que el procesamiento de las células de tamaño fijo es sencillo, predecible y fiable, es posible realizar la conmutación ATM a nivel de hardware en vez de requerir de un costoso y complejo software para gestionar el control de flujo, buffer y otros aspectos de administración.

- Nivel de servicio garantizado. Los retardos de espera en las colas sufridas en la red y en los conmutadores son más predecibles en el caso de células de datos de tamaño fijo. Por lo tanto, es posible diseñar los conmutadores para que proporcionen los niveles de servicio garantizados para todo tipo de tráfico, incluso para servicios sensibles al retardo, como voz y video.

- Procesamiento paralelo. Las células de longitud fija permiten a los conmutadores encargados de retransmitir las células procesarlas en paralelo, alcanzando velocidades que exceden las limitaciones de las arquitecturas de conmutación basadas en bus.

- Posibilidad de procesar voz. Aunque las células ATM sólo requieran ancho de banda cuando existe tráfico, aún así pueden proporcionar el equivalente a una ranura de tiempo, como la generada por un mutiplexor o división en el tiempo, para tráfico continuo. De esta manera, ATM es capaz de gestionar igualmente bien tráfico continuo en tiempo real como la voz digitalizada y tráfico a ráfagas como las transmisiones LAN.

La célula ATM se emplea para transportar los datos que se transmiten entre los conmutadores. Un segmento de 48 bytes, correspondiente a los datos útiles del usuario, se sitúa en una célula junto a una cabecera de 5 bytes, formando una célula ATM de 53 bytes. La cabecera de la célula transporta la información necesaria para la operación de conmutación.

Conmutación ATM

ATM no emplea ancho de banda compartido, en su lugar, cada uno de los puertos de un conmutador ATM se dedica a un único usuario. Un conmutador ATM estable una conexión virtual entre un nodo transmisor y un nodo receptor. Esta conexión se realiza en función de la dirección destino de cada célula, y solo dura en lo que tarda en transferir una célula. Esta transferencia de datos pueden tener lugar en paralelo de la velocidad que tiene la red. Puesto que la célula se transmite únicamente al puerto asociado con una dirección de destino específica, ningún otro puerto recibe la célula, lo cual proporciona un tráfico reducido y, como valor añadido alta seguridad. Para comunicarse a través de la red, las aplicaciones deben inicialmente, establecer una conexión virtual (VC Virtual Connection) entre los conmutadores. Un VC es un camino de transmisión para una célula de datos ATM. El VC se extiende a través de uno o más conmutadores, estableciendo una conexión de extremo a extremo para la transmisión de los datos de la aplicación de las células ATM.

Los VC se pueden establecer de 2 maneras. La primera, el administrador de la red puede configurar manualmente un circuito virtual permanente (PVC Permanent virtual Circuit). Un PVC consiste en un ancho de banda dedicado que garantiza el nivel de servicio a una determinada estación. Los administradores de red podrán configurar un PVC para aplicaciones críticas que siempre deben considerarse de alta prioridad o para conexiones permanentes como las existentes entre ruteadores y switches. La segunda manera de establecer un VC es el circuito virtual conmutado (SVC Switched Virtual Circuit). Un SVC es un VC estableciéndose adecuadamente según las necesidades de la aplicación.

Todas las células ATM son del mismo tamaño, al contrario de los sistemas de retransmisión de tramas y las redes de área local que tienen paquetes de tamaños variables. La utilización de células del mismo tamaño permiten:

- Ancho de banda garantizado. Los paquetes de longitud variable pueden causar retardos en los conmutadores.
- Alto rendimiento. Grandes volúmenes de datos pueden fluir de manera concurrente a través de una única conexión física.
- Conmutación hardware. A corto plazo esto dará lugar a un mayor caudal de información y con el tiempo, la tecnología podrá continuar sacando partido de la mejora de la relación precio-prestaciones a medida que se incremente la potencia de los procesadores y se reduzca el costo.
- Prioridad de los datos. ATM puede enviar una respuesta determinística, aspecto escencial para transportar comunicaciones (sensibles a la latencia) como video animado y audio o tráfico interactivo de datos correspondiente a aplicaciones críticas.

Ancho de banda dedicado

Diferentes tipos de tráfico requieren diferente comportamiento respecto al retardo, variación de retardo y caracteristicas de pérdida. ATM proporciona calidades de servicio diferentes para acomodarse a esas diferencias. Igualmente asigna ancho de banda a cada una de las estaciones activas. La estación solicita el ancho de banda apropiado para cada conexión en la red, automáticamente, asigna este ancho de banda al usuario. En realidad, el ancho de banda no se dedica por si mismo. Se comparte con otros usuarios, pero la red asegura el nivel de servicio solicitado. La red puede hacer esto porque controla el número de conversaciones simultáneas en la red.

Para acceder a la red la estación solicita un circuito virtual entre los extremos transmisor y receptor. Durante el establecimiento de la señal, la estación receptora puede solicitar la calidad de servicio que necesita para adaptarse a los requerimientos de la transmisión, y los conmutadores ATM garantizarán la solicitud si existen suficientes recursos de red disponibles. El nivel de servicio garantizado del acceso por conmutación basado en células es particularmente útil para transportar comunicaciones interactivas en tiempo real como la voz y el video. ATM utiliza un protocolo denominado interfaz del usuario a la red (UNI

User to Network Interface) para establecer los niveles de ancho de banda dedicados a las estaciones y aplicaciones.

Interfaces de usuario de red (User-to-Network Interfaces, UNI)

El protocolo UNI de ATM proporciona múltiples clases de servicio y reservas de ancho de banda durante el establecimiento de la llamada de una conexión virtual conmutada. UNI define interoperabilidad entre el equipo del usuario y el puerto del conmutador ATM. Una interfaz SONET o DS3. Una UNI privada, por otra parte, define una interfaz ATM entre el usuario final y un conmutador ATM privado, que muy probablemente tenga una interfaz de cable de cobre o de fibra óptica.

Mientras que el ATM Forum ha conseguido con éxito estandarizar el protocolo UNI, existen un par de aspectos clave para los administradores de red que deberían considerar a la hora de elegir los productos. En los protocolos UNI seleccionados por el ATM Forum se debe coordinar el ancho de banda asignado localmente entre los conmutadores y segmentos de LAN interconectados. También debe soportar diversos sistema operativos de red para garantizar múltiples clases de servicio. Estos aspectos afectan a la interoperabilidad de la red ATM y, por tanto, los adminstradores de red deberían seleccionar los productos que permiten el diseño y los equipos actuales de la red.

Modo de operación

La combinación de células y de las conexiones punto a punto, con los consiguientes números de conexión reducidos, permiten a ATM dividir la tarea principal de interconexión de dos componentes separados; determinación de la ruta y reenvío de datos (más conocidos como encaminamiento y conmutación), cada uno de ellos tratado por una tecnología diferente.

Determinación de la ruta

La determinación de la ruta es una función que exige un procesamiento intensivo por parte de la computadora, usualmente basado en software, y que requiere un conocimiento dinámico de la topología global de la red. La determinación de la ruta en ATM se realiza mediante el establecimiento de conexiones virtuales y se produce sólo una vez por sesión de transferencia de datos. ATM elige un camino para las células de la conexión (encamina la conexión) durante el establecimiento de la conexión y todas las células de la conexión siguen el mismo camino.

El medio ATM

La independencia del medio es un principio impulsor de ATM. Se especifican muchos niveles físicos, comenzando por 25 Mbps, incluyendo algunos para 100 y 150 Mbps, y continuando hasta 622 Mps. ATM a 155 Mps incluirá soporte para redes de área local que utilicen UTP Categoría 3, 4 y 5, STP Tipo 1, cable de fibra óptica y fibra monomodo.

Interfaz física para la red de área extensa

La interfaz WAN de 155 Mps a los proveedores de redes públicas se basará en la red óptica síncrona (*Synchronous Optical Network*, SONET). SONET es un sistema de transporte de nivel físico internacionalmente admitido y desarrollado a principios de los años ochenta.

Instalación y Configuración

La administración de ATM es diferente a la de cualquier protocolo de LAN. Mientras que los procesos de instalación y configuración no son difíciles físicamente, si son complejos, requieren de un nivel detallado de conocimiento sobre ATM, así como de una elaborada planificación. Por tanto, hay que estar preparado para gastar dinero y tiempo en formación, planificación y consultoría antes de llevar a cabo una implementación de ATM.

Escalabilidad

ATM puede incrementar la escalabilidad de las redes con protocolos heredados. Por ejemplo, en la *figura 3.37*, la red se encuentra conectada mediante conmutadores Ethernet de 24 puertos, cada uno de ellos con dos enlaces 100 Base-TX conectados a los otros dos conmutadores para formar una malla. Esta red podría suministrar servicio no bloqueante a 60 usuarios Ethernet –menos de los actualmente conectados-. además, a medida que creciera el número de usuarios y conmutadores debería dedicarse mayor capacidad de conmutación a los enlaces troncales que a las interfaces de los equipos de sobremesa.

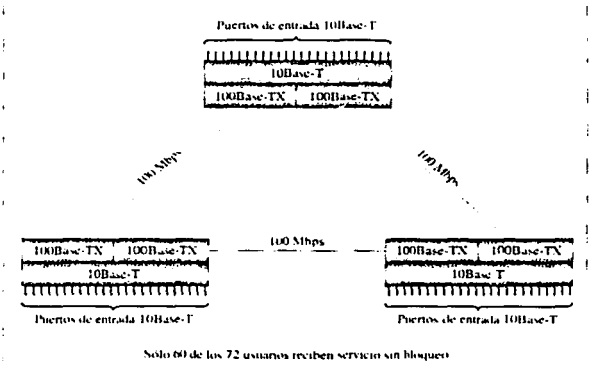


Figura 3.37 Red Ethernet conmutada 10/100

La actualización de un conmutador ATM a 155 Mps añadiría diez puertos ATM, cada uno a 155 Mps, como lo muestra la *figura 3.37*. Sólo se requiere un puerto ATM de cada uno de los conmutadores Ethernet para proporcionar conectividad entre todos los puertos.

Mientras que la red de la *figura 3.38* sólo podía admitir 60 usuarios, la red puede suministrar servicio no bloqueante a 240 usuarios Ethernet dedicados, con posibilidades de ampliación.

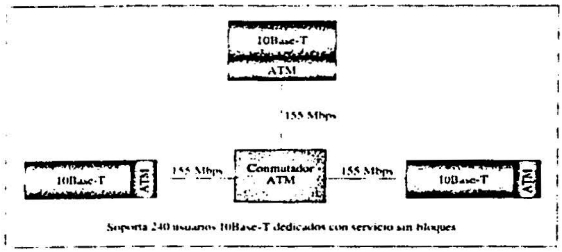


Figura 3.38 Red Ethernet con una red dorsal ATM.

Facilidad de administración

Los enlaces dorsales ATM son más fáciles de administrar que la mayoría de las redes que emplean encaminadores, porque ATM elimina gran parte de la complejidad requerida para configurar grandes redes interconectadas que posen diferentes esquemas de direccionamiento y procedimientos de encaminamiento. Los concentradores ATM proporcionan conexiones entre dos puertos cualesquiera del concentrador, con independencia del tipo de dispositivo conectado a él. Las direcciones de estos dispositivos están predefinidas, facilitando el envío de un mensaje, por ejemplo, de un nodo a otro, independientemente del tipo de red a que están conectados los nodos. De hecho, para muchos usuarios, la razón principal para migrar a una solución ATM puede ser la administración de la red antes, incluso, que los requisitos de rendimiento que dicta la transición.

LAN virtuales

El establecimiento de filtros y restricciones entre los diferentes grupos de usuarios resulta difícil y costoso, utilizando los puentes y encaminadores convencionales. Los administradores de red piensan en términos de grupos de trabajo, no en la posición física de los usuarios. Por tanto, no debería tener que establecer una serie de normas de filtrado basadas en los puertos físicos. La naturaleza orientada a conexión de ATM y el rendimiento de la conmutación de células mediante hardware permiten la creación de redes virtuales.

En vez de configurar y reconfigurar los encaminadores cada vez que una estación cambia de sitio, los administradores de red pueden implementar LAN virtuales. Una LAN virtual es una lista de direcciones de control de acceso al medio (Media Access Control, MAC) de los dispositivos o direcciones de red independientes del puerto físico. Sin embargo, las LAN virtuales tienen significado en la totalidad de la red. Un dispositivo

puede acceder a cualquier otro dispositivo de la misma red virtual. Las LAN virtuales pueden definir filtros entre ellas mismas, al igual que los encaminadores.

Dispositivos en distintos medios pueden ser miembros de la misma LAN virtual. Además, los usuarios pueden transladar las estaciones a cualquier segmento dentro de la subred virtual sin necesidad de reconfigurar la dirección.

Las LAN virtuales permiten a los administradores de red agrupar los dispositivos lógicamente, con independencia de la ubicación física, y suministrar a cada uno de ellos ancho de banda y servicios específicos, como muestra la *figura 3.39.*

Los usuarios pueden conectarse a cualquier puerto de la red y la LAN virtual se encarga del resto. Además de gestionar los filtros, las LAN virtuales también proporcionan:

- Simplificación de los translados, adiciones y modificaciones.
- Asignación del ancho de banda.
- Características de seguridad.

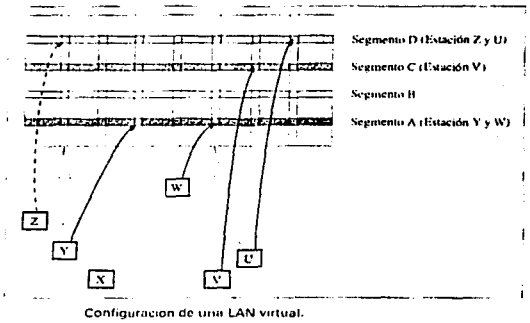


Figura 3.39 Configuración de una LAN virtual

Simplificación de los translados, adiciones y modificaciones

Uno de los principales problemas que los administradores de red tienen en las grandes redes que emplean encaminadores es el considerable esfuerzo administrativo requerido para realizar traslados, adiciones y modificaciones. Esto es particularmente cierto en las redes con Protocolo Internet (Internet Protocol, IP), donde cada LAN física se encuentra asociada a una subred lógica, como muestra la *figura 3.40.* Si un usuario necesita trasladarse de una planta a otra de un edificio, por lo general, la estación de trabajo tiene que ser reconfigurada con una dirección IP válida en la nueva subred.

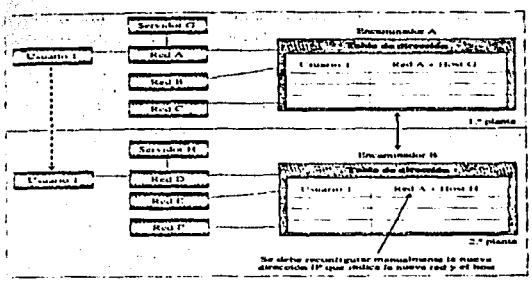


Figura 3.40 Efecto de un translado físico en un esquema direccionamiento de un protocolo internet

Para gestionar tales traslados, los administradores de las redes existentes han de reconfigurar manualmente los encaminadores. Las LAN virtuales, sin embargo, suprimen la labor manual de resolución y reconfiguración de direcciones. Las LAN virtuales permiten a los administradores de red agrupar los dispositivos de manera lógica independientemente de su localización física, y proporcionar ancho de banda y servicios específicos a cada uno, como lo muestra la *figura 3.41.*

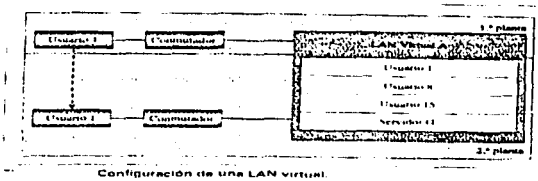


Figura 3.41 Configuración de una LAN virtual

Si bien las redes, obviamente, requieren de la posibilidad de encaminamiento, a los administradores de red les gustaría evitar tener que reconfigurar manualmente las asignaciones de direcciones de red cada vez que los usuarios se trasladan de un segmento de red a otro. Las redes virtuales les permiten hacer precisamente eso mediante la identificación de la dirección física de un nuevo dispositivo y su asociación con una dirección de red a nivel de red, basada en una asignación predefinida sin intervención humana en el sistema o en las estaciones. Los usuarios pueden conectarse a cualquier puerto de red y la LAN virtual realiza el resto.

Rendimiento

Los conmutadores ATM proporcionan una transferencia de datos de alto rendimiento: toda la información se convierte a un formato común de células de 53 bytes. Al contrario que los encaminadores o conmutadores de paquetes, que se ven forzados a procesar paquetes relativamente grandes y de tamaño variable mediante procesos software, ATM o

los conmutadores de retransmisión de células siempre tratan con unidades de datos de tamaño pequeño y uniforme. Esto permite que las funciones básicas de conmutación sean implementadas por hardware. El resultado de un procesamiento y conmutación de células muy rápido y la capacidad de construir grandes redes al mismo tiempo que los retardos de propagación se mantienen aceptables. Esto es crítico para permitir aplicaciones multimedia como video y voz, donde la información es dependiente del tiempo y debe ser transmitida con una latencia baja y regular.

Tolerancia a fallos

En el área de la tolerancia a fallos ATM permite conexiones redundantes, lo que incrementa la tolerancia a fallos y consecuentemente, la fiabilidad. Sin embargo, para permitir a una red ser lo suficientemente rápida como para admitir tasas de transferencia del orden de mutimegabit. ATM no proporciona detección de errores ni retransmisiones, así pues el administrador debe ser precavido.

Seguridad

La naturaleza orientada a conexión de ATM conlleva a potenciales ventajas adicionales relacionadas con la seguridad. La utilización explícita de procedimientos de establecimiento de llamada permite que la seguridad sea implementada en función de la llamada en contraposición a la basada en paquete, de manera que los usuarios no tienen acceso automático a otros recursos. La red podría determinar de forma inteligente qué tráfico debería dejar pasar en función de las entidades emisora y destino. Además, es posible implementar la autentificación de usuario que restringe a los usuarios el acceso a la totalidad de los recursos de la red. La naturaleza orientada a conexión de ATM asegura, también, que el tráfico sólo es enviado al destino al que iba dirigido: no existe desperdicio de recursos de la red con innecesarias difusiones ni riesgos en la seguridad. Este protocolo elimina la necesidad de filtros en el protocolo para mejorar la eficiencia.

Seguridad y LAN virtuales

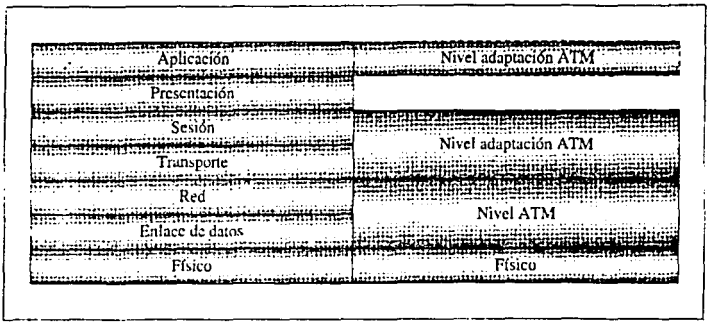
Las LAN virtuales pueden incrementar la seguridad en las redes ATM. Los administradores pueden utilizar LAN virtuales para definir restricciones de filtrado entre los grupos de dispositivos, proporcionando una elevada seguridad. Los conmutadores ATM, además, ofrecen seguridad a nivel de puerto, al permitir a los administradores restringir las subredes virtuales a determinado puertos físicos.

El costo de la propiedad

Posiblemente, ATM es la tecnología más cara; los productos ATM tienen un costo relativo superior debido, según todos los indicios, al ensamblado de células y a los servicios adicionales. Sin embargo, no sólo los adaptadores y conmutadores ATM son caros, sino que, actualmente, son de propiedad privada. Esto significa que la formación y la experiencia en el producto será específica del vendedor. Si se cambia de vendedor, por consiguiente, los costos incluirán, con toda certeza, unos elevados gastos de formación e integración.

ATM y el modelo OSI

La relación de ATM con el modelo OSI supera al de la mayoría de los protocolos de transporte, como lo muestra la *figura 3.42.* Por tanto, para beneficiarse completamente de ATM, así como para integrarlo en las redes existentes basadas en protocolo heredados, las aplicaciones deben desarrollarse de manera que soporte las implicaciones del nivel superior del modo de transferencia asíncrono.



Relación entre los modelos de referencia ISO-OSI, RDSI-BA y ATM.

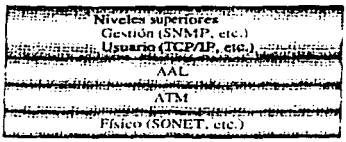
Figura 3.42 Relación entre los modelos de referencia OSI,RDSI-BA y ATM

Capa ATM

Lo que se ha tratado hasta ahora son operaciones que tienen lugar en la capa ATM, que corresponde, en cierta manera, a los niveles de enlace de datos y de red del modelo OSI. Si ATM fuera como otros protocolos, estos serían los único niveles afectados por ATM. Para asegurar los niveles de servicio a las estaciones o aplicaciones mediante ancho de banda dedicado, así como para integrar redes de otros protocolos de transporte en la red ATM, es necesario explorar el nivel superior en el modelo de referencia ATM.

Capa de adaptación ATM (ATM Adaption Layer, AAL)

La capa de adaptación ATM (AAL) se sitúa sobre la capa ATM, tal como se muestra en la *figura 3.43.* En esta capa es donde ATM convierte el tráfico de usuario procedente de las aplicaciones en formato ATM. En esta capa ATM proporciona el soporte para las aplicaciones orientadas a conexión y no orientadas a conexión, las aplicaciones de tasa de bit variable (como X.25 y el tráfico en las redes de área local, respectivamente), además de las aplicaciones de tasa de bit constante (como video y multimedia).



El modelo de referencia de la red digital de servici banda ancha y su relación con otros protocolos.

Figura 3.43 El modelo de referencia de la red digital de servicios de banda ancha y su relación con otros protocolos.

Verdaderamente, la capa de adaptación ATM está compuesta por dos subcapas: la subcapa de convergencia (Convergence Sublays, CS), y la subcapa de segmentación y reensamblado (Segmentation and Reassembly Sublayer, SAR).

Subcapa de convergencia (CS)

La subcapa de convergencia permite la restauración de voz, video y tráfico de datos a través de la misma infraestructura de conmutación. Interpreta los datos procedentes de la aplicación del nivel superior y los prepara para su procesamiento por parte de la subcapa de segmentación y reensamblado. Obviamente, las operaciones y funciones realizadas por la CS varían en función del tipo de formato de los datos recibidos.

Subcapa de segmentación y reensamblado (SAR)

Antes de que la aplicación transmita los datos a través de una red ATM, la SAR segmenta los datos en células de datos ATM de 48 bytes. Una vez que las células ATM alcanzan su destino, la SAR reensambla las células en datos de nivel superior y transmite esos datos a sus dispositivos locales correspondientes.

AAL-5

Puesto que ATM puede transportar múltiples tipos de tráficos, en la subcapa de adaptación existen varios protocolos de adaptación, todos ellos funcionando simultáneamente. Por ejemplo, la redes de área local utilizan, con frecuencia, el protocolo de adaptación AAL-5, diseñado específicamente para tratar este tipo de tráfico de datos de velocidad variable. En la subcapa de convergencia AAL-5, se añade un campo de 8 bytes – incluyendo la longitud de los datos y una suma de verificación de detección de errores- a una trama (o bloque) de información de usuario (hasta 64 KB de longitud) procedente de la aplicación de nivel superior. A continuación, la subcapa de segmentación y reensamblado fragmenta la trama AAL-5 en un flujo de células de datos de 48 bytes y las envía a su destino. En la estación receptora, la SAR reensambla las células en tramas y la CS las procesa, eliminando, entonces, el campo de 8 bytes correspondiente a la longitud de los datos y a la suma de verificación de detección de errores; a continuación se pasa la trama al protocolo del nivel superior.

Problemas en ATM

En el pasado los protocolos de comunicaciones de datos evolucionaron en respuesta a circuitos poco confiables. Los protocolos en general detectan errores en bits y tramas perdidas, luego retransmiten los datos.

Los usuarios puede que jamás vean estos errores reportados, la degradación de respuesta o de caudal (throughput) serían los únicos síntomas.

A diferencia de los mecanismos de control extremo a extremo que utiliza TCP en internerworking, la capacidad de Gbit/seg de la red ATM genera un juego de requerimientos necesarios para el control de flujo. Si el control del flujo se hiciese como una realimentación del lazo extremo a extremo, en el momento en que el mensaje de control de flujo arribase a la fuente, ésta habría transmitido ya algunos Mbytes de datos en el sistema, exacerbando la congestión. Y en el momento en que la fuente reaccionase al mensaje de control, la condición de congestión hubiese podido desaparecer apagando innecesariamente la fuente. La constante de tiempo de la realimentación extremo a extremo en las redes ATM (retardo de realimentación por producto lazo - ancho de banda) debe ser lo suficientemente alta como para cumplir con las necesidades del usuario sin que la dinámica de la red se vuelva impractica.

Las condiciones de congestión en las redes ATM están previstas para que sean extremadamente dinámicas requiriendo de mecanismos de hardware lo suficientemente rápidos para llevar a la red al estado estacionario, necesitando que la red en sí, éste activamente involucrada en el rápido establecimiento de este estado estacionario. Sin embargo, esta aproximación simplista de control reactivo de lazo cerrado extremo a extremo en condiciones de congestión no se considera suficiente para las redes ATM.

El consenso entre los investigadores de este campo arroja recomendaciones que incluyen el empleo de una colección de esquemas de control de flujo, junto con la colocación adecuada de los recursos y dimensionamiento de las redes, para que aunados se pueda tratar y evadir la congestión ya sea:

- Detectando y manipulando la congestión que se genera tempranamente monitoreando de cerca las entradas/salidas que están dentro de los conmutadores ATM y reaccionando gradualmente a medida que vaya arribando a ciertos niveles prefijados.

- Tratando y controlando la inyección de la conexión de datos dentro de la red en la UNI (unidad interfaz de red) de tal forma que su tasa de inyección sea modulada y medida allí primero, antes de tener que ir a la conexión de usuario a tomar acciones mas drásticas.

El estado de la red debe ser comunicado a la UNI, generando rápidamente una celda de control de flujo siempre que se vaya a descartar una celda en algún nodo debido a congestión. La UNI debe entonces manejar la congestión, cambiando su tasa de inyección o

notificándola a la conexión de usuario para que cese el flujo dependiendo del nivel de severidad de la congestión.

El mayor compromiso durante el control de congestión es el de tratar y afectar solo a los flujos de conexión que son responsables de la congestión y actuar de forma transparente frente a los flujos que observan buen comportamiento. Al mismo tiempo, permitir que el flujo de conexión utilice tanto ancho de banda como necesite sino hay congestión.

La recomendación UIT - T I. 371 especifica un contrato de tráfico que define como el tráfico del usuario seria administrado. El contrato que existe para cada conexión virtual (virtual path o virtual channel), es básicamente un acuerdo entre el usuario y la red con respecto a la Calidad de Servicio (Quality Of Service - Q o S) y los parámetros que regulan el flujo de celdas. Estos descriptores de trafico dependen de una particular clase de servicio y pueden incluir bajo la especificación del ATM Forum UNI / a cinco Q o S referenciados en los AALS. El objetivo de estas sub clases de servicio es agrupar características de servicio como requerimiento de ancho de banda similares, sensibilidad a la perdida de datos y retardos para un correcto manejo de los datos en los puertos de acceso ATM, etc. Estos parámetros pueden incluir el Sustained Cell Rate (SCR), el Mínimum Cell Rate (MCR), el Peak Cell Rate (PCR) y/o el Burst Tolerance (BT). Para soportar todas las diferentes clases de servicios definidos por los estándares el switch ATM debe ser capaz de definir éstos parámetros en base a cada VC o cada VP y debe proveer amortiguadores (buffers) para absorber las ráfagas de trafico.

Líneas de producto incompletas

Las líneas de producto son, probablemente, el problema más grande asociado con la migración a una red ATM. Muchos vendedores tiene una línea de producto, pero muy pocos vendedores ofrecen una gama completa desde adaptadores de red hasta conmutadores troncales. actualmente, pocos vendedores pueden ofrecer una red ATM completa, que comprenda todos los conceptos, por tanto será necesario mezclar y emparejar productos de diferentes vendedores. Dada la naturaleza propietaria de ATM y la consiguiente carencia de compatibilidad entre productos ATM, la interoperabilidad es esencialmente imposible. La falta de una adecuada planificación detallada para la arquitectura ATM por parte de los vendedores es el principal obstáculo.

Detalles en la formación

Muchas estrategias ATM de los vendedores son altamente complejas y exigen a los usuarios ser expertos en las líneas de producto de múltiples vendedores. Dado que estos productos son propietarios, la formación sobre el conmutador ATM no garantiza un conocimiento aplicable a los productos ATM de otro vendedor. Además, el ATM forum se halla todavía en proceso de desarrollo de muchas de las especificaciones necesarias para implementar la interoperabilidad entre redes ATM, por consiguiente no es posible una formación sólida en estas interfaces porque la información simplemente no se encuentra disponible.

Documentación de red

Cuando sé esta evaluando la configuración de una red y más tarde la resolución de problemas, se debería documentar cada conexión en la red cuando esta es instalada. La documentación podría incluir la longitud de cada segmento de cable conectado, incluyendo todos los transceivers y cables de patcheo. Además, se debería incluir el tipo de cable usado en cada segmento y toda la información que se puede recolectar de las características del cable.

Dominio de Colisión

Las guías de configuración para multi-segmentación aplican al dominio de colisión para la tecnología Ethernet, es decir al Protocolo de Control de Acceso al Medio. Un dominio de colisión es formalmente definido como un medio en el cual podría haber una colisión si 2 computadoras transmiten al mismo tiempo.

En un sistema Ethernet compuesto por un solo segmento o múltiples segmentos conectados con hubs constituyen un solo dominio de colisiones. La *figura 3.44* muestra 2 hubs donde se conectan 3 computadoras. Ya que solo están conectados hubs para comunicar toda la red, todos los segmentos y computadoras están en el mismo dominio de colisión.

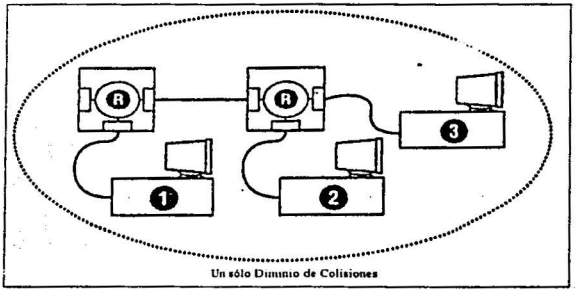


Figura 3.44 Un sólo Dominio de Colisiones

Otro importante punto es que todos los segmentos con el mismo dominio de colisión operan a la misma velocidad. Esto es porque los hubs asumen que todos los segmentos conectados a hubs operan a la misma velocidad y en consecuencia tienen los mismos tiempos de respuesta. Además, existen 3 guías de configuración, una para cada una de las velocidades en Ethernet: 10, 100 y 1000 Mbps, cada una de estas velocidades tienen su propio tiempo de respuesta y sus propias guías de configuración.

Las guías de configuración que se describen son tomadas directamente del estándar IEEE 802.3 quienes describen los estándares para la operación de una red de área local

(LAN). Por lo tanto, estas guías solo aplican a un simple dominio de colisión y no mencionan nada sobre combinar múltiples dominios de colisión con paquetes de dispositivos de switcheo. Los switches permiten que se puedan crear nuevos dominios de colisión en cada puerto, permitiendo tener conectados muchas redes juntas. Se puede también conectar segmentos operacionales de diferentes velocidades con los switches.

Guías de Configuración para 10 Mbps

Modelo 1.- Guía de configuración para 10 Mbps

El primer modelo tomado del estándar IEEE 802.3, describe un conjunto de reglas de configuración para combinar varios segmentos a 10 Mbps. Las reglas se describen a continuación:

Un conjunto de repetidores son requeridos para la interconexión de todos los segmentos. Un conjunto de repetidores es un repetidor y transceiver adicionales, así como los cables de interconexión necesarios entre estos equipos.

Los repetidores de cable UTP, la fibra óptica y el cable coaxial típicamente usan MAU's (Unidades Agregadas al Medio) internos localizado en cada uno de los puertos de los repetidores.

La trayectoria de transmisión permitido entre 2 DTE's podría consistir de 5 segmentos, 4 repetidores (2 MAU's y 2 AUI's). El conjunto de repetidores son asumidos por tener su propio MAU's, quién no esta contenido con esta regla.

Los cables AUI para 10 Base FP y 10 Base FL no deben exceder los 25 m (dado que solo 2 MAU's por segmento son requeridos, resulta que se requieren 50 m para todo el segmento).

Cuando una red consiste de 4 repetidores y 5 segmentos, 3 de los segmentos podrían estar mezclados y los restantes conectados. Cuando 5 segmentos están presentes, cada segmento conectado en fibra óptica no debería exceder los 500m. Un segmento compartido es definido como un segmento que podría tener más de 2 interfaces dependientes del medio (MDI) agregados. Un segmento conectado es definido como un medio para conectar 2 y solo 2 MAU's.

Cuando una trayectoria de transmisión consiste de 3 repetidores y 4 segmentos, las siguientes restricciones son aplicadas:

La longitud máxima permitida para los repetidores de fibra no deberán exceder los 1000 m para 10 Base FB y 10 Base FL.

La longitud máxima permitible para repetidores DTE de fibra óptica no deberían exceder los 400 m para segmentos 10 Base FL y 300 m para 10 Base FP.

Estas no son restricciones para el número de combinaciones en estos casos. En otras palabras, cuando se usan 3 repetidores y 4 segmentos, todos los segmentos son combinables si se desea

La *figura 3.45* muestra un ejemplo de una posible configuración que mantienen las reglas básicas. EL máximo de paquetes transmitidos por la ruta en este sistema entre la estación 1 y 2, es que son 4 repetidores y 5 segmentos en esta trayectoria particular, 2 de los segmentos en la trayectoria son combinados y otros 3 segmentos son conectados.

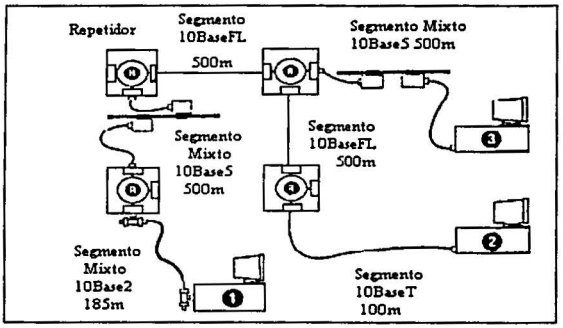


Figura 3.45 Ejemplo de configuración de 10Mbps del modelo 1.

Modelo 2.- Guía de configuración para 10 Mbps

El segundo modelo provee un conjunto de reglas que hacen posible que se puedan checar la validez de los sistemas Ethernet más complejos. Se podría describir modelos de red y tiempos de respuesta que provean un estándar para hacer este modelo.

Mientras la descripción de este modelo podría parecer complejo, en realidad el método es muy simple basado en la multiplicación y adición.

Hay 2 conjuntos de reglas que proveen un estándar para evaluar el rendimiento de los sistemas Ethernet. El primer conjunto de reglas verifica el tiempo de retardo del viaje de la señal de ida y vuelta, mientras que el segundo conjunto verifica la cantidad de espacio que disminuye como limite normal. Ambos cálculos están basados en modelos de red que evaluan la peor trayectoria hacia la red.

Modelos de red y Valores de Retardo

Los Modelos de red y los valores de retardo proveen guías en el Modelo 2 donde deliberadamente se esconde la complejidad mientras que hacen posible el cálculo de los valores del tiempo de retardo para cualquier sistema Ethernet. Cada componente en un sistema Ethernet provee una cierta cantidad de retardo.

La regla 5-4-3

Una versión simplificada del Modelo 1 a 10 Mbps, llamado la regla 5-4-3, ha estado circulando por varios años. Varias formas de esta regla han sido publicadas y algunos términos publicados en ellas son incorrectos. Para citar más ampliamente la guía de configuración, la regla 5-4-3 significa que podría haber hasta 5 segmentos conectados en la red. Esta guía va más allá y describe que 4 repetidores son conectados y solo 3 segmentos son poblados. Un segmento poblado es definido como un segmento con PC's.

La regla 5-4-3 no aplica a cable coaxial debido a 2 condiciones: primero, el segmento coaxial no fue creado para soportar PC"s y segundo, el segmento fue solo usada como un segmento de conexión hacia un repetidor final, Como sea, esto es incorrecto.

Un segmento de conexión es definido en el estándar IEEE 802.3 como un segmento full-duplex punto a punto que conecta 2 y solo 2 MAU's. Un medio ful-duplex significa que el medio provee trayectorias separadas de transmisión y recepción.

Encontrando el caso de la peor trayectoria

Se puede iniciar el proceso de checar un sistema Ethernet encontrando el camino en la red con el máximo retardo. Este es el camino en el que hay un mayor tiempo de retardo y un mayor número de repetidores entre 2 estaciones. En algunos casos, se podría decidir si se tiene más de un candidato para la peor trayectoria en el sistema. En estos casos, se debería identificar todos los posibles conjuntos en la red que parecen cumplir con la definición de la peor trayectoria.

Siguiendo esto, se puede colocar cada camino malo que sea encontrado y si alguno de los caminos excede los límites de los tiempos de retardo, entonces la red no pasará la prueba.

Se debería tener un completo mapa de la topología de red a la mano en el que se pueda identificar la peor trayectoria entre 2 estaciones. Como sea, si la red no esta bien documentada, entonces se tendría que investigar el mapa de la red por sí mismo. La información que se necesita incluir es:

- Tipo de medio utilizado.
- Longitud de los segmentos.
- Localización de todos los repetidores en el sistema.

Una vez que se tiene la información, entonces se puede determinar cual es el camino máximo entre 2 estaciones y que tipos de segmentos son usados en ese camino.

Guías de Configuración para 100 Mbps

Modelo 1.- Guía de Configuración para Fast-Ethernet

Este modelo provee una guía de configuración simplificada. La meta de esta guía es estar seguro de la importancia de los requerimientos de los tiempos de respuesta para Fast-Ethernet, de modo que el protocolo de control de acceso al medio (MAC) podría funcionar correctamente. Las reglas básicas de configuración Fast-Ethernet incluyen:

- Todos los segmentos de par trenzado deberán tener una longitud máxima de 100m.
- La longitud máxima para un segmento es fibra óptica será de 412m.
- Si una interface independiente del medio (MII) es usada, esta no debería de exceder de 0.5m.

Modelo 2.- Guía de Configuración para Fast-Ethernet

Este modelo provee un conjunto de cálculos que verifican el tiempo estimado de respuesta de una red Fast-Ethernet half-duplex más compleja. Estos cálculos son muy simples solo el modelo usado para el sistema a 10 Mbs, desde que el sistema Fast Ethernet se uso solo como segmento de conexión.

El máximo diámetro y el número de segmentos y repetidores en un sistema half-duplex 100 Base T son limitados por las señales de tiempo de retardo requerido para garantizar que los mecanismos de detección de colisiones puedan trabajar correctamente. Los cálculos del modelo 2 proveen información que necesita verificar el tiempo estimado de un conjunto de estándares en el segmento 100 Base T y repetidores. Esto garantiza la combinación de las señales de retardo combinadas con los tiempos estimados requeridos en el estándar.

Guías de Configuración para 1000 Mbps

Modelo 1.- Guía de Configuración para Gigabit-Ethernet

La meta de esta guía de configuración es garantizar que los tiempos requeridos para Gigabit Ethernet sean mantenidos de modo que el protocolo de acceso al medio (MAC) pueda funcionar adecuadamente. Estas reglas de configuración half-duplex para Gigabit Ethernet son:

- El sistema es limitado a un solo repetidor.
- La longitud de los segmentos son limitados a 316m como distancia máxima para la transmisión.

A continuación se muestra una *tabla 3.11* que contiene el dominio máximo de colisiones en Gigabit Ethernet en metros:

Configuración	Cat. 5 UTP	1000 Base CX	Fibra óptica 1000Base SX/LX	Cat. 5 y Fibra óptica	1000Base CX y 1000Base SX/LX
DTE-DTE	100	25	316	N/A	N/A
Repetidor	200	50	220	210	220

Tabla 3.11 Dominio máximo de colisiones Gigabit ethernet.

Modelo 2.- Guía de Configuración para Gigabit Ethernet

De igual manera, esta guía provee un conjunto de cálculos que verifican los tiempos de retardo para una red LAN half-duplex en Gigabit Ethernet. Estos cálculos son tan simples como los modelos para 10 y 100 Mbps, desde que Gigabit Ethernet solo era usado como segmento de conexión que permite un repetidor.

Capítulo IV

Rediseño de la Red de Cómputo del Instituto de Geofísica.

CAPÍTULO IV:
REDISEÑO DE LA RED DE CÓMPUTO DEL INSTITUTO DE GEOFÍSICA

A menudo es sencillo asumir que todos los problemas de la red son el resultado de no tener la última tecnología, la más nueva y/o la más rápida. Y lo mismo ocurre con el rendimiento de la red. Cuando la red se vuelve lenta, el primer pensamiento podría ser el convertir la red – o al menos los segmentos rápidos de la red – en una que utilice los nuevos protocolos de alta velocidad. Después de todo, incrementar la tasa de transferencia (throughput- cantidad de datos que se puede transmitir por un canal u otro dispositivo por segundo -) diez veces o más tienen que mejorar el rendimiento de la red, incluso aunque el tráfico excesivo de la red no sea el único culpable.

Hasta hace poco las redes de alta velocidad eran caras y por lo tanto inalcanzables para muchas empresas. Eso se debía a que si se deseaba una red rápida, sólo se tenía la opción de FDDI. Originalmente, el elegir FDDI también suponía cambiar el cableado para utilizar fibra óptica, lo que implicaba un costo extra, lo que impidió que muchas empresas entrasen en el mercado de la redes de alta velocidad.

Sin embargo, con el surgimiento de nuevos protocolos de transporte rápido se están abaratando los costos en comparación con equipos con estándares de 10 Mbps. Además, algunos de ellos pueden utilizar el cableado de categoría 5 existente, aunque otros todavía requieren de cableado de fibra óptica. Por lo tanto, parece natural que el administrador de redes necesitado de rendimiento piense que ha llegado el momento de implementar una red de alta velocidad.

Al dar el paso de cambiar a una red de alta velocidad, el mayor reto es la selección del protocolo de transporte. Desafortunadamente, no es el primer reto al que se tienen uno que enfrentar.

Es fácil atribuir un bajo rendimiento de la red a una escasez de ancho de banda. También es fácil asumir la idea de que "más es mejor" y pasar a las redes de alta velocidad porque no pueden hacer daño. Ninguna de estas suposiciones es cierta, y ambas son peligrosas. El momento de aprender si las redes de alta velocidad pueden subsanar los síntomas de la red es antes de invertir tiempo y dinero en la misma.

Antes de continuar con la planeación de la migración hacia las redes de alta velocidad, habrá que preguntarse el por qué se están considerando estas redes. ¿Se debe a que se sufre actualmente un bajo rendimiento en la red? o ¿a que los planes de interconexión de redes para el futuro cercano implican una aplicación que necesitan de un gran ancho de banda como multimedia o videoconferencia ?

A menudo, un rendimiento de la red pobre es el resultado de un tráfico de red excesivo. Hay muchos factores que podrían estar contribuyendo al incremento del tráfico en la red. Si hay demasiadas estaciones de trabajo en un segmento se puede estar generando más tráfico del que puede manejar el ancho de banda disponible.

También existe la tendencia en las aplicaciones de utilizar más ancho de banda, debido fundamentalmente a la popularidad creciente de las aplicaciones multimedia. Finalmente, el tamaño del paquete medio en todas las aplicaciones está creciendo, aunque actualmente el tamaño del paquete puede variar entre 256 y 512 bytes, y con tendencias a crecer. Para determinar si lo que causa el problema de red es el tráfico excesivo, se debería colocar un analizador de protocolo en cada segmento de red afectado. El analizador se puede configurar para que supervise los paquetes para la topología y protocolo específicos del segmento, permitiendo supervisar el tráfico en el segmento al que se está conectando. Un analizador de protocolo permite ayudar a determinar no sólo la utilización de ancho de banda media en el segmento, sino también el tamaño de paquete medio y su composición. Además, el analizador puede ayudar en el momento de detectar tendencias en cuanto a tráfico, períodos de tráfico máximo y dispositivos que están generando paquetes incorrectos o que actúan como cuellos de botella en la red.

En cualquier caso, no se debe comenzar con los planes para implementar una red de alta velocidad hasta que se haya supervisado la red con un analizador de protocolo y decidido que el problema es la escasez de ancho de banda. Esta es la única manera de estar seguro de que una red de alta velocidad supondrá una mejora en el rendimiento de la red.

A pesar de todos los beneficios de un ancho de banda mayor para la red, una red de alta velocidad no es una panacea. Hay muchos problemas de red que reducirán el rendimiento y que no tienen nada que ver con el ancho de banda suficiente. Si por ejemplo, el problema real en la red es la E/S de disco de los servidores, el aumento del ancho de banda no va a suponer un incremento en el rendimiento. A continuación se mostrarán algunos problemas que alentan la red y que no se evitarán con un protocolo de alta velocidad, y por lo tanto habrá que revisar con detenimiento.

La manera en que estos problemas sean atacados define cada una de las metodologías presentadas.

4.1.- Metodología presentada por Teré Parnell

En esta metodología se propone una secuencia específica a seguir en el momento en la que el tráfico en la red comienza a alentarse. Esta secuencia de pasos se define a continuación.

Problemas de rendimiento relacionados con el servidor

Hay varios componentes del servidor que afectan al rendimiento de la red. Antes de considerar una red de alta velocidad, habrá que comprobar primero los siguientes cuellos de botella potenciales en el servidor.

Velocidad del procesador.

La velocidad real del procesador es un factor importante que afecta al rendimiento del servidor. Un servidor muy utilizado con un procesador que no es el apropiado simplemente no puede hacer frente a las peticiones de datos que recibe. Entonces habrá que asegurar que los servidores tienen la potencia de procesamiento adecuada.

Incluso si se confirma que los servidores tienen la potencia adecuada en ese momento, es posible que se necesite sustituirlo o mejorarlo cuando se implemente una red de alta velocidad. Las interfaces de red de alta velocidad exigen más al CPU del servidor (después de todo, se está solicitando que el servidor procese los paquetes entrantes que estén llegando mucho más rápido). Por lo tanto, antes de instalar el adaptador de red de alta velocidad, hay que asegurar de que el servidor tenga potencia de procesamiento de reserva.

Subsistema de disco.

Un servidor de archivos proporciona servicios de archivos: acceso a los datos y archivos de aplicación almacenados en el subsistema de disco del servidor de archivos. El subsistema de disco es el propio disco duro y la controladora de disco que gestiona la transferencia de datos entre el disco y el procesador del servidor. Si el subsistema de disco no puede proporcionar un acceso lo suficientemente rápido a los archivos almacenados en él, los usuarios de red perderán mucho tiempo esperando los datos que han enviado o solicitado al servidor de archivos para su procesamiento. La velocidad de transferencia de datos, o la velocidad a la que un servidor puede transferir los archivos entre su procesador y el subsistema de disco, es una función del propio disco, de la controladora y de las interfaces de bus situadas entre el disco y la controladora de disco y entre ésta y el procesador. Cuanto más rápidos sean estos componentes, más rápido será el tiempo de respuesta de la red.

El primer signo de que el subsistema de disco está disminuyendo el rendimiento se observa cuando las solicitudes del servidor para leer y/o escribir datos están a la espera en la entrada/salida de disco. Si se observa que las solicitudes están a la espera demasiado tiempo (y esto variara entre los distintos servidores y redes, por lo que "demasiado" se deberá definir en función de una red en particular), probablemente sea el momento de considerar la instalación de un subsistema de disco más rápido.

Memoria de acceso aleatorio.

Si la memoria de acceso aleatorio (RAM) es pequeña o está mal configurada, se puede reducir el rendimiento de la red. Cuando se llena toda la memoria que el servidor ha asignado como memoria próxima (cache), escribe los datos más antiguos en disco. Si el servidor tienen muy poca RAM, perderá una cantidad excesiva de tiempo yendo al disco a recuperar los datos. El leer los datos de la unidad de disco es mucho más lento que leer la información de la RAM.

La velocidad de la RAM del servidor también afecta al rendimiento global. Por lo tanto, se debería comprobar que la velocidad de la memoria se corresponde con su utilización.

Problemas de rendimiento relacionados con la red

Algunos problemas de rendimiento están relacionados con la conexión entre el dispositivo central y los elementos de la red, pero no son consecuencia de un ancho de banda insuficiente. A continuación se presentan los problemas más habituales que acaban con el rendimiento y se producen en la conexión de red.

Selección de la tarjeta de interfaz de red.

La elección de las tarjetas de interfaz de red, tanto en el servidor como en la estación de trabajo, pueden afectar drásticamente al rendimiento de la red. Estas tarjetas pueden variar en gran medida en rendimiento y costo por lo que se tendrá que evaluar los beneficios de un rendimiento mayor frente al costo relativo de las tarjetas. Al escoger una tarjeta interfaz de red, habrá que evaluar lo siguiente:

- Tasa de transferencia (throughput) de datos. Es la velocidad a la que la tarjeta de interfaz de red transfiere los datos entre la memoria de la computadora y la red. La tasa de productividad de datos depende de la anchura de la interfaz de bus con el procesador central y el método que utiliza la tarjeta de interfaz de red para transferir los datos.

Actualmente las anchuras de bus (host) son 8, 16 ó 32 bits. Cuanto más ancho sea el bus de datos, más rápidamente transferirá los datos la tarjeta de interfaz de red. Las diferentes arquitecturas de bus de dichas tarjetas ofrecen distintas anchuras de bus: las tarjetas de Arquitectura estándar de la industria (ISA, Industry Standard Architecture) ofrecen buses de 8 y 16 bits, y las tarjetas de la Arquitectura extendida estándar de la industria (EISA, Extended Industry Standard Arquitecture) y las tarjetas de la Interfaz de componentes periféricos (PCI, Peripheral Component Interface) ofrecen buses de 32 bits.

Los servidores que tengan un tráfico denso a través de sus tarjetas de interfaz de red realmente deberían ser computadoras diseñadas con uno de los buses de arquitectura de 32 bits y equipadas con sus tarjetas correspondientes.

- Procesador en la tarjeta. Las tarjetas de interfaz de red que utilizan un procesador eficiente en la tarjeta pueden mejorar el rendimiento en la tarjeta, y por lo tanto, en toda la red. En definitiva, para mejorar el rendimiento, se recomienda utilizar tarjetas que tengan procesadores de alto rendimiento en la tarjeta.

Tarjetas ruidosas.

Si la tarjeta de red hace ruido, es decir, transmite flujos de paquetes erróneos, el aumentar el ancho de banda no mejorará el rendimiento de la red. La razón es que es muy probable que el mal funcionamiento de la red inunde el ancho de banda disponible con paquetes errantes, lo que significa que incrementar el ancho de banda a 1 Gbps sólo supondrá obtener mil veces la basura de red que ya se tenía.

Si los controladores (líneas de código que traducen las llamadas de programa de redirección de red a instrucciones para las tarjetas de interfaz de red), están poco optimizados (controladores de tarjetas de red genéricos), los usuarios sufrirán todo tipo de dificultades en la red, incluyendo un bajo rendimiento. Este bajo rendimiento se debe a que se necesita una retransmisión para enviar un paquete con éxito desde la tarjeta de interfaz de red a su dirección.

Problemas de rendimiento relacionados con la estación de trabajo

Otro aspecto del rendimiento de la red del que se prescinde a menudo es el rendimiento de la estación de trabajo. Las estaciones de trabajo con procesadores lentos, discos fijos lentos y/o memoria insuficiente no serán capaces de procesar con rapidez todos los datos que envían y reciben del servidor. Esto hará que los usuarios tengan la impresión de que la red es lenta, aunque en realidad el problema sea otro.

Como determinar si la red de alta velocidad va a ayudar.

Ahora que ya se conoce un poco el ámbito de muchos problemas que la redes de alta velocidad no van a resolver, la siguiente pregunta que se debe contestar es el cómo determinar si se resolverán las dificultades de la red en particular. Las hojas de trabajo basadas en columnas y el diagrama de flujo *(figura 4.1)* ayudarán a determinar si estas redes servirán realmente de ayuda para la red.

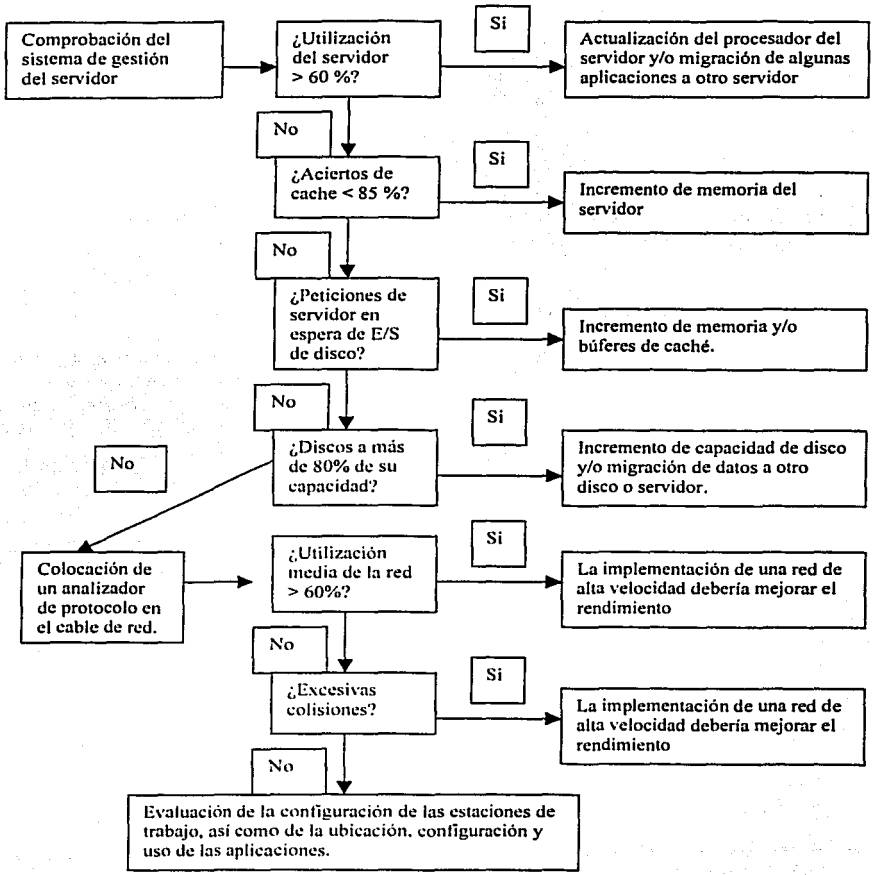


Figura 4.1 Diagrama de flujo que resume cómo localizar y diagnosticar un rendimiento pobre de la red.

Paso 1. Evaluar la utilización del servidor.

Dentro de la metodología se sugiere utilizar el formulario siguiente para determinar si el servidor está sufriendo problemas de rendimiento.

- Utilización del servidor.- La utilización media del servidor debería ser probablemente menor del 60 %. Sin embargo, esto variará de un sistema operativo a otro y entre distintas redes. Si la utilización media es superior al 60 %, entonces habrá que pensar en actualizar el procesador del servidor o en transferir algunas aplicaciones a otro servidor.

- Utilización de la memoria próxima (cache).- Los aciertos de cache deben ser de medida un 85 % aproximadamente. Si no es así, hay que comprobar la cantidad de memoria y los bufers de cache asignados. La regla para la mayoría de los sistemas operativos de red es: cuanta más memoria mejor. Sin embargo, hay excepciones, especialmente cuando se trabaja con versiones antiguas de dichos sistemas.

- Utilización e intercambio (swapping) de disco.- Si las soluciones del servidor están a la espera de la entrada/salida de disco, o si el servidor está utilizando el intercambio de disco (disk swapping, consiste en la utilización de almacenamiento de disco para aumentar la memoria de acceso aleatorio), se debe considerar el añadir memoria o incremento de los buffers de memoria cache. Si el propio disco del servidor está ocupado más de un 80 %, se necesitará incrementar la capacidad del disco o eliminar algunos datos de los discos existentes.

- Utilización de dispositivos de componentes.- Con tecnologías de dispositivos de componentes como la Interfaz de sistemas de pequeñas computadoras (SCSI, Small Computer System Interface), el rendimiento siempre se reduce al mínimo común denominador. Por lo tanto, si se tienen varios dispositivos conectados a un solo adaptador de nodo central SCSI, el rendimiento de señalización de la cadena completa será igual al del dispositivo más lento de la cadena.

Paso 2. Evaluar la configuración de los servidores principales.

Utilizando el formulario siguiente, se recomienda describir el hardware y configuración de los servidores principales.

Servidor n+1.
Procesador.
Tipo.
Velocidad del reloj.

Memoria de acceso aleatorio.
Cantidad.
Velocidad.
Bufers de memoria cache totales.
Subsistema de disco.
Tipo de controladora.
Velocidad de acceso al disco.
Capacidad de disco.
Tarjeta de interfaz de red.
Fabricante.
Modelo.
Anchura de bus anfitrión.
Tipo de procesador en la tarjeta.
Nombre del controlador.

Paso 3. Evaluar las estaciones de trabajo.

Es importante evaluar la potencia de procesamiento de las estaciones de trabajo de los segmentos de la red que están sufriendo un rendimiento bajo. Aunque el servidor y la red funcionen bien, una estación de trabajo de potencia reducida puede dar a los usuarios la impresión de que la red es lenta.

Servidor n+1.
Procesador.
Tipo.
Velocidad del reloj.
Memoria de acceso aleatorio.
Cantidad.
Velocidad.
Bufers de memoria cache totales.
Subsistema de disco.
Tipo de controladora.
Velocidad de acceso al disco.
Capacidad de disco.
Tarjeta de interfaz de red.
Fabricante.
Modelo.
Anchura de bus anfitrión.
Tipo de procesador en la tarjeta.
Nombre del controlador.

Paso 4: Evaluar los requisitos de las aplicaciones actuales.

Se debe enumerar en el formulario siguiente el nombre y tipo de las aplicaciones que residen en cada servidor. Las aplicaciones de base de datos, de modelado estadístico y de CAD/CAM ponen en aprietos a los recursos del servidor. Si se observa que en un servidor (o un disco de un servidor) tienen un número desproporcionado de aplicaciones de este tipo, habrá que transferir algunas aplicaciones a otros servidores u otros discos para intentar equilibrar la carga. Por otra parte, las aplicaciones de tratamiento de imágenes y multimedia generan una gran cantidad de tráfico de red, por lo que son un indicativo de la necesidad de un protocolo de red de alta velocidad.

Del mismo modo, hay que contabilizar el número de usuarios de cada aplicación y la ubicación de estos usuarios. Obviamente, cuantos más usuarios haya, más carga tendrá el servidor y también será mayor el tráfico en la red. Es más, los usuarios que deben atravesar puentes para acceder a los servidores estarán generando tráfico en otras redes distintas de su segmento local.

Servidor n+1.
Disco n+1
Sistema operativo.
Número de usuarios.
Ubicación de los usuarios.
Tipo de aplicación.
Número de usuarios.

Paso 5: Evaluar los requisitos de las aplicaciones futuras.

Hay que observar los planes estratégicos y de presupuesto de la red y, enumerar el nombre y tipo de las aplicaciones que se esperan añadir en los próximos 18 meses. Al lado de cada una, se debe anotar el número y ubicación de los usuarios de estas aplicaciones.

Paso 6: Evaluar la utilización de la red.

Si a pesar de realizar los cambios en la red que se sugieren, todavía se tienen problemas de rendimiento, es el momento de colocar un analizador de protocolo en la red. Este dirá la cantidad y tipo del tráfico que se genera. También mostrará que tiene problemas relacionados con la red, como tarjetas ruidosas, que provocarán un rendimiento pobre de la red.

Si la supervisión del tráfico con un analizador de protocolo revela una utilización excesiva de la red, caracterizada a menudo por una abundancia de colisiones, es el momento de comenzar a planificar una red de alta velocidad.

4.1.2.- Metodología presentada en DGSCA

Al reportar lentitud o algún otro tipo de problema en una red perteneciente a Red-UNAM, el procedimiento a seguir para la detección y corrección del mismo, es el siguiente:

1. Verificar el funcionamiento del switch que da red a la dependencia que reporta el problema, lo anterior para verificar que la red este tanto transmitiendo como recibiendo tráfico adecuadamente.

   La manera de verificación en cada switch depende de sistema operativo de cada fabricante de los switches, así como de la versión de cada uno de ellos. Pero de manera general el procedimiento es el siguiente:

   - Verificar que el puerto este habilitado.
   - Aunque la fibra óptica o el cable UTP este transmitiendo información, está no podrá ser procesada si el puerto no esta habilitado.
   - Verificar que haya actividad en el puerto del enlace.
   - Si no existe actividad en algún extremo del medio de transporte, esto podría ser debido a que en el switch de acceso o en el switch de la dependencia existe algún tipo de problema; desde que el equipo puede estar apagado hasta que el mismo ya esta presentando fallas graves.
   - Verificar que por el puerto se este tanto transmitiendo como recibiendo información.
   - Una vez que ya se a verificado el estado correcto de los switches y que aún así no hay transmisión de información, el causante de esto puede ser que el medio de transmisión presente fallas.
   - Checar el estado del puerto para observar si en este existen colisiones y/o errores.

   En caso de que en los switches se presenten estos tipos de problemas, esto puede ser causado por un puerto del switch en mal estado, una tarjeta que hace ruido, una ataque a alguno de los servidores, etc. Entonces es el momento de pensar en colocar un analizador de tráfico en la red.

2. Verificar la utilización del segmento en ese instante mediante una herramienta gráfica llamada HP OPEN View.

   Esta herramienta monitorea el rendimiento del switch. Es una herramienta gráfica en la cual se modelan los switches de la capa de distribución y la cual maneja alarmas de colores para indicar el estado del switch (verde = estado óptimo, amarillo = inestable y rojo = inactivo). De igual manera monitorea el estado de cada uno de los puertos, dentro de los parámetros que monitorea están:

   - Distribución por el tamaño de los paquetes.
   - Ráfagas de los paquetes por errores, colisiones y broadcast.
   - Porcentaje de utilización del ancho de banda.

3. Checar la utilización de la red a lo largo del día y semana, mes y año para verificar que el problema no se haya repetido en otras ocasiones, mediante una herramienta llamada MRTG.

   MRTG es igualmente una herramienta gráfica, en la cual podemos observar la utilización del ancho de banda de cada uno de los puertos de los switches. El tráfico tanto de entrada como de salida es graficado de la siguiente manera: cada 5 minutos MRTG obtiene el valor de utilización del ancho de banda del switch y lo guarda en un archivo, 5 minutos después vuelve a hacer la petición y hace el promedio entre el valor anterior y el actual, el resultado es entonces graficado en una página con formato html. Este resultado es mostrado en el promedio diario de utilización del ancho de banda, del promedio diario se hace el promedio semanal, del semanal el mensual y finalmente a partir de este último se obtiene el promedio anual.

4. En caso de que el problema no sea momentáneo, entonces se procede a acudir a la Dependencia para colocar una analizador de tráfico y con ello detectar el problema real de la red. Sin embargo, la Dependencia debe contar ya con la siguiente información con el fin de acelerar la detección del problema.

   - Documentación actualizada ante en Centro de Información de la Red de la UNAM (NIC-UNAM). La documentación se refiere a una lista con la siguiente información:

     - Host de la máquina.
     - Dirección MAC.
     - Sistema Operativo.
     - Tipo de servicio proporcionado (aplicaciones).
     - Ubicación física.

   - Direcciones IP validas y asignadas por el NIC.

   - Oficio dirigido al Jefe del Departamento de Operación de la Red. Este deberá incluir una breve descripción del problema o falla.

   - Es necesaria la presencia indiscutible del administrador de la red, así como la herramienta necesaria para tener acceso al equipo de comunicaciones involucrado (llaves, passwords de los equipos, etc).

   - La problemática deberá reflejar un problema específico; es decir, el administrador de la red deberá ya tener un posible diagnóstico de las fallas en la red.

   - Todos los equipos deberán estar etiquetados con la dirección IP y nombre del equipo.

   - Croquis con la ubicación de los equipos dentro de las Dependencias con cotas.

- Croquis con las conexiones físicas de los puntos de red.
- Al programar la cita, esta deberá considerar lo siguiente:

  - Tiempo de mayor cargar del tráfico.
  - Tiempo de atención.
  - Topología de la red.
  - Tipo de equipos conectados.
  - Tipos de tarjeta de red.

Por su parte, el Centro de Asistencia Técnica (TAC-UNAM, departamento encargado de la administración de Red-UNAM) se compromete a realizar lo siguiente:

- Atención del problema en no más de 72 horas.
- Entregar un reporte (si es solicitado) de los resultados del análisis de la red.
- Asesoría telefónica o presencial por parte del personal de TAC-UNAM.
- El análisis de la red será de acuerdo a la disponibilidad en horarios y recursos del personal del TAC respetando las 72 horas.

La información pedida es totalmente indispensable, ya que el analizador de protocolos arroja resultados referentes a hosts, IP's y/o direcciones MAC. Los resultados pueden contener información sobre fallas físicas haciendo referencia a una máquina; el exceso de tráfico generado por alguna PC a causa de una incorrecta instalación de alguna aplicación; etc. Cada uno de los problemas detectados puede ser originado por diversas fuentes de falla, lo que ocasiona que cada falla pueda ser interpretada de diferente manera, por lo que se requiere trabajar en conjunto con el administrador de red local.

4.1.3.- Metodología propuesta

Las metodologías de análisis de redes presentadas anteriormente atacan cada una de ellas diferentes momentos en la problemática de la red. La metodología usada por DGSCA es un poco más completa considerando que está hecha para atacar los problemas de red específicos presentados en las Dependencias de Red-UNAM; es decir, existe un seguimiento desde el momento en que se presenta el problema por primera vez hasta el momento en que el problema llega a ser resuelto.

Cabe mencionar que no siempre es necesaria la aplicación de todos los pasos para la solución del problema presentado, debido a que no siempre la problemática requiere de un análisis de red.

Por otra parte, la metodología presentada por Teré Parnell es un poco más enfocada al análisis posterior a la presencia de la problemática en la red, aunque también hace énfasis en tareas para tratar de prevenir que se originen fallas en la red, sin embargo, esta ya es una tarea que le corresponde a los administradores locales de las distintas dependencias de la UNAM.

Por lo expuesto anteriormente, la metodología propuesta consiste en una combinación de las dos metodologías ya presentadas. Debido a la naturaleza misma de la problemática que representa el analizar una red de este tamaño, no se va a profundizar en el análisis de todos los servidores, estaciones de trabajo y demás PC's, es decir una vez que el analizador arroje los resultados se procederá a evaluar las características de las máquinas que se muestren con problemas.

En resumen, la metodología a utilizar será la siguiente:

- Revisar el diseño general de la red.
- Verificar el funcionamiento del switch que proporciona el servicio de red a la Dependencia que reporta el problema.
- Verificar la utilización del segmento en ese instante mediante el HP OPEN View.
- Checar la utilización de la red a lo largo del día y semana, mes y año para verificar que el problema no se haya repetido en otras ocasiones, mediante el MRTG.
- En caso de que el problema no sea momentáneo, entonces habrá que acudir a la Dependencia para colocar un analizador de tráfico y con ello detectar el problema real de la red.
- Una vez que se muestren los resultados del analizador de redes, poner especial atención en:
  - Evaluar la utilización de los servidores principales.
  - Evaluar la configuración de los servidores principales.
  - Evaluar las principales estaciones de trabajo.
  - Evaluar los requisitos de las aplicaciones actuales.
  - Evaluar los requisitos de las aplicaciones futuras.
  - Evaluar la utilización de la red.

Lo que procede ahora, es comenzar con el proceso del análisis de la red propuesta anteriormente. Se presenta el análisis con cada herramienta y los resultados arrojados por las mismas.

Análisis:

1. Verificación del funcionamiento del switch que da red al Instituto de Geofísica Campus C.U.

El switch que alimenta a esta dependencia es un switch 3Com (Lanplex 2500) de capa 3, con 4 módulos, de los cuales 2 estas ocupados; uno de ellos con una tarjeta con un puerto para recibir un enlace a 100Base-FX (Fast Ethernet) y una segunda tarjeta con capacidad de 8 puertos para dar red al mismo número de Dependencias. Estos puertos tienen tecnología a 10Base-FL (Ethernet), de los cuales 2 están destinados a dar red al Instituto de Geofísica; un puerto para el Edificio Principal y el segundo para el Edificio nuevo.

La manera de administrar estos switches es mediante una conexión física al puerto de consola, por una conexión vía módem, o bien vía telnet (remotamente). En el momento en que se presento el problema, la conexión al switch se mostraba inestable, lo que hacia imposible el verificar el funcionamiento de este equipo en ese instante. Sin embargo, las otras Dependencias que cuelgan del mismo switch aunque también estaban intermitentes tenían conexión a red, pero con problemas de lentitud.

Debido a que en esos momentos no se tenía acceso al equipo vía remota y a que no se realizó la visita al sitio, en ese momento no se verifico su configuración; sin embargo, a continuación se muestra la configuración del mismo una vez que el problema estuvo resuelto *ver figura 4.2*.

Select menu option (bridge/vlan): det

Index	Protocol	Identifier	Ports
1	IP	7	2, 6
2	IP	1	1, 9
3	IP	2	5
4	IP	3	3, 4
5	IPX	5	3
6	IPX	6	1
7	IP	4	2, 6
8	IP	8	2, 6
9	Apple	9	2
10	IP	10	3, 4

Index	Name	Layer 3
1	Geofisica_nuevo	132.248.6.0 255.255.255.0
2	I_Geografia	132.248.254.0 255.255.255.0
3	I Geog	132.248.14.0 255.255.255.0
4	FOP_DGAE.MCU	132.248.211.0 255.255.255.0
5	IPX.FOP_DGAE.MCU	none
6	IPX.ATM	none
7	Geofisica_182	132.248.182.0 255.255.255.0
8	SSN	192.100.200.96 255.255.255.240
9	AppleTalk.Igeof	none
10	FOP_DGAE.MCU2	132.248.46.0 255.255.255.0

Figura. 4.2 Configuración del Lanplex 2500

2. Verificación de la utilización del ancho de banda asignado al Instituto de Geofísica mediante el HP OPEN View.

HP OPEN View es una herramienta gráfica en la que se puede monitorear entre otras cosas la utilización del ancho de banda de este Instituto. Con esta herramienta se pueden monitorear algunos parámetros de cada uno de los puertos de los switches de capa 3 (Lanplex 2500) y otros switches capa 2.

Como esta es una herramienta que verifica el estado de los switches en tiempo real, del mismo modo que con la configuración del switch, fue imposible el verificar el estado del switch en el momento en que se presento el problema. Lo único que se realizó para la verificación en ese instante, fueron las alarmas que arrojo el switch colocado en el Instituto de Geografía, que es de donde se proporciona red al Instituto de Geografía. Un ejemplo de este tipo de alarma se muestra en la *figura 4.3.*

Para poder monitorear el puerto deseado, es necesario posicionarse sobre el esquema del switch adecuado y en el menú superior seleccionar la opción Transcend y posteriormente Display View Tool, lo que mostrará una pantalla como la que se muestra en la *figura 4.4*, y en ese menú seleccionar el puerto a analizar. Para el caso del Instituto de Geofísica, hubo que seleccionar el puerto 1 y el puerto 5 de la tarjeta Ethernet ,Módulo 3.

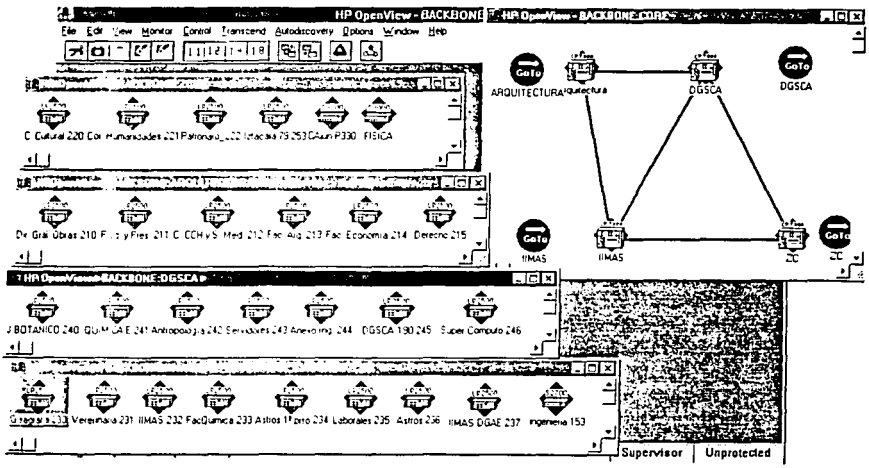


Figura 4.3.- Alarma que muestra HP OPEN View cuando un equipo deja de responder.

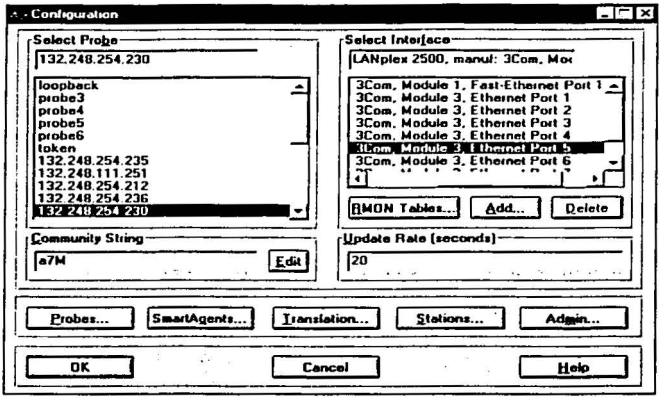


Figura 4.4.- Disposición de los puertos en el Lanplex 2500.

3. Verificación de la utilización de la red mediante el MRTG.

Como ya se comentó, MRTG obtiene los bits de entrada y de salida de utilización del ancho de banda asignado a una Dependencia mediante peticiones vía SNMP (Simple Network Managment Protocol) a los switches correspondientes cada 5 minutos (300 segundos). La utilización se obtiene realizando la diferencia de los valores obtenidos por el poleo realizado cada 300 segundos, dicha diferencia de la utilización en t menos la utilización de t+300 nos da la utilización diaria entrante y saliente, para después poder obtener la utilización entrante y saliente semanal, mensual y anual.

Debido a que el poleo se realiza cada 5 minutos, el resultado de las gráficas de la utilización pueden ser mejor vistas. A continuación se muestra los resultados arrojados por el MRTG los días en que se presentó la problemática.

- Porcentajes muy altos en el tráfico interno de la red, los cuales en la mayoría de los días del análisis rebasaban el 30% recomendable para una red tipo Ethernet.

- El excesivo tráfico interno de la red provocaba que las conexiones externas también fueran afectadas de modo que los enlaces internacionales tenían un tiempo de respuesta muy alto lo que perjudicaba el intercambio de información con otras Instituciones dentro y fuera de país.

- Se observó que el tráfico interno se mantenía estable por intervalos de tiempo aleatorios y de la misma manera se mostraban ráfagas de un excesivo tráfico que iban desde 5 minutos hasta más de 1 hrs.

- Con esta misma herramienta se observo un ligero aumento de tráfico en las redes que eran alimentadas por el equipo de quién dependía el Instituto, es decir el problema local ya estaba afectando a terceros.

A continuación se expone una página generada por MRTG donde se observa el tráfico de entrada y salida hacia al segmento del Instituto de Geofísica, esta muestra un tráfico en el momento del análisis en el día de 16.0 y 3.5 % respectivamente, semanal de 17.2 y 3.0%, mensual de 19.3 y 3.0% y durante el año de 7.2 y 1.5%. Como se observa, la velocidad que se marca en el gráfico corresponde a 20 Mbps, este valor se toma así, debido a que el Instituto cuenta con 2 enlaces a 10 Mbps y la manera en que esta configurado MRTG registra el tráfico por VLAN's y no por puerto, es decir, estos valores numéricos son solo la mitad del tráfico real capturado en esos momento. Por otro lado, se observa que la gráfica si representa los valores reales del tráfico.

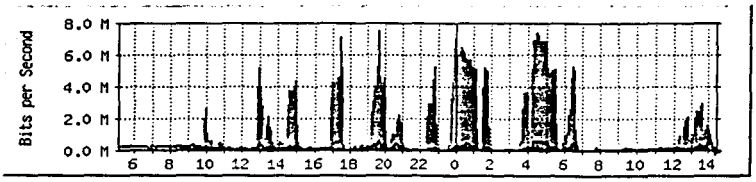
La escala del gráfico se actualiza automáticamente, es decir, en el momento en que exista un pico de 100%, la escala llegará a ese valor, en caso de que durante el periodo de 24 horas el pico llega a un 15%, entonces la gráfica tomara la escala de ese valor.

Análisis de Tráfico

Segmentos:	132.248.6.0 y 132.248.182.0
Dependencia:	Instituto de Geofísica
Velocidad:	20 Mbits/s
Administrador:	Centro de Asistencia Técnica
Equipo:	CoreBuilder 3com 2500. Módulo 3, Puertos Ethernet 1 y 5
IP:	132.248.254.230

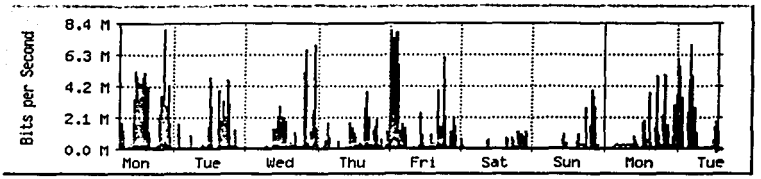
The statistics were last updated **Tuesday, 14 March 2000 at 19:11**

'Daily' Graph (5 Minute Average)



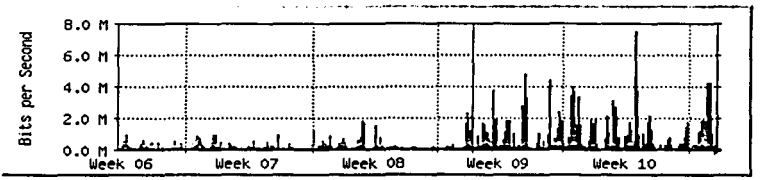
Max In:	7568.6 kb/s (75.7%)	Average In:	1467.6 kb/s (14.7%)	Current In:	1600.7 kb/s (16.0%)
Max Out:	682.0 kb/s (6.8%)	Average Out:	172.0 kb/s (1.7%)	Current Out:	353.6 kb/s (3.5%)

'Weekly' Graph (30 Minute Average)



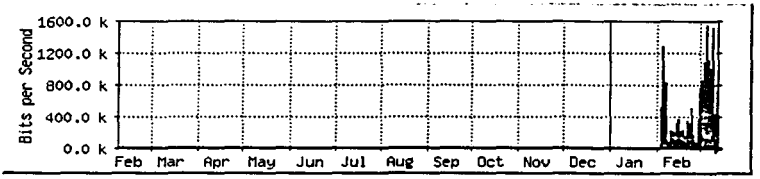
Max In:	8008.8 kb/s (80.1%)	Average In:	1002.1 kb/s (10.0%)	Current In:	1721.6 kb/s (17.2%)
Max Out:	689.9 kb/s (6.9%)	Average Out:	115.4 kb/s (1.2%)	Current Out:	297.1 kb/s (3.0%)

'Monthly' Graph (2 Hour Average)



Max In:	7542.4 kb/s (75.4%)	Average In:	530.8 kb/s (5.3%)	Current In:	1932.0 kb/s (19.3%)
Max Out:	628.9 kb/s (6.3%)	Average Out:	93.7 kb/s (0.9%)	Current Out:	298.2 kb/s (3.0%)

'Yearly' Graph (1 Day Average)



Max In:	1561.3 kb/s (15.6%)	Average In:	509.2 kb/s (5.1%)	Current In:	721.4 kb/s (7.2%)
Max Out:	190.8 kb/s (1.9%)	Average Out:	88.0 kb/s (0.9%)	Current Out:	147.9 kb/s (1.5%)

GREEN ### Incoming Traffic in Bits per Second
BLUE ### Outgoing Traffic in Bits per Second

Como se advierte a través de las gráficas, existen momentos en los días en que el porcentaje de utilización del ancho de banda llega a alcanzar casi el 80 %, e incluso existen intervalos de casi 2 horas en que el rendimiento de la red no es ni por mucho el óptimo. Como se puede observar, el problema se ha presentado en una forma intermitente, sin embargo muestra en varios momentos del día durante 3 semanas aproximadamente. La primera semana en que el problema apareció, fue de una manera un tanto irregular y esporádica, ya que para la segunda y tercera semana los síntomas se expusieron de una manera constante. Durante esos días se revisó constantemente la configuración y estado físico del switch y los puertos de alimentación sin que existieran esos problemas, por lo que se hacía suponer que el problema era interno. En vista de lo acontecido, el siguiente paso fue la instalación de un analizador de tráfico dentro de las instalaciones del Instituto de Geofísica.

4.- Instalación de un analizador de tráfico en el Instituto de Geofísica.

Una vez que no se detectaba la causa real del problema que provocaba la lentitud en la red del Instituto de Geofísica, entonces fue necesaria la instalación de una consola que capturara el tráfico de la red del Instituto, tal consola se administra y se observan los resultados remotamente, ya que cuenta con un software que lee el tráfico capturado de una dirección IP configurada en la consola.

La consola fue instalada en diferentes puntos de la red del Instituto, esta consola fue alternada de lugar aproximadamente cada tercer día para observar si el problema era de algún Departamento en particular o estaba presente a lo largo de toda la red.

El software que acompaña a la consola se le conoce como Sniffer. El Sniffer se encarga de mostrar los resultados que están siendo capturados en línea y posteriormente si los archivos generados (archivos con extensión enc) son almacenados, para una vista posterior. Adicionalmente se cuenta con otro software llamado Reporter que es más completo y genera gráficas de los resultados de las estaciones que generan más tráfico, el tipo de protocolos utilizados, etc; el Reporter trabaja con otro tipo de archivos cuya extensión es csv, que deben ser procesados al ser colocados en una base de datos SQL

La consola permaneció analizando el tráfico durante y después de que se presentó el problema y los resultados arrojados son los siguientes.

Con la ayuda del Sniffer se observó que la red no generaba una considerable cantidad de errores ni colisiones dado la cantidad de frames que se estaban transmitiendo durante el intervalo del análisis, con lo que se descarto posibles errores físicos tales como fallas en el cableado o tarjetas de red dañadas. Muestra de ello es la siguiente imagen:

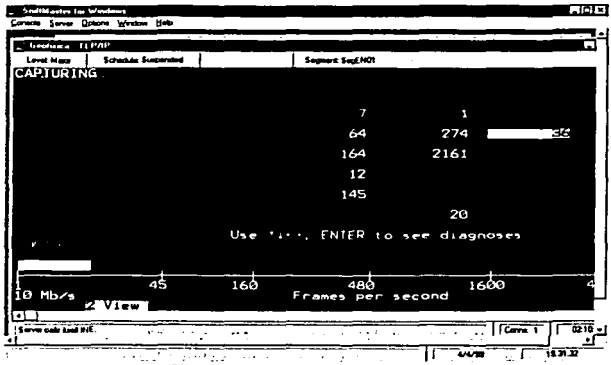


Figura 4.5 Resultados de la consola.

Como se observa, el analizador sólo esta detectando 13 colisiones de un total de 77,615 paquetes que han viajado a través de la red. Se han detectado 64 conexiones hacia dentro y fuera del Instituto, 164 estaciones de red de la cual se observan 2,161 síntomas (aplicaciones e intercambio de información que han sido detectadas entre las estaciones detectadas). En la *figura 4.6*, se muestra que durante la segunda captura de tráfico no existieron colisiones de un total de 2,389 paquetes que viajaron por la red en el instante de la captura. Por lo tanto se asegura que el problema de la lentitud de la red no es causado por problemas físicos descritos anteriormente, por lo que es necesario prosegir a una segunda etapa del análisis con el Sniffer.

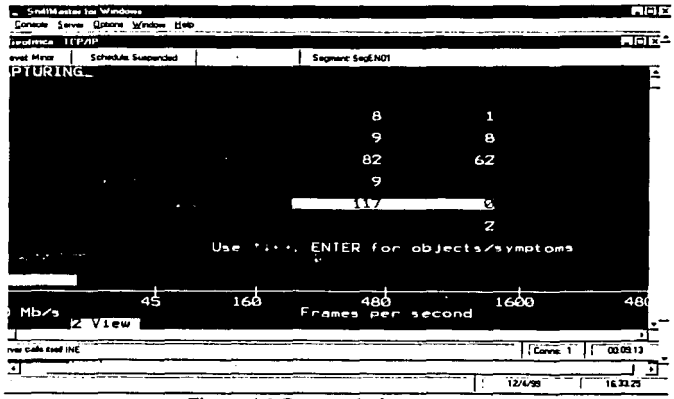


Figura 4.6 Captura de datos.

Con los archivos generados por el Sniffer se recrearan en otra herramienta llamada Reporter, en la que se observo que las estaciones que más generaban tráfico eran las pertenecientes al segmento de Sismología, las gráficas obtenidas con esta herramienta se muestran a continuación.

Estaciones con más actividad por cantidad de frames, *figura 4.7.*

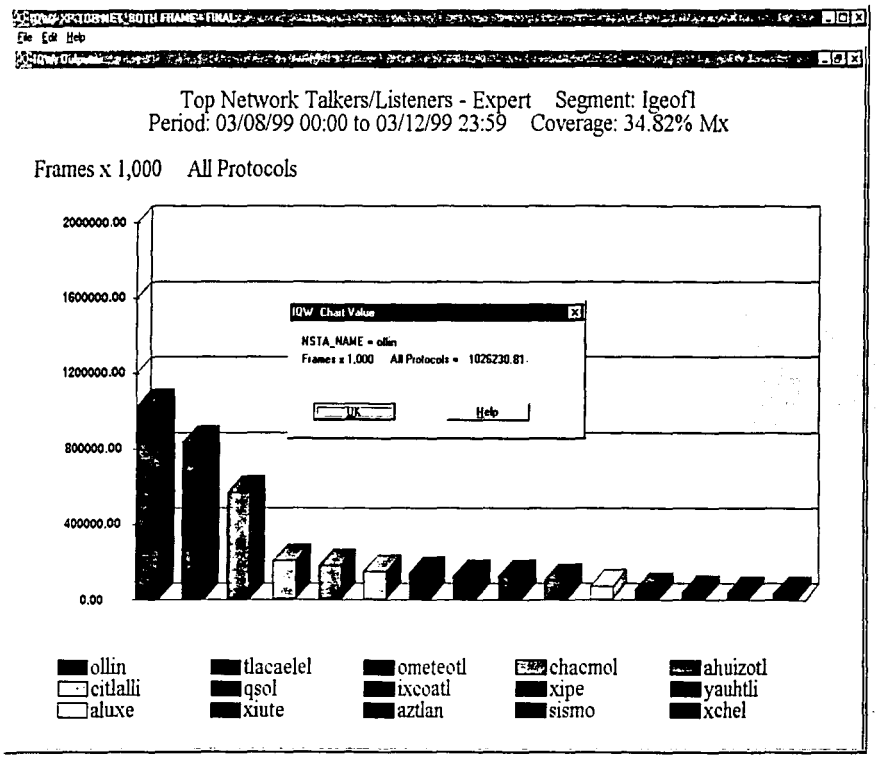


Figura 4.7 Estaciones por cantidad de frames.

Estaciones con más actividad por cantidad de bytes, *figura 4.8.*

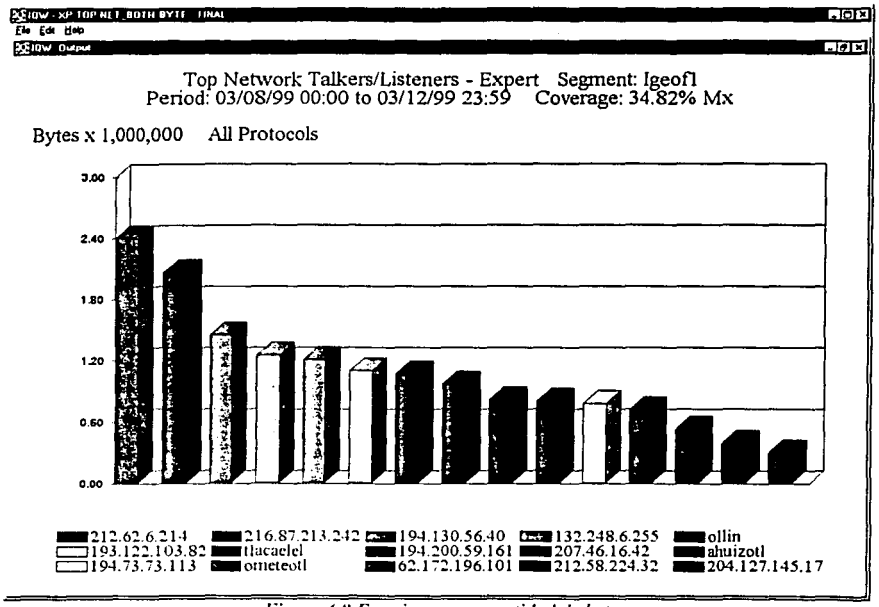


Figura 4.8 Estaciones por cantidad de bytes.

Las estaciones con host: ollin, tlacaelel y ometeotl, son quienes reciben y envían la mayor cantidad de frames y por ende de bytes. Al analizar las aplicaciones que se ejecutan en las estaciones, se tiene que tanto ellas como la mayoría de las estaciones del departamento de Sismología cuentan con el servicio NIS (Network Information System), el cual provoca un tráfico innecesario de frames entre las estaciones que comparten tal servicio, por lo que se recomendó quitar este e instalar lo más pronto posible NIS PLUS, que es mejor en cuanto reglas de intercambio de datos que su versión anterior.

Al continuar el monitoreo con el MRTG, se advierte una imperceptible disminución en el porcentaje de tráfico de la red interna del Instituto, por lo que se continuo con el análisis.

Cabe destacar que durante el análisis, se percibió como estaba la distribución de los protocolos de acuerdo al ancho de banda que esta siendo utilizado en esos instantes. Como se ve a continuación en la *figura 4.9*, aún existían altos porcentajes de utilización del ancho de banda del Instituto.

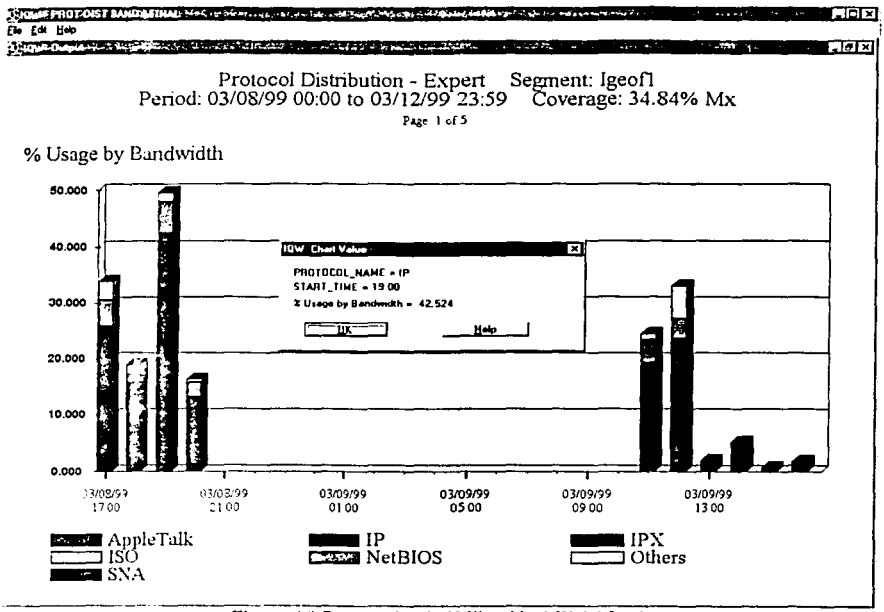
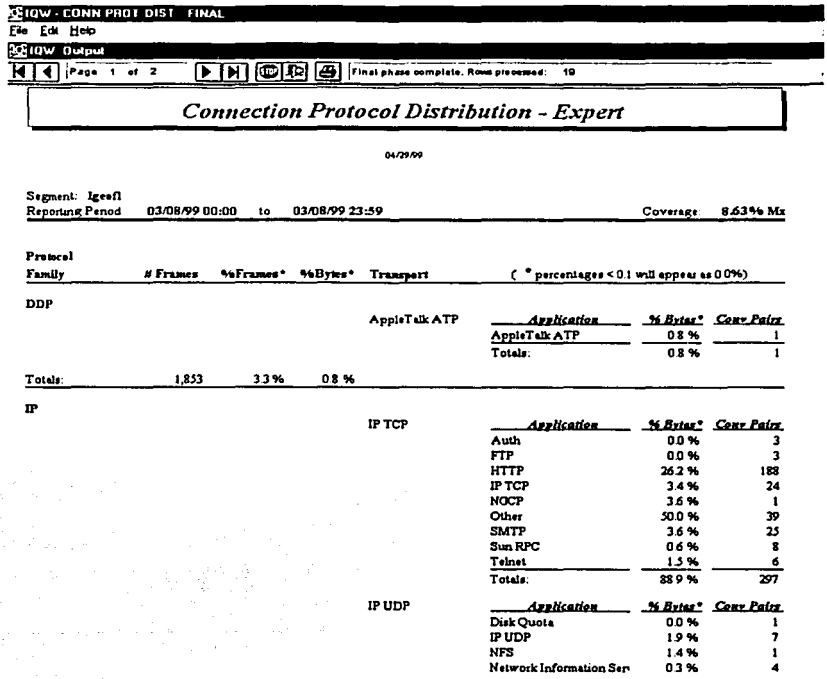


Figura 4.9 Porcentajes de Utilización BW del Instituto

De acuerdo a la figura anterior, aún existen ráfagas altas de utilización de red correspondiente a un 50 % del ancho de banda disponible, de lo cual también se observa que aproximadamente el 80 % de todo el tráfico de la red corresponde a tráfico IP en sus distintos protocolos, IPX en un 10 % del total y el restante se reparte entre AppleTalk, NetBIOS y otros protocolos.

Ahora bien, como se puede leer en la *figura 4.10*, dentro del tráfico IP el 50 % del total se le atribuye a protocolos no identificados por el Reporter, un 26.2 % de tráfico HTTP y SMTP (Simple Mail Tranfer Protocol) de un 3.6%, entre otros.



IQW - CONN PROT DIST FINAL
File Edit Help
IQW Output
Page 1 of 2
Final phase complete. Rows processed: 19

Connection Protocol Distribution - Expert

04/29/99

Segment: lgeafl
Reporting Period 03/08/99 00:00 to 03/08/99 23:59 Coverage: 8.63% Mx

Protocol Family	# Frames	%Frames*	%Bytes*	Transport	(* percentages < 0.1 will appear as 0.0%)		
DDP							
				AppleTalk ATP	Application	% Bytes*	Conv Pairs
					AppleTalk ATP	0.8 %	1
					Totals:	0.8 %	1
Totals:	1,853	3.3%	0.8 %				
IP							
				IP TCP	Application	% Bytes*	Conv Pairs
					Auth	0.0 %	3
					FTP	0.0 %	3
					HTTP	26.2 %	188
					IP TCP	3.4 %	24
					NCCP	3.6 %	1
					Other	50.0 %	39
					SMTP	3.6 %	25
					Sun RPC	0.6 %	8
					Telnet	1.5 %	6
					Totals:	88.9 %	297
				IP UDP	Application	% Bytes*	Conv Pairs
					Disk Quota	0.0 %	1
					IP UDP	1.9 %	7
					NFS	1.4 %	1
					Network Information Ser	0.3 %	4

Figura 4.10 Tráfico IP.

Con el Sniffer se logró ver una gran cantidad de protocolo ICMP (Internet Control Message Protocol) que es el protocolo encargado de, entre otras cosas, informar de errores y problemas en la red *ver figura 4.11*. Esta forma de Ataque ICMP-Ping en una de la formas de lo que se llama NUKE, es decir, la caída de una conexión TCP/IP por un agente externo.

El Ataque ICMP, consiste en enviar al cliente o al servidor un paquete ICMP indicando que la conexión no puede continuar debido a uno de los siguientes errores:

- Red inalcanzable.
- Host inalcanzable.
- Protocolo incorrecto.
- Puerto incorrecto.

Es decir, el agente "enemigo" envía paquetes al cliente diciéndole que el servidor tiene alguno de los problemas anteriores, o viceversa. En realidad las cosas son un poco más complicadas, ya que el ataque debe acertar con los puertos que están utilizando en esa conexión en particular.

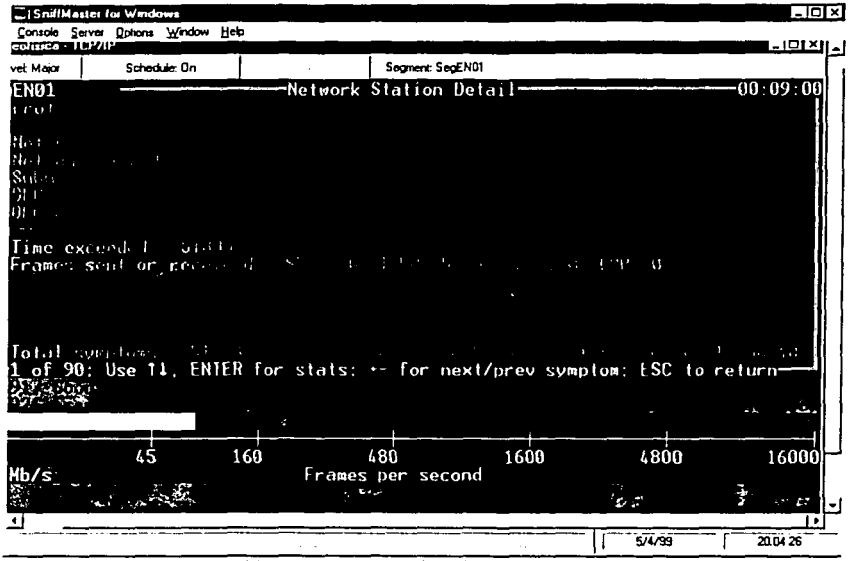


Figura 4.11.- Detección del ataque NUKE.

Existe una variedad del Ataque Ping, que resulta impresionante, llamado "SMURFING", que consiste en enviar un ICMP a la dirección de broadcast (aunque a cualquier otra dirección causa un efecto similar) de toda una subred, poniendo de remitente el sistema que se quiere atacar. Las consecuencias son que todas las direcciones de esa subred contestan a la petición de broadcast, de manera que la red se satura en esos momentos. Otra forma de ataque es hacer un ping a cualquier dirección del segmento, aumentando el número de bytes que por default maneja el ping.

Una vez detectado el problema e identificada la dirección IP causante del problema, se procedió a filtrar la dirección que originaba estas peticiones con una herramienta llamada Filter Builder *figura 4.12,* de manera que se impidió la comunicación de los segmentos del Instituto con este destino.

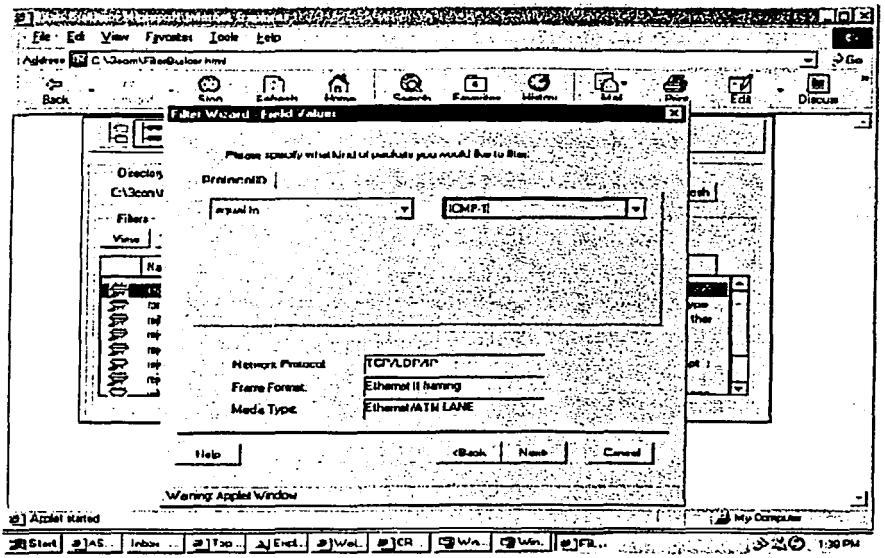


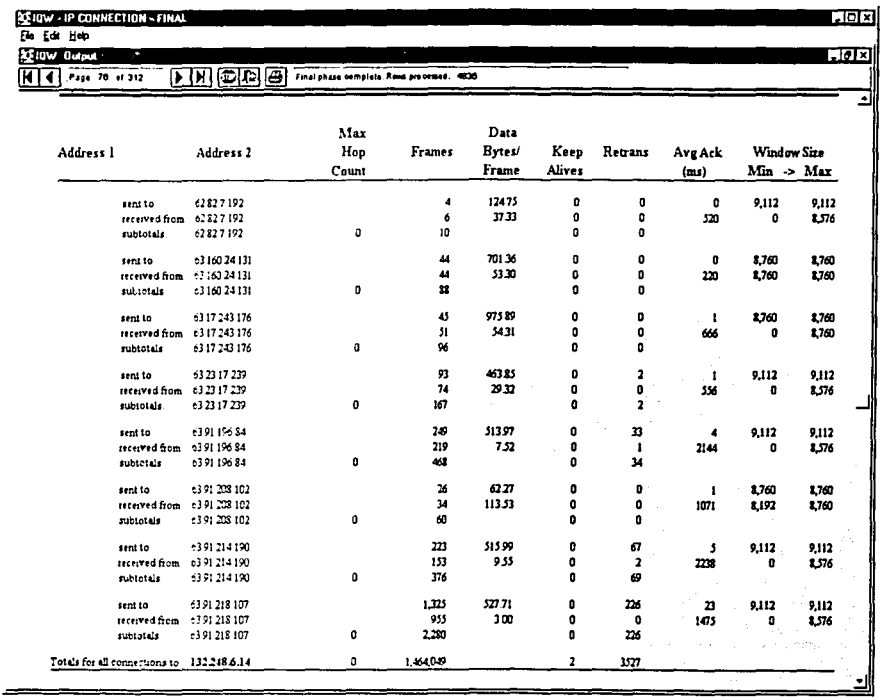
Figura 4.7.- Herramienta utilizada para filtrar el tráfico ICMP

Al continuar con el análisis mediante el MRTG se observó una disminución considerable del tráfico de la red así como una mejoría importante en el desempeño interno y al exterior de los segmentos del Instituto.

El análisis del desempeño de la red se continuo unos días más para estar seguros que el problema estaba resuelto. Durante dicho tiempo se observó que las estaciones Ollin (132.248.6.21), Tlacaelel (132.248.6.14) y Ometeotl (132.248.6.43) seguían generando un trafico excesivo entre ellas 3 y en ocasiones con estaciones como Ahuizotl (132.248.6.119), dicho tráfico comparado con el generado por el servidor de correo principal (Tonatiuh-132.248.6.20) era un tanto anormal por lo que se sugirió una reestructuración no solo del segmento de Sismología, si no del Instituto por completo, ya que este aún contaba con demasiados segmentos en coaxial.

A continuación se presentan gráficas donde se compara la cantidad de tráfico generada por estas estaciones:

Tlacaelel 132.248.6.14


IQW - IP CONNECTION - FINAL

File Edit Help

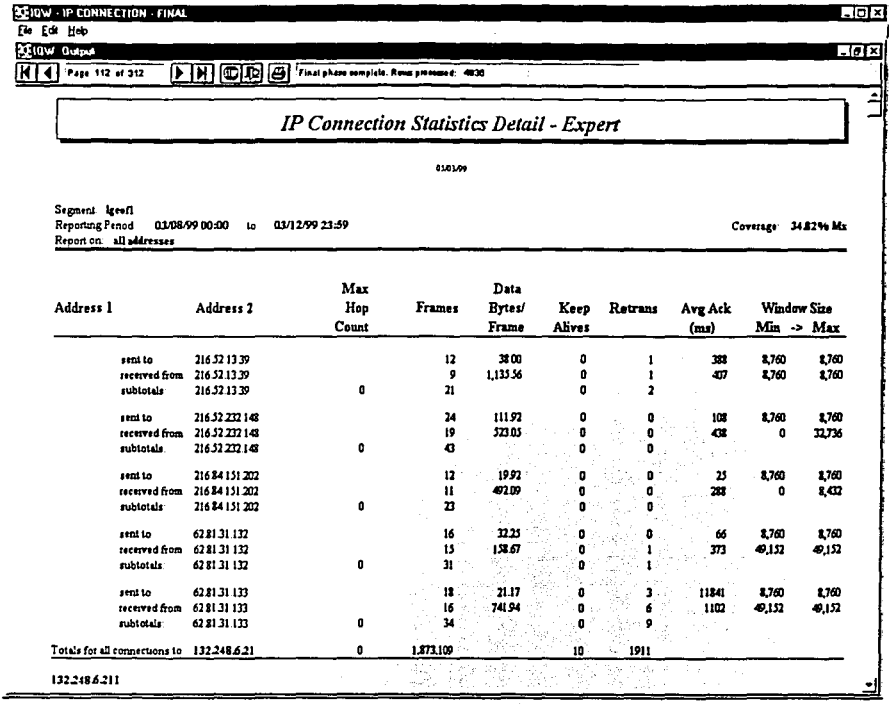
IQW Output

Page 76 of 312 — Final phase complete. Rows processed: 4836

Address 1	Address 2	Max Hop Count	Frames	Data Bytes/ Frame	Keep Alives	Retrans	Avg Ack (ms)	Window Size Min -> Max
sent to	62 82 7 192		4	124 75	0	0	0	9,112 9,112
received from	62 82 7 192		6	37 33	0	0	520	0 8,576
subtotals	62 82 7 192	0	10		0	0		
sent to	63 160 24 131		44	701 36	0	0	0	8,760 8,760
received from	63 160 24 131		44	53 30	0	0	220	8,760 8,760
subtotals	63 160 24 131	0	88		0	0		
sent to	63 17 243 176		45	975 89	0	0	1	8,760 8,760
received from	63 17 243 176		51	54 31	0	0	666	0 8,760
subtotals	63 17 243 176	0	96		0	0		
sent to	63 23 17 239		93	463 85	0	2	1	9,112 9,112
received from	63 23 17 239		74	29 32	0	0	556	0 8,576
subtotals	63 23 17 239	0	167		0	2		
sent to	63 91 196 84		249	513 97	0	33	4	9,112 9,112
received from	63 91 196 84		219	7 52	0	1	2144	0 8,576
subtotals	63 91 196 84	0	468		0	34		
sent to	63 91 208 102		26	62 27	0	0	1	8,760 8,760
received from	63 91 208 102		34	113 53	0	0	1071	8,192 8,760
subtotals	63 91 208 102	0	60		0	0		
sent to	63 91 214 190		223	515 99	0	67	5	9,112 9,112
received from	63 91 214 190		153	9 55	0	2	2238	0 8,576
subtotals	63 91 214 190	0	376		0	69		
sent to	63 91 218 107		1,325	527 71	0	226	23	9,112 9,112
received from	63 91 218 107		955	3 00	0	0	1475	0 8,576
subtotals	63 91 218 107	0	2,280		0	226		
Totals for all connections to	132.248.6.14	0	1,464,049		2	3527		

Gráfica 4.1 Tlacaelel.

Ollín: 132.248.6.21



10W - IP CONNECTION - FINAL

File Edit Help

10W Output

Page 112 of 312 — Final phase complete. Rows processed: 4836

IP Connection Statistics Detail - Expert

01/01/99

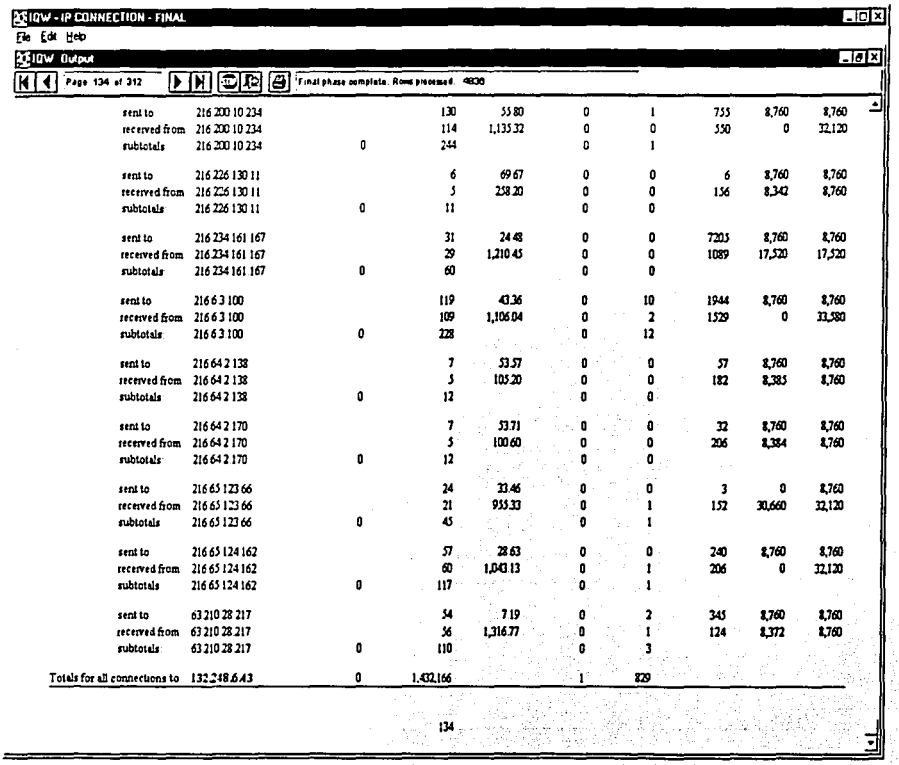
Segment kgeofl
Reporting Period 03/08/99 00:00 to 03/12/99 23:59 Coverage 34.82% Mx
Report on all addresses

Address 1	Address 2	Max Hop Count	Frames	Data Bytes/ Frame	Keep Alives	Retrans	Avg Ack (ms)	Window Size Min -> Max
sent to	216.52.13.39		12	38.00	0	1	388	8,760 8,760
received from	216.52.13.39		9	1,133.56	0	1	477	8,760 8,760
subtotals	216.52.13.39	0	21		0	2		
sent to	216.52.222.148		24	111.92	0	0	108	8,760 8,760
received from	216.52.222.148		19	523.05	0	0	438	0 32,736
subtotals	216.52.222.148	0	43		0	0		
sent to	216.84.151.202		12	19.92	0	0	25	8,760 8,760
received from	216.84.151.202		11	492.09	0	0	288	0 8,432
subtotals	216.84.151.202	0	23		0	0		
sent to	62.81.31.132		16	32.25	0	0	66	8,760 8,760
received from	62.81.31.132		15	158.67	0	1	373	49,152 49,152
subtotals	62.81.31.132	0	31		0	1		
sent to	62.81.31.133		18	21.17	0	3	11841	8,760 8,760
received from	62.81.31.133		16	741.94	0	6	1102	49,152 49,152
subtotals	62.81.31.133	0	34		0	9		
Totals for all connections to	132.248.6.21	0	1,873,109		10	1911		

132.248.6.211

Gráfica 4.2. Ollín.

Ometeotl: 132.248.6.43



IQW - IP CONNECTION - FINAL

File Edit Help

IQW Output

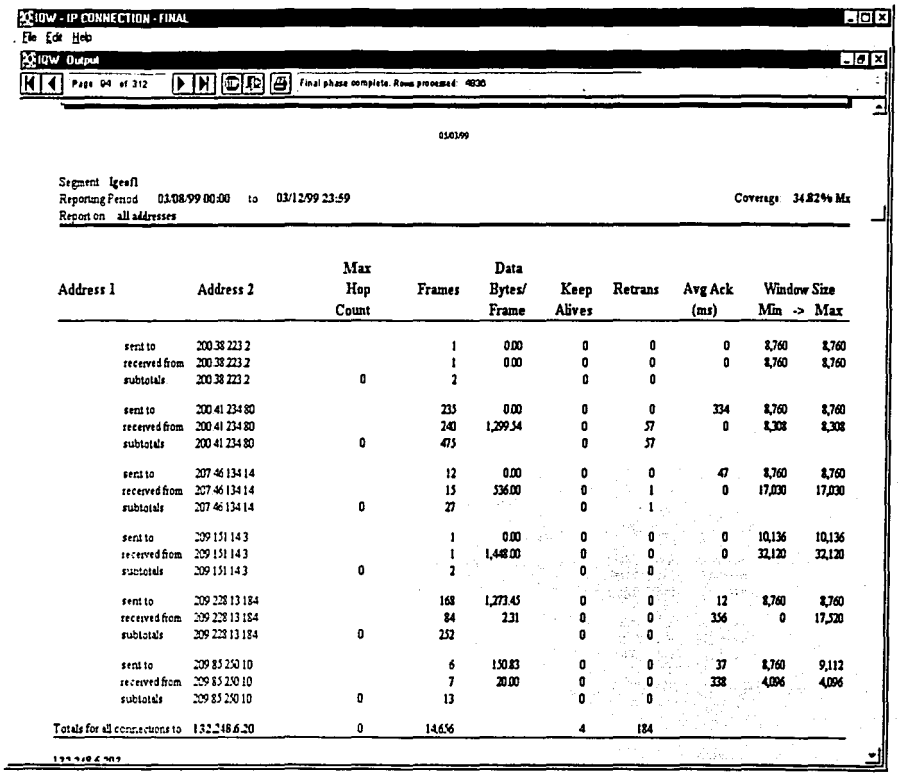
Page 134 of 312 — Final phase complete. Rows processed: 4836

sent to	216 200 10 234		130	55 80	0	1	735	8,760	8,760
received from	216 200 10 234		114	1,135 32	0	0	550	0	32,120
subtotals	216 200 10 234	0	244		0	1			
sent to	216 226 130 11		6	69 67	0	0	6	8,760	8,760
received from	216 226 130 11		5	258 20	0	0	156	8,342	8,760
subtotals	216 226 130 11	0	11		0	0			
sent to	216 234 161 167		31	24 48	0	0	7203	8,760	8,760
received from	216 234 161 167		29	1,210 45	0	0	1089	17,520	17,520
subtotals	216 234 161 167	0	60		0	0			
sent to	216 6 3 100		119	43 36	0	10	1944	8,760	8,760
received from	216 6 3 100		109	1,106 04	0	2	1529	0	33,580
subtotals	216 6 3 100	0	228		0	12			
sent to	216 64 2 138		7	53 57	0	0	57	8,760	8,760
received from	216 64 2 138		5	105 20	0	0	182	8,585	8,760
subtotals	216 64 2 138	0	12		0	0			
sent to	216 64 2 170		7	53 71	0	0	32	8,760	8,760
received from	216 64 2 170		5	100 60	0	0	206	8,384	8,760
subtotals	216 64 2 170	0	12		0	0			
sent to	216 65 123 66		24	33 46	0	0	3	0	8,760
received from	216 65 123 66		21	955 33	0	1	152	30,660	32,120
subtotals	216 65 123 66	0	45		0	1			
sent to	216 65 124 162		57	28 63	0	0	240	8,760	8,760
received from	216 65 124 162		60	1,043 13	0	1	206	0	32,120
subtotals	216 65 124 162	0	117		0	1			
sent to	63 210 28 217		54	7 19	0	2	345	8,760	8,760
received from	63 210 28 217		56	1,316 77	0	1	124	8,372	8,760
subtotals	63 210 28 217	0	110		0	3			
Totals for all connections to	132.248.6.43	0	1,432,166		1	829			

134

Gráfica 4.3 Ometeotl.

Tonatiuh: 132.248.6.20



IQW - IP CONNECTION - FINAL

File Edit Help

IQW Output

Page 94 of 312 — Final phase complete. Rows processed: 4836

01/01/99

Segment lgeofl
Reporting Period 03/08/99 00:00 to 03/12/99 23:59 Coverage 34.82% Mx
Report on all addresses

Address 1	Address 2	Max Hop Count	Frames	Data Bytes/ Frame	Keep Alives	Retrans	Avg Ack (ms)	Window Size Min -> Max
sent to	200.38.223.2		1	0.00	0	0	0	8,760 8,760
received from	200.38.223.2		1	0.00	0	0	0	8,760 8,760
subtotals	200.38.223.2	0	2		0	0		
sent to	200.41.234.80		235	0.00	0	0	334	8,760 8,760
received from	200.41.234.80		240	1,299.54	0	57	0	8,308 8,308
subtotals	200.41.234.80	0	475		0	57		
sent to	207.46.134.14		12	0.00	0	0	47	8,760 8,760
received from	207.46.134.14		15	536.00	0	1	0	17,030 17,030
subtotals	207.46.134.14	0	27		0	1		
sent to	209.151.143		1	0.00	0	0	0	10,136 10,136
received from	209.151.143		1	1,448.00	0	0	0	32,120 32,120
subtotals	209.151.143	0	2		0	0		
sent to	209.228.13.184		168	1,273.45	0	0	12	8,760 8,760
received from	209.228.13.184		84	2.31	0	0	356	0 17,520
subtotals	209.228.13.184	0	252		0	0		
sent to	209.85.250.10		6	150.83	0	0	37	8,760 9,112
received from	209.85.250.10		7	20.00	0	0	338	4,096 4,096
subtotals	209.85.250.10	0	13		0	0		
Totals for all connections to	132.248.6.20	0	1466		4	184		

Gráfica 4.4 Tonatiuh.

Finalmente, para corroborar que el problema ya no esta presente, se procedió a verificar la utilización de ambos segmentos del Instituto con el HP OPEN View *figura 4.13* ; y los resultados fueron los siguientes:

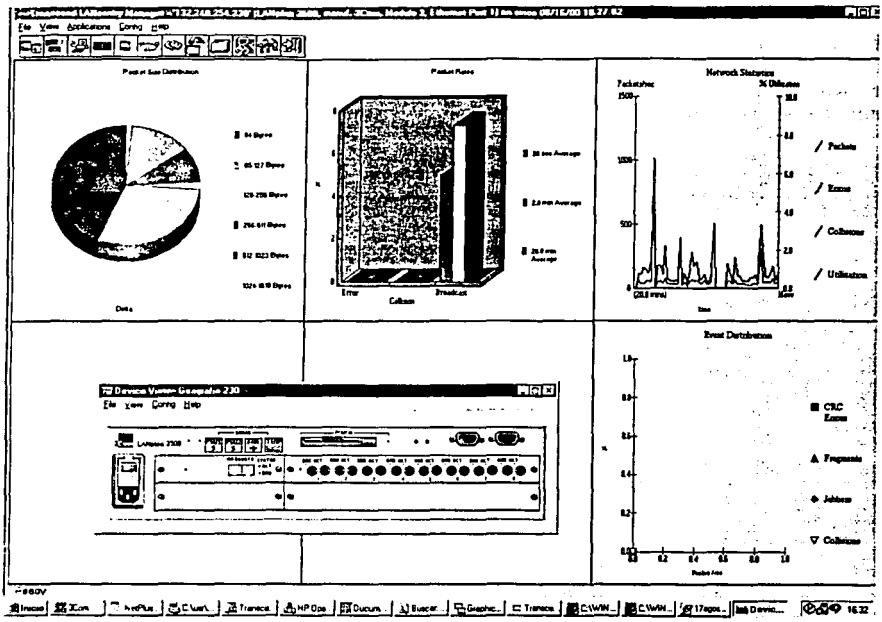


Figura 4.13 Verificación de la utilización puerto1 módulo3.

Como se puede observar, ya los problemas relacionados con la utilización excesiva del ancho de banda de la red del Instituto han quedado atrás. Este tráfico corresponde al medido en el puerto número 1 del módulo 3, que es quién da red al edificio Principal que es quién tiene la mayor cantidad de carga en cuanto a tráfico y equipo de cómputo se refiere. Según se observa, en los 20 minutos del monitoreo existe un pico de 7 % de utilización, sin errores ni colisiones y con ráfagas de broadcast normales debido al tipo de equipos de interconexión que se tienen (hubs).

Las ráfagas de broadcast que están presentes son las que perduran durante 20 segundos y 2 minutos, es decir que no representan problemas graves en el rendimiento de la red.

Para el puerto 5 del módulo 3, conexión al Edificio Nuevo, la utilización del ancho de banda es aún menor que el del puerto 1, debido a que en este edificio la cantidad de equipo de cómputo y tráfico por aplicaciones es menor. De igual manera, para este puerto no existen colisiones ni errores, solo esta presente una ráfaga de broadcast con duración de 2 minutos, lo que no representa problema alguno, *figura 4.14.*

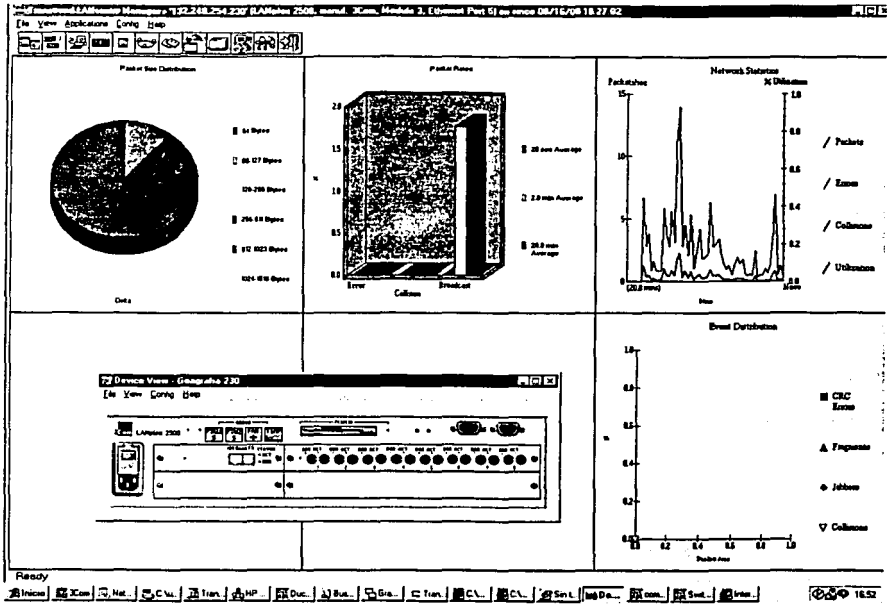


Figura 4.14 Verificación de la utilización puerto5 módulo3.

4.2.- Rediseño de la red de cómputo del Instituto de Geofísica

En el capítulo I Planteamiento y Análisis de la Problemática se mostró brevemente el diseño de la red del Instituto, este estudio se concentró en la manera en que la red se conectaba al backbone de Red-UNAM y en una descripción de la red interna, con el objeto de presentar una primera perspectiva del funcionamiento de esta red. Sin embargo, para comenzar con el rediseño de la red habrá que estudiar más a fondo el funcionamiento de la misma, como se muestra a continuación.

4.2.1.- Estudio del Edificio Principal

Este Edificio es el que concentra la mayor parte de servicios de cómputo y cuenta con 3 pisos. En cada uno de los estos pisos se trato de hacer una división por Departamentos, aunque en realidad muchos de los investigadores están asignados a varios Departamentos, por lo que se hace imposible segmentar los grupos de trabajo mediante VLAN's debido a que dichos investigadores necesitan tener su información disponible desde cualquier punto del Instituto en donde se encuentren.

En el *anexo A* se presentan los croquis de las 3 plantas con que cuenta el Edificio Principal la *figura A1: Planta Baja, la figura A2: Primer Piso y la figura A3: Segundo Piso* y se verá como se ha tratado de dividir los pisos por departamentos, para después presentar como se encuentra distribuida la red de cómputo en cada piso.

4.2.1.1- Edificio Principal: Planta Baja

Como se comentó anteriormente, es en este edificio y en esta planta donde llega el enlace principal de Red-UNAM. La llegada de fibra óptica se localiza en la sala principal del Centro de Cómputo de este Instituto, por lo que los administradores de esta Dependencia tienen el control y seguridad total de este enlace. A continuación se detalla la parte de red de este piso *diagrama 4.1.*

- El primer puerto recibe la fibra óptica de Red-UNAM a través de un transceiver de fibra óptica 10 FL a cable coaxial que esta directamente conectado a un Multiconect (hub de cable coaxial) marca 3Com.

- Del puerto número 2, sale un tramo de cable coaxial al cual se conectan directamente 11 PC's y al final de este tramo se conecta un hub con 18 PC's conectadas a 10/100 en UTP.

- En el puerto 3 hay otro tramo de cable coaxial con 5 PC's conectadas directamente, después esta conectado un hub con 4 PC's conectadas y al final del tramo hay una PC más conectada.

- En el puerto número 4 esta conectado el Servicio Sismológico Nacional (SSN). El tramo consta de una PC conectada al cable coaxial, 18 PC's conectadas a un hub a 10/100 Mbps en UTP y finalmente 10 máquinas más conectadas al cable coaxial.

- En el puerto quinto existe un transceiver de AUI a fibra óptica 10 FL que va al edificio donde se encuentra en Departamento de Física Espacial. Esta fibra es recibida en un transceiver del mismo tipo que esta directamente conectado a otro Multiconect.

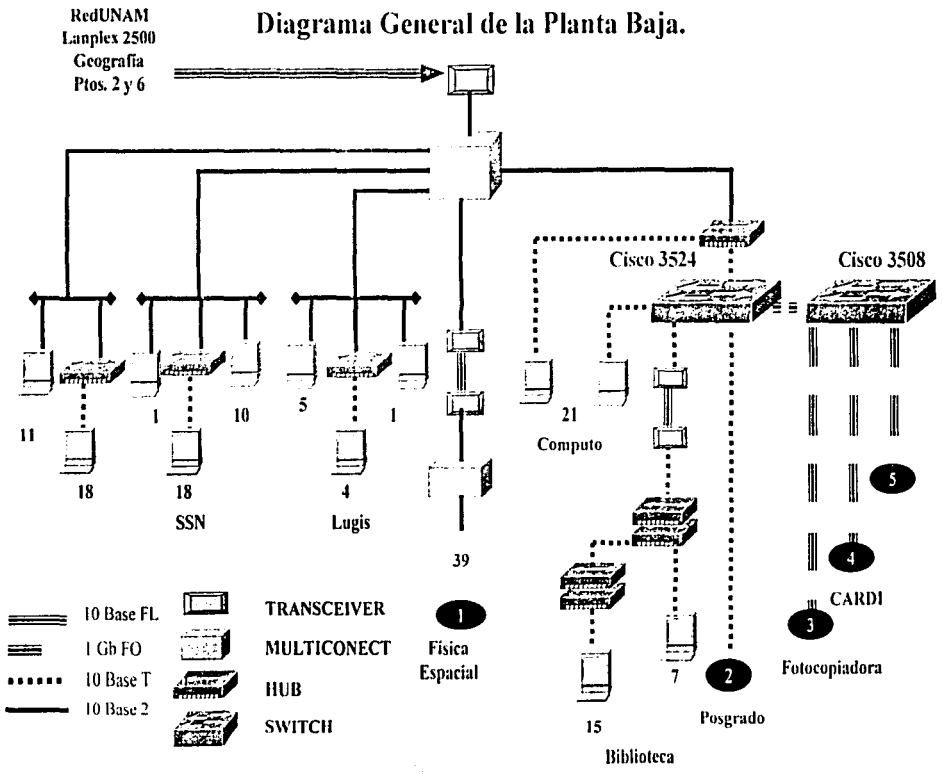


Diagrama 4.1 Edificio Principal Planta Baja.

- Del sexto puerto sale un cable coaxial que se conecta a un hub con un puerto en coaxial y 8 puertos en 10/100 Mbps en UTP. De uno de los puertos UTP se conecta un switch mediante un cable UTP hacia un puerto del mismo tipo; de este switch se alimentan 14 PC's. De este primer switch (2 puertos en Gigabit y 24 puertos a 10/100 Mbps en UTP) se utiliza un puerto en Gigabit para conectar un segundo swicth con 8 puertos en Gigabit, el cual distribuye la comunicación hacia los otros pisos. Como se había mencionado antes, de un puerto del switch se alimenta al edificio donde se ubica la Biblioteca mediante un transceiver de UTP a fibra óptica 10 FL, la cual es recibida en un transceiver del mismo tipo, conectando el UTP a un arreglo de hubs.

4.2.1.2.- Edificio Principal: Primer Piso

En este primer piso llegan 2 fibras ópticas, que a su vez llegan a switches que se encargan de la distribución de la red en el piso. Cada una de ellas se describe a continuación *ver diagrama 4.2*.

- La primera de las fibras ópticas llega a un switch ubicado en el Departamento del CARDI en su puerto en Gigabit, este switch cuenta con 2 puertos en Gigabit y 24 puertos a 10/100 Mbps en UTP. Este switch alimenta a 15 PC's.

- La segunga fibra óptica igualmente llega a un puerto en Gigabit de otro switch (2 puertos en Gigabit y 24 puertos a 10/100 Mbps en UTP) ubicado en el cuarto de la fotocopiadora; de éste solo es utilizado un puerto en UTP que va a un transceiver de UTP a AUI. El puerto AUI esta directamente conectado a un Multiconect. De este hub en coaxial se desprenden otros 4 puertos que alimentan al mismo número de tramos de red, los cuales son:

  - Este primer tramo de cable coaxial alimenta al Departameto de Paleomagnetismo con 5 PC's conectadas directamente al cable coaxial, 5 PC's más conectadas a un hub con un puerto en coaxial y por último, se conectan 11 PC's más conectadas al cable coaxial.

  - El segundo tramo alimenta a otra parte del departamento de Paleomagnetismo y al Departamento de Vulcanología. Las PC's están conectadas de la siguiente manera: 6 PC's conectadas directamente al cable coaxial, 5 PC's alimentadas a través de un hub, 2 PC's también conectadas directamente al coaxial, 4 PC's conectadas a través de otro hub y por último 3 PC's más conectadas directamente al cable coaxial.

  - El tercer tramo alimenta a la Dirección a través de 2 hubs; uno de ellos con 10 puertos UTP utilizados y de él se conecta en cascada otro hub con 18 puertos utilizados.

Diagrama General del Primer Piso.

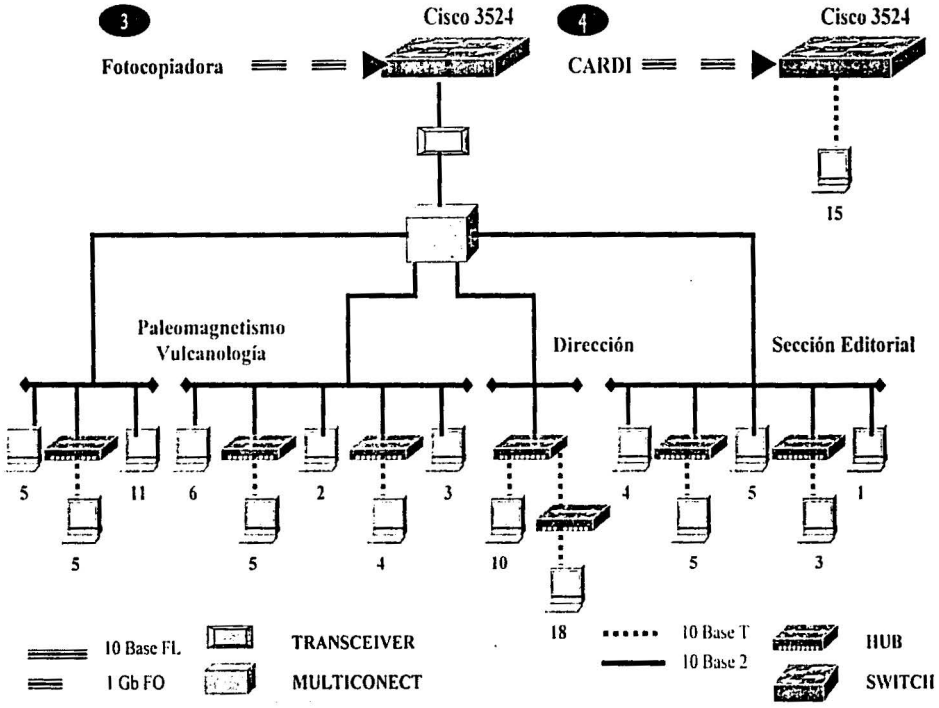


Diagrama 4.2 Edificio Principal Primer Piso.

- El último de los tramos alimenta a la Sección Editorial además de otros cubículos en esa misma área. Este tramo alimenta a 18 Pc's de la siguiente manera: 4 PC's conectadas al coaxial, 5 conectadas a través de un hub, 5 PC's también conectadas al coaxial, 3 más alimentadas por un hub y por último, una PC conectadas directamente al cable coaxial.

4.2.1.3.- Edificio Principal: Segundo Piso

En este piso llega solo una fibra óptica y un cable UTP proveniente de la planta baja que alimenta a un Multiconect *ver diagrama 4.3.*

1. La fibra óptica llega a un switch conectada a uno de los 2 puertos en Gigabit y 24 puertos en UTP a 10/100 Mbps. Este switch alimenta a 15 PC's conectadas directamente y 7 más conectadas a través de un hub conectado en cascada con el switch.

2. El Multiconect ubicado en el Departamento de Posgrado, es alimentado a través de un transceiver de UTP a AUI, el UTP llega de un puerto de switch ubicado en la planta baja. Este Multiconect alimenta a 6 segmentos de red que están distribuidos por todo el segundo piso de la siguiente manera:

   - Los primeros 3 tramos alimentan a los Departamentos de Posgrado y el resto del Departamento de Sismología. El primer tramo esta organizado como sigue: 3 PC's conectadas a través de un hub, 2 PC's alimentadas por otro hub, 5 PC's conectadas directamente al cable coaxial, 3 PC's alimentadas por un hub, 7 PC's conectadas al coaxial, 3 PC's alimentadas por un hub, 3 PC's más conectadas al coaxial, otras 3 PC's alimentadas por otro hub y por último, 3 PC's más conectadas al coaxial.

   - El segundo tramo alimenta solo a 11 PC's de la siguiente manera: 9 PC's alimentadas por un hub y una PC's conectada al coaxial en cada extremo de este tramo.

   - El tercer tramo alimenta a 7 PC's conectadas directamente al cable coaxial.

   - Los siguientes 3 tramos proveen de red al Departamento de Recursos Naturales. El primero de estos tramos alimenta a 8 PC's conectadas al cable coaxial.

   - El segundo tramo de este Departamento tiene 3 PC's conectadas al coaxial, 4 PC's alimentadas a través de un hub, 4 PC's más conectadas al coaxial, 7 Pc's con red a través de otro hub y por último, 4 PC's más conectadas directamente al cable coaxial.

   - El último de los tramos alimenta a 15 PC's conectadas directamente al cable coaxial.

Diagrama General del Segundo Piso.

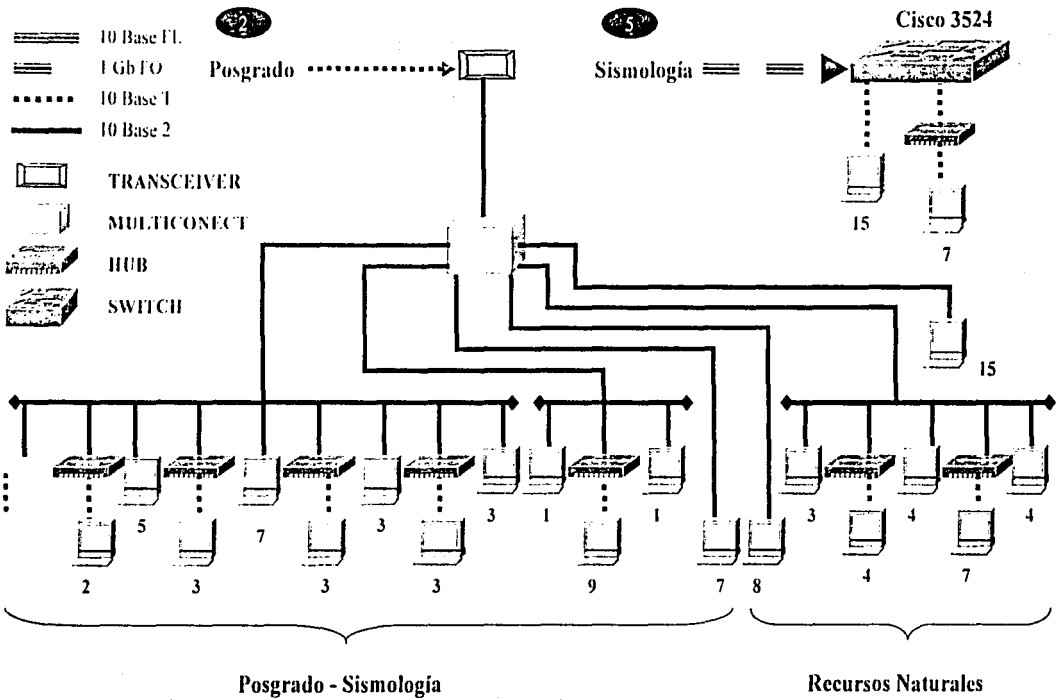


Diagrama 4.3 Edificio Principal Segundo Piso

4.2.2.- Estudio del Edificio II (Departamento de Física Espacial)

En este edificio el Instituto comparte instalaciones con el Instituto de Astronomía, pero no así el segmento de red. El edificio consta de 2 plantas, de las cuales la mitad de la Planta Baja y la mitad del Primer Piso pertenecen al Instituto de Geofísica como se muestra en el *Anexo A en la figura A4.*

Este enlace alimenta a 2 Departamentos: Física Espacial y Radiación Solar. La fibra óptica proveniente de la planta baja del edificio principal, es recibida en un transceiver de fibra óptica 10 FL a AUI que esta directamente conectada a uno de los puertos de un Multiconect. Este hub cuenta con 2 puertos más que están distribuidos de la siguiente manera *ver diagrama 4.4.*

- El primer segmento de cable coaxial alimenta al Departamento de Física Espacial ubicado en el Primer Piso del Edificio II. Este tramo tiene conectadas 4 PC's directamente al coaxial, 8 PC's a través de un hub, 2 PC's más conectadas directamente al cable coaxial, 5 PC's conectadas mediante otro hub y finalmente, 8 PC's conectadas directamente al segmento de coaxial.

- El segundo segmento alimenta al Departamento de Radiación Solar ubicado en la Planta Baja del mismo edificio y alimenta a 12 PC's conectadas directamente al cable coaxial.

4.2.3.- Estudio del Edificio III (Biblioteca)

Al igual que el Edificio II, estas instalaciones también son compartidas con el Centro de Información Científica y Humanística (CICH) y de igual manera, los segmentos de red son independientes. El croquis de las instalaciones se muestra en el *Anexo A en la figura A5.*

La alimentación de Red-UNAM hacia la Biblioteca se da de la siguiente manera: de un puerto a 10/1000 Mbps de UTP se conecta un tramo de UTP que ya hacia un transceiver de UTP a fibra óptica 10 FL, del cual sale una fibra óptica que va a la Biblioteca. La fibra óptica llega aun transceiver de fibra óptica 10 FL a UTP, el cual es conectado a un hub con puertos a 10/100 Mbps en UTP, del cual se desprenden las siguientes conexiones *ver figura 4.5.*

- El hub al que esta conectado al transceiver esta a su vez conectado en stack (apilamiento) a otro hub también con 12 puertos a 10/100 Mbps en UTP. De este arreglo de hubs están alimentadas 7 PC's, un puerto más es utilizado para conectar en cascada otro arreglo de hubs al otra ala de la Biblioteca.

- El segundo arreglo de 2 hubs con 12 puertos a 10/100 Mbps en UTP, también están conectados en stack (apilamiento). De este arreglo se alimentan 15 PC's.

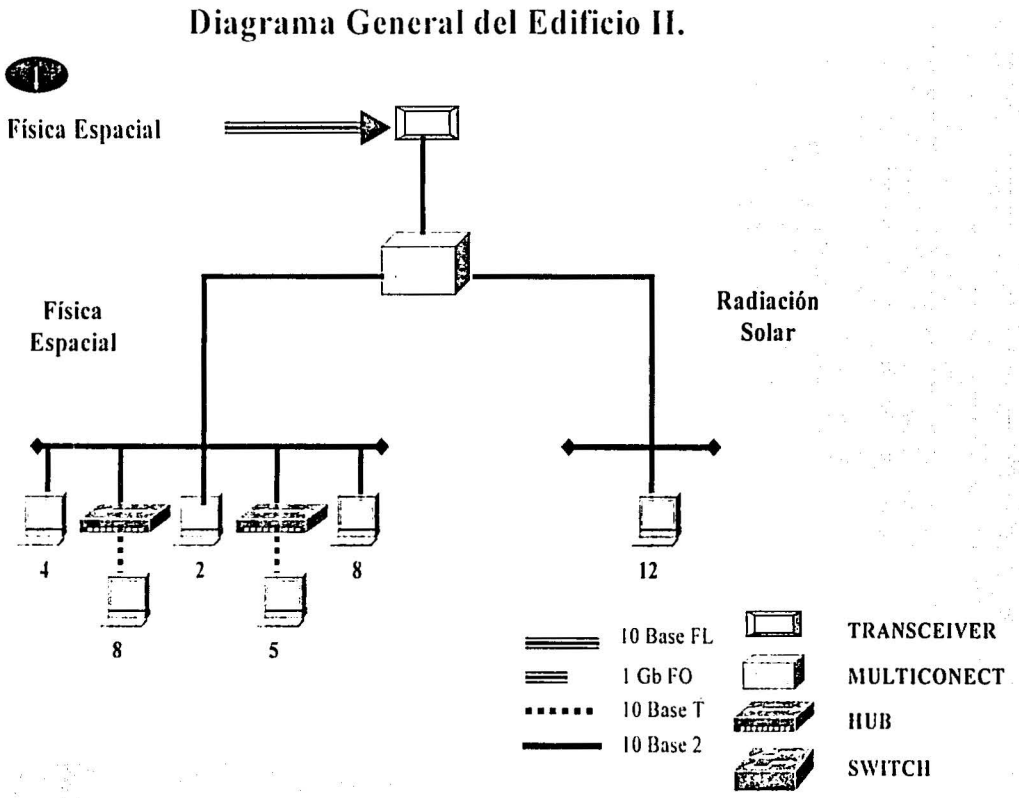


Diagrama 4.4 Edificio II Física Espacial.

Diagrama General Biblioteca.

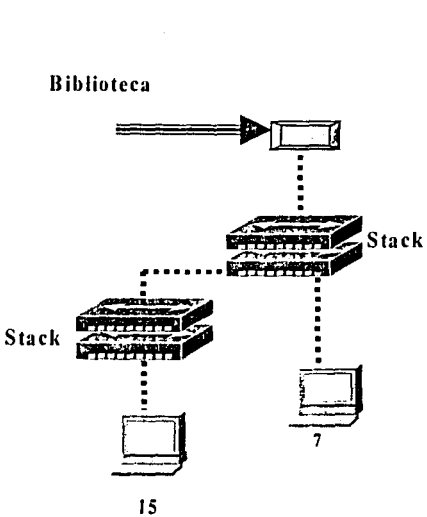
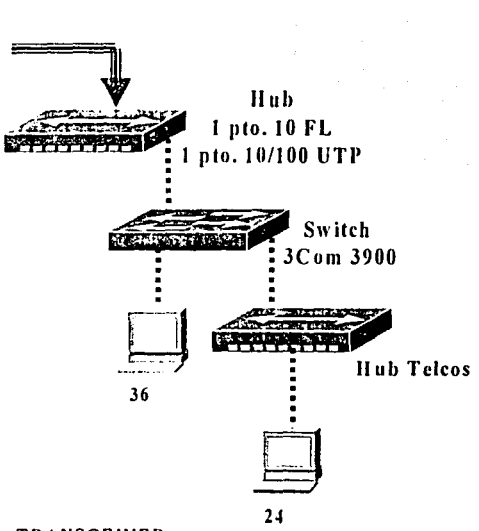


Diagrama 4.5 Edificio III .Biblioteca

Diagrama General Edifico Nuevo Anexo.



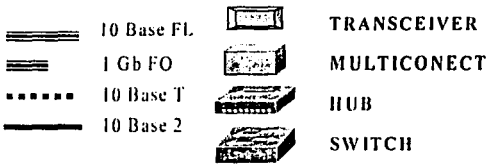


Diagrama 4.6 Edificio IV Anexo.

4.2.4.- Estudio del Edificio IV (Edificio Anexo)

Este edificio se termino a fines del año 2000 y se construyó debido al crecimiento del personal asociado al Instituto.

El segundo enlace de fibra óptica 10 FL en recibido en el Edificio Anexo del Instituto de Geofísica Campus C.U. Como se había mencionado antes, el enlace llega a un hub con un puerto en fibra óptica 10 FL y un puerto en cable par trenzado (UTP); del puerto en UTP sale un cable que se conecta a un switch con 36 puertos a 10/100 Mbps en UTP. En este switch sale un cable que alimenta en cascada a otro hub con 2 puertos en Telcos, que alimenta a 24 computadoras más, *ver diagrama 4.6.*

4.3.- Deficiencias encontradas en la estructura actual de la red de cómputo del Instituto de Geofísica

Una vez que se ha descrito la manera en que se encuentra la red de cómputo en cada uno de los Edificios y pisos que componen el Instituto, es hora de descubrir no solo las deficiencias de la red, sino también los puntos en que esta puede mejorar sin que ello signifique que estaba del todo en un lugar incorrecto.

La descripción de las mejoras que se harán en la red se describirán de manera General y por Edificio y por piso, como se realizó en el momento en que se realizó el estudio de la red de cómputo.

4.3.1.- Deficiencias encontradas en el estudio General del Instituto

Como se puede observar en el Diagrama General de la red de Cómputo del Instituto, las deficiencias encontradas son las siguientes.

Edificio Principal.

Como se había comentado antes, el enlace principal llega a un transceiver que alimenta a un Multiconect (hub de coaxial), y a partir de este la red del Instituto comienza a extenderse sin llevar un orden adecuado, es decir:

- Los switches deben ir como un equipo de Core en la red, sin embargo los hubs son quienes tienen esta función en la red.

- Existe un mal diseño de la red, de modo que un usuario que quiera salir a Internet tendrá que pasar por el hub de la Dirección, el hub del Dpto. de Exploración, el multiconect de la Fotocopiadora, el switch de la copiadora, los 2 switches de cómputo, el hub de cómputo y finalmente por el multiconect principal, es decir, tendrá que pasar por 8 equipos antes de salir a Internet.

- Observando el problema anterior, se concluye que el principal problema de esta red, fuera de que aún cuenta con cable coaxial, es que no hay un verdadero diseño de la red y por lo tanto el crecimiento se hace de una manera descontrolada.

Edificio Anexo.

Aquí el problema es que el enlace principal es recibido en un hub que actúa como tranceiver en lugar de ser recibido en un switch.

Biblioteca.

En realidad este edificio no tiene problemas, considerando que es el único que tiene cableado estructurado, sin embargo sería conveniente cambiar dichos hubs por switches.

La estructura general de la red del Instituto se muestra en el *diagrama 4.7.*

4.3.2.- Deficiencias encontradas en el estudio del Edificio Principal

Como se ha venido observando, este Edificio es quién concentra aproximadamente el 80 % de la utilización del ancho de banda asignado al Instituto, por lo que el adecuado funcionamiento de los principales equipos de interconexión de redes para este Instituto, implica que la información e investigaciones generadas aquí brinden los resultados esperados a la Universidad.

El enlace de Red-UNAM es recibido en la Planta Baja de este Instituto por lo que el funcionamiento adecuado de este enlace repercutirá en el resto de la red de esta Dependencia.

4.3.2.1- Deficiencias encontradas en el estudio de la Planta Baja del Edificio Principal

Las deficiencias encontradas en este piso se irán describiendo de acuerdo como se vaya bajando a través de la red.

a) El enlace principal de Red-UNAM llega primero a un transceiver de fibra óptica a AUI, para luego conectarse directamente al Multiconect (hub de coaxial). Una conexión más adecuada sería conectar el enlace principal al switch que se encuentra en el Centro de Cómputo. El hub es un medio compartido por lo que el aseguramiento del mismo ancho de banda para todos los puertos del switch son una mejor opción.

b) Es obvio que al observar la anterior deficiencia, el switch debería estar en los más alto del esquema de esta red

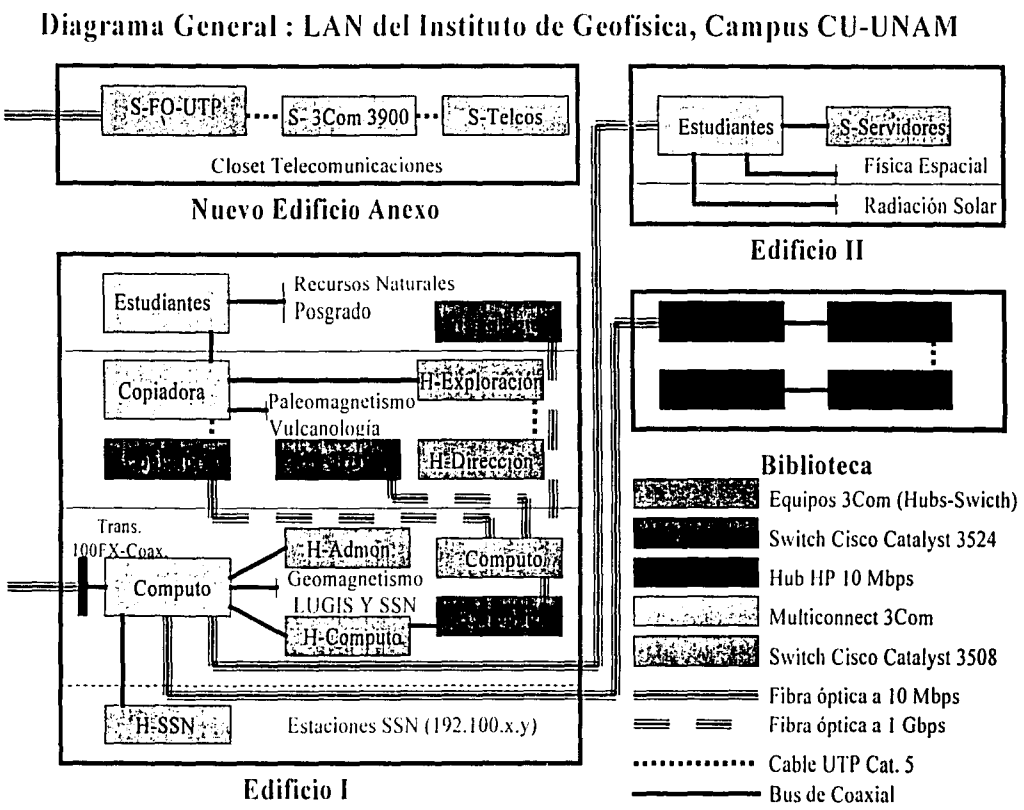


Diagrama 4.7 Estructura General del Instituto de Geofísica

c) La otra deficiencia importante en esta red, que es quién hace que la misma no pueda crecer y que tenga repetidas deficiencias, es que la red aún cuenta con demasiados segmentos de red en cable coaxial. Esta característica impide la instalación de una red switcheada, por lo que el segundo paso para el rediseño de esta red será el cambiar el cableado de esta red, de cable coaxial a cable UTP en el escritorio y de fibra óptica en el backbone de la red de este Instituto.

d) Un error más que se observa, es que existen cubículos donde existe solo un punto de conexión a la red y, cada investigador instala hubs sin previa supervisión de los administradores de la red; por lo que en el rediseño se habrán de considerar la instalación de puntos adicionales de red donde así se requiera.

e) El enlace que va hacia el departamento de Física Espacial, de igual manera presenta deficiencias ya que este se realiza de una conexión en cable coaxial a un transceiver de fibra óptica para luego ser recibido por otro transceiver para ser conectado a otro Multiconect. Si consideramos que cada transceiver tiene la misma deficiencia de un hub (medio compartido), el enlace hacia este departamento ya esta excediendo los 4 hubs permitidos por las reglas de cableado estructurado.

4.3.2.2- Deficiencias encontradas en el estudio del Primer Piso del Edificio Principal

En este Primer Piso las deficiencias encontradas son las siguientes:

a) A pesar de que en éste piso se encuentran 2 switches que segmentan el tráfico en este piso, hay un de ellos del que se conecta un Multiconect que contiene demasiada carga. Esta carga no puede ser repartida en el switch hasta el momento de que se cambie el cableado de coaxial a UTP.

b) Un segundo punto, es que existen PC´s que requieren un ancho de banda reservado para que puedan correr mejor y que a su vez no disminuya el rendimiento en el intercambio de información.

4.3.2.3- Deficiencias encontradas en el estudio del Segundo Piso del Edificio Principal

En este piso se observan más problemas que en el anterior.

a) El Multiconect de este piso muestra una muy excesiva sobrecarga de tráfico en cada uno de sus puertos. A pesar de que uno de estos departamentos cuenta con un switch, no es posible el interconectar otros departamentos y/o segmentos de red debido a las características de la construcción y a la independencia de los diferentes departamentos.

b) Al igual que en los pisos estudiados, el principal problema es que aún existe un exceso de red interconectada con cable coaxial lo que impide el crecimiento de la red.

c) Un síntoma más que se repite, es que los servicios no están etiquetados y por lo tanto es muy difícil poder encontrar rápidamente el origen de los problemas.

4.3.3.- Deficiencias encontradas en el Estudio del Edificio II (Departamento de Física Espacial)

Este edificio presenta los mismos síntomas que ocurren en todo el Instituto, es decir:

a) Aunque el Multiconect tiene una carga de tráfico adecuada, el hub no es la mejor opción para ser el equipo principal de interconexión para el edificio.

b) Aunque el cable coaxial en esos momentos no era causa de problemas, si era necesario el sustituirlo para poder migrar la red hacia tecnología Fast Ethernet y Gigabit Ethernet.

4.3.4.-Deficiencias encontradas en el Estudio del Edificio III (Biblioteca)

Este es un caso especial, ya que este parte del Instituto es quién cuenta con cableado reestructurado, sin embargo a pesar de ello, hay una recomendación que hacer.

A pesar de que los hubs están en un arreglo de stack (operativamente se ven estos equipos como un solo), lo recomendable es que estos equipo fueran sustituidos por switches para que cada uno de los hosts conectados a estos puertos tuviesen garantizado su ancho de banda, que es una característica propia de los switches.

4.3.5.-Deficiencias encontradas en el Estudio del Edificio IV (Anexo)

A pesar de que este edificio fue el último en el cual se instaló la red, este presenta deficiencias.

El enlace de Red-UNAM para este edificio se recibe en un hub que solo hace la función de cambiador de medio (fibra óptica a UTP) y a partir de él se conecta un switch y después un hub de telcos. La óptimo sería que el enlace en fibra se recibiera directamente en un switch y los servicios a los hosts se repartieran de la misma fuente.

4.4.- Propuesta de rediseño del Backbone de Red-UNAM

El rediseño del backbone de Red-UNAM se da debido a las crecientes necesidades de correr diferentes aplicaciones que requieren cada vez más un mayor ancho de banda. Las nuevas aplicaciones que necesitan correr las diferentes dependencias tienen como base la tecnología sobre Internet 2 e Ipv6, es decir, implica un mayor ancho de banda entre las conexiones entre las diferentes dependencias ya que estas aplicaciones cada vez necesitan más del trabajo interdiciplinario de los diferentes investigadores en la Universidad.

Cabe destacar que este rediseño se realizará paulativamente, ya que se necesita la participación de las diferentes Dependencias para poder cambiar el equipo de interconexión adecuado. En resumen, el rediseño consistirá en los siguientes cambios:

- La delta redundante que es el backbone de Red-UNAM que interconecta equipos Passport de Nortel Networks con tecnología ATM quedará intacta. Cada uno de estos equipos se encuentran en los sites de DGSCA, IIMAS y Zona Cultural. El ancho de banda con la que se interconectan estos equipos son mediante enlaces tipo OC-3 (155 Mbps). Esta delta se mantendrá para brindar los servicios de voz, multimedia y videoconferencia , ya que mediante ATM se pude ofrecer QoS (calidad de servicio) a estos servicios.

- Los equipos directamente conectados a cada uno de los Passport (Cellplex 7000 de 3Com con protocolo LAN Emulation) serán cambiados paulativamente, con el objeto de sustituirlos por equipos capaces de manejar tecnología Ethernet, Fast Ethernet, Gigabit Ethernet y con la capacidad de llegar a soportar 10 Gigabit Ethernet. La velocidad de interconexión entre los Passport y los nuevos equipos de capa 3 será igualmente mediante enlaces OC-3 y estos equipos a su vez repartirán el enlace hacia otros equipos mediante tecnología Ethernet a velocidades de 10, 100, 1,000 y 10,000 Mbps .

- Cada uno de los equipos de Core que sustituirán a los Cellplex alimentará a otros switches capa 3, algunos puertos alimentarán directamente a algunas dependencias y otros se conectarán a equipos de distribución.

- Los Lanplex 2500 que servían de equipos de distribución serán cambiados por equipos también de capa 3 con un menor cantidad de puertos que los equipos de Core. Como estos equipos no soportan conexiones 10 Base FL, momentaneamente tendrán conectados los Lanplex 2500 y 3500, a las Dependencias que tarden en reestructurar sus redes locales a tecnología Fast Ethernet.

Como se había comentado, este rediseño se realizará paulativamente y la primera etapa consistirá en cambiar los 4 equipos que sustituirán a los Cellplex en los nodos de DGSCA, IIMAS, Zona Cultural y Arquitectura. Así mismo, en esta primera etapa se cambiarán los equipos de distribución en los sites donde existan dependencias cuyas aplicaciones y consumo de ancho de banda lo requieran.

Otro cambio importante, es que la LAN de Red-UNAM dejará de ser una red switcheada y pasará a ser una red ruteada, ello con el objeto de acelerar el intercambio de información entre la dependencias y el tiempo en que se resuelve el destino de dicha información. El protocolo de ruteo que se tenía en la red era IGRP y el objetivo en pasar a OSPF, debido a sus características y a que no es un protocolo de ruteo propietario.

El esquema general de los cambios en el Backbone de Red-UNAM se muestra en el *diagrama4.8*.

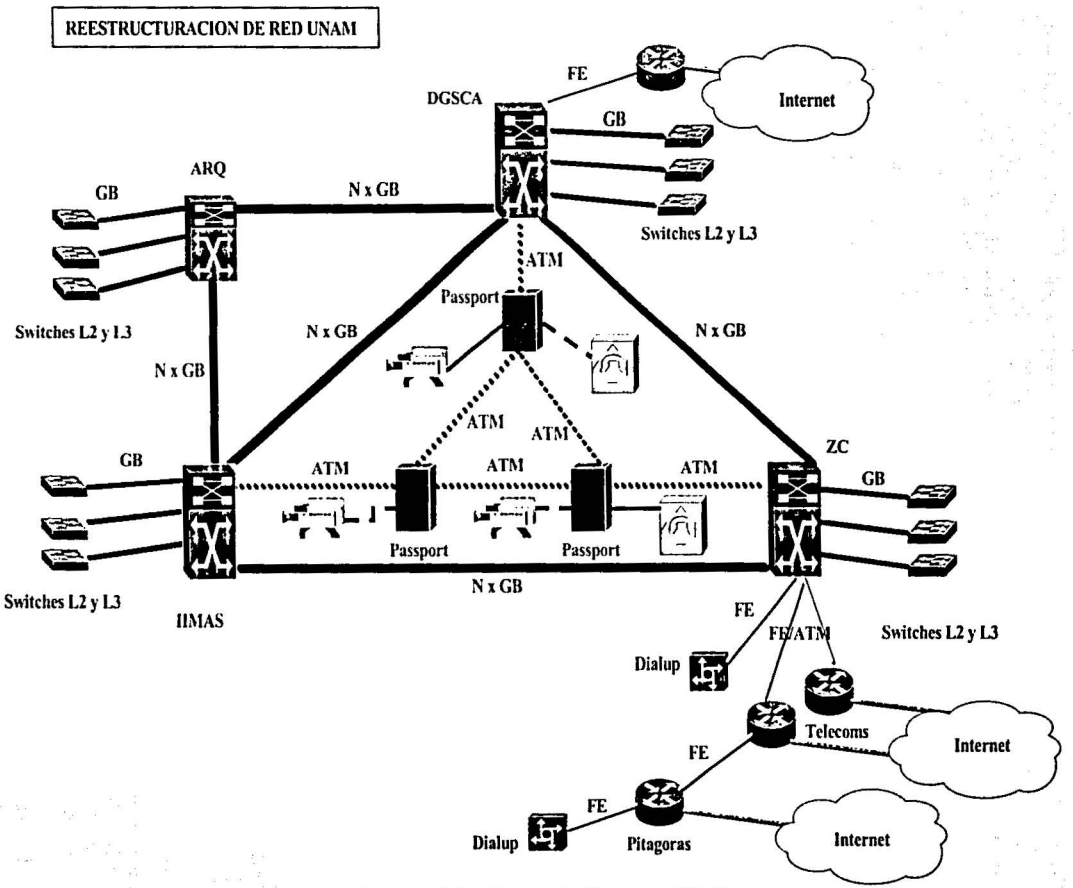


Diagrama 4.8 Cambios en el Backbone de RedUNAM.

4.5.- Propuesta Inmediata

Una vez que se ha realizado tanto el estudio de la red y se han identificado las deficiencias encontradas en su diseño actual, ahora se procederá a describir las mejoras paulatinas que se fueron recomendando para esta red según se iba avanzando en su análisis. La presentación de esta propuesta se realizará siguiendo la forma que se tomo al describir el estudio y las deficiencias; es decir, se irá pasando por edificio y por cada uno de los pisos que componen este Instituto.

4.5.1.- Propuesta para el Edificio Principal

Como se ha venido comentado a lo largo del desarrollo de este capítulo, del enlace que se encuentra en la Planta Baja de este edificio depende la mayor parte del tráfico que se presenta en el Instituto, por lo que una mejora en la forma de interconexión de los equipos repercutirá en un mejor rendimiento del ancho de banda asignado.

Propuesta para la Planta Baja.

a) El principal punto fue el eliminar el Multiconect en la parte más alta de la red, en lugar de ello se recomendó la compra e instalación de un transceiver de fibra óptica a cable UTP, para poder conectar inmediatamente después el switch Cisco Catalyst 3524 que ya se tenía. El Multiconect y los segmentos que dependían de él quedaron conectados a un puerto del switch mientras se cambiaba el cable coaxial de esos segmentos por cable UTP. De igual manera se recomendó la compra e instalación de un transceiver más de fibra óptica a UTP, para poder conectar directamente el segmento de Física Espacial al switch y así poder liberar tráfico en el Multiconect. El hub que se muestra conectado al switch se dejó en ese lugar, ya que existen estaciones de trabajo que presentaban problemas al conectarse con los puertos a 10/100 Mbps del switch.

b) Con los cambios anteriores, el switch pasó a ser el equipo de Core en el esquema de red del Instituto. El transceiver instalado solo servirá de paso en los que se le dota al Instituto de un enlace a 100 o 1,000 Mbps. El objetivo de este rediseño, es dotar a la red de este Instituto con una red Jerárquica y donde sea necesario dotarla de enlaces redundantes y seguros.

c) El cambio de cable coaxial a cable UTP, es un paso obligado si se quiere crecer el ancho de banda asignado a esta red. Así mismo, la instalación de fibra óptica para los enlaces con los equipos de los diferentes departamentos hace ver que estos equipos tendrán que ser switches.

d) Para el problema de la instalación de hubs sin previo aviso, se recomendó que cuando se instalará el nuevo cableado se dejarán por lo menos 2 puntos de red en cada uno de los cubículos, si es que el investigador no necesitaba más puntos de red.

e) El problema del enlace a Física Espacial esta parcialmente resuelto, ya que se eliminó el paso del tráfico por un transceiver. Sin embargo, esto no quedará totalmente resuelto hasta el momento en que el cableado en este Departamento sea cambiado a UTP y sea instalado un switch que cubra sus necesidades.

Propuesta para el Primer Piso.

a) Como se observa en el esquema de la red del Primer Piso, la repartición de tráfico no es posible hasta el momento de que se cambie el cableado a UTP. Momentáneamente solo pasaron algunas máquinas de la Sección Editorial al switch del CARDI, así como el hub que daba red a las principales máquinas de la Dirección.

b) Para el problema de que para algunas PC's era necesario el reservar algún ancho de banda debido a las aplicaciones que corrían, estas se concentraron momentáneamente en una sala de cómputo donde las conexiones eran directas al switch.

Propuesta para el Segundo Piso.

a) Para la carga de tráfico excesiva en el Multiconect, se pasó el tráfico del Departamento de Sismología que se encontraba en el otro extremo del pasillo al switch de este Departamento. Además, las máquinas de este departamento que causaban problemas fueron reinstaladas y los recursos, periféricos y aplicaciones fueron redistribuidos entre ellas.

b) En este parte la instalación del cableado estructurado en UTP, ya presentaba un adelanto.

c) Obviamente, con la instalación del cableado estructurado, el problema de la no identificación de los servicios quedó resuelto.

4.5.2.- Propuesta para el Edificio II

Aunque el Multiconect no tiene una excesiva carga de trabajo, si es recomendable la instalación de un switch para que todo el Instituto quede switcheado y obviamente con cableado estructurado.

4.5.3.- Propuesta para el Edificio III (Biblioteca)

Aquí la única recomendación es la instalación de switches y la prevención de los puertos en este para un futuro crecimiento de la red en este segmento.

4.5.4.- Propuesta para el Edificio IV (Anexo)

En este punto sería recomendable la instalación de un switch que estuviese preparado con un puerto para poder recibir en un futuro un enlace a 100 o 1,000 Mbps. La instalación podría ser de un switch o un arreglo de estos capaces de soportar el número de servicios que se ofrecen actualmente y que tengan una holgura para soportar el crecimiento de la red en este Edificio.

Según se describió anteriormente, los cambios principales solo se realizaron en la Planta Baja del Edificio Principal y se muestran en el *diagrama 4.9.*

4.6.- Propuesta Optima

Una vez presentada la propuesta de solución inmediata para el mejoramiento del rendimiento de la red de cómputo del Instituto, ahora toca el turno de presentar la manera en que se hubiese realizado el diseño de esta red si el edificio se hubiera encontrado sin red alguna, es decir, se presentará como en la concepción de quienes desarrollamos esta tesis hubiese quedado la red del Instituto considerando un edificio nuevo y que no hubiese problemas de presupuesto (*diagrama 4.10*).

Edificio Principal.

a) Si consideramos que el futuro enlace que será entregado a este Instituto será de 1 Gigabit, necesitaríamos de un equipo de Core de capa 3 con las siguientes características:

   - Un mínimo de 16 puertos en Gigabit Ethernet, para poder conectarse directamente con los otros switches instalados en los diferentes departamentos, así como a los servidores que así lo requieran.

   - Una tarjeta en fibra óptica a 100 Mbps en caso de ser necesaria.

   - Un mínimo de 96 puertos a 10/100 Mbps para poder dar servicio a las máquinas del Centro de Cómputo y a los departamentos que se encuentran junto a este.

b) Los equipos de distribución y/o acceso se encontrarán en cada una de las esquinas del primer y segundo piso(equipos capa 2), con esto se pretende que cada uno de los Departamentos cuenten con su propio switch dada la autonomía que los Departamentos presentan. Para el Departamento de Física Espacial y Radiación Solar, se pretende la instalación de un switch por Departamento al igual que para la Biblioteca. Al ser estos los equipos de distribución y/o acceso, estos por lo menos deberán de contar con un puerto en Gigabit Ethernet para conectarse con el equipo de Core que se encontrará en la Planta Baja del Edificio Principal (Centro de Cómputo). De la misma manera cada uno de estos switches deberán de contar con 24, 48 o los puertos necesarios para dar servicios a las PC's y estaciones de trabajo que así lo requiera.

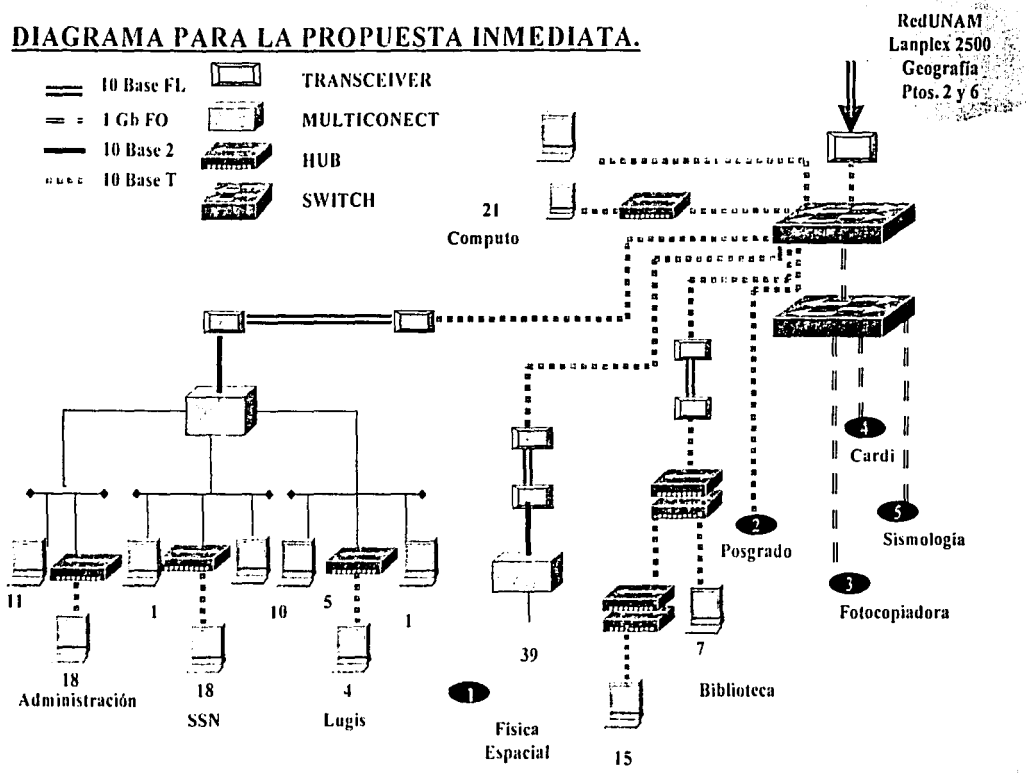


Diagrama 4.9 Cambios en el Edificio Principal Planta Baja.

Edificio Anexo.

Para este caso, se requiere de un equipo de Core (capa 3) más pequeño, que cuente con por lo menos 3 puertos Gigabit Ethernet (uno para recibir el enlace de Red-UNAM, otro para prever un crecimiento de la red y el tercero para recibir el enlace redundante del Edificio Principal), con un mínimo de 6 puertos en fibra óptica a 100 Mbps y con 98 puertos a 10/100 Mbps para cubrir las necesidades actuales y futuras de la red.

Como se puede percatar, ambos edificios (Principal y Anexo) cuenta con 2 niveles del modelo de redes Jerárquico. Esto se debe, a que como ya se había mencionado, depende del tamaño de la red para decidir sin son necesarios los 3 niveles del modelo Jerárquico.

Respecto a la Redundancia de la red, esta se podrá dar mediante una conexión directa vía fibra óptica a 1 Gbps entre los equipos de Core del Edificio Principal y el Edificio Anexo, en el momento que se cambie el equipo que da red a este Instituto, es decir, cuando se cambie el switch Lanplex 2500 que se encuentra en el Instituto de Geografía.

Se propone que ambos equipos de Core en los edificios sean de capa 3, para que estos sean quienes resuelvan las peticiones de red de los hosts que están debajo de ellos, es decir que estas peticiones no tengan que subir hasta el equipo instalado en el Instituto de Geografía y así competir por el procesamiento de los paquetes con las otras Dependencias. Una razón más para la recomendación de estos equipos, es la cantidad de hosts que se manejan en el Instituto de Geofísica (más de 600 equipos), lo cual permitiría aislarse del tráfico de broadcast y colisiones generado por otras Dependencias con la generación de VLAN's por puerto.

La manera de funcionar del enlace redundante implicaría configurar los 3 equipos de capa 3 involucrados (equipos del Instituto de Geografía y los dos del Instituto de Geofísica). El protocolo de ruteo a configurar sería OSPF, ya que este es el manejado en el backbone de Red-UNAM. Cuando algún enlace entre el equipo en el Instituto de Geografía y los equipos en el Instituto de Geofísica se perdiera, la configuración hecha permitiría que si el enlace del puerto 6 se perdiera, la red del Edificio Anexo convergería por el enlace del puerto 2; y si el enlace del puerto 2 se perdiera, la red del Edificio Principal convergería por el enlace del puerto 6, es decir la redundancia estaría dada.

Respecto al diseño de Seguridad de la red, este aún se encuentra en discusión debido a que se han estado probando diferentes herramientas que realizan la función de un Firewall. Así mismo, el definir donde se coloca una zona militarizada y/o una desmilitarizada dependerá de las necesidades de cada departamento y de cómo vayan saliendo las pruebas de los diferentes Firewalls (software o hardware). Sin embargo, un primer acercamiento hacia un diseño de Seguridad implicaría un Firewall con políticas no tan restrictivas en la entrada de cada enlace (Edificio) y Firewalls individuales en cada Departamento con políticas más restrictivas dependiendo de las necesidades de los usuarios. Una herramienta más que es útil para agilizar el tráfico en la red interna, es una herramienta llamada Web-

DIAGRAMA PARA LA PROPUESTA ÓPTIMA

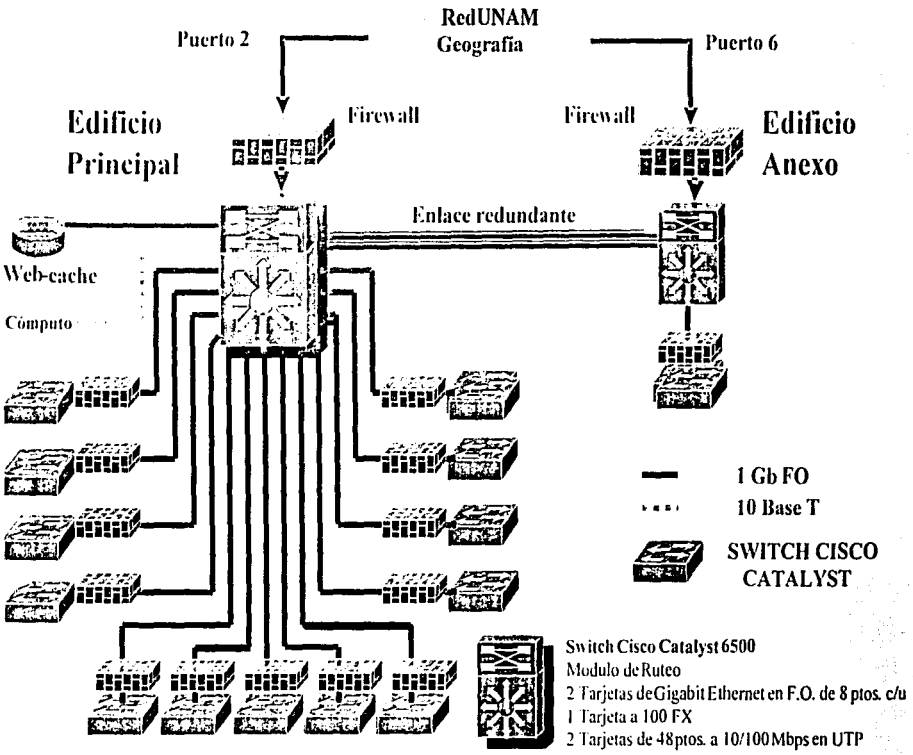


Diagrama 4.10 Proyección ideal de la red del Instituto.

Cache (software o hardware), que se instala dentro de la red local y nos sirve para almacenar las páginas más visitadas por el personal del Instituto, es decir, si una segunda persona necesita checar una página, no tiene la necesidad de conectarse hasta el servidor donde se aloja la página, debido a que esta ya se almaceno en el Web-Cache la primera vez que fue consultada por el personal dentro de la red del Instituto.

4.7.- Propuesta final

Como se observa en el punto anterior, es más sencillo planear el cableado estructurado de una red y los equipos de interconexión para la misma si no existe la necesidad de trabajar con el edificio ocupado o con problemas de presupuesto. Sin embargo, con el análisis que antecede al rediseño de la red y con la disponibilidad de las autoridades del Instituto, ha sido posible llegar a un diseño que si bien, no es el óptimo, por lo menos se asemeja mucho a éste. En la propuesta final, presentamos como quedará finalmente la red de cómputo del Instituto con los equipos que se tenían, los cambios que se recomendaron y los equipos de nueva adquisición (*diagrama 4.11*).

Edificio Principal.

a) El equipo de Core será un arreglo en stack de 2 switches Cisco Catalyst 3508 y un switch Cisco Catalyst 3548, es decir, un arreglo con 18 puertos en Gigabit Ethernet. Este arreglo se dio, debido a que en el momento del análisis 2 de estos equipos ya se encontraba en el Instituto y el tercero ya estaba pedido (Catalyst 3508). De los puertos que quedarán libres (uno será ocupado para el enlace de Red-UNAM y otros para la interconexión vía GIGA STACK – un puerto de cada switch), cada uno de ellos se ocupará para la interconexión de los switches que quedarán alojados en cada uno de los Departamentos en el Primer y Segundo Piso. La desventaja de este arreglo de switch respecto al switch propuesto en el punto anterior, es la capacidad en el número de paquetes que se maneja y la velocidad en que resuelve el camino de la información de manera interna.

b) Respecto a los equipos de distribución y/o acceso, no habrá mayor problema debido a que los switches con que se contaban y los recomendados cumplen con las características deseadas. Solo existe la pequeña dificultad, de que el algunos casos, como en el switch de la Fotocopiadora, existía un switch de 24 puertos a 10/100 Mbps y dado el crecimiento de los Departamentos que allí se encuentran, será necesario cambiarlo por uno de 48 puertos, pero afortunadamente esto es solo un problema trivial.

Edificio Anexo.

Aquí se recomendó la instalación del equipo de acceso, ya que los equipos que se encuentran en este edificio (hubs) son obsoletos y propensos a fallas debido a que estos equipos antes de ser instalados en este edificio, estaban instalados en otras Dependencias. El equipo instalado fue un switch Catalyst 3548 que se encontraba en el Edificio Principal (equipos capa 2).

DIAGRAMA PARA LA PROPUESTA FINAL

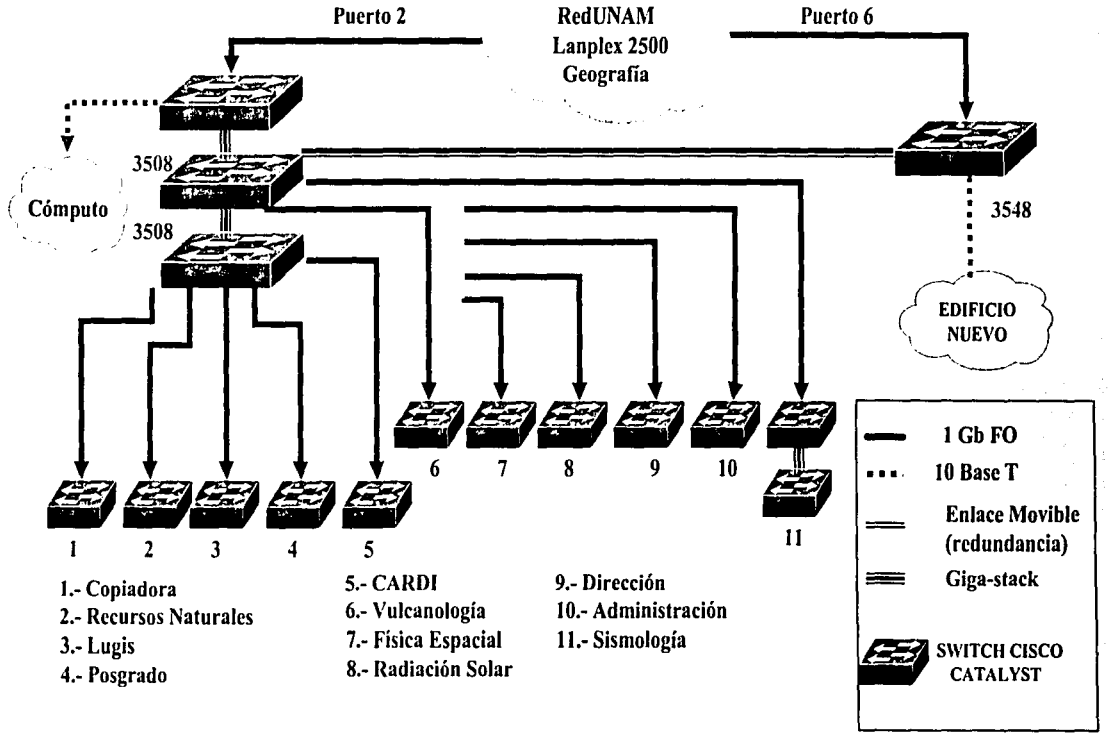


Diagrama 4.11 Proyección de la red del Instituto.

En cada una de éstas propuestas, el problema principal (después del adjudicamiento de recursos), son las obras y molestias necesarias para poder hacer el cableado estructurado y pasar las fibras ópticas a través de cada piso, debido a que para hacer esto se deben retirar lámparas y secciones de techo, sin embargo con la contratación de personal para realizar estas tareas se resolvió el problema.

La manera en que funcionará la redundancia en este diseño se dará de la siguiente manera:

- Antes de cambiar el Lanplex 2500 en el Instituto de Geografía.

Cuando se pierda el enlace entre el puerto 2 y el Edificio Principal, o cuando se pierda el enlace entre el puerto 6 y el Edificio Anexo, el enlace redundante será conectado entre los switches del Edificio Principal y el Edificio Anexo, de manera que ambos segmentos puedan salir por el mismo puerto.

- Al cambiar el equipo en el Instituto de Geografía.

Cuando el Lanplex 2500 sea cambiado por un equipo que soporte el protocolo STP (Spanning Tree Protocol), entonces el enlace redundante entre el Edificio Principal y el Edifico Anexo quedará permanente. Es decir, habrá que configurar los equipos de Geografía y Geofísica con el protocolo STP para que cuando se pierda el enlace en alguno de los puertos, los equipos automáticamente reconozcan el enlace redundante y trasporten por ese medio el tráfico correspondiente al enlace perdido.

Cabe destacar, que si los recursos del Instituto así lo permiten, se puede llegar a la instalación de equipos de capa 3 en el nivel de Core de ambos Edificios, de modo que se estaría llegando cada vez más cerca al diseño óptimo planteado anteriormente.

4.8.- Propuesta económica

La presentación de la propuesta económica se hará en base a la evaluación que se realizo en el Departamento de Redes en DGSCA de las características de los equipos que se evaluaron para la rediseño del Backbone de Red-UNAM. A continuación se presenta una lista de las características que se evaluaron en los equipos de Cisco System, Foundry Networks y Extreme Networks. Por razones de confidencialidad, no se presentan a detalle los puntos que cada una de estas compañías cumplió o no.

Pruebas UNAM
VLAN'S
Configuración de Vlans con 802.1q
Configuración de Vlans con 802.1q con terceros
Facilidad de configuración de Vlans y asignación
Diversidad de Vlans(Mac,puerto,Protocolo,authenticada)
Relay de DHCP
Comunicación entre diferentes tipos de Vlans
Spanning Tree

Gigabit Ethernet
Interoperabilidad con equipos de cómputo y switches de terceros
Comportamiento del switch con carga
Soporte de interfases SX y LX
Non-Blocking
Link Agregation (Trunking)
Capacidad de trunking
Redundancia en el trunking
Balanceo en el trunking
Servicios de capa 3
Soporte OSPF
Soporte RIP/RIP II
Soporte de BGP v4
Soporte de IP, IPX,
Limpieza de las tablas de ruteo y MAC
Creacion de Filtros (BGP) por AS, Prefijo
Modificacion de propiedades (Pre-end, Local preference, metric)
Creacion de Filtros para OSPF, RIP por puerto y por subred
Seguridad
Soporte de servicios AAA
Soporte de NAT
Listas de Acceso(por IP,MAC,Puerto de TCP/UDP
Creacion listas Via consola
Creacion listas Via plataforma de Administración
QoS
Configuracion de 802.1p
DiffServ
Redundancia
Hotswap
Redundancia en servicios L2/L3
Redundancia fuentes de poder
Tiempo en levantar todos los servicios (Segundos)
Monitoreo y Administración
Grupos de RMON
Soporte para NTP
Configuracion de Vlans y asignaciones de puertos
Funcionalidades de inventario
Rastreo de usuarios
SNMP
Respaldo de configuraciones TFTP, FTP, SCP
Actualizaciones de Software TFTP, FTP, SCP
Port Mirror
Multicast
PIM SM
PIM DM
DVMRP

Varias
IPv6
DHCP Server
NAT
MBGP
MSDP
Vlans Por MAC
SSH Versión 1 y 2
Web Cache Redirect
TACACS, RADIUS
MLPS

4.9.- Relación Costo-Beneficio

Igualmente que en el punto anterior, por razones de confidencialidad no se pueden exponer los precios que se dieron de los equipos antes expuestos, sin embargo si se puede presentar una tabla con las características generales evaluadas a los equipos participantes.

	Rendimiento	Soporte	Precio
Cisco	2	1	2
Foundry	1	3	1
Extreme	3	2	3

Tabla 4.1.- Relación costo – beneficio.

La calificación otorgada, va del 1 al 3, siendo el 1 la más alta.

4.10.- Justificación de la tecnología seleccionada

En el análisis de las tecnologías de alta velocidad hecha en el capítulo anterior, se evaluaron las tecnologías de Fast Ethernet, Gigabit Ethernet, ATM y FDDI. Cada una de estas tecnologías pueden funcionar como la tecnología de una red tipo LAN, sin embargo las últimas 2 son tecnologías enfocadas a redes WAN.

Finalmente, con el rediseño del Backbone de Red-UNAM y su cambio parcial de un protocolo ATM (LAN Emulation) a una tecnología en Gigabit Ethernet, la decisión de instalar una red en el Instituto de Geofísica con tecnología Ethernet en su etapa en Gigabit fue la correcta. Además que la infraestructura de la red y el tipo de aplicaciones que en ella se corren daba una dirección hacia esta tecnología que era imposible ignorar.

4.11.- Justificación de la propuesta económica seleccionada

Como se observa en la tabla 4.1, cada una de las propuestas económicas presenta sus pros y sus contras, pero habría que tomar una decisión que no afectara la interoperabilidad de los equipos, cosa que fue probada y aprobada en la evaluación hecha por el equipo del Departamento de Redes en DGSCA.

Los equipos de Extreme Networks, presentaban el costo más alto de los equipos evaluados, un soporte técnico medio y el rendimiento menor de las 3 opciones.

Los equipos de Foundry Networks, presentaban el menor costo, el mejor rendimiento y sin embargo, tenían el soporte técnico más bajo.

Finalmente, los equipos de Cisco System, presentaban un costo medio, un rendimiento medio y el mejor soporte técnico de las opciones evaluadas.

Considerando, que la diferencia de precios no era muy notable, que el rendimiento del equipo presentaba algunas fallas en la parte administrativa (deficiencia no crítica) y que es un compañía con muchos años en el mercado y por lo tanto con soporte técnico calificado y comprobado, la propuesta seleccionada fue la de Cisco System. Además con ello se aseguraba la perfecta comunicación e interoperabilidad entre los equipos (switches) que ya existían en el Instituto y los que se recomendarían para las nuevas adquisiciones.

4.12.- Presentación y análisis de los resultados obtenidos

De las pruebas realizadas encontramos que el problema principal fue que la red estaba sufriendo constantes ataques a la dirección de broadcast, pero debido a que estos ataques solo se presentaban como ráfagas no se pudo saber con exactitud hasta el momento de que la perturbación tuvo un periodo de duración más largo; estos ataques provocaban que todas la IP's activas mandaran su respuesta a la petición de esta manera se generaba un tráfico excesivo en la red que a su vez provocaba que la información importante para la red tuviese que esperar a ser transmitida.

Otro problema encontrado fue que a pesar de que la red no tiene demasiados errores y/o colisiones debido al cable coaxial (10Base2), existe la dificultad de que no se cuenta con un cableado estructurado lo que provoca que una estación para poder comunicarse con otra tenga que viajar a través de diversos dispositivos lo que hace que haya demasiado tráfico y que la información tarde y pierda claridad al momento de llegar a su destino.

Un problema más que se encontró, es que en el caso del departamento de Sismología habría que redefinir la manera en que estas instalados los servicios y recursos (llámense cintas, discos duros, etc) que son compartidos, ya que el tráfico que es generado entre las estaciones de este mismos segmento es excesivo a pesar de las aplicaciones que corren.

Propuesta de solución

Para el caso de ataques a la dirección de broadcast, se recomendó la instalación de un Firewall a la entrada de los segmentos y de cada uno de los Departamentos para asegurar la entrada y salida de información hacia el Instituto.

Como se comentó antes, se necesitan redefinir la manera en que están montadas las aplicaciones y recursos que están compartidos en cada departamento.

Para el problema de lentitud en la red, éste se resuelve combinando las siguientes medidas: se recomienda el cambio inmediato de los segmentos de red que aún se encuentran con cable coaxial (10Base2) hacia cable UTP (10BaseT), además de las recomendaciones adicionales en cuanto a la reestructuración de la red del Instituto, las cuales ya fueron descritas. Además se observó que parte de la lentitud de la red se debió a la gran demanda de utilización que está siendo requerida por los servidores para aplicaciones utilizadas por el Instituto; los 10 Mbps empiezan a ser insuficientes por lo cual se requiere incrementar el ancho de banda de 10 a 10/100 Mbps al escritorio y 100/1000 entre los equipos de distribución siendo también recomendable cambiar de un medio compartido (Hubs) a un medio conmutado (Switch).

Lo anterior para poder tener mayores posibilidades de crecimiento y de funcionalidad para en el futuro poder dar un mejor soporte a aplicaciones que lleguen a ser requeridas en proyectos posteriores como Internet 2 donde serán necesarios mayores ancho de banda.

Capítulo V

Políticas para la Administración de las Redes de Cómputo.

CAPÍTULO V:
POLÍTICAS PARA ADMINISTRACIÓN DE REDES DE CÓMPUTO

Hoy en día, instalar una red de área local (LAN) en una empresa, es cada día más sencillo; sin embargo, los problemas pueden comenzar cuando se intenta administrarla. En este sentido, el trabajo de los administradores de redes puede resultar muy complejo. Su misión principal consiste en mantener el funcionamiento de recursos tales como ruteadores y switches, así como cada uno de los dispositivos críticos que conforman la red, con el fin de proveer a los usuarios de un ambiente confiable, óptimo y seguro para realizar su trabajo.

Las principales actividades que día con día realizan los administradores son: controlar las operaciones de las distintas partes de la red, descubrir las piezas que faltan para repararlas y evitar que se caiga el sistema. Los problemas más comunes en lo que a administración de redes se refiere, provienen de los recursos de los usuarios y de la seguridad de la información.

El riesgo principal de un administrador es no tener el control de lo que está sucediendo en el sistema. Generalmente este descontrol es provocado por un desconocimiento parcial o total de la red que se está administrando. Por eso, la administración de sistemas implica el cumplimiento de ciertas normas y una documentación adecuada de los procesos.

En la mayoría de las organizaciones, el área de cómputo controla solamente el 60% de la infraestructura, mientras que el 40% restante es desconocida. Esta situación se refleja en los tiempos de respuesta que el área de cómputo le da a los usuarios.

En términos generales, la administración de redes puede clasificarse en administración reactiva (el administrador reacciona cuando surge un problema y lo trata de solucionar) y administración proactiva (el administrador prevé todos los eventos para que éstos sucedan de manera adecuada).

La administración también puede ser centralizada o descentralizada. La primera permite administrar todos los servicios y recursos desde un solo punto, mientras que la descentralizada permite administrar la red por segmentos, localidades o componentes.

¿Qué hay de la administración?

La mayoría de los proyectos de administración de tecnología han fracasado en su implantación porque no se encauzan a la tecnología, la cual es una parte importante de una organización, pero por sí misma no lo es todo. Si no existe un proceso que nos indique cómo usar la tecnología en beneficio de la organización, ésta no ofrece ningún rendimiento.

Una administración de redes inadecuada puede provocar que una organización emplee más recursos, lo que incrementará sus costos. También puede provocar pérdidas de oportunidades de negocio. Por esas razones, la visión actual de la administración de redes tiende a alinear la tecnología con los objetivos de la organización.

Si un administrador ofrece un esquema de administración que reduzca el costo total de propiedad (TCO – Total Cost of Ownership) de la tecnología, hará más productiva a la organización.

Para que la organización reduzca el TCO de sus redes y reciban un retorno de capital, a partir de sus inversiones informáticas, hoy existen soluciones integradas y estándares que reúnen las diversas herramientas de administración en un solo producto. Este tipo de herramientas controlan redes heterogéneas desde una consola operada a distancia por un administrador, y también pueden manejarse desde cualquier PC o estación de trabajo que esté conectada al administrador central. Estas soluciones pueden reducir hasta en un 80% el TCO, porque realizan tareas a distancia que antes implicaban tiempo, dinero y presencia física de un administrador.

Para conocer si se están llevando a cabo las actividades del área de cómputo de manera óptima, hay que hacerse las siguientes preguntas:

1. ¿Se conoce toda la infraestructura de IT con la que cuenta la organización?
2. ¿Se conoce cada uno de los componentes de la red?
3. ¿Se sabe planear y administrar todos los recursos de la red?
4. ¿Se tiene el control de toda la infraestructura?
5. ¿Se cuentan con procesos definidos de cada una de las tareas que se llevan a cabo?
6. ¿Se documenta y registran todas las actividades y procesos?
7. ¿Se tienen calendarizadas el mayor número de actividades proactivas que reactivas?
8. ¿Se es capaz de prever los problemas antes de que ocurran?
9. ¿Se está compenetrado con los objetivos de la organización?
10. ¿Se orientan las actividades de la administración hacia los objetivos del negocio?
11. ¿Se sabe cuáles son las expectativas de la alta dirección?
12. ¿Se mantiene una relación estrecha con los usuarios para conocer sus demandas?
13. ¿Se brinda a los usuarios el nivel de servicios se estos demandan?
14. ¿Se busca una retroalimentación con los usuarios?
15. ¿Se es creativo y paciente?
16. ¿Se capacita el personal constantemente?
17. ¿Se sabe cómo impactarán en el sistema los diferentes cambios en la tecnología?
18. ¿Se saben sacar ventajas y beneficios de los cambios en la tecnología?
19. ¿Se documentan todos los cambios que se realizan (a nivel infraestructura, procesos y personal)?

Principales tareas que realizan las soluciones de administración de redes:

1. Monitoreo del funcionamiento de cada PC o servidor en tiempo real.
2. Administración de bases de datos.
3. Realización de upgrades de aplicaciones y carga de programas nuevos.
4. Estandarización de las configuraciones de software en las estaciones de trabajo.
5. Reinicio de equipos encendidos a distancia.
6. Eliminación de archivos, carga de software y bloqueo o acceso de los usuarios a ciertas aplicaciones.
7. Captación de información acerca de las aplicaciones de una red para detectar su funcionamiento y problemas.
8. Transferencia de archivos en diferentes puntos de red.
9. Configuración de nuevos servicios y ejecución de inventarios de hardware, software y de todos los dispositivos de red.
10. Persecución y eliminación de virus.
11. Manejo de alarmas que alertan sobre fallas, robos de memoria o de espacio en el disco duro.
12. Cambio de la configuración en las PC's y en las direcciones IP de las estaciones de trabajo.
13. Detección de falta de memoria en el disco duro.
14. Seguridad de la red y correcta distribución de software.
15. Actualización del BIOS (sistema básico de entrada y salida) de las máquinas.
16. Monitoreo de archivos críticos para descubrir las modificaciones que hacen los usuarios en sus estaciones de trabajo.
17. Administración remota: permite que el administrador maneje a distancia las computadoras de los usuarios para enseñarles a ejecutar una aplicación o resolverles un problema sin ir al escritorio de cada uno. El administrador conecta, a través de la red, el mouse y el teclado del usuario a su propia PC y los maneja en su pantalla para dominar la computadora a distancia, mientras el usuario observa los procedimientos en su propia pantalla.

5.1 Políticas de seguridad para la Red de Cómputo del Instituto de Geofísica

Antes de comenzar a describir las políticas de seguridad, es conveniente definir algunos conceptos que son importantes en este momento.

- Administrador: persona responsable de mantener en operación continua los recursos de cómputo con los que cuenta un sitio.

- Seguridad en cómputo: conjunto de recursos destinados a lograr que los activos de una organización sean *confidenciales*, *integros*, *consistentes* y *disponibles* a sus usuarios, *autentificados* por mecanismos de *control de acceso* y sujetos a *auditoria*.

  - *Confidencial*: La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.

- *Íntegro*: La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo.

- *Consistente*: el sistema, al igual que los datos, debe comportarse como uno espera que lo haga.

- *Disponible*: La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos.

- *Autentificado*: Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.

- *Control de acceso*: Debe conocerse en todo momento quién entra al sistema y de dónde procede.

- *Auditoria*: Deben conocerse en cada momento las actividades de los usuarios dentro del sistema.

➢ Herramientas de seguridad: programas que no permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas, casi todas de libre distribución. Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son:

- Para el manejo de contraseñas: *anipasswd*, *passwd+*, *crack*, *John The Ripper*, *S/Key*.
- Para el manejo de autenticación: *Kerberos*, *SecureRPC*.
- Para el monitoreo de redes: *Satan*, *ISS*.
- Para auditoría interna: *COPS*, *Tiger*, *Tripwire*.
- Para control de acceso: *TCP-Wrapper*, *PortSentry*.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Las políticas permiten a los administradores disminuir los riesgos, y permiten actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. Como usuarios, indican la manera adecuada de usar un sistema, indicando lo que puede hacerse y lo que debe evitarse en un sistema de cómputo, contribuyendo a que no ser "malos vecinos" de la red sin saberlo. El tener un esquema de políticas facilita la introducción de nuevo personal, teniendo ya una base escrita y clara para capacitación; dando una imagen profesional a la organización y facilitando una auditoria.

Es necesario hacer énfasis en que el apoyo por parte de la gente con el poder de decisión (cuerpo directivo, dueños de los recursos, gerencia, etc.) es fundamental para el éxito de un esquema de seguridad, ya que sin él, algunos elementos de dicho esquema no tendrían validez. A su vez, es vital mantener en constante capacitación tanto al personal antiguo como al nuevo mediante cursos, seminarios, congresos, etc.

Los usuarios deben conocer el uso adecuado de los sistemas de cómputo y saber cómo protegerse a sí mismos de accesos no autorizados.

El primer paso a considerar en un esquema de seguridad, que muchas veces no recibe suficiente atención, es la *seguridad física* (las medidas que se usan para proteger las instalaciones en las que reside un sistema de cómputo: llaves, candados, tarjetas de acceso, puertas, ventanas, alarmas, vigilancia, etc.). Recomendaciones para el Instituto respecto a la seguridad física incluyen:

- Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
- Colocarlas fuera del alcance de rayos, vibraciones, insectos, ruido eléctrico (balastras, equipo industrial, etc.), agua, etc.
- Mantener las computadoras alejadas de comida y bebida.
- No desatender las sesiones de trabajo activas.

El segundo paso es establecer políticas de seguridad que son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen y qué hacer ante un incidente de seguridad.

Mientras las políticas indican el "qué", los procedimientos indican el "cómo". Los procedimientos son los que permiten llevar a cabo las políticas. Algunas de las actividades dentro del Instituto que requieren la creación de un procedimiento son:

- Otorgar una cuenta.
- Conectar una computadora a la red.
- Actualizar el sistema operativo.
- Instalar software localmente o vía red.
- Actualizar software crítico.
- Exportar sistemas de archivos.
- Respaldar y restaurar información.
- Manejar un incidente de seguridad.

Para que esto sirva de algo, las políticas deben ser:

- Apoyadas por los directivos y/o académicos.
- Únicas.
- Claras (explícitas).
- Concisas (breves).
- Bien estructuradas.
- Revisadas por abogados.
- Dadas a conocer.
- Firmadas por los usuarios.
- Mantenerse actualizadas.

Al diseñar un esquema de políticas de seguridad, conviene se divida el trabajo en diferentes políticas específicas a un campo - cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, personal, etc. De esta manera, para la implementación de políticas en el Instituto se deberá tener en cuenta los siguientes puntos:

- *Políticas de cuentas*: Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas.

  - Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos (personal solo del Instituto de Geofísica).
  - Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
  - El nombre de usuario de una cuenta deberá estar conformado por la primera letra de su nombre y su apellido paterno.

- *Políticas de contraseñas*: Son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada, etc.

  - La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el usuario. Todas las contraseñas deberán contar con al menos siete caracteres.
  - Para las contraseñas, no deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
  - Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas ya utilizadas.

- *Políticas de control de acceso*: Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autentificarse.

  - Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada (SSH v2).
  - Si un usuario está fuera del sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta, hacer la conexión a la computadora deseada.
  - Al momento de ingresar al sistema, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del sistema

- *Políticas de uso adecuado*: Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que está prohibido dentro del sistema de cómputo.

Para la elaboración de Políticas de uso adecuado, existen dos enfoques: *permisivo* (todo lo que no esté explícitamente prohibido está permitido) y *paranoico* (todo lo que no esté explícitamente permitido está prohibido). Cuál de estas elegir dependerá del tipo de organización y el nivel de seguridad que esta requiera.

Tras haber aclarado estos últimos puntos, a continuación se mencionan algunas políticas de ambos enfoques para la administración de la red de esta Dependencia:

- Está prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.
- Está prohibido hacer uso de herramientas, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos.
- Está prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador.
- No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro.

- *Políticas de respaldos*: Especifican qué información debe respaldarse, con qué periodicidad, qué medios de respaldo utilizar, cómo deberá ser restaurada la información, dónde deberán almacenarse los respaldos, etc.

- El administrador del sistema es el responsable de realizar respaldos de la información periódicamente.
- La información respaldada deberá ser almacenada en un lugar seguro y distante del sitio de trabajo.
- Deberá mantenerse siempre una versión reciente impresa de los archivos más importantes del sistema.
- En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada antes de deshacerse del medio.

- *Políticas de correo electrónico*: Establece tanto el uso adecuado como inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario del Instituto debe hacer valer y cumplir al respecto.

- El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo
- Está prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades laborales.

- No se permite el uso de la cuenta de correo electrónico para subscribirse a listas electrónicas de discusión de interés personal El usuario deberá limitarse a estar subscrito a las listas indicadas y aprobadas por la organización.

➢ *Políticas de contabilidad del sistema:* Establecen los lineamientos bajo los cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo, así como la manera en que debe manejarse la contabilidad del sistema y el propósito de la misma.

- Deberán ser registrados en bitácoras todos los comandos emitidos por todos los usuarios del sistema, para propósitos de contabilidad.

- Cada semana deberá hacerse el corte de contabilidad del sistema, cifrándose y respaldándose la información generada en un dispositivo de almacenamiento permanente.

➢ Un esquema de políticas de seguridad debe llevar ciertos pasos, para garantizar su funcionalidad y permanencia en la institución. La propuesta para esta red es seguir los pasos que detallamos a continuación:

- *Preparación* - La recopilación de todo tipo de material relacionado con cuestiones de seguridad en la organización: Manuales de procedimientos, planes de contingencia, cartas compromiso, etc.
- *Redacción* - Escribir las políticas de una manera clara, concisa y estructurada. Requiere de la labor de un equipo en el que participen abogados, directivos, usuarios y administradores.
- *Edición* - Reproducir las políticas de manera formal para ser sometidas a revisión y aprobación.
- *Aprobación* - Probablemente, la parte más difícil del proceso, puesto que es común que la gente afectada por las políticas se muestre renuente a aceptarlas. En esta etapa es fundamental contar con el apoyo de los directivos.
- *Difusión* - Dar a conocer las políticas a todo el personal de la organización mediante proyecciones de video, páginas Web, correo electrónico, cartas compromiso, memos, *banners*, etc.
- *Revisión* - Las políticas son sometidas a revisión por un comité, que discutirá los comentarios emitidos por las personas involucradas.
- *Aplicación* - Es peor tener políticas y no aplicarlas que carecer de ellas. Una política que no puede implementarse o hacerse cumplir, no tiene ninguna utilidad.
- *Actualización* - En el momento requerido, las políticas deberán ser revisadas y actualizadas, respondiendo a los cambios en las circunstancias. El momento ideal es justo después de que ocurra un incidente de seguridad.

Para las políticas para la reacción ante un incidente de seguridad, hay dos estrategias básicas:

➢ Proteger y perseguir

- El principal objetivo es proteger y preservar los servicios del sitio, y restablecerlos lo más rápido posible.
- Se realizan acciones drásticas, tales como dar de baja los servicios, desconectar el sistema de la red, apagarlo, etc.
- Se utiliza cuando:
  - Los activos están bien protegidos.
  - Se corre un gran riesgo debido a la intrusión.
  - No existe la posibilidad o disposición para enjuiciar.
  - Se desconoce la base del intruso.
  - Los usuarios son poco sofisticados y su trabajo es vulnerable.
  - Los recursos de los usuarios son minados.

➢ Perseguir y enjuiciar

- Su objetivo principal es permitir que los intrusos continúen con sus actividades en el sistema hasta que pueda identificarse a los responsables
- Se utiliza cuando:
  - Los recursos están bien protegidos.
  - Se dispone de respaldos confiables.
  - El riesgo para los activos es mayor que el daño de esta y futuras intrusiones.
  - El ataque proviene de un sitio con el que guardamos cierta relación, y ocurre con cierta frecuencia e intensidad.
  - El sitio posee cierta atracción para los intrusos.
  - El sitio está dispuesto a correr el riesgo a que se exponen los activos al permitir que el ataque continúe.
  - Puede controlarse el acceso al intruso.
  - Se cuenta con herramientas de seguridad confiables.
  - El personal técnico conoce a profundidad el sistema operativo y sus utilerías.

5.2 Administración y documentación de la Red

5.2.1 El lado administrativo de la gestión de red

a) El aspecto de una red.

Es importante visualizar lo que es una red. Una red es una serie de dispositivos que interactúan entre sí para proporcionar comunicación. Cuando un administrador de red analiza una red, debe verla como un todo en lugar de como partes individuales. En otras palabras, cada dispositivo en una red afecta otros dispositivos y la red como un todo. Nada está aislado cuando se encuentra conectado a una red.

Lo importante al administrar una red es recordar que se debe considerar como una unidad y no como un grupo de dispositivos individuales conectados. Esto también se aplica a las conexiones de área amplia que se usan al conectarse a Internet. Los cambios realizados a los routers en su ubicación afectarán directamente la eficiencia y confiabilidad de la comunicación en todo el sistema.

b) Comprensión y establecimiento de las fronteras de la red.

En una red es importante que el personal del Instituto relacionado con la red conozca sus responsabilidades. El personal de red ¿es responsable por el diagnóstico de problemas en el escritorio del usuario, o simplemente debe determinar si el problema del usuario no está relacionado con las comunicaciones? El personal de red ¿sólo se responsabiliza por lo que ocurre hasta la placa de cableado de pared, o debe ocuparse de toda la instalación hasta la NIC?

Estas definiciones son muy importantes para un departamento de Cómputo, ya que afectan la carga de trabajo de cada persona, y el costo de los servicios de red para el Instituto. Cuanto mayor sea la responsabilidad del personal de red, mayor será el costo de los recursos.

El trabajo de la administración de red puede incluir todos los aspectos de la red, o puede limitarse a ciertos componentes. Estas responsabilidades deben definirse e implementarse por departamento. La clave para comprender esta relación es que, si las responsabilidades abarcan demasiado, esto puede sobrecargar los recursos del departamento, pero si las responsabilidades son demasiado pequeñas, puede resultar difícil resolver los problemas de la red de forma efectiva. Aquí la recomendación es compartir la responsabilidad entre Departamentos y entre el usuario y los administradores.

c) Costos de una red.

La administración de red incluye varias responsabilidades, incluyendo el análisis de costos. Esto implica la determinación no sólo del costo del diseño e implementación de la red, sino también el costo del mantenimiento, actualización y monitoreo de la red. La determinación del costo de la instalación de la red no es una tarea particularmente difícil para la mayoría de los administradores de red. Las listas y costos de los equipos se pueden establecer fácilmente; los costos laborales se pueden calcular mediante porcentajes fijos. Desafortunadamente, el costo del desarrollo de la red es sólo el principio.

Estos son algunos de los factores de costos que se deben tener en cuenta: el crecimiento de la red con el tiempo; la capacitación de técnicos y usuarios; reparaciones y distribución de software. Estos costos son mucho más difíciles de proyectar que el costo de desarrollo de la red. El administrador de red debe estar capacitado para analizar las tendencias de crecimiento de la empresa e históricas para proyectar el costo del crecimiento en la red. Un administrador debe examinar el nuevo software y hardware para determinar si la empresa necesitará implementarlo y cuándo, así como las necesidades de capacitación del personal para brindar soporte a estas nuevas tecnologías.

El costo del equipo redundante para operaciones fundamentales de trabajo también se debe agregar al costo del mantenimiento de la red.

d) Documentación de errores.

La efectiva administración de red requiere documentación completa, de manera que, en caso de problemas, se debe elaborar algún tipo de documentación de los errores.

Esta documentación se utiliza para reunir la información básica necesaria para identificar y asignar un problema de red, y también ofrece una manera para hacer un seguimiento del progreso y eventual solución del problema. Los informes de problema pueden ofrecer los motivos que justifiquen la contratación de nuevo personal, adquisición de equipos y ofrecimiento de capacitación adicional por parte de la gerencia de nivel superior. Esta documentación también brinda soluciones para problemas recurrentes que ya han sido resueltos.

5.2.2 Administración de la red

La administración de la red incluye áreas distintas; entre ellas: documentación de la red, seguridad de la red, mantenimiento de la red, administración del servidor y mantenimiento del servidor.

Al terminar la configuración de la red es cuando empieza la verdadera tarea de un administrador de red, al tener que contar con el siguiente material de la red del Instituto.

a) Diagramas de planes de distribución. El componente principal y más crítico para una red de buena calidad es la documentación la cual representa la memoria del administrador de la red y está compuesta por el diario de ingeniería, pero además incluye:

   Diagramas que indican la disposición, del cableado físico, el tipo de cables, la longitud de cada cable, el tipo de terminación para el cable, la ubicación física de cada uno de los tomacorrientes o paneles de conexión y un esquema de rotulación para identificar con facilidad cada cable.

b) Disposiciones de los MDF (Cuarto de Telecomunicaciones primario) e IDF (Cuarto de Telecomunicaciones secundario). Contiene una disposición física y lógica del Servicio de Distribución Principal y de todos los Servicios de Distribución Intermedia en la red.

c) Por último, este documento contiene la ubicación física, el usuario y la información de identificación de red (dirección IP, dirección MAC, subred, topología) acerca del computador. Además, en este documento se incluye la fecha de compra y la información acerca de la garantía.

d) Listados de software.

e) Registros de mantenimiento.

f) Medidas de seguridad incluye no sólo seguridad relacionada con el software, como los derechos del usuario, la definición de contraseña y el soporte de firewall sino también seguridad física.

g) Políticas para el usuario. Contienen la forma en que los usuarios pueden interactuar con la red.

5.2.3 Seguridad de red.- Panorama General

a) Acceso de red. La seguridad de red involucra dos componentes principales: el primero es proteger la red contra el acceso no autorizado y el segundo es la habilidad para recuperar datos ante eventos catastróficos.

b) Recuperación de datos. La recuperación de datos, que constituye la segunda parte de la seguridad de red, implica proteger los datos ante pérdidas. Tres de los métodos populares para la protección de datos son la copia de seguridad de la cinta que contiene los datos, las configuraciones de disco a prueba de fallas y el uso de sistemas de alimentación no interrumpida (UPS) para evitar que el equipo deje de funcionar cuando se producen interrupciones del suministro eléctrico.

5.2.4 Factores ambientales

a) Estática, polvo, suciedad y calor. Otro de los aspectos de una buena administración de red es manejar los factores ambientales que pueden afectar a una red. Si se controlan estos factores, se puede obtener una red más estable y confiable.

b) Acondicionamiento de la alimentación. Se debe proteger el equipo contra las irregularidades del cableado eléctrico del edificio. La forma más sencilla de proteger el equipo de red y computadores es colocarlos en circuitos individuales en el edificio. Existen dispositivos que se pueden utilizar para controlar las irregularidades del suministro eléctrico:

- Transformador separador.
- Reguladores.
- Acondicionador de línea.
- Sistema de alimentación no interrumpida.

c) Interferencia electromagnética e interferencia de la radiofrecuencia. Otra fuente de problemas con las comunicaciones de red puede ser el mismo equipo.

d) Virus del software. Todos los temas descritos anteriormente que pueden afectar el desempeño de una red se han referido al aspecto físico de la red. El último de los factores que se describe y que puede afectar el desempeño de la red es el software. Específicamente, un tipo de software cuyo propósito exclusivo es obstaculizar el funcionamiento de una red.
- Un gusano
- Un Virus
- Un Troyano

5.2.5 Desempeño de la red

a) Nivel básico, actualizaciones y verificación de cambios de la red.

Junto con la seguridad de red y la redundancia, otra de las consideraciones importantes con respecto a la administración de la red es el desempeño de la red. El desempeño de la red es una medición de la rapidez y la confiabilidad de la red. La combinación del hardware, software y cableado de la red y de los computadores tienen un desempeño de red distinto. Esto nos lleva a la conclusión de que, para saber si la red funciona de forma defectuosa, se debe contar con una medición con la que se pueda comparar el desempeño. Esta medición se denomina nivel básico. El nivel básico se establece después de que se ha instalado y configurado la red de forma adecuada.

Para establecer un nivel básico, se puede utilizar herramientas que registran varios tipos de datos del desempeño de la red, incluyendo el porcentaje de uso de la red, el número de colisiones, los errores de trama y el tráfico de broadcast (por ejemplo, el Sniffer).

Al establecer una medición del nivel básico cuando el sistema de red se ubica en los niveles de desempeño normal óptimos, el administrador de red cuenta con un valor de comparación que se puede utilizar para determinar la buena salud de la red.

A medida que la red crece y cambia, la medición del nivel básico, al igual que cualquier otra documentación, se debe actualizar periódicamente.

Cuando se realizan cambios en la red, como mover una pieza de equipo desde una ubicación a otra. Es importante verificar el funcionamiento correcto de dicha pieza del equipo en la nueva ubicación antes de actualizar la medición del nivel básico. Esto es particularmente importante al realizar cambios para reducir el tráfico de red en un segmento de red en particular. Aunque el dispositivo funcionara correctamente en el segmento antiguo, es posible que no funcione correctamente en el segmento nuevo, y esto afectará el desempeño de la red.

5.2.6 Administración del servidor

a) Comunicación de igual a igual.

Hay dos tipos de redes que los administradores de red deben conocer. Los dos tipos son las redes de punto a punto y de cliente-servidor

- La red de punto a punto.

La red de también se denomina red de grupo de trabajo. Las ventajas de una red de punto a punto es el costo inferior de creación y operación, en comparación con las redes cliente-servidor; que permite que los usuarios controlen sus propios recursos; que no requiere un servidor dedicado y que no se requiere ningún software adicional, aparte de un sistema de operación adecuado. Las desventajas incluyen que no se suministra ningún punto central de administración y que cada usuario debe crear identificadores para cada usuario que comparte los recursos de la máquina.

- La red de Cliente-servidor.

Los sistemas operativos de red son el núcleo de la red cliente-servidor. Estos sistemas controlan los recursos y la administración de la red de área local. Las ventajas de las redes cliente-servidor son que suministran un punto centralizado de administración de usuario, seguridad y recursos. La operación y el mantenimiento de la red requieren que haya personal especialmente capacitado para mantener la red. Esto, junto con el software y hardware especiales, hacen que el costo de operación se encarezca. Incluso con sus desventajas, la red cliente-servidor en realidad es la única opción para las organizaciones con más de diez usuarios.

b) Control de la red.

Una cuenta de conexión identifica al usuario de red en el sistema de red. Esta cuenta, junto con la contraseña del usuario, identifican y suministran acceso a los recursos del sistema de red. Los derechos del usuario son establecidos por un administrador para permitir o denegar el acceso a un recurso de la red en particular.

Los grupos son agrupaciones lógicas de usuarios en la red. La forma en que funcionan los grupos es que los derechos y permisos se otorgan al grupo, en lugar de que se le otorguen a un usuario individual. Pero el método más eficiente en redes grandes es trabajar con grupos.

Los términos política y perfiles no tienen que ver con los recursos del sistema sino con la forma en que el usuario interactúa con la estación de trabajo.

Todos los aspectos se pueden resumir de este modo. Los derechos de red, las cuentas de conexión, las contraseñas y los grupos, así como también los perfiles y las políticas suministran una forma para que el administrador del sistema pueda controlar el acceso y las restricciones a los servicios de red y pueda controlar la estación de trabajo de usuario local. Ser un administrador de red también implica un conjunto de derechos y privilegios otorgados en la red.

5.2.7 Resolución de problemas de la red

Método científico.

La resolución de problemas de la redes es un proceso sistemático que se aplica para solucionar los problemas en la red. Una técnica para diagnosticar las fallas es el método científico. En la primera lista aparece el método científico real y en la segunda lista aparece el método científico que apunta específicamente a la resolución de problemas.

Método científico:

a) Observar algún aspecto del universo.
b) Inventar una teoría que sea coherente con lo que se haya observado.
c) Utilizar la teoría para hacer predicciones.
d) Probar esas predicciones mediante experimentos u observaciones futuras.
e) Modificar la teoría según los resultados.
f) Ir al paso c.

Método científico para la resolución de problemas:

a) Identificar el problema de la red/el usuario.
b) Reunir datos acerca del problema de la red/del usuario.
c) Analizar los datos para obtener una solución posible para el problema.
d) Implementar una solución en la red para tratar de corregir el sistema.

e) Si no se puede solucionar el problema, deshacer los cambios anteriores y modificar los datos.
f) Ir al paso c.

Es necesario saber cómo mantener la red y hacer que funcione a un nivel aceptable. Esto significa que se debe saber diagnosticar los problemas a medida que surjan. Además, se debe saber cuándo resulta necesario expandir o cambiar la configuración de la red para cumplir con las necesidades cambiantes de los usuarios de la red en el Instituto.

5.2.8 Monitoreo de la red

a) Monitoreo de la red.

Los dos motivos principales para el monitoreo de una red, son la predicción de los cambios para el crecimiento futuro y la detección de cambios inesperados en el estado de la red. Entre los cambios inesperados se pueden incluir cosas tales como la falla de un router o un switch, un "hacker" que intenta obtener acceso ilegal a la red, o una falla de enlaces de comunicación. Si no tiene la capacidad para monitorear la red, un administrador sólo puede reaccionar a los problemas a medida que ocurren, en lugar de prevenir estos problemas antes de que se produzcan.

b) Monitoreo de las conexiones.

Una de las formas más básicas de monitoreo de las conexiones se produce diariamente en una red. El proceso de conexión de los usuarios a la red verifica si las conexiones funcionan correctamente; de lo contrario, será necesario contactarse con el departamento de Cómputo de inmediato. Este no es el método más eficiente o preferible para monitorear las conexiones. Existen programas simples que permiten que el administrador ingrese una lista de direcciones IP de hosts, y se hace ping a estas direcciones de forma periódica. Si hay un problema de conexión, el programa advierte al administrador con el resultado del ping. Esta es una forma muy ineficiente y primitiva de monitorear la red, pero siempre es mejor que no hacer nada.

c) Monitoreo del tráfico.

El monitoreo del tráfico es un método mucho más sofisticado de monitoreo de la red. Analiza el tráfico real de paquetes en la red y genera informes basados en el tráfico de la red.

d) Protocolo de administración de red simple.

SNMP es un protocolo que permite que la administración transmita datos estadísticos través de la red a una consola de administración central. SNMP es un componente de la Arquitectura de Administración de Red. La Arquitectura de Administración de Red se compone de cuatro componentes principales.

- Estación de administración es la interfaz del administrador de red al sistema de red. Posee los programas para manipular los datos y controlar la red. La estación de administración también mantiene una base de datos de información de administración (MIB) extraída de los dispositivos bajo su administración.

- Agente de administración es el componente incluido en los dispositivos que se deben administrar. Puentes, routers, hubs y switches pueden contener agentes SNMP que les permitan ser controlados por la estación de administración.

- Base de información de administración. La base de información de administración tiene una estructura de base de datos y reside en cada dispositivo administrado. La base de datos contiene una serie de objetos, que son datos sobre recursos reunidos en el dispositivo administrado. Algunas de las categorías en el MIB incluyen datos de interfaz de puerto, datos de TCP y datos de ICMP.

- Protocolo de administración de red. El protocolo de administración de red utilizado es SNMP. SNMP es un protocolo de capa de aplicación diseñado para comunicar datos entre la consola de administración y el agente de administración. Una de las mejoras principales de SNMP se denomina Monitoreo Remoto (RMON). Las extensiones de RMON a SNMP brindan la capacidad para observar la red como un todo, en contraste con el análisis de dispositivos individuales.

e) Monitoreo remoto (RMON).

Las sondas reúnen datos remotos en RMON. Una sonda tiene la misma función que un agente SNMP. Una sonda tiene capacidades de RMON; un agente no las tiene. Al trabajar con RMON, tal como ocurre con SNMP, una consola de administración central es el punto de reunión de datos. Una sonda RMON se ubica en cada segmento monitoreado de la red. Estas sondas reúnen los datos especificados de cada segmento y los derivan a la consola de administración.

La extensión RMON del protocolo SNMP crea nuevas categorías de datos. Estas categorías agregan más ramas a la base de datos MIB.

- Grupo de estadísticas de Ethernet.
- Grupo de control de historial.
- Grupo de alarma.
- Grupo de host.
- Grupo de Host TOPN.
- Grupo de matriz.
- Grupo de filtro.
- Grupo de paquete.
- Grupo de sucesos.
- Grupo Token-Ring.

Conclusiones.

CONCLUSIONES

El rediseño de la red se realizó de acuerdo a las necesidades presentes y futuras del personal del Instituto. En primera instancia, se planteó un nuevo cableado (recableado) en zonas especificas que abarca más de un 80% de la red del Instituto, ya que el cableado principal en su mayoría utilizaba cable coaxial lo cual fue un factor importante ya que es la antesala para obtener una red eficiente. El cableado es estructurado conforme a las especificaciones planteadas en el estudio realizándose en UTP categoría 5e. Es decir se identifican cada uno de los servicios de red para una mejor administración y una pronta respuesta de parte del administrador en caso de presentarse alguna contingencia.

El diseño de la red se planteó como un diseño Jerárquico, Redundante y de Seguridad, permitiendo un crecimiento adecuado y ordenado de la misma. En donde el rediseño se dio a través de una red switcheada en su totalidad, lo que permitirá la inclusión de nuevas tecnologías para obtener otros servicios dentro de la red tales como: Voz sobre IP (VoIP) y videoconferencia sobre IP.

El funcionamiento de la red tuvo una mejora significativa en los tiempos de respuesta de la red interna, debido a las medidas implementadas tales como:

La redefinición de los recursos y servicios. Un balanceo adecuado de los servidores, estaciones, impresoras y de más equipo así como las aplicaciones instaladas en ellos, es decir, existían servidores que tenían mucha demanda de recursos y servicios, a los que se les fue quitando la sobrecarga y repartirla adecuadamente entre los demás, los cuales tenían una baja demanda.

La red switcheada permitió un intercambio de información mucho más ágil y eficiente, esto de manera interna, sin embargo el intercambio de información con el exterior –Internet-, aunque mejoró aceptablemente, sigue dependiendo de los enlaces que Red-UNAM tiene hacia Internet y, por lo tanto, a la saturación de la misma.

Las políticas presentadas para el Instituto pretenden que cada uno de los usuarios respete los lineamientos y derechos que corresponden solo a los administradores de la red de cómputo, tales como la instalación de puntos de red, instalación de hubs, switches y otros dispositivos para aumentar el número de servicios en un lugar. Además se presentan políticas sobre el uso adecuado de los recursos de red, sobre la confidencialidad de la información y sobre todo de su seguridad.

Con las medidas anteriormente mencionadas y las pruebas hechas en DGSCA, se pretende que la red funcione eficientemente por los próximos 5 años, con un adecuado mantenimiento preventivo y correctivo .

La red soporta actualmente tecnologías Ethernet, Fast Ethernet y Gigabit Ethernet; y en un futuro muy próximo y en el caso que se requiriere, soportará las nuevas tecnologías como 10 Gigabit Ethernet; sólo haciendo modificaciones en el equipo de core de la red del Instituto.

De acuerdo al comportamiento de la red en el momento en que se estuvieron haciendo los cambios, se externa la satisfacción total del rediseño de esta red al observar los tiempos de respuesta en el intercambio de información de manera interna y dentro de los límites de Red-UNAM, y a su vez un mejoramiento en el intercambio de información hacia Internet.

Anexo A

Croquis de las Instalaciones del Instituto de Geofísica.

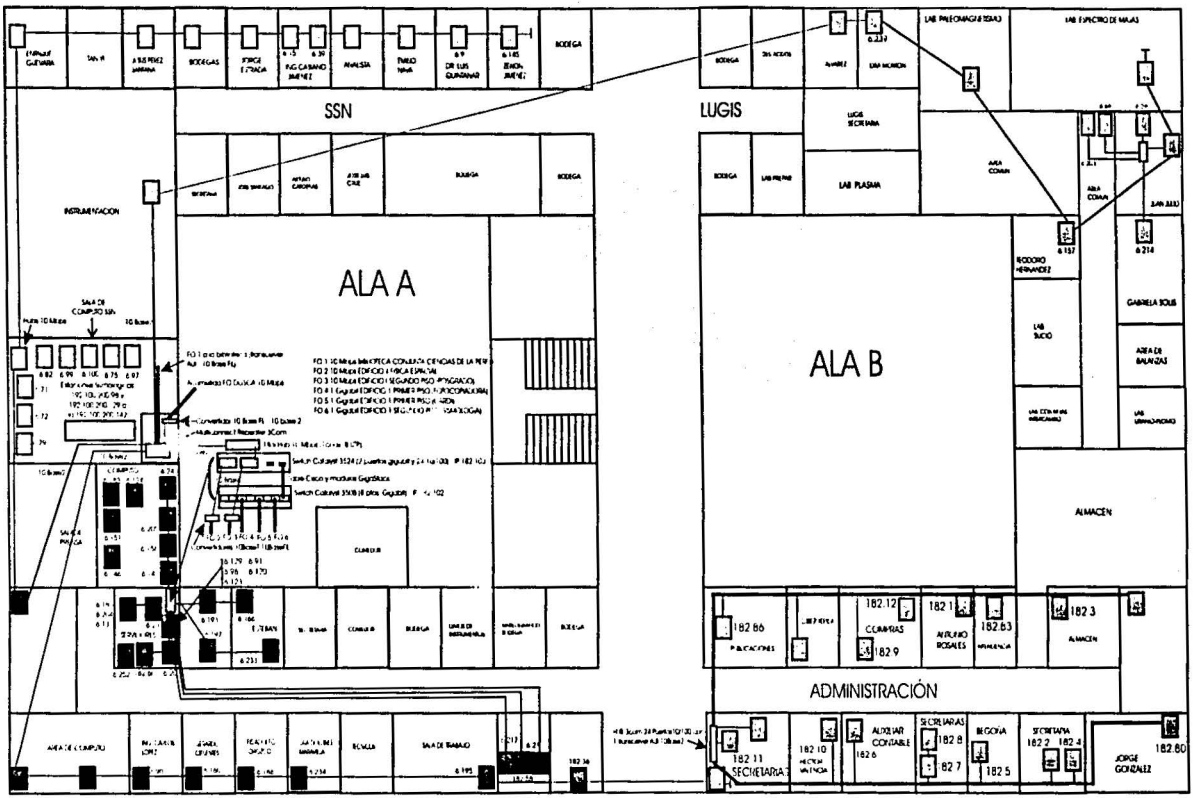


Figura A1. Edificio I Planta Baja.

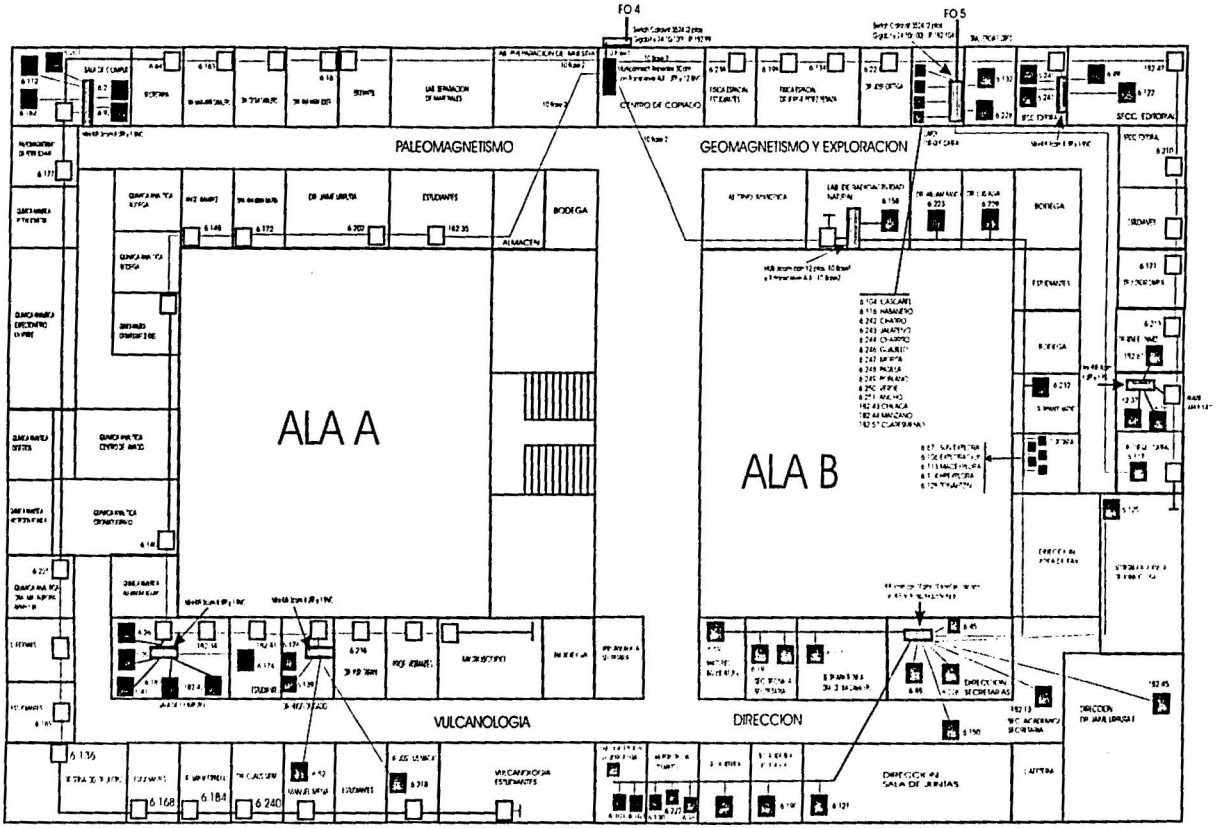


Figura A2. Edificio I Primer Piso.

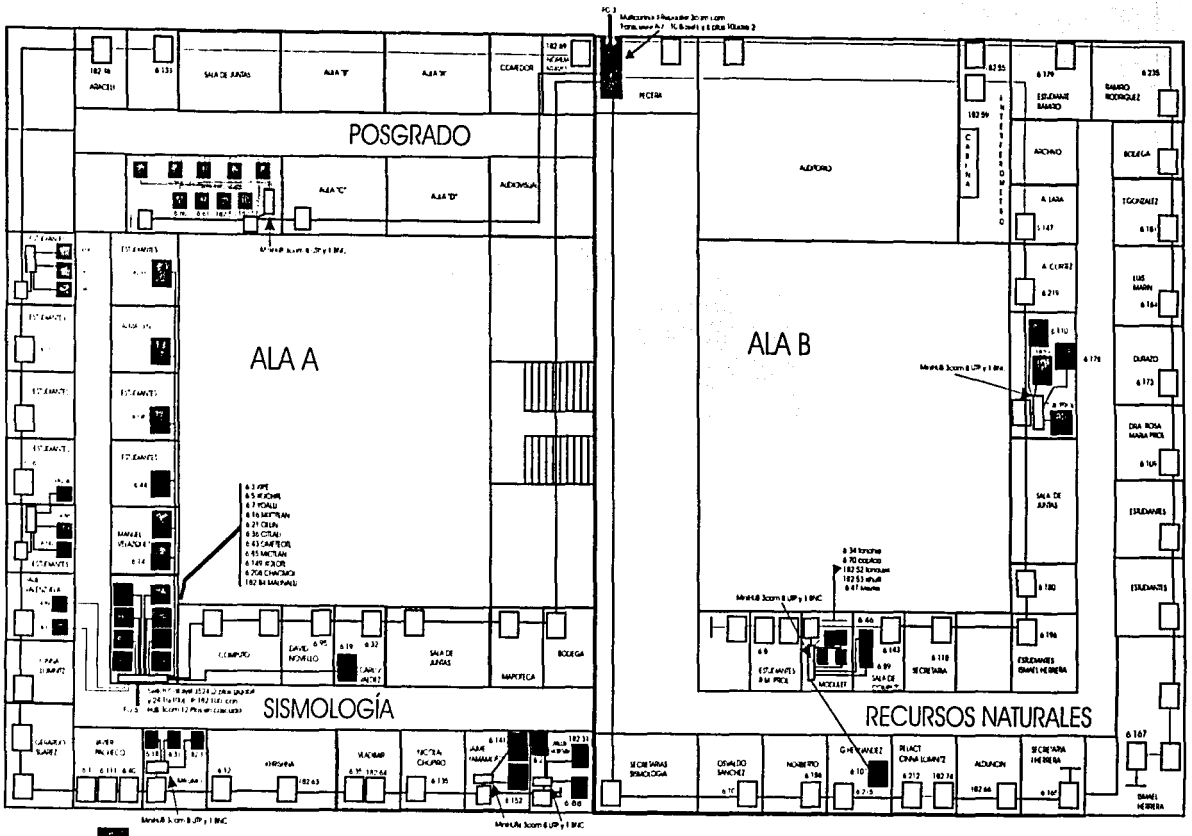


Figura A3. Edificio I Segundo Piso.

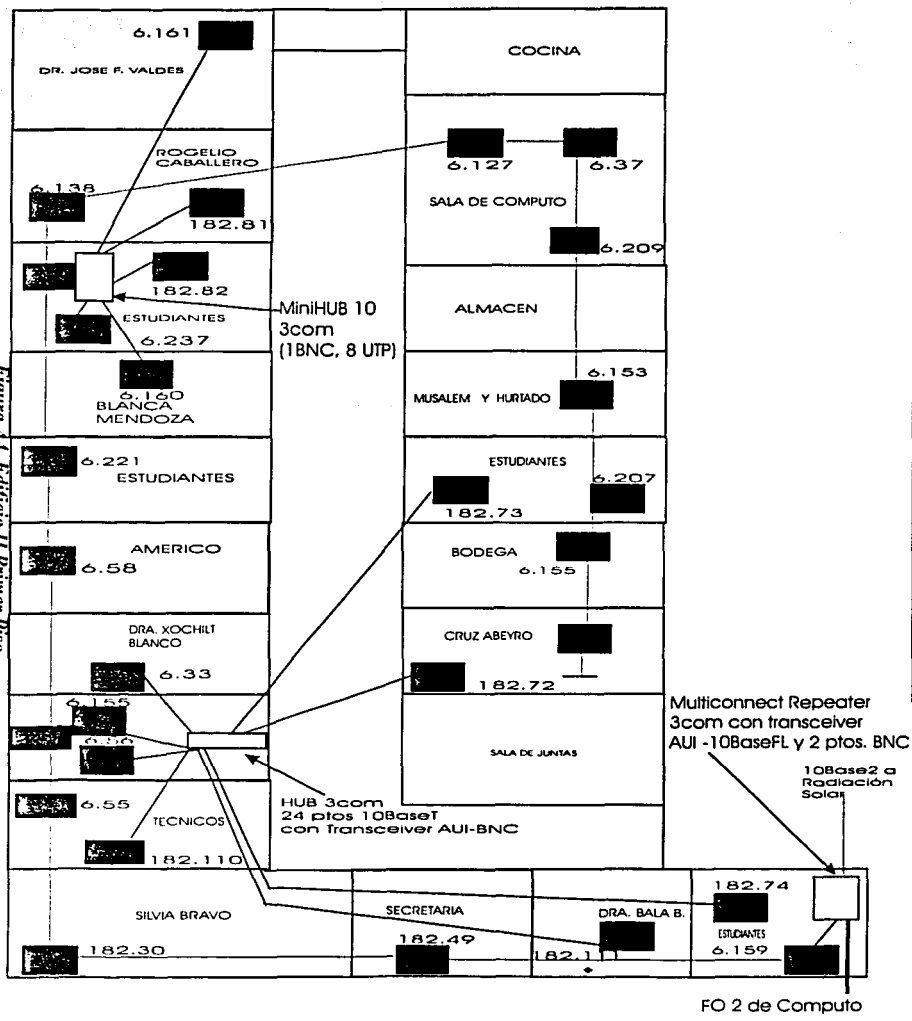


Figura A4. Edificio II Primer Piso.

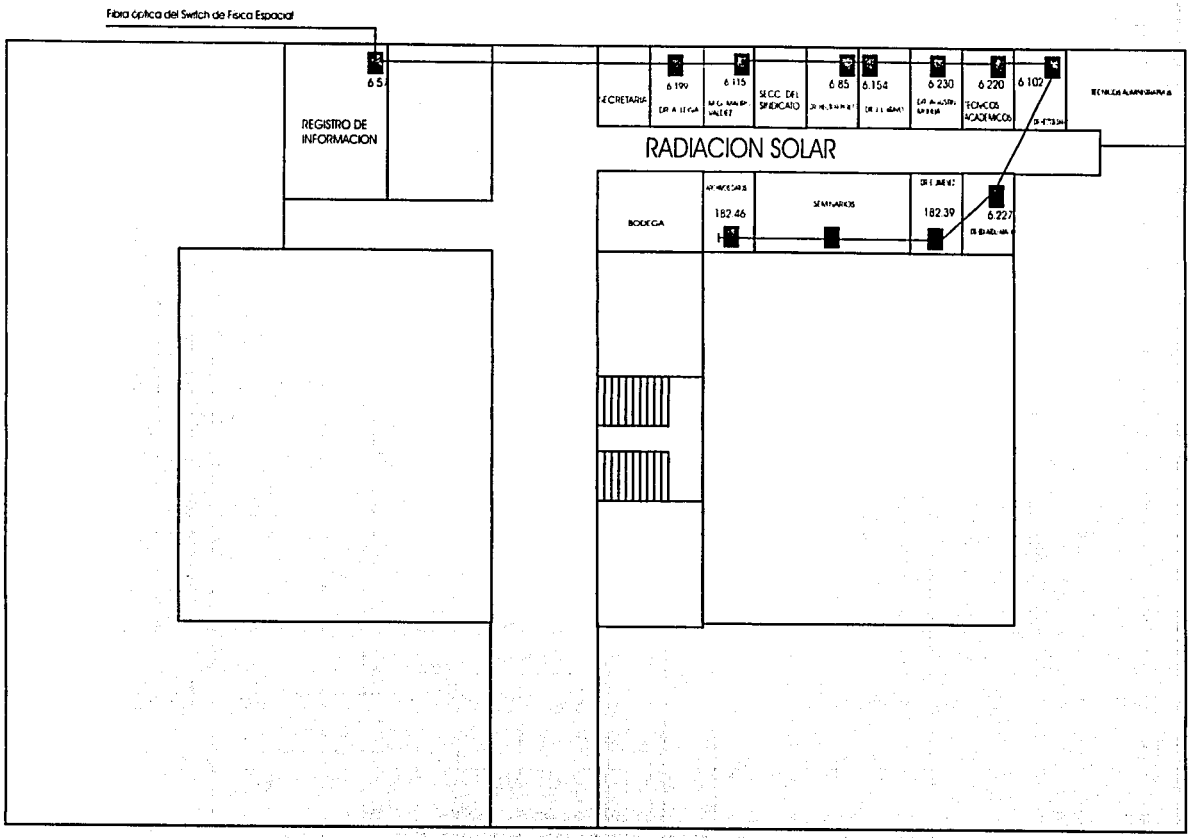


Figura A5. Edificio II Planta Baja.

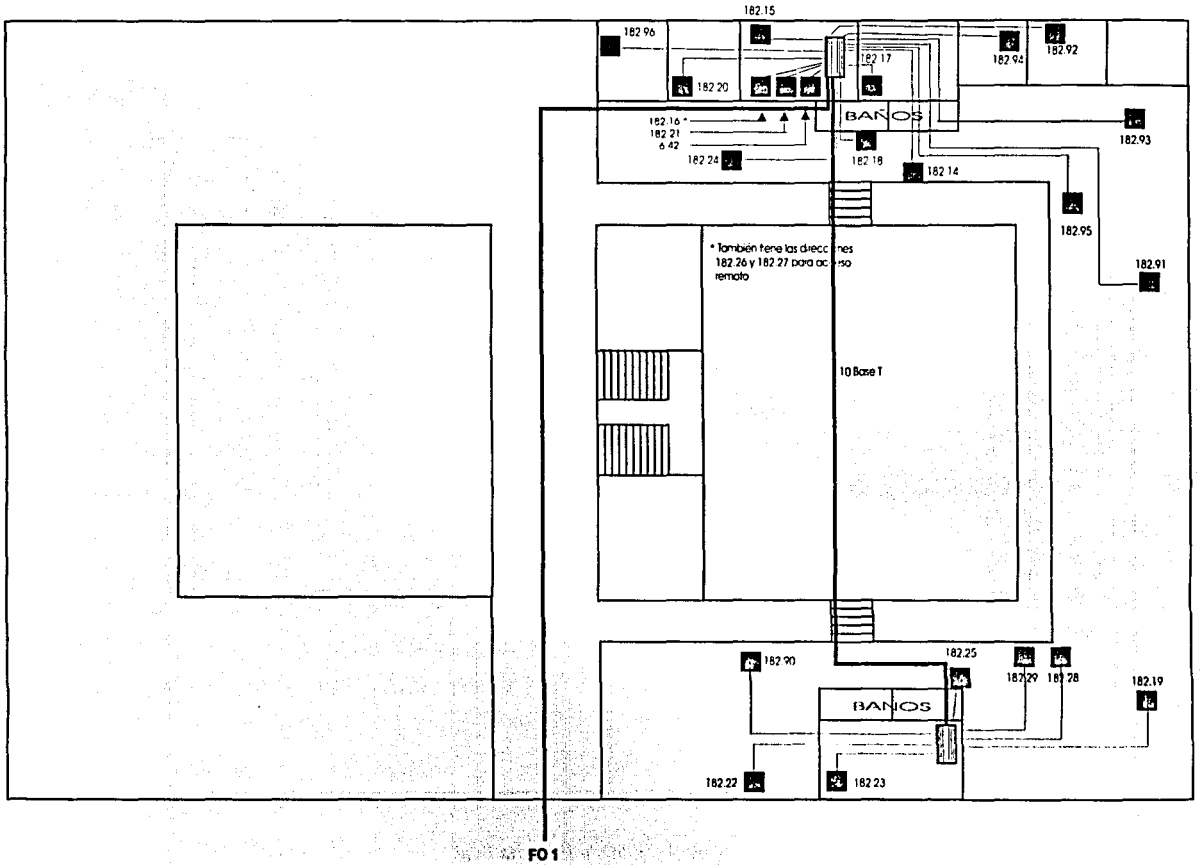


Figura A6. Biblioteca – Ciencias de la Tierra.

Anexo B

Imágenes del Equipamiento de la Red de Cómputo.

ANEXO B: IMÁGENES DEL EQUIPAMIENTO DE LA RED DE CÓMPUTO DEL INSTITUTO DE GEOFÍSICA

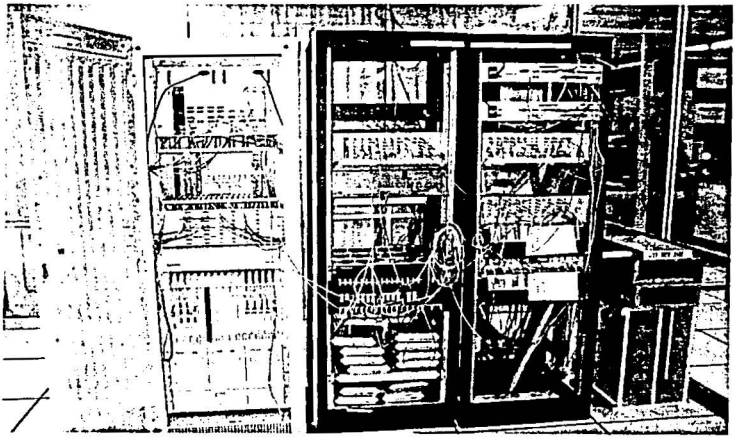


Figura B1. Rack en el edificio de IIMAS.

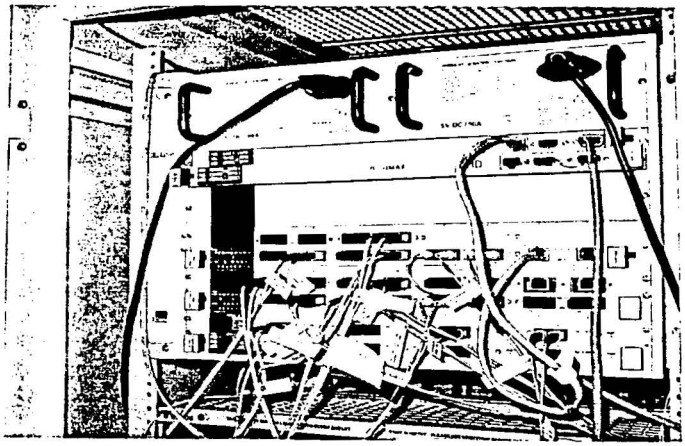


Figura B2. Cellplex en IIMAS (Conexión hacia Instituto de Geografía).

Figura B3.- Instituto de Geografía.

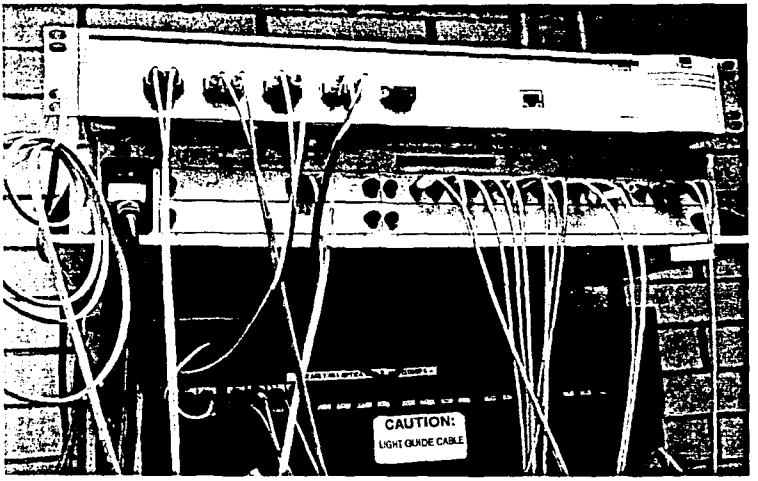


Figura B4.- Lanplex 2500 en ele Instituto de Geografía (Conexión hacia el Instituto de Geofísica).

INSTITUTO DE GEOFÍSICA.

Figura B5.- Edificio principal del Instituto de Geofísica.

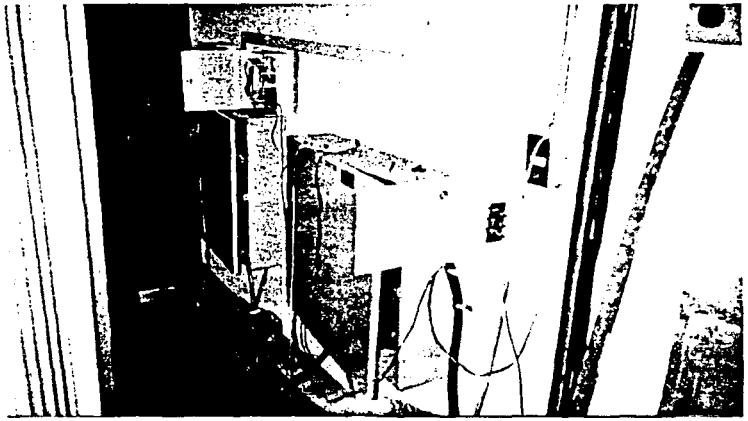


Figura B6.- Llegada del Lanplex 2500 del Instituto de Geografía (puerto 2) al enlace principal en el Instituto de Geofísica.

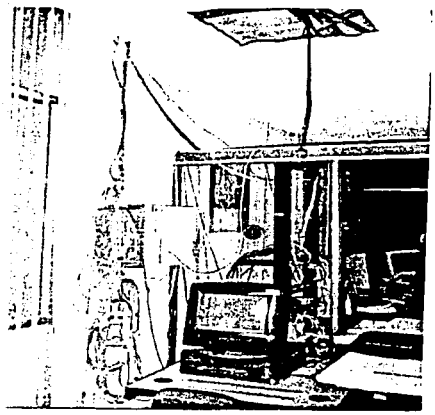


Figura B7.- Multiconect para la llegada del enlace principal al Instituto (antes).

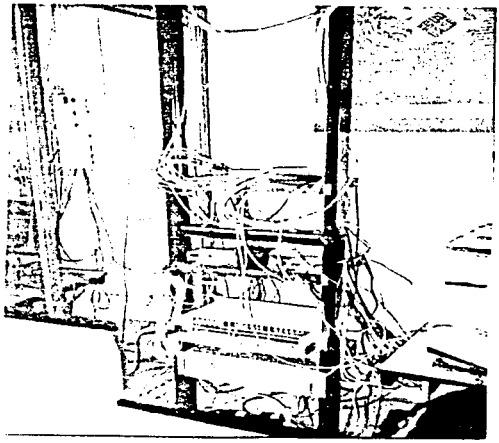


Figura B8.- Rack principal en el Departamento de Cómputo del Instituto -antes- (Contiene: Switch Catalyst 3524 MXL, Switch Catalyst 3508 MXL, hub de 8 puertos a 10/100 Mbps).

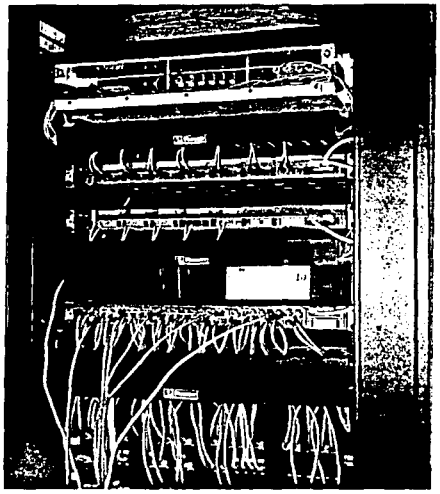


Figura B9.- Rack actual en el Departamento de Cómputo del Instituto (Contiene: Switch Catalyst 3524 MXL, 2 Switches Catalyst 3508 MXL, hub de 8 puertos a 10/100 Mbps y patchs panels).

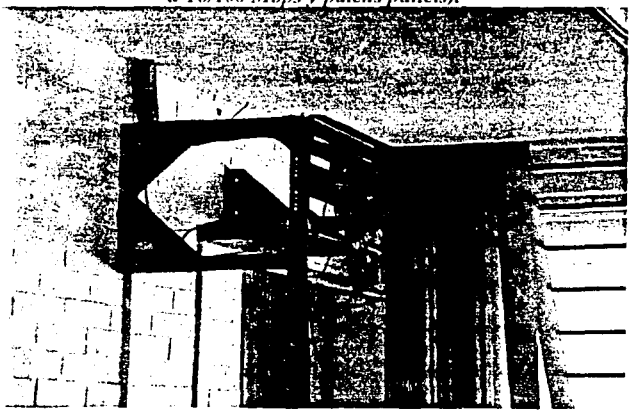


Figura B10.- Switch Catalyst 3524 MXL en el LUGIS (cuarto limpio).

PRIMER PISO DEL INSTITUTO DE GEOFÍSICA.

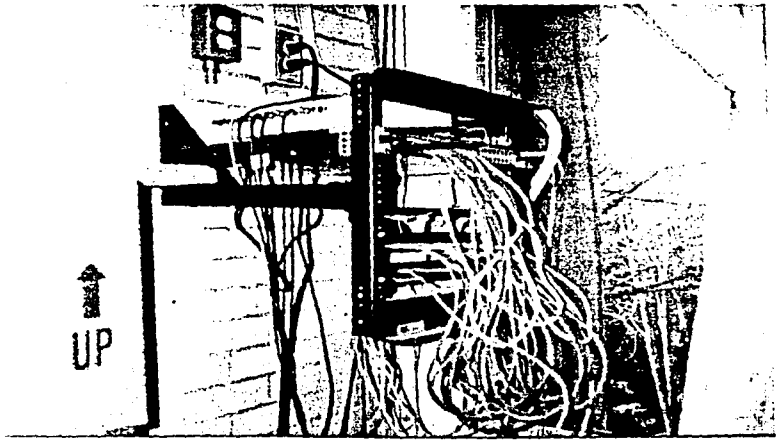


Figura B11.- Switch 3548 MXL en el Centro de Fotocopiado.

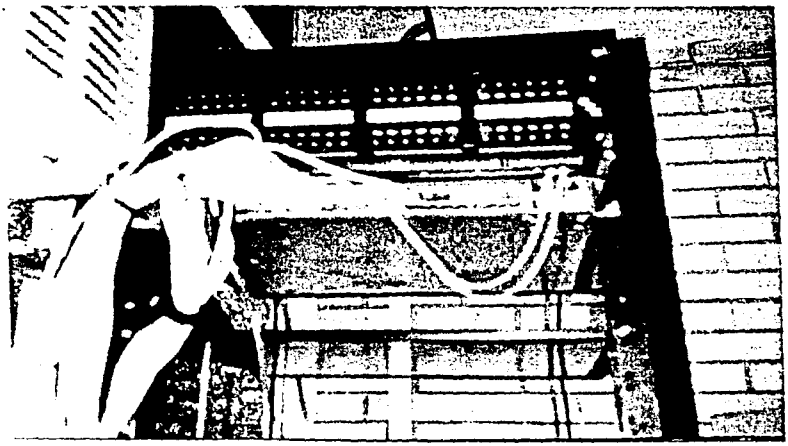


Figura B12.- Switch Catalyst 3548 MXL en el CARDI.

SEGUNDO PISO DEL INSTITUTO DE GEOFÍSICA.

Figura B13.- Entrada al Departamento de Sismología.

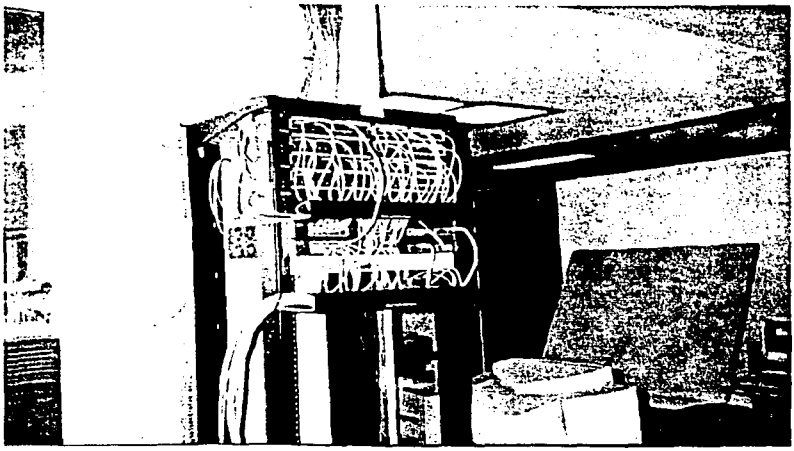


Figura B14.- Switches Catalyst 3524 MXL en el Departamento de Sismología.

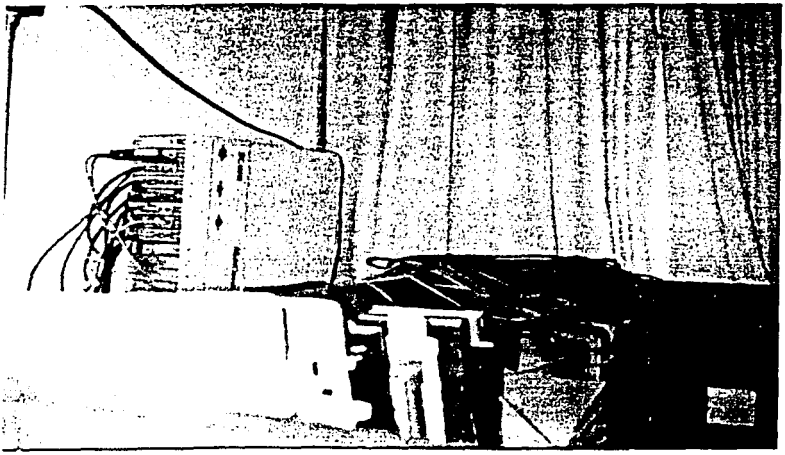


Figura B15.- Multiconect de Posgrado (antes de la sustitución).

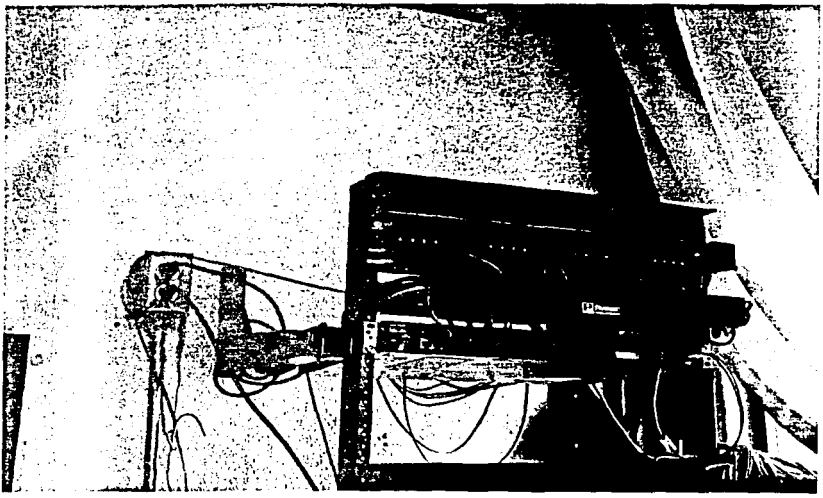


Figura B16.- Switch de Posgrado (después de la sustitución).

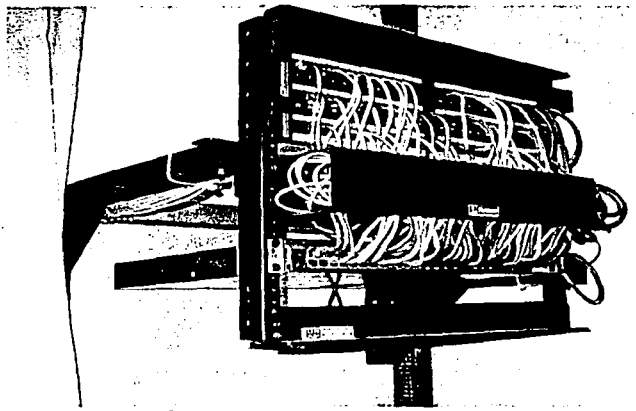


Figura B17.- Switch Catalyst 3548 MXL en el Departamento de Recursos Naturales.

EDIFICIO II.

Figura B18.- Edificio II del Instituto de Geofísica.

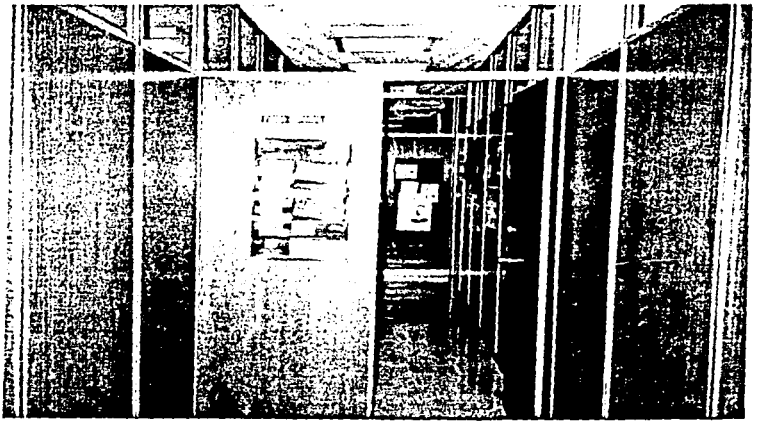


Figura B19.- Entrada al Primer Piso del Edificio II (Física Espacial).

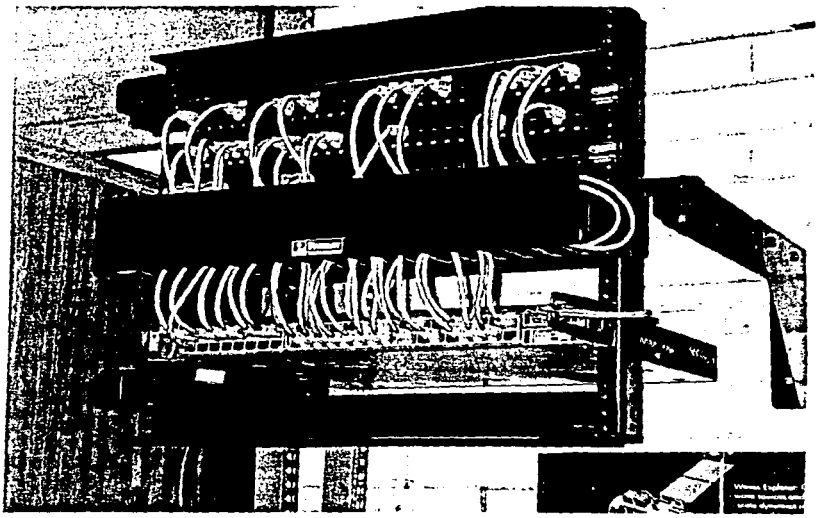


Figura B20.- Switch Catalyst 3548 MXL en el Departamento de Física Espacial.

Figura B21.- Entrada a la Planta Baja del Edificio II (Radiación Solar).

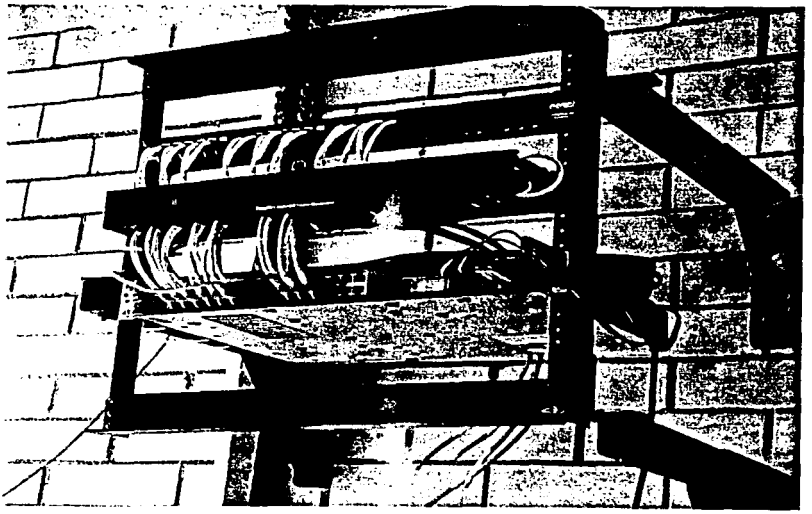


Figura B22.- Switch Cisco Catalyst 3524 M-XL en el Departamento de Radiación Solar.

EDIFICIO ANEXO.

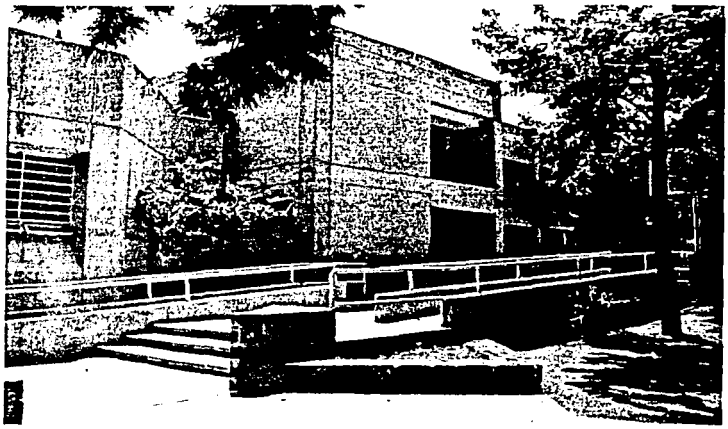


Figura B23.- Edificio Anexo.

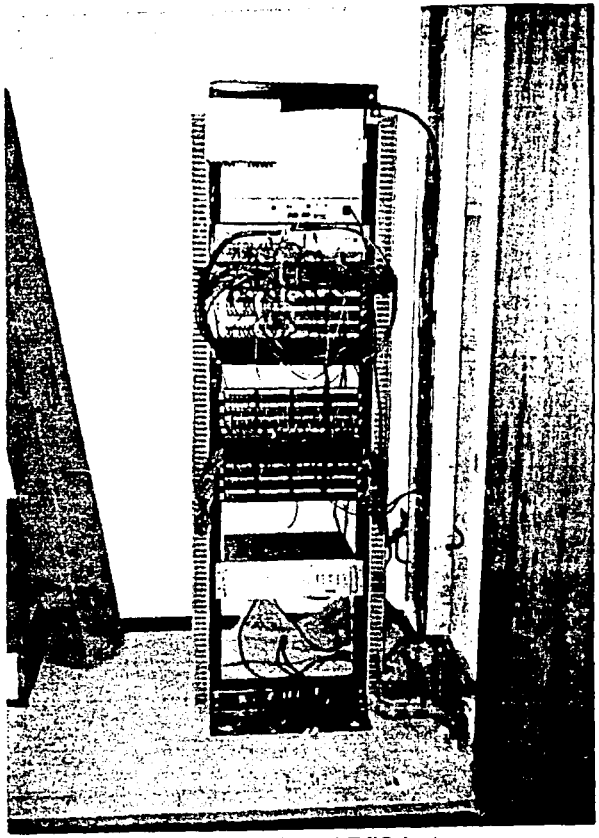


Figura B24.- Rack en el Edificio Anexo
(Conexión del Instituo de Geografía, puerto 6 del Lanplex 2500).

BIBLIOTECA.

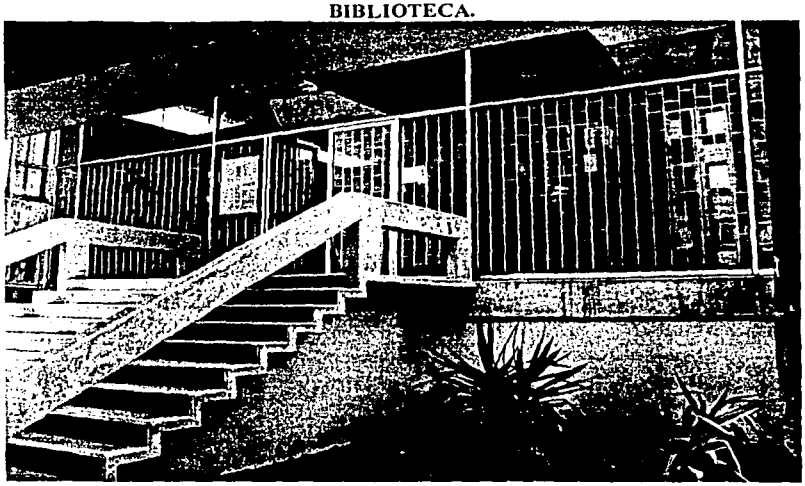


Figura B25.- Entrada a la Biblioteca del Instituto de Geofísica. (Edificio conjunto con el CICH).

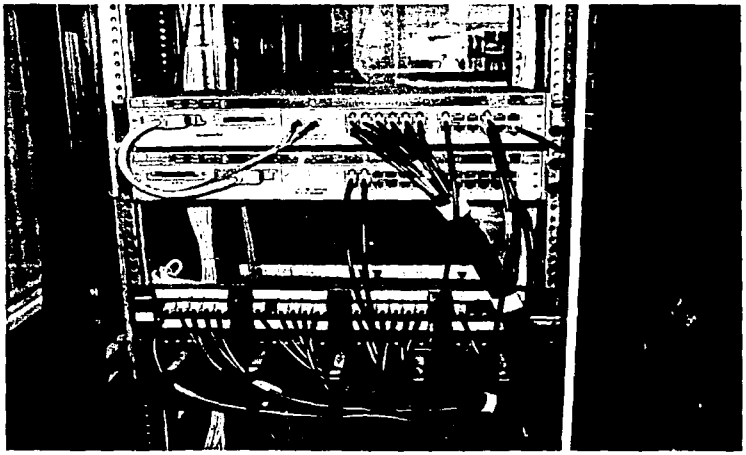


Figura B26.- Hubs apilados en el rack de la Biblioteca.

Anexo C

Normatividad de Telecomunicaciones DGSCA-U.N.A.M.

ANEXO C: NORMATIVIDAD DIRECCIÓN DE TELECOMUNICACIONES DGSCA, UNAM

Una vez que se ha culminado con el análisis y el rediseño de la red de cómputo del Instituto de Geofísica, ahora sólo nos resta proponer las Políticas para la Administración de la Red de Cómputo del Instituto, con esto obtener un correcto funcionamiento de la red, un adecuado crecimiento de ella, además información segura y confiable.

Cabe señalar, que por ser una Dependencia de la UNAM, el Instituto debe de cumplir con algunas de las reglas generales que son publicadas por DGSCA, que se aplican a todas y cada una de las Dependencias universitarias. De igual manera, es necesario tener presente las políticas de seguridad de la información, publicadas por el Área de Seguridad en Cómputo de la DGSCA.

En este capítulo, se presentarán en primera instancia las principales Políticas de DGSCA[1] en su área de Telecomunicaciones que hacen referencia al uso adecuado de los recursos de red y conectividad de cada una de las redes de las dependencias universitarias. El segundo plano se presenta un compendio de políticas del Área de Seguridad de DGSCA (www.asc.unam.mx) y de otras políticas publicadas en diversos artículos en la página de Cisco System (www.cisco.com), todas ellas aplicables al Instituto de Geofísica. con el fin de mantener protegida la información de posibles violaciones, ataques y huecos donde se puedan infiltrar terceros (intrusos).

Disposiciones generales publicadas por la dirección de telecomunicaciones de la DGSCA

1. Para efectos del presente documento se entenderá por:
   DGSCA: a la Dirección General de Servicios de Cómputo Académico

2. La DGSCA será la única instancia facultada para regular la instalación del equipo de telecomunicaciones.

3. La DGSCA se encargará de unificar y estandarizar la tecnología en materia de telecomunicaciones para ofrecer un adecuado servicio a las dependencias.

4. La DGSCA mantendrá y garantizará la seguridad e integridad de la infraestructura de telecomunicaciones, por tal motivo se restringe el uso de equipos y programas de análisis y medición de la red de telecomunicaciones (Sniffer y Scanners) a esta instancia.

[1] Las políticas de DGSCA se encuentran disponibles en la siguiente liga : http://www.dtd.unam.mx/Normatividad.html

5. La DGSCA establecerá los procedimientos necesarios para que todo gasto generado por la instalación de los servicios de telefonía y red quede reflejado por dependencia.

6. Con objeto de planear y coordinar los cambios derivados de remodelaciones o modificaciones a sus instalaciones, las dependencias deberán notificar a la DGSCA para que coordine la proyección de los cambios que afecten la infraestructura de Telecomunicaciones, evitando de esta forma que se dañe o fraccione la misma en las dependencias universitarias.

7. La Comisión de Telecomunicaciones propondrá proveedores para la adquisición de equipo de telecomunicaciones, y de esta forma el Comité de Compras y Servicios de la UNAM designe a los mejores, conforme a la normatividad vigente.

8. La DGSCA, después de evaluar la calidad, seriedad y solidez de las empresas de mantenimiento de equipo de telecomunicaciones, emitirá un catálogo de proveedores registrados que darán mantenimiento al equipo de telecomunicaciones.

9. El titular de cada dependencia será responsable de que todo el equipo de telecomunicaciones cuente con mantenimiento preventivo y correctivo durante la vida útil del equipo.

a) Disposiciones particulares

La DGSCA será la instancia facultada para el desarrollo y administración de RedUNAM con las siguientes atribuciones:

10. Administrará y asignará todas las direcciones IP de la UNAM.

11. Cederá o retirará la administración total o parcial de las direcciones IP de la UNAM a las dependencias universitarias, cuando lo considere conveniente.

12. Representará a Red-UNAM ante los organismos reguladores de Internet a nivel nacional e internacional.

13. Administrará todos los dominios y subdominios asignados a la UNAM y de los servidores encargados de su resolución.

14. La DGSCA será la única instancia facultada para proveer la conexión de Red-UNAM a instituciones externas.

15. Cualquier servicio de Red UNAM no puede ser usado para transferir información cuyo contenido sea ilegal, peligroso, invasor del derecho de la privacidad, en cualquier otra forma ofensivo a tercero o violador de los derechos de autor, marcas o patentes.

16. Para cualquier trámite o servicio de Red-UNAM que el usuario solicite a DGSCA, este queda obligado a proporcionar información verídica, correcta, actual y completa a esta.

17. No se permite enviar a través de Red UNAM mensajes no solicitados (SPAM o de la misma índole), mensajes tipo cadenas o con archivos que contengan virus que dañen equipo de cómputo de terceros.

18. La DGSCA se reserva el derecho de cancelar o inhabilitar cualquier tipo de servicio de Red-UNAM al usuario o dependencia que incurran en incumplimiento de cualquier punto del presente título o que afecten la operación general de Red-UNAM.

19. La dependencia deberá establecer uno o dos responsables que sea(n) el o los único(s) contacto(s) para trámites técnico-administrativos de la red de esa dependencia ante la DGSCA.

20. La información y los recursos disponibles a través de Red-UNAM son privados y sus dueños tienen todos los derechos, a menos que renuncien explícitamente a ellos.

21. RedUNAM no tiene ninguna responsabilidad por el contenido de los datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

22. Los usuarios serán responsables del uso que le den a Red-UNAM y no utilizarán sus servicios de manera desmedida para evitar cargas excesivas.

23. Las actividades de los usuarios de la red no podrán ser interferidas o entorpecidas por cualquier medio o evento que no haya sido solicitado expresamente por los mismos.

24. Cuando se detecte un uso indebido de la Red-UNAM, se cancelarán las claves de usuario o se desconectarán los equipos o redes involucrados, temporal o permanentemente.

b) De la conectividad

25. Cada dependencia contará con un plan de desarrollo a mediano plazo que abarque, entre otros puntos, el crecimiento de su red local basado en criterios de uso.

26. Las dependencias que requieran una conexión a Red-UNAM, expansión en su red local o reubicación de puntos de red por remodelaciones en sus instalaciones, lo solicitarán a la DGSCA mediante el procedimiento establecido para tal efecto.

27. Toda expansión o cambio en la estructura de la red de una dependencia será asesorada, supervisada y autorizada por la DGSCA.

28. Las dependencias que no cuenten con un proyecto para la expansión o remodelación de su red, serán apoyadas por la DGSCA con la asesoría para el diseño de la red local, diseño de las canalizaciones o ductos internos y externos, tecnología de cableado, cuantificación y características del equipo activo.

29. Las dependencias que cuenten con un proyecto para efectuar una expansión en su red o una remodelación en sus instalaciones, que afecte la estructura de la misma, solicitarán a la DGSCA la revisión y Vo.Bo de dicho proyecto, y de no aprobarse, la DGSCA propondrá un nuevo proyecto a la dependencia en cuestión.

30. Las dependencias universitarias asignarán a una persona encargada de la administración de la red local el cual cumplirá con las siguientes funciones

- Fungirá como punto de contacto con la DGSCA para el seguimiento y resolución de las fallas, actualización de las bases de datos del servicio de resolución de nombre (DNS, Domian Name Service), solicitud de asignación de direcciones IP y asesorías técnicas;

- Administrará las Direcciones IP de la dependencia;

- Proporcionará a la DGSCA documentación actualizada de la red local: planos de cableado, ubicación del equipo y relación de las asignaciones de direcciones IP;

- Administrará los servicios locales de red como son WWW, correo electrónico, servidor de FTP y servidores de aplicaciones en red, entre otros;

- Solucionará fallas menores como son: cables desconectados, pérdida de suministro de energía eléctrica en los equipos de datos, desconfiguración de las computadoras de los usuarios o direcciones IP repetidas.

31. Cada dependencia fomentará el desarrollo de aplicaciones y servicios propios de la dependencia, entre ellos: servicio de correo electrónico basado en el protocolo SMTP(Simple Mail Transfer Protocol), servidor de WWW, servidor FTP, configuración de equipos y servidor de impresión.

c) De las cuentas de correo electrónico y de acceso a Internet vía módem a través de RedUNAM

32. La DGSCA será la única instancia autorizada para proveer el servicio de acceso a Internet vía módem a través de Red-UNAM.

33. La asignación de las cuentas se otorgará dando prioridad al personal académico y a los estudiantes de la UNAM.

34. La renovación de claves de correo electrónico y de acceso vía telefónica se efectuará de acuerdo al procedimiento establecido para tal efecto.

35. Todas las cuentas de acceso a Internet vía módem a través de Red-UNAM y a los servidores son personales e intransferibles, por lo que únicamente pueden ser usadas por los propietarios de las mismas, siendo el poseedor de la clave el responsable de la confidencialidad de la contraseña correspondiente.

Bibliografía.

BIBLIOGRAFÍA

ACADEMIA DE NETWORKING DE CISCO SYSTEMS: GUIA DEL PRIMER AÑO.
AMATO VITO.
EDITORIAL: CISCO SYSTEMS.

REDES DE COMPUTADORAS. PROTOCOLOS, NORMAS E INTERFACES.
BLACK ULYSES.
EDITORIAL: ALFA OMEGA

SWITCHED, FAST, AND GIGABIT ETHERNET.
BREYER ROBERT & SEAN RILEY.
EDITORIAL: McMILLAN TECHNICAL PUBLISHING.

COMUNICACIONES Y REDES DE PROCESAMIENTO DE DATOS.
GONZÁLES SAINZ, NESTOR.
EDITORIAL: McGRAW-HILL.

APRENDIENDO REDES EN 24 HORAS
HAYDEN MATT
EDITORIAL: PRENTICE HALL

TECNOLOGÍAS DE INTERCONECTIVIDAD DE REDES.
MERILEE FORD, KIM LEW.
EDITORIAL: PRENTINCE HALL.

TOP AND DOWN NETWORK DESIGN.
OPPENHEIMER, PRISCILLA.
EDITORIAL: CISCO PRESS.

GUÍA DE REDES DE ALTA VELOCIDAD.
PARNELL TERÉ
SERIE: LAN TIMES.
EDITORIAL: OSBORNE McGRAW-HILL.

GUÍA DE REDES DE ÁREA EXTENSA.
PARNELL TERÉ
SERIE: LAN TIMES.
EDITORIAL: OSBORNE McGRAW-HILL.

REDES DE ORDENADORES.
TANENBAUM ANDREWS.
EDITORIAL: PRENTINCE HALL HISPANOAMERIACANA.

ENCYCLOPEDIA OF NETWORKING.
SHELDON TOM.
SERIE: LAN TIMES.
EDITORIAL: OSBORNE McGRAW-HILL.

ETHERNET: THE DEFINITIVE GUIDE.
SPURGEON CHARLES E.
EDITORIAL: O'REILLY.

TODO ACERCA DE REDES DE COMPUTACIÓN.
STOLTZ, KEVIN.
EDITORIAL: PRENTINCE HALL HISPANOAMERIACANA.

DIRECCIONES ELECTRÓNICAS

AMERICAN NATIONAL STANDARDS INSTITUTE
www.ansi.org

ÁREA DE SEGURIDAD EN CÓMPUTO, DGSCA. UNAM
www.asc.unam.mx/Tutoriales/Tutoriales/politicas/index.html

CISCO SYSTEMS
www.cisco.com

- Interworking Design Basics
  www.cisco.com/univered/cc/td/doc/cisintwk/idg4/nd2002.htm

- Gigabit Campus Netwok Design. Principles and Architecture
  www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.htm

DIRECCIÓN DE TELECOMUNICACIONES, DGSCA, UNAM
www.dtd.unam.mx/Normatividad

EXTREME NETWORKS
www.extremenetworks.com

FOUNDRY NETWORKS
www.foundrynetworks.com

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
www.ieee.org

RED IRIS
www.rediris.es/rediris/boletin/46-47/ponencia9.html