UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

OPTIMIZACIÓN DE LA RED DE DATOS LAN PARA UNA INSTITUCIÓN EDUCATIVA

T E S I S

Que Para Obtener El Título De

Ingeniero En Computación

P r e s e n t a n

HUGO FABIAN GARCIA REYES

MIGUEL ANGEL VALDES ZARRAGA

DIRECTOR DE TESIS:
M.C. MARCO ANTONIO VIGUERAS VILLASEÑOR

Ciudad Universitaria Mayo de 2004

TESIS DE LICENCIATURA

OPTIMIZACIÓN DE LA RED DE DATOS LAN PARA UNA INSTITUCIÓN EDUCATIVA

Agradecimientos:

Mamá
Esto es lo menos que te puedo entregar para compensar el esfuerzo que has entregado en cada momento de mi vida y esto haga que pueda seguir soñando. Eres sinónimo de Superación y Lucha Gracias Mamá.

Papá
Por la confianza que siempre me has tenido y el apoyo moral e incondicional. Gracias Papá.

Arturo
Por siempre tener palabras de aliento para impulsarme para adelante y por adentrarme a esta profesión.

Ale y Vero
Por esa Energía y esa Alegría que le han inyectado a mi vida, no dejen de mirar nunca para adelante.

Abue
Donde quiera que te encuentres se que siempre estas ahí para escucharme. Gracias

Mamita
Por todo el apoyo a mi y a mi familia y también por esa disciplina por la cual siempre la admirare.

Amigos
Por eso que nunca les voy a poder regresar y que es tan valioso... su tiempo, el cual dedicaron para compartirlo conmigo y dejarme así formar parte de sus vidas.

Faculta de Ingeniería
Por Ayudarme a sacar el carácter y poder vencer mis temores, por esa formación profesional siempre estaré agradecido.

Universidad Nacional Autónoma de México
A mi alma Mater por todo lo que me dio, por esa formación personal y por la cual siempre me sentiré Orgullosamente Universitario.

Por Mi Raza Hablará El Espíritu

México, a 21 de Junio de 2004

Hugo García

Cuando empecé a escribir este trabajo pensé que seria una buena idea marcarme un esquema con los principales capítulos y puntos que debería contener. Uno de los primeros que surgió fue éste, el de los agradecimientos. Pensé en él, como un mero tramite. Al fin y al cabo todo el mundo lo incluye en su trabajo. De hecho hasta me había planteado previamente unas líneas básicas con el fin de no olvidar nada y, sobre todo a nadie. Sin embargo, ahora que el proyecto ya esta llegando a su culminación, ahora que he pasado algunos meses inmerso en su redacción, ahora que he podido tratar y trabajar con tanta gente distinta, ahora que he tenido que robar tantas y tantas horas a mi familia y amigos, ahora que... ahora ya no me parece un mero tramite.

Se que muchos de los que lleguen realmente a leer este apartado esperarán verse reflejados de alguna forma en él. Por esta razón, quiero comenzar pidiendo mis mas sinceras disculpas a todas aquellas personas a las que no haya mencionado explícitamente y que seguro que, si están leyendo esto, deberían aparecer. Y es que en eso si tengo experiencia. Siempre hay alguien muy importante, muy cercano, muy implicado, del que me olvido.

En fin, ha llegado la hora de la verdad y, ante todo, ya tengo bastante claro por donde empezar. Mis mas sinceros agradecimientos y mi mas sincero cariño a mis padres y mi hermana. Aunque siempre que he leído esto en algún libro, no he podido dejar de pensar que suena totalmente a tópico. También en este caso, la realización de la tesis de licenciatura, me ha enriquecido de humildad. Al fin y al cabo, si ahora estoy aquí escribiendo esto, en gran medida se los debo a ellos, que fueron los primeros en creer en mi. Gracias itzel (no te preocupes te voy a pagar el dinero que me prestaste para imprimir esta tesis) pero, sobre todo, gracias mamá, gracias papá.

En segundo lugar, mis agradecimientos mas sinceros a Marco, mi director de tesis. Me siento agradecido con él por haber hecho que este trabajo haya sido muy dinámico y ameno.

En tercer lugar, a todas las personas que me hacen pasar momentos inolvidables en tantas fiestas (Augusto, Erick, Ubaldo, Bruno, Adriana, Rajael, Chinchan, PK, Elcira, Rafa, Raciel, Ciego, Pollo, Flagelo y sus hijos Diego e Irvin q.e.p.d., Gaby, David, sigan pegándole al kitsch), a todos con los que comparto experiencias memorables en el estadio y fuera de el (Bruno, Mauricio, Sochil Paola, Almudena, Ro, Pablo, Jorge, Gabriel y su novia, somos campeones Pumas), a Hugo con el que realice este proyecto y que además, es un muy buen amigo. A mi buen guru el Morris que me enseña el camino de la luz y la sabiduría. Finalmente quiero agradecer a los Pumas por el campeonato obtenido. En resumen, a todos, mi mas sincero agradecimiento. Espero tener la posibilidad de poder devolverles su inestimable ayuda y continuo apoyo.

Quiero agradecer profundamente a la Facultad de Ingeniería, por todo lo que en ella he aprendido y por brindarme una educación completa, gracias a todos los maestros que tuve el placer de conocer.

Finalmente, agradezco infinitamente a mi Alma Mater La Universidad Nacional Autónoma de México, por todo lo que representa ser la Máxima Casa de Estudios y tener el orgullo de ser miembro de ella.

Por Mi Raza Hablará El Espíritu

México, a 21 de Junio de 2004

Miguel Valdés

Índice

AGRADECIMIENTOS

FIGURAS

TABLAS

INTRODUCCIÓN 1

MOTIVACIÓN 3

ESTADO DEL ARTE 4

FORMULACIÓN DEL PROBLEMA 8

OBJETIVOS 9

ESTRUCTURA DE LA TESIS 10

CAPÍTULO 1

ASPECTOS TEÓRICOS 12

1.1 REDES DE DATOS 12

1.1.1 REDES CONMUTADAS 13

1.1.2 REDES DE DIFUSIÓN 14

1.1.3 TOPOLOGIAS DE REDES 14

1.1.4 TOPOLOGÍA JERÁRQUICA 15

1.1.5 TOPOLOGÍA EN BUS 16

1.1.6 TOPOLOGÍA EN ESTRELLA 16

1.1.7 TOPOLOGÍA EN ANILLO 17

1.2 CLASIFICACIÓN DE REDES 18
1.2.1 REDES LAN 18
1.2.2 REDES WAN 20
1.2.3 REDES WIRELESS 23

1.3 MODELO DE REFERENCIA OSI 24
1.3.1 LA CAPA FÍSICA 26
1.3.2 LA CAPA DE ENLACE 26
1.3.3 LA CAPA DE RED 29
1.3.4 LA CAPA DE TRANSPORTE 29
1.3.5 LA CAPA DE SESIÓN 30
1.3.6 LA CAPA DE PRESENTACIÓN 31
1.3.7 LA CAPA DE APLICACIÓN 31

1.4 TCP/IP 31
1.4.1 CAPAS DEL PROTOCOLO 32
1.4.2 ARP 35
1.4.3 ICMP 36
1.4.4 IP 36
1.4.5 TCP 36
1.4.6 UDP 37
1.4.7 CLASES DE REDES 37
1.4.8 MASCARA DE RED 38

1.5 VLAN'S 39

CAPÍTULO 2

PLANIFICACIÓN DE LA NUEVA RED 44

2.1 ANÁLISIS DE LA RED 44
2.1.1 DESCRIPCIÓN DE LA RED 44
2.1.2 ANÁLISIS DEL COMPORTAMIENTO DE LA RED 47
2.1.3 ANALIZADORES Y MONITORES DE LA RED 48

2.2 PLANIFICACIÓN DE LA NUEVA RED 50

2.3 PROPUESTA DE PLAN DE ACCIÓN 51
2.3.1 CONCEPTO DE SEGMENTO 53
2.3.2 SEGMENTACIÓN: SUS NECESIDADES 53

2.4 DISEÑO DE LA NUEVA RED 56
2.4.1 SWITCH SECUNDARIO DE DISTRIBUCIÓN DMZ 58
2.4.2 EQUIPOS DE ENLACE DE MICROONDAS 59
2.4.3 EQUIPO DE SEGURIDAD FIREWALL IP330 60

2.5 POSIBLES FALLAS EN EL DISEÑO 61

2.6 VENTAJAS Y DESVENTAJAS DEL NUEVO DISEÑO 63

CAPÍTULO 3

RECONFIGURACIÓN DE LA RED 65

3.1 RECONFIGURACIÓN DE LA RED 65
3.1.1 DISEÑO DNS SPLIT 67

3.2 DIRECCIONAMIENTO 69
3.2.1 PROCEDIMIENTO DE MIGRACIÓN (OPCIÓN 1) 70
3.2.2 PROCEDIMIENTO DE MIGRACIÓN (OPCIÓN 2) 72

3.3 SEGMENTACIÓN 73

3.4 CREACIÓN VLAN'S 73

3.5 IMPLICACIONES 74

3.6 RESOLUCIÓN DE PROBLEMAS 75
3.6.1 WINS 75

CAPÍTULO 4

MONITOREO Y ADMINISTRACIÓN 81

4.1 MONITOREO Y ADMINISTRACIÓN 81
4.1.1 OPERACIONES DE LA ADMINISTRACIÓN DE RED 82
4.1.2 FUNCIONES DE ADMINISTRACIÓN DE RED DEFINIDAS POR OSI 83
4.1.3 NORMAS PARA LA ADMINISTRACIÓN DE RED 84
4.1.4 PROTOCOLOS DE ADMINISTRACIÓN 84
4.1.5 MIB 85
4.1.6 SNMP 86
4.1.7 MONITORES DE RED 88

4.2 MÉTODOS Y PROCEDIMIENTOS 89
4.2.1 SCRIPT DE MONITOREO DEL TRÁFICO DE LA RED 89

4.3 RESPALDOS Y PLANES DE EMERGENCIA 95
4.3.1 MONITOREO DE FALLAS 95

4.4 PRUEBAS Y ANÁLISIS 96

CAPÍTULO 5

CONCLUSIONES 99

5.1 CONCLUSIONES 99

5.2 APORTACIONES 99

5.3 LÍNEAS DE CONTINUACIÓN 101

APÉNDICE A

I TABLAS DE COMPARACIÓN DE EQUIPOS DE COMUNICACIONES 102

I.I TABLA DE COMPARACIÓN DEL SWITCH PRINCIPAL 102
I.II TABLA DE COMPARACIÓN DEL SWITCH SECUNDARIO 106
I.III TABLA DE VENTAJAS Y DESVENTAJAS DEL SWITCH SECUNDARIO 108

APÉNDICE B

II LÍNEAS DE CONFIGURACIÓN 110

APÉNDICE C

III SCRIPTS DE CONFIGURACIÓN DE EQUIPOS 117

III.I SCRIPT PARA CREACIÓN DE PUERTO ESPEJO 117
III.II SCRIPT DE ACTUALIZACIÓN DE FIRMWARE 121

REFERENCIAS BIBLIOGRAFICAS 128

GLOSARIO DE TÉRMINOS 130

Figuras

Figura I	Segmentación utilizando un router	7
Figura II	Segmentación utilizando un switch	7
Figura 1.1	Topología Jerárquica	15
Figura 1.2	Topología en Bus	16
Figura 1.3	Topología en Estrella	17
Figura 1.4	Topología en Anillo	17
Figura 1.5	Servidor de acceso	22
Figura 1.6	Modelo de referencia OSI	25
Figura 1.7	Campos de la Subcapa MAC.	28
Figura 1.8	Descripción del modelo DOD y su referencia con TCP/IP	32
Figura 1.9	Encabezados de un paquete TCP	34
Figura 2.1	Red Anterior de la Universidad.	46
Figura 2.2	Capturas de tráfico desde diferentes puntos de la Red de la Institución.	48
Figura 2.3	Tráfico de MAC	49
Figura 2.4	Tráfico IP	49
Figura 2.5	Red inicial con topología lógica en bus y física en estrella a través de un hub.	52
Figura 2.6	Si se necesita ampliar la red, una solución puede ser esta, pero no mejora el rendimiento de la red porque lógicamente está vista como una única red.	53
Figura 2.7	Una solución para ampliar la red puede ser esta, y en esta situación mejora el rendimiento de la red.	53
Figura 2.8	Red con el nuevo ruteador.	57
Figura 2.9	Panel frontal del equipo SSR-2B-128 o X-PEDITION 2000	58
Figura 2.10	Diseño con el Switch VH-2402SM.	58
Figura 2.11	Panel frontal del equipo VH-2402SM	59
Figura 2.12	Red Institución Educativa con equipos de enlace de microondas de 11 Mbps.	60

Figura 2.13	Vista frontal del Firewall Nokia IP330.	61
Figura 2.14	Diseño final	61
Figura 3.1	Resolución de nombres DNS	67
Figura 3.2	Configuración del DNS Split	68
Figura 3.3	Red Actual de la Universidad	80
Figura 4.1	PRTG Paessler Router Traffic Grapher	90
Figura 4.2	Alta de Interfaz	90
Figura 4.3	Configuración de IP y comunidad SNMP	91
Figura 4.4	Conexión establecida	91
Figura 4.5	Interfaz a monitorear	92
Figura 4.6	Envío de mensajes importantes	92
Figura 4.7	Intervalos de tiempos	93
Figura 4.8	Gráficas obtenidas	93
Figura 4.9	Interfaz de Ruteo WAN	94
Figura 4.10	Interfaz Wireless Outdoor	94
Figura 4.11	Tráfico de broadcast disminuido	97
Figura 4.12	Tráfico IP después de la optimización	98
Figura C.1	Telnet al default gateway	117
Figura C.2	Pantalla donde es requerido un password y un Login	117
Figura C.3	Sesión para configurar el equipo	118
Figura C.4	Líneas de configuración.	118
Figura C.5	Comando Search	119
Figura C.6	Invalidación de las líneas de configuración	119
Figura C.7	Comando: show scrachtpad	120
Figura C.8	Grabamos los cambios	120
Figura C.9	Puerto espejo configurado	121
Figura C.10	Management Setup Menu	122
Figura C.11	Nombre del Firmware	122
Figura C.12	Servidor TFTP	123
Figura C.13	System Restart Menu	123
Figura C.14	Restart System	124
Figura C.15	Main Menu	124
Figura C.16	Device Control Menu	125

Figura C.17 Declaración de VLAN's 125
Figura C.18 Declaración de puertos 802.1qtrunk 126
Figura C.19 Declaración de puerto por el cual nos enlazamos al IDF principal. 126

Tablas

Tabla 2.1 Necesidades de interconectividad y su solución. 52
Tabla 2.2 Topologías utilizadas y la longitud máxima de segmentación. 54
Tabla 2.3 Dispositivos de interconexión y su referencia con el modelo OSI. 55
Tabla 2.4 Desventajas de optimizar una red utilizando la segmentación. 63
Tabla 2.5 Ventajas de optimizar una red utilizando la segmentación. 64
Tabla 3.1 IDF's que se conectan al Switch SSR 70
Tabla 3.2 Segmentos de red para los IDF's. 70
Tabla 3.3 Especificaciones Switch ruteador. 74
Tabla A.1 Comparación de Switches. 106
Tabla A.2 Comparativo del Switch secundario de distribución DMZ. 108
Tabla A.3 Ventajas y Desventajas de los switches secundarios de distribución DMZ. 109

Introducción

El objetivo de una red de datos consiste en facilitar la consecución de un incremento de la productividad vinculando todas las computadoras y redes de computadoras de manera que los usuarios puedan tener acceso a la información con independencia del tiempo, ubicación y tipo de equipo informático.

En general, la filosofía de trabajo es centralizada; bien se disponen de computadoras personales (PC) independientes con tareas perfectamente desvinculadas entre ellas o bien de un gran servidor (Tipo UNIX o similar) con las bases de datos, los programas de gestión y una serie de terminales mas o menos autónomas sirviéndose de dicho servidor central.

Ante esta nueva perspectiva, los administradores pasan la mayor parte de su tiempo intentando que el sistema, en su conjunto, se mantenga operativo. Ahora, la mayoría de ellos son capaces de ver que el sistema tradicional de administración es más que insuficiente. Aparecen varios intentos para adoptar dicho sistema a los nuevos sistemas, mucho más distribuidos.

El problema radica en que el sistema se ha vuelto tan complejo y las tareas cotidianas del administrador tan absorbentes que difícilmente un administrador puede dedicarse a la tarea de especificar e implementar una solución global. Estamos observando cambios de escala:

- La implantación de sistemas más sofisticados y aumento de la diversidad de prestaciones para la oferta de servicios que precisan estar perfectamente operativos de manera continua: correo electrónico, video-conferencia, servidores de comercio electrónico, Intranet, etc.

- La información que se maneja va creciendo día a día debido a la incorporación de las tecnologías multimedia en los procesos habituales, la creciente utilización de servidores de documentos que pretenden sustituir al soporte en papel y el abaratamiento en los medios de almacenamiento, de esta forma nos encontramos con volúmenes de información muy por encima de la capacidad en espacio y tiempo de los sistemas de almacenamiento masivo utilizado en la gestión de copias de seguridad.

- En estos momentos ya no podemos asegurar que un proceso empezará y terminará en un mismo equipo y, mucho menos, que la información que utilice esté ubicada en un punto fijo.

- Finalmente, el número de nodos interconectados crece de manera rápida, obligando a diseñar estructuras de comunicación mucho más intrincadas que fuerzan a introducir nuevos dispositivos específicos como puentes (Bridges), routers (ruteadores), switches, concentradores etc. Que también deben ser considerados en la planificación global de la administración del sistema. A medida que crece, el sistema se vuelve más heterogéneo.

Ahora ya no se trata sólo de mantener operativos los nodos como si se tratara de entes individuales, el nuevo objetivo debe ser mantener el sistema como un todo, como un solo ente.

Las redes de datos han cambiado nuestra forma de ver a nuestras empresas y a los usuarios. Ya no es necesario mantener una ubicación común para todos los usuarios si se quiere acceder a la información que estos necesitan para desarrollar su trabajo. Debido a esto, hay muchas organizaciones que han cambiado sus estrategias comerciales para utilizar estas redes de la forma en que llevan a cabo su actividad empresarial. Es muy frecuente que una empresa organice la red de tal forma que permita optimizar sus recursos.

Las demandas del usuario y las aplicaciones de red han obligado a los administradores de las redes a utilizar patrones de tráfico en la red como criterio para construir una red de trabajo común. Las redes no pueden ser divididas en subredes basándose únicamente en el número de usuarios. La aparición de servidores capaces de ejecutar aplicaciones globales tiene también una incidencia directa en la carga de la red. Un tráfico elevado en la red global supone tener que emplear técnicas de enrutamiento y conmutación más eficaces.

Los desarrollos tecnológicos y las siempre cambiantes realidades de la organización se han convertido en agentes que han obligado a los diseñadores a repensar la estructura de la red. El incremento en el número de usuarios y en el número de aplicaciones que utilizan la red incrementó el tráfico a volúmenes muy grandes, se hizo entonces necesario concebir su estructura como una estructura jerárquica, con diferentes requerimientos de capacidad y desempeño en cada nivel, y obligó a entender su diseño como un proceso.

El diseño de interconexión de redes se ha convertido en un problema fundamental en el área de Tecnologías de la Información y de las Comunicaciones. La optimización de las estructuras de interconexión y de esquemas de transporte y difusión de la información, tanto en sistemas multiprocesadores como en sistemas distribuidos y de telecomunicación, da lugar a diversos problemas de naturaleza combinatoria que constituyen el eje fundamental del proyecto que se presenta.

Estamos entonces ante una situación en la cual se aumenta el número de usuarios de red, el de aplicaciones de red y el tamaño de los bloques de información que transitan a través de ella.

Motivación

Las redes de hoy, más que redes de datos, son redes de información: flujos de información de datos, de voz y de video surcan las redes modernas, los dispositivos de ínterconectividad deben estar en capacidad de reconocerlos y darles un tratamiento diferenciado, aspecto al que llamaremos "calidad de servicio". La red debe estar en capacidad de comprometerse a ofrecer servicios de diferente tipo, dependiendo del tipo de información que se quiera transferir a través de ella, los requerimientos de retraso en la transferencia, de variación en el mismo y de capacidad de transmisión deben ser reconocidos y entendidos por los diferentes dispositivos que conforman la arquitectura de una red.

Por otra parte, la estructura de la red se ha vuelto jerárquica, funcionalmente modular, con tecnologías de conmutación de diferente nivel y capacidad de transmisión variable en cada uno de sus niveles. La red corporativa ha adquirido el compromiso de ofrecer servicios diferenciados a aplicaciones y a usuarios que necesitan transferir información de cualquier índole a través de ella.

Tanto el tamaño actual de las redes de computadoras como su complejidad varían considerablemente, desde pequeños sistemas organizados en LAN, hasta los millones de nodos que conforman la propia Internet. Estas redes tienden a ser más heterogéneas a medida que aumenta su tamaño, incrementándose más su complejidad y haciendo que los tradicionales sistemas de gestión de redes queden totalmente sobrepasados.

Las tecnologías de red han evolucionado para dar servicio a las aplicaciones de elevado ancho de banda a las que atienden. En la actualidad, el 98 por ciento del tráfico de datos asociado al extremo de aplicación es Ethernet [Apachon D, 2003]. Este tipo de servicio requiere agregación dinámica y flexible en el extremo de la red, y un elevado ancho de banda unido a una gran fiabilidad en el núcleo. Gracias al bajo costo de los dispositivos Ethernet, hoy en día desplegar conexiones Ethernet en el extremo local resulta fácil y económico. Sin embargo, hasta ahora, el tramo de transporte de tráfico comprendido entre la red local y el núcleo de la red del operador ha carecido de la eficiencia y eficacia que la red de transporte necesitaría para poder ofrecer el grado de fiabilidad y diferenciación de servicios que exigen las nuevas aplicaciones.

En general, la administración de redes abarca tanto la monitorización como su control. Un sistema de administración de redes debe incluir, entre otras tareas, las de configuración de la red, garantía de su propio funcionamiento, mantenimiento, control de la seguridad, recolección y archivo de datos y gestión de errores.
Por esta razón, uno de nuestros objetivos será proponer organizaciones de la red que permitan llevar a la práctica las propuestas que se desprendan de esta optimización.

Estado del Arte

El primer aspecto en el que nos hemos centrado es en el de analizar los trabajos o proyectos que se hubieran realizado o se estuvieran realizando con un planteamiento similar a nuestra propuesta de optimización de la red.

En el actual entorno de comunicaciones se está produciendo una tendencia hacia redes cada vez más heterogéneas. Esta diversidad requiere que los administradores de red manejen más información sobre la misma, viéndose obligados a recopilar enormes cantidades de datos que deben ser analizados antes de abordar la administración propiamente dicha. Por otro lado, también encontramos que se ha producido una enorme expectación en el incremento de la fiabilidad y la calidad del servicio por parte de los actuales usuarios de redes.

Las redes de comunicación surgieron a partir de la necesidad que tenían los usuarios de compartir un conjunto diverso de recursos distribuidos, dichas redes se convirtieron en el vehículo que permitió el intercambio de información.

En el caso de las redes locales (*LAN's Local Area Networks*) prevalecieron las llamas redes de difusión. Una red de difusión es aquella en la cual todas las estaciones comparten el canal de comunicaciones y cuando una de ellas transmite, todas las demás la escuchan [Oppenheimer, 1999]. Dos formas básicas de interconexión y de acceso al canal de comunicaciones pelearon para obtener la supremacía; de un lado estaban las topologías en bus, y por otro las redes que tenían topología de anillo. En las redes que tenían topología en anillo un "testigo" (*Token*) mediaba el acceso al canal, sólo aquella estación que tenía en su poder el testigo podía enviar información a través del canal. Razones de orden económico hicieron que las redes con topología en bus y con protocolo de acceso al canal basado en contienda prevalecieran. Las redes del tipo Ethernet, como son conocidas, reinan desde entonces en el ambiente de las redes locales, el hecho de pelear por el canal, de generar colisiones, tiene un efecto directo sobre el desempeño de la red ya que resulta imposible predecir con exactitud el momento en el cual una terminal de la red pueda transmitir. En esta evolución histórica, las redes Ethernet de medio compartido se constituyen el punto de partida.

Las redes Ethernet utilizaban generalmente cable coaxial delgado, del tipo RG-58, y conectores del tipo BNC. La topología física de la red era en bus y se instalaba en cada terminal una tarjeta de red que tenia una interfaz física que la conectaba al canal. No existía ningún tipo de jerarquía, la red era completamente plana y la topología física (la forma como se conectaban las terminales) coincidía con la topología lógica (la forma en como las terminales peleaban por el canal).

Las terminales de red interconectadas con topología en bus dieron lugar al concepto de dominio de colisión [Apachon D. 2003]. Dominio de colisión es el conjunto de todas aquellas estaciones que en un momento dado pelean o compiten por el uso del canal. En medida que el dominio de colisión sea más grande, mayor será el número potencial de colisiones, y por consiguiente, menor el desempeño de la red. El incremento en el número de

usuarios que hacen parte de una red corporativa tendrá grandes efectos sobre este tipo de redes.

Las redes Ethernet de medio compartido fueron muy populares en las organizaciones, sin embargo, muy pronto las dificultades empezaron a surgir; la administración y la solución de problemas se volvieron prácticamente inmanejables. Los conectores de tipo BNC obligaban a cortar físicamente el cable coaxial y cuando, por alguna razón, se desconectaba el segmento físico del cable del conector, la conexión en bus desaparecía y la comunicación no era posible, existían entonces N puntos de falla en la red.

La gran mayoría de las dificultades asociadas con la administración en las redes Ethernet de medio compartido basadas en cable coaxial se encontraban en el nivel físico; el cableado estructurado resolvió muchas de estas dificultades. El cable coaxial fue cambiado por cable UTP (*Unshielded Twisted Pair*), lo cual significó un retroceso en términos del canal, dado que las características de transmisión del cable coaxial son superiores a las que ofrece el cable UTP. Sin embargo, la diferencia fundamental radicó en la utilización de un concentrador (*hub*), el cual se constituyó en el núcleo de una topología física en estrella que permitió centralizar muchas de las tareas de administración.

El cableado estructurado produjo un cambio significativo en la estructura de la red. A partir de este momento las redes tienen una topología punto a punto, son redes que físicamente tienen una topología en estrella, sin embargo; y gracias al comportamiento del concentrador, la topología lógica seguía siendo en bus, cuando una terminal quiere transmitir, el concentrador se encarga de repetir aquello que "escucho" a cada uno de los puertos restantes, es decir, "cuando alguien habla, todos escuchan".

Hasta entonces, la tarjeta de red era un periférico que se cotizaba de manera independiente y opcional por parte del proveedor; a partir de éste instante, los equipos de procesamiento de datos tienen incorporada la tarjeta de red en su configuración estándar porque se supone que serán utilizados como terminales en alguna red. En el software, se incrementa significativamente el número de aplicaciones que operan en un ambiente de red; por otra parte, el tamaño de los bloques de información que son transmitidos a través de la red también se amplían.

Es una situación en la cual se aumenta el número de usuarios en la red, el de aplicaciones de red y el tamaño de bloques de información que transitan a través de ella. Esto trae como resultado un incremento en el tráfico que la red debe administrar. Es aquí donde se paga el precio de haber optado por una tecnología de contienda en el uso de canal. El gran crecimiento en el volumen de tráfico generado en el dominio de colisión produjo un colapso en las redes, la demanda de ancho de banda de los usuarios y sus aplicaciones empezaba a superar la oferta que era capaz de presentar la red.

Para solucionar este problema se presentaron dos alternativas: la utilización de tecnologías de alta velocidad y la segmentación. La primera implicaba desarrollar o actualizar mecanismos que permitieran enviar una mayor tasa de bits por segundo en el canal, aquí también se presentaron dos posibles

soluciones: la primera romper de una vez por todas con las redes Ethernet y volver a pensar en el mecanismo de acceso al medio surgiendo alternativas como FDDI (*Fiber Distributed Data Interface*), una propuesta de ANSI (*American National Standards Institute*) para contar con un anillo de fibra óptica a 100 Mbps; la otra tecnología representante de esta variante fue 100 VGAnyLAN en la que también se replanteaba el mecanismo de acceso al medio. El optar por este camino hubiera significado, en todos los casos, haber cambiado todas las tarjetas de comunicación, aspecto que desde el punto de vista económico y práctico resultaba inmanejable. La segunda de las soluciones proponía incrementar la tasa de transmisión de la Ethernet convencional; en lugar de contar con un canal de capacidad nominal de 10 Mbps, se dispondría de un canal de 100 Mbps, esta alternativa fue la que finalmente se impuso y parecía que iba a ser la solución definitiva a no ser por un aspecto de trascendental importancia: este enfoque de solución se concentraba en atacar los síntomas del problema pero no en resolver las causas del mismo, si bien resultaba posible contar con un canal de mayor capacidad no se hacia nada respecto del tamaño del dominio de colisión, la fuente del problema.

La otra posible solución al problema de la crisis de ancho de banda estaba en la segmentación. Segmentar una red implica descomponer un dominio de colisión en dos o más [Tanenbaum 1996], de tal manera que se disminuya el número de terminales de red que pelean por el uso del canal. Este enfoque de solución realmente enfrenta las causas del problema y provocó un replanteamiento en el diseño y en la estructura de la red.

Inicialmente, la segmentación fue realizada utilizando puentes (*bridges*) o enrutadores (*routers*). Los bridges y los routers son dispositivos de interconectividad su tarea principal es la de conectar redes. En estos dispositivos se aprovecha el proceso de filtrado, uno de los procesos básicos que gobiernan su operación para efectuar la segmentación.

El proceso de filtrado trabaja de la siguiente manera: cuando la terminal A desea enviar información a la terminal B, esta claro que tanto como la terminal origen como la terminal destino se encuentran en el mismo segmento de red, por lo tanto, el dispositivo de interconectividad (*router o bridge*) no retransmiten la información hacia el otro segmento. Ello permite que C pueda estar simultáneamente comunicándose con D, de esta manera, el tamaño de los dominios de colisión se hace más pequeño y en promedio cada terminal tendrá la posibilidad de transmitir una mayor cantidad de información (Ver figura I).

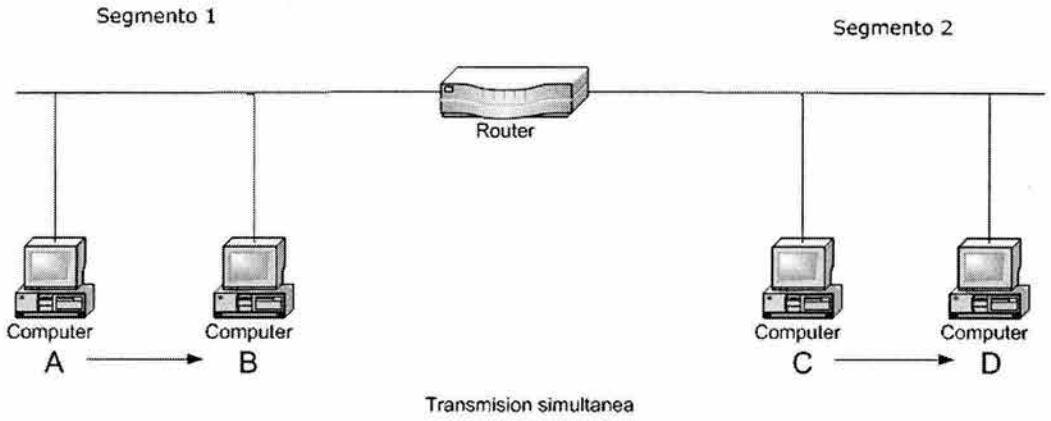


Figura I: Segmentación utilizando un router.

Surgió entonces la necesidad de contar con un dispositivo que permitiera realizar la segmentación de las redes: El Switch, un dispositivo especializado en realizar conmutación de tramas. En esencia, un switch es un bridge multipuerto con hardware especializado en conmutación [Switched Networks, 2000]. Cada uno de sus puertos da lugar a un dominio de colisión independiente permitiendo, en el mejor de los casos, que toda la capacidad del canal se asigne a una terminal de la red. El switch cambio sustancialmente el diseño de la red, permitiendo la evolución desde una red de medio compartido hasta una red de medio dedicado. En la figura II, la presencia del switch da lugar a dos segmentos. En el primero, las terminales A y B constituyen el primer dominio de colisión, y en el segundo, la terminal C constituye el segundo dominio de colisión. En este caso, la terminal C no pelea con ninguna otra por el acceso al canal.

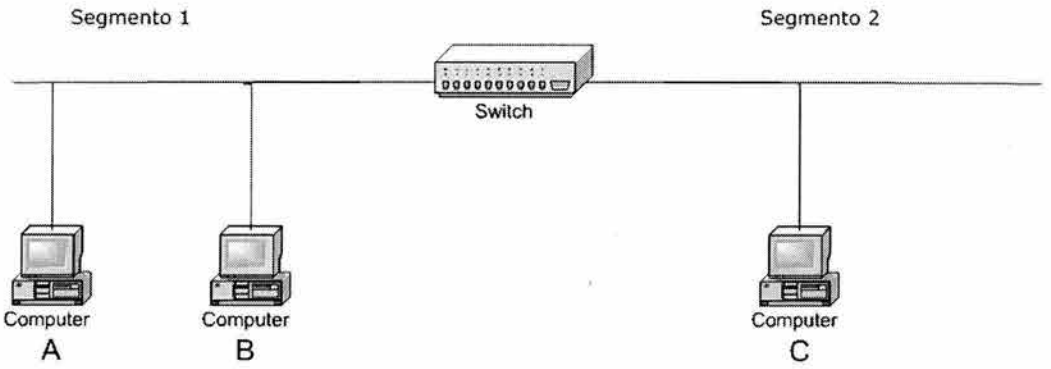


Figura II: Segmentación utilizando un switch.

Hasta ahora, las redes tenían una estructura plana, no existía una jerarquía. Es por ello que se determinó establecer una jerarquía en los switches de la red. Igualmente, la capacidad en los enlaces no es uniforme como lo era anteriormente, ahora resulta posible tener enlaces de alta capacidad entre los switches, o entre los switches y los servidores (*Ethernet a 100 Mbps o Fast Ethernet*) y enlaces convencionales (*Ethernet a 10 Mbps*) entre los switches y las terminales de la red.

Un siguiente paso hacia la segmentación lo observamos en el domino de broadcast. Un dominio de broadcast es el conjunto de terminales que "escuchan" un mensaje de broadcast (un mensaje generado por una terminal en particular para todas las terminales que componen la red) [Apachon D., 2003]. El switch, como dispositivo que trabaja en la capa dos del modelo de referencia OSI, es incapaz de contener el tráfico de broadcast, este tipo de tráfico puede ser limitado por un router, un dispositivo que trabaja en la capa tres del modelo de referencia OSI.

El broadcast excesivo tiene un efecto indeseado sobre el desempeño de la red, en primer lugar porque la congestiona (es tráfico que efectivamente viaja a través de los diferentes enlaces) y en segundo lugar porque al estar dirigido hacia todas las terminales debe ser procesado por ellas, lo que implica un consumo de recursos de cómputo en cada terminal. Muchos protocolos y servicios de red utilizan el broadcast como estrategia de notificación a las demás terminales de la red.

Sin embargo, el switch es incapaz de contener el tráfico de broadcast, se hace necesario entonces ascender un nivel e ir desde el nivel dos (nivel de enlace de datos) hasta el nivel tres (nivel de red) para resolver el problema.

Para contener o limitar el tráfico de broadcast se han propuesto dos opciones: una la utilización de redes virtuales (*VLAN's*), y la otra, extender el concepto de conmutación al nivel tres y utilizar switches de nivel tres. Una red virtual (*VLAN, Virtual LAN*), como su nombre lo sugiere es agrupamiento virtual de nodos en un dominio de broadcast [Oppenheimer, 1999]. La gran ventaja derivada de la utilización de las VLAN's es que permiten contener el tráfico de broadcast y efectuar una separación de los flujos de tráfico. Para permitir la comunicación entre usuarios que pertenecen a diferentes redes virtuales es necesario utilizar una función de nivel tres, a través de un router o de un switch de nivel tres.

Toda esta reflexión nos conduce a pensar en la necesidad de contar con una metodología que permita abordar con éxito el proceso de diseño de una red.

Formulación del problema

Actualmente la Institución Educativa en la cual nos basamos para realizar este proyecto, cuenta con 4 planteles: Principal, Anexo Bachillerato, Anexo Posgrado y Anexo Regional, teniendo como sede primordial el plantel Principal, en dicha sede se concentra la mayoría de equipo de cómputo para el buen funcionamiento de las otras tres sedes. Esta Institución, esta apostando a un mayor crecimiento a nivel comunicaciones entre sus planteles, tomando en cuenta seguridad, tipo de comunicación entre los planteles, bases de datos, intranet e Internet, a partir de esta necesidad ha sido necesario plantearse la idea de una optimización en la red con la que cuenta en este momento dicha institución, con el único fin de que la intercomunicación entre dichos planteles sea lo más eficiente, refiriéndonos a velocidad y seguridad. El problema en sí, radica en la necesidad urgente de hacer cambios a nivel direcciones IP's, una nueva segmentación de la

red para evitar conflictos de tráfico en la red sin descuidar el aspecto de la seguridad.

El alcance que provocaría esta reestructuración seria en el aspecto económico y productivo ya que es preciso destacar que el plantel en ningún momento puede dejar de funcionar la red, ya que es una institución que ofrece servicios y el aspecto productividad es muy importante.

Es importante saber la relevancia que esto conlleva ya que si alguna otra institución con características similares o alguna pequeña empresa que tiende a crecer en el aspecto comunicaciones, puede ser de gran utilidad para tener una idea de los elementos que debe considerar al realizar una optimización en la empresa, refiriéndonos en el campo de las comunicaciones.

La estructuración del proyecto para implementar la red de datos se remonta a la continuación del proyecto de la primera fase en el año 2001. Todo esto con la finalidad de contar con una infraestructura homogénea.

Con la finalidad de robustecer la sección central del Site de cómputo en el edificio Principal, se realizarán las siguientes implementaciones:

- Instalación de un CORE central del tipo Switch Ruteador.
- Instalación de Radio enlaces a 11 Mbps.
- Actualización del equipo Nokia IP330.
- Implementación de salida a Internet para obtener una distribución de carga de salida y entrada.

Derivado del diagnostico efectuado se propone el desarrollo de un esquema de comunicación de datos ruteada por medio del cual se pueda realizar el intercambio de servicios entre los edificios: Principal, Anexo Bachillerato y Anexo Posgrado, además de realizar en un futuro cercano, filtrado de contenido y control absoluto de usuarios.

Objetivos

La Institución tiene actualmente requerimientos importantes en la comunicación de transferencia de datos, los cuales tienen como finalidad llevar a cabo el intercambio de servicios de forma eficiente y oportuna.

Para enfrentar los nuevos retos de eficiencia y calidad en la prestación de servicios informáticos. Esta Institución, ha considerado la importancia de consolidar el desarrollo de una red de datos ruteada para mejorar la calidad de comunicaciones entre los equipos de datos.

El aprovechamiento adecuado de las innovaciones tecnológicas en el área de comunicaciones permitirá a la Institución modernizar sus esquemas de operación y reducir los costos actuales de operación.

El objetivo de esta propuesta es realizar un planteamiento efectivo para la optimización de una red en una institución privada.

De acuerdo a las necesidades en materia de transferencia de datos, en cada punto requerido de los clósets de comunicaciones en los edificios de la Institución, se estructurará una red de datos segmentada y apoyada por redes virtuales VLAN's, la cual se encontrará configurada y entrelazada al Firewall Nokia IP330.

- El objetivo preciso de realizar dicha optimización es realizar una mejor administración de la red satisfaciendo las necesidades tanto de directivos como de los usuarios de esta institución, cuidando aspectos importantes como seguridad, disminución de tráfico en la red y una conexión eficiente entre todos los planteles.

- Con el resultado de éste trabajo de investigación pretendemos tener una red efectiva refiriéndonos a productividad, es decir, una red segura, con el menor tráfico posible, con el menor número de fallos operativos y obviamente que en ningún momento deje de funcionar, puede decirse que estos cambios sean transparentes tanto para el personal que labora en la institución como para los usuarios del plantel.

- Por último se pretende establecer un esquema técnico y económicamente viable para desarrollar una red de datos, por medio de la cual, sea posible el intercambio de información entre los edificios: Principal, Anexo Bachillerato y Anexo Posgrado, la comunicación con instancias externas, el acceso a redes públicas y optimizar el uso de los recursos informáticos que se encuentren conectados a la misma.

Deseamos que este trabajo sea una fuente de apoyo para otras empresas, que sirva como referencia en dado caso que pretendan realizar alguna optimización similar a la que pretendemos realizar.

Estructura de la Tesis

El capitulo 1 comprenderá los aspectos teóricos que serán fundamentales para el entendimiento de este proyecto de tesis.

El capitulo 2 estará dedicado a sentar las bases de un diseño formal en el cual nos apoyaremos el resto del proyecto y sobre el que especificaremos nuestra optimización de la red con el mayor rigor posible.

En el capitulo 3 continuamos con el diseño de la red, presentando una nueva configuración de la red; posteriormente establecemos las soluciones que nos permitirán la optimización y el mejor funcionamiento para el proyecto; seguidamente analizaremos las implicaciones que conllevan estas soluciones; finalmente en este mismo capitulo, se analizan las soluciones a los problemas que puedan presentar durante dicha optimización.

En el capitulo 4, una vez establecida la optimización de la red, planteamos la manera en que será administrada la red. En primer lugar nos

dedicaremos a su monitorización especificando los métodos y procedimientos utilizados, en segundo lugar, presentar los planes de emergencia que utilizaremos en caso de fallas en la red, finalmente, realizaremos pruebas de la optimización de esta red y un análisis de su funcionamiento.

Finalmente, dedicaremos el capitulo 5 para presentar las principales conclusiones del trabajo, aportaciones y plantear las líneas futuras de continuación que se desprenden del mismo.

Capítulo 1

1.1 Redes de datos

Las redes están compuestas generalmente por un pequeño número de máquinas localizadas en el mismo edificio, o incluso en una sola planta que están interconectadas para proporcionar un entorno de trabajo homogéneo. Es común que se quiera compartir archivos entre estos nodos, o ejecutar aplicaciones distribuidas en diferentes computadoras. Estas tareas requieren una aproximación completamente diferente a las redes. En lugar de reenviar archivos completos con una descripción del trabajo, todos los datos se fragmentan en pequeñas unidades (paquetes), que se envían inmediatamente al nodo destino, donde son reensamblados.

Se denomina topología a la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que las conectan. [Raya, 1997] Por lo tanto, la topología establece la forma (en cuanto a conectividad física) de la red. Al diseñarse una red se tienen tres objetivos para establecer la topología de la misma:

- Proporcionar la máxima fiabilidad a la hora de establecer el tráfico.
- Encaminar el tráfico utilizando la vía de costo mínimo entre los nodos, no obstante, en ocasiones no se escoge la vía de costo mínimo porque otros factores, como la fiabilidad, pueden ser más importantes.
- Proporcionar al usuario final un rendimiento óptimo y el tiempo de respuesta mínimo.

El concepto de fiabilidad cuando hablamos de redes, hace referencia a la capacidad de enviar los datos correctamente entre los nodos. La fiabilidad también tiene que ver con el mantenimiento del sistema.

Como segundo parámetro al establecer una topología de red es proporcionar el camino de costo mínimo, para ello es necesario: minimizar la longitud real del canal entre los componentes que se comunican. Para lo cual se debe encaminar el tráfico pasando por el menor número posible de nodos intermedios. Asimismo, es necesario proporcionar el canal más económico para una aplicación determinada.

Por último, el tercer objetivo es proporcionar el mínimo tiempo de respuesta y el máximo rendimiento. Para minimizar el tiempo de respuesta hay que procurar minimizar el retardo entre la transmisión y la recepción de datos entre los componentes de la red. El rendimiento tiene que ver con la transmisión de la máxima cantidad de datos en un periodo determinado.

Dependiendo de su arquitectura y de los procedimientos empleados para transferir la información las redes de comunicación se clasifican en:

- Redes conmutadas
- Redes de difusión

[González Fernández, 1998]

1.1.1 Redes conmutadas

Consisten en un conjunto de nodos interconectados entre sí, a través de medios de transmisión (cables), formando la mayoría de las veces una topología mallada, donde la información se transfiere encaminándola del nodo de origen al nodo destino mediante conmutación entre nodos intermedios [González Fernández, 1998]. Una transmisión de este tipo tiene 3 fases:

- Establecimiento de la conexión.
- Transferencia de la información.
- Liberación de la conexión.

Se entiende por conmutación en un nodo, a la conexión física o lógica, de un camino de entrada al nodo con un camino de salida del nodo, con el fin de transferir la información que llegue por el primer camino al segundo. Un ejemplo de redes conmutadas son las redes de área extensa.

Las redes conmutadas se dividen en:

- Conmutación de paquetes.
- Conmutación de circuitos.

Conmutación de paquetes

Se trata del procedimiento mediante el cual, cuando un nodo quiere enviar información a otro, la divide en paquetes. Cada paquete es enviado por el medio con información de cabecera. En cada nodo intermedio por el que pasa el paquete se detiene el tiempo necesario para procesarlo [González Fernández, 1998]. Otras características importantes de su funcionamiento son:

- Los paquetes se numeran para poder saber si se ha perdido alguno en el camino.
- Todos los paquetes de una misma transmisión viajan por el mismo camino.
- Pueden utilizar parte del camino establecido más de una comunicación de forma simultánea.

Conmutación de circuitos

Es el procedimiento por el que dos nodos se conectan, permitiendo la utilización de forma exclusiva del circuito físico durante la transmisión. En cada nodo intermedio de la red se cierra un circuito físico entre un cable de entrada y una salida de la red. La red telefónica es un ejemplo de conmutación de circuitos [González Fernández, 1998].

1.1.2 Redes de difusión

En este tipo de redes no existen nodos intermedios de conmutación; todos los nodos comparten un medio de transmisión común, por el que la información transmitida por un nodo es conocida por todos los demás [González Fernández, 1998]. Ejemplo de redes de difusión son:

- Comunicación por radio.
- Comunicación por satélite.
- Comunicación en una red local.

1.1.3 Topologías de redes.

La topología de una red define únicamente la distribución del cable que interconecta las diferentes computadoras, es decir, es el mapa de distribución del cable que forma la Intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes [González Fernández, 1998]. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El costo que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una Intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba:

- La topología.
- El método de acceso al canal.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al medio, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

Topología Física

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen cuatro topologías físicas puras:

- Topología en anillo.
- Topología en bus.
- Topología en estrella.
- Topología jerárquica

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por más de una topología física.

Topología Lógica

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas:

- Topología anillo-estrella: implementa un anillo a través de una estrella física.
- Topología bus-estrella: implementa una topología en bus a través de una estrella física.

1.1.4 Topología jerárquica.

Es una de las más usadas comúnmente, es relativamente simple y proporciona un punto de concentración para control y resolución de errores.

Una red jerárquica representa una red completamente distribuida en la que computadoras transmiten información a otras computadoras, que a su vez transmiten información a otras (Ver Figura 1.1).

Actualmente los sistemas de redes están construidos sobre un concepto de "niveles o capas de servicios" cuando nosotros tratamos de mandar información de un lugar a otro corremos el riesgo de perder algunos bits en el trayecto.

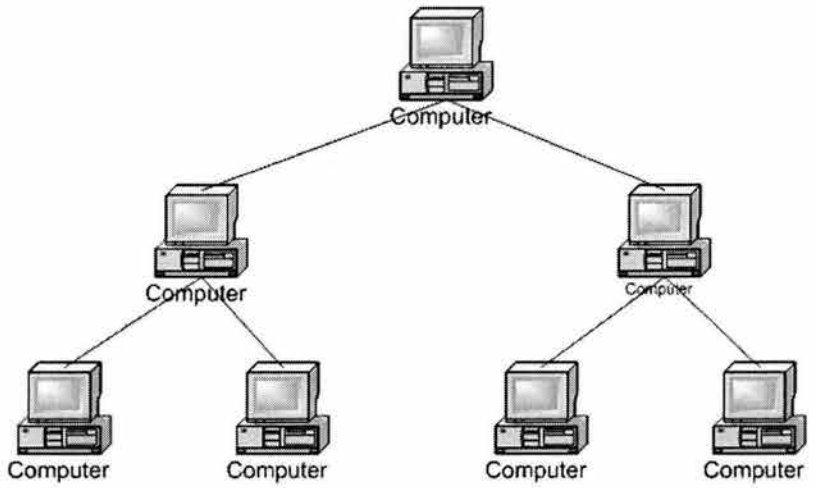


Figura1.1: Topología Jerárquica.

1.1.5 Topología en bus

Consta de un único cable que se extiende de una computadora a la siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada terminador, que además de indicar que no existen más computadoras en el extremo, permiten cerrar el bus [González Fernández, 1998] (Ver Figura 1.2).

Sus principales ventajas son:

- Fácil de instalar y mantener.
- No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría sin funcionar a todas las estaciones.

Sus principales desventajas son:

- Si se rompe el cable en algún punto, la red queda sin funcionar por completo.
- La longitud no puede sobrepasar los 2.000 metros [Raya, 1997].
- El control de flujo, ya que varias estaciones intenten transmitir a la vez, como hay un único bus, solo una de ellas podrá hacerlo, por lo que será mas complicado el control del flujo cuantas más estaciones tenga la red. Este control del flujo se puede realizar de dos maneras: por el método de acceso múltiple por detección de portadora con detección de colisiones (*CSMA/CD*) o por el paso de testigo.

Esta configuración es fácil de instalar, la cantidad de cable es mínima. Tiene una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones.

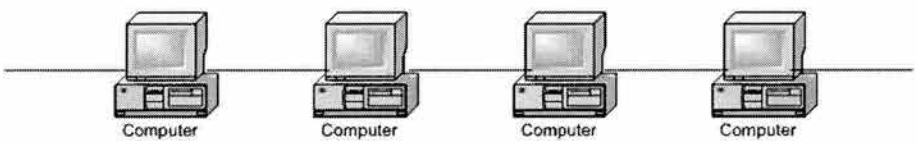


Figura 1.2: Topología en Bus.

1.1.6 Topología en estrella

Esta forma es de las más antiguas; en ella, todas las estaciones están conectadas directamente al servidor o a una computadora central y todas las comunicaciones se han de hacer necesariamente a través de él [Raya, 1997] (Ver Figura 1.3).

Tiene un tiempo de respuesta rápido en las comunicaciones de las estaciones con el servidor o con la computadora central, y lento en las comunicaciones entre las distintas estaciones de trabajo.

Si se produce un fallo en una de las estaciones no repercutirá en el funcionamiento general de la red pero, si se produce un fallo en el servidor o en la computadora central, la red completa se vendrá abajo.

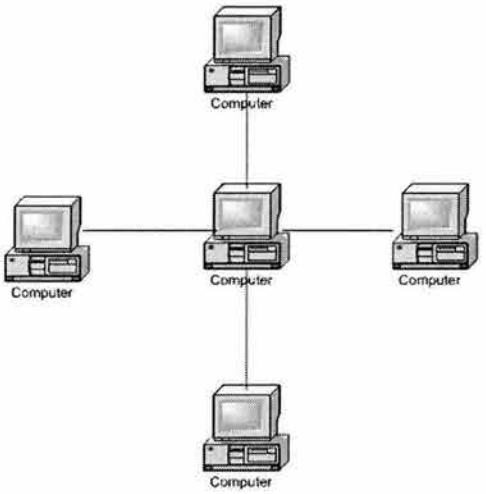


Figura 1.3: Topología en Estrella.

1.1.7 Topología en anillo

En ella, todas las estaciones están conectadas entre sí formando un anillo, de forma que cada estación solo tiene contacto directo con otras dos. Este tipo de redes permite aumentar o disminuir el número de estaciones sin dificultad, pero a medida que aumenta el flujo de información, será menos la velocidad de respuesta de la red [Raya, 1997] (Ver Figura 1.4).

Algunas veces, las redes anulares utilizan esquemas de transmisión de señales para determinar qué nodo puede tener acceso al medio. La ventaja de una red en anillo es que puede operar a grandes velocidades, y los mecanismos para evitar colisiones son sencillos.

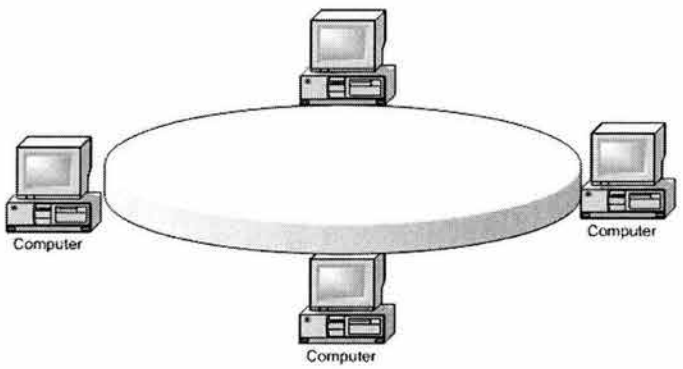


Figura 1.4: Topología en Anillo.

1.2 Clasificación de Redes

El tipo de recurso de comunicación de datos que se utilice dependerá de la naturaleza de la aplicación, del número de computadoras implicadas y de su separación física.

Existen dos parámetros importantes para determinar la clasificación de redes: el tipo de transmisión y la escala [Tanenbaum, 1996]. A su vez, existen dos tipos de transmisión:

- Redes tipo Broadcast.
- Redes Point to Point o redes punto a punto.

Las redes que utilizan broadcast constan de un canal sencillo de comunicación, que es compartido por todas las terminales en la red. Pequeños paquetes son enviados por la red hacia todas las terminales y son recibidos a su vez, por todas las demás terminales.

En estos paquetes va incluida una dirección especifica que determina hacia quien va dirigido el paquete. Si la dirección corresponde a esa estación recibe el paquete, de lo contrario, el paquete es ignorado. Estos paquetes son intercambiados sobre toda la red. Es por ello que las redes pueden ser divididas en Local Area networks (*LAN*), Metropolitan Area Networks (*MAN*) y Wide Area Networks (*WAN*). La distancia de la red es importante para su clasificación, ya que existen diferentes técnicas de comunicación que son usadas para cada una de ellas.

1.2.1 Redes LAN (Local Area Networks)

Una LAN es una red de datos de alta velocidad, tolerante a fallas, que cubre un área geográfica relativamente pequeña. Por lo general conecta estaciones de trabajo, computadoras personales, impresoras y otros dispositivos. Las LAN 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. Las redes de área local pueden tener radios que varían de algunos cientos de metros a cerca de 50 kilómetros. [Madron, 1992].

Según el comité 802 del IEEE: "Una red local es un sistema de comunicaciones de datos que permite a un número de dispositivos independientes comunicarse entre sí." Una LAN puede clasificarse además como:

- Intrainstitucionales, de propiedad privada, administradas por el usuario y no sujetas a la regulación de FCC: de esta categoría se excluyen a empresas de servicios comunes, tales como sistemas telefónicos públicos y sistemas comerciales de televisión por cable.
- Integradas a través de la interconexión vía un medio estructural continuo: pueden operar múltiples servicios en un mismo juego de cables.
- Capaces de ofrecer conectividad global.
- Que soportan comunicaciones de datos a baja y alta velocidad: las LAN no están sujetas a las limitaciones de velocidad impuestas por

empresas de servicios comunes tradicionales y pueden ser diseñadas para soportar dispositivos cuya velocidad va de 75 b/s (*bits por segundo*) con base en casi cualquier tecnología a cerca de 140 Mb/s (Mega (millones de) bits por segundo) en el caso de LAN de fibras ópticas disponibles en el mercado.

Las redes locales distribuyen casi siempre el procesamiento entre muchos nodos inteligentes, por lo general (aunque no necesariamente) enlazados por conexiones fijas. Dicha red local puede convertirse después en un nodo inteligente de una red global.

Métodos de acceso a medios de LAN

Los protocolos LAN suelen utilizar uno de los métodos para acceder al medio físico de la red: CSMA/CD (*Acceso Múltiple por Detección de Portadora con Detección de Colisiones)* y estafeta circulante.

En el esquema de acceso a medios CSMA/CD, los dispositivos de la red compiten por el uso del medio de transmisión físico de la red. Por esta razón, al CSMA/CD a veces se le llama acceso por contención. Ejemplos de LAN's que utilizan el esquema de acceso a medios CSMA/CD son las redes Ethernet/IEEE 802.3, incluyendo a 100BaseT [Merilee Ford, 1998].

En el esquema de acceso a medios llamado estafeta circulante, los dispositivos de la red acceden al medio de transmisión con base en la posesión de una estafeta. Ejemplos de LAN que utilizan este esquema son Token Ring/IEEE 802.5 y FDDI [Merilee Ford, 1998].

Métodos de transmisión en las LAN

La transmisión de datos en las LAN cae dentro de tres clasificaciones: unidifusion, multidifusion y difusión. En cada tipo de transmisión, se envía un solo paquete a uno o más nodos.

En las transmisiones de unidifusion, se envía un solo paquete desde el origen a un destino de la red. Primero, el nodo origen direcciona el paquete utilizando la dirección del nodo de destino. Luego el paquete es enviado a la red y, finalmente, la red transfiere el paquete a su destino [Merilee Ford, 1998].

Las transmisiones de multidifusion constan de un solo paquete de datos que se copia y envía a un subconjunto específico de nodos en la red. Primero, el nodo origen direcciona el paquete utilizando una dirección de multidifusión. Luego, el paquete es enviado a través de la red, la cual genera copias del paquete y envía estas copias a cada uno de los nodos que se indican en la dirección de multidifusion [Merilee Ford, 1998].

Las transmisiones de difusión constan de un solo paquete de datos que se copia y envía a todos los nodos de la red. En este tipo de transmisiones, el nodo origen dirige el paquete utilizando la dirección de difusión. El paquete es enviado a través de la red, la cual hace copias del paquete y las envía a cada uno de los nodos de la red [Merilee Ford, 1998].

Dispositivos de las LAN's

Entre los dispositivos de uso más común en las LAN están los repetidores, concentradores, puentes y switches de LAN.

Un repetidor es un dispositivo de la capa física (Modelo de referencia OSI) que se utiliza para interconectar los segmentos de cable en 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 la 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. El total de repetidores y segmentos de red que se pueden conectar esta limitado por la temporización y otros problemas [Merilee Ford, 1998].

Un concentrador (*o hub*), es un dispositivo de la capa física (modelo de referencia OSI) que conecta varias estaciones de usuario por medio de un cable dedicado. Las interconexiones eléctricas se establecen dentro del concentrador. Los concentradores se utilizan para conformar una red con topología física en estrella que a su vez conserva la topología lógica en bus o la configuración en anillo de LAN [Merilee Ford, 1998].

Un puente es un dispositivo de capa dos (Modelo de Referencia OSI), esta designado para crear 2 o mas segmentos de LAN, donde cada segmento tiene distinto dominio de colisión. Los puentes son mas inteligentes que los hubs, ya que, analizan los paquetes entrantes y puede dejarlos pasar o "tirarlos " basándose en la dirección MAC. También los puentes mantienen una tabla con las direcciones MAC.

Un switch de LAN es un dispositivo multicapa de acceso remoto que se conecta a un ruteador host. Los switches de LAN transfieren el tráfico de todos los protocolos estándar de la capa de red como IP, IPX, y AppleTalk, y filtran el tráfico con base en la dirección MAC o el tipo de protocolo de la capa de red. Los switches de LAN son fácilmente escalables debido a que el ruteador host elimina las señales de multidifusion y difusión no deseadas. Los switches de LAN, sin embargo, no pueden segmentar el tráfico o crear barreras de protección [Merilee Ford, 1998].

1.2.2 Redes WAN (Wide Area Networks)

Una WAN es una red de comunicación 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. Las tecnologías WAN operan en las tres capas inferiores del modelo de referencia OSI: la capa física, la capa de enlace de datos y la capa de red.

Un enlace *punto a punto* proporciona una sola trayectoria de comunicaciones WAN preestablecida desde las instalaciones del cliente, a través de una red de transporte como una compañía telefónica, hasta una

red remota. A los enlaces punto a punto también se les conoce como líneas privadas, puesto que su trayectoria establecida es permanente y fija para cada red remota a la que se llegue a través de las facilidades de larga distancia.

Circuitos Virtuales WAN

Un circuito virtual es un circuito lógico creado para asegurar una comunicación confiable entre dos dispositivos de red. Hay dos tipos de circuitos virtuales: SVCs (*Circuitos Virtuales Conmutados*) y PVCs (*Circuitos Virtuales Permanentes)* [Merilee Ford, 1998].

Los SVC son circuitos virtuales que se establecen dinámicamente por demanda y se terminan al finalizar la transmisión. La comunicación a través de un SVC tiene tres fases: el establecimiento del circuito, la transferencia de datos y la terminación del circuito. La fase de establecimiento implica la creación de un circuito virtual entre los dispositivos origen y destino. La transferencia de datos implica la transmisión de datos entre los dispositivos a través del circuito virtual, y la fase de terminación del circuito implica la desconexión del circuito virtual entre los dispositivos de origen y de destino. Los SVC se utilizan en situaciones donde la transmisión de datos entre los dispositivos es esporádica, en gran medida porque con los SVC se incrementa el ancho de banda utilizado, debido a las fases de establecimiento y terminación del circuito, pero disminuyen los costos asociados con la disponibilidad constante del circuito virtual.

Un PVC es un circuito virtual que se establece de manera permanente y consta de un solo modo: transferencia de datos. Los PVC se utilizan en situaciones donde la transferencia de datos entre los dispositivos es constante. Con los PVC disminuye el uso del ancho de banda asociado con el establecimiento y terminación de circuitos virtuales, pero se incrementan los costos debido a la constante disponibilidad del circuito virtual [Merilee Ford, 1998].

Servicios de Marcado de WAN

Los servicios de marcado ofrecen métodos para llevar a cabo la conectividad a través de las WAN. Las dos implementaciones más comunes son DDR (Ruteo de Marcación por Demanda) y el respaldo de marcación [Merilee Ford, 1998].

DDR es una técnica por medio de la cual un ruteador puede iniciar y terminar, de manera dinámica, una sesión de conmutación de circuitos a medida que las estaciones terminales de transmisión lo requieran. Se configura un ruteador para que considere cierto tráfico interesante y el resto del tráfico no interesante. Cuando el ruteador recibe tráfico interesante destinado a la red remota, se establece un circuito y se transmite el tráfico de manera normal. Si el ruteador recibe tráfico no interesante, y ya esta establecido un circuito en ese momento, ese tráfico también se transmite de manera normal [Merilee Ford, 1998] (Ver Figura 1.5).

La implementación de respaldo de marcación es un servicio que activa una línea serial de respaldo bajo determinadas condiciones. La línea serial secundaria puede actuar como un enlace de respaldo que se utiliza cuando el enlace principal falla, o como una fuente que proporciona ancho de banda adicional cuando la carga en el enlace principal alcanza un cierto umbral.

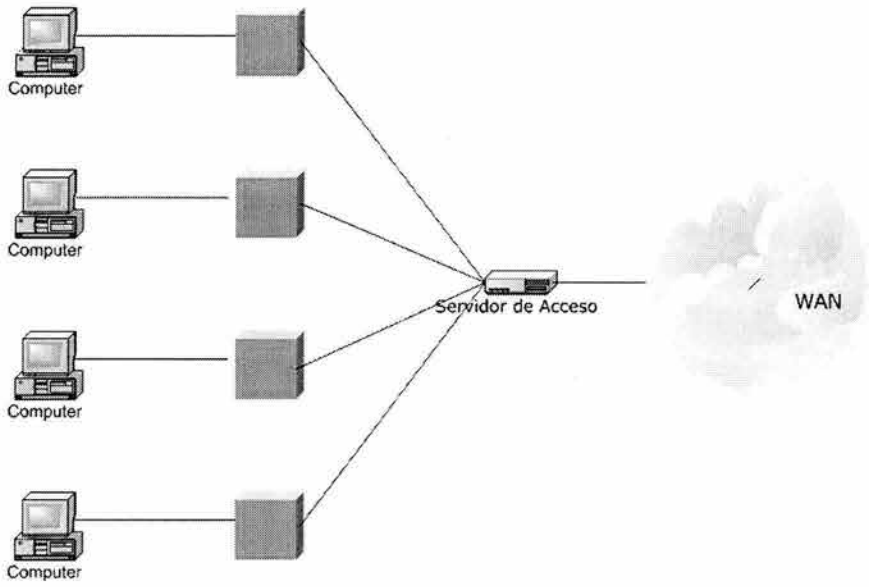


Figura 1.5: Servidor de acceso.

Dispositivos WAN

Las WAN utilizan gran número de tipos de dispositivos específicos para los ambientes WAN.

Switch WAN

Este es un dispositivo multipuesto de interconectividad de redes que se utiliza en las redes de transporte. Por lo general, estos dispositivos conmutan tráfico como el Frame Relay, X.25 y SMDS y operan en la capa de enlace de datos del modelo de referencia OSI [Merilee Ford, 1998].

Servidor de Acceso

Actúa como un punto de concentración para conexiones de marcación hacia a dentro y hacia fuera [Merilee Ford, 1998].

MODEM

Es un dispositivo que interpreta señales analógicas y digitales, permitiendo de esta manera que los datos se transmitan a través de líneas telefónicas sonoras. En el punto de origen las señales digitales son convertidas a una forma apropiada para su transmisión a través de equipos de comunicación

analógica. En el punto destino, estas señales analógicas son convertidas de nuevo a su forma digital original [Merilee Ford, 1998].

CSU/DSU

Una CSU/DSU (*Unidad de Servicio de Canal/ Unidad de Servicio de Datos)* es un dispositivo de interfaz digital que adapta la interfaz física de un dispositivo DTE (*Equipo Terminal de Datos),* como una terminal, a la interfaz del dispositivo DCE (*Equipo de Comunicación de Datos),* como un switch, en una red conmutada de transporte. La CSU/DSU también proporciona la temporizacion de la señal para la comunicación entre estos dispositivos [Merilee Ford, 1998].

1.2.3 Redes Wireless

Las computadoras móviles, como las notebook y los asistentes digitales personales (PDA's), es el área con más rápido crecimiento en la industria de las computadoras. Muchos de los dueños de estas computadoras tienen PC's sobre LAN's y WAN's en la oficina y desean ser conectados a su hogar aunque se encuentren lejos de casa o de viaje.

Las comunicaciones digitales Wireless no es una idea nueva. A principios de 1901 el físico italiano Gugliemo Marconi, demostró la idea de una comunicación wireless con el telégrafo utilizando el código Morse. Los sistemas digitales wireless tienen un mejor rendimiento, pero la idea básica es la misma [Tanenbaum, 1996].

Las redes wireless tienen muchos usos. El más común es tener una oficina portátil. Mucha gente usa equipo electrónico portátil para enviar y recibir llamadas telefónicas, faxes y correo electrónico, conectarse a una computadora remota para compartir archivos, y desean hacerlo de cualquier lugar ya sea tierra, mar o aire.

Asimismo, las redes inalámbricas y la computación móvil generalmente están relacionas pero, nos son idénticas. Las computadoras portátiles están algunas veces conectadas. Por ejemplo, si un viajante conecta su computadora portátil al teléfono en un hotel, tenemos movilidad sin usar una red inalámbrica. Otro ejemplo es, alguien que carga una computadora portátil mientras inspecciona un tren con problemas técnicos. Aquí el cable esta detrás (modelos de aspiradora).
Por otro lado, algunas computadoras inalámbricas no son portátiles. Un importante ejemplo seria una compañía dueña de un edificio que no tiene cables de red instalados y quiere conectar sus computadoras.

Del mismo modo las LAN's inalámbricas son fáciles de instalar pero tienen algunas desventajas. Generalmente tienen una capacidad de 1-2 Mbps que es muchísimo más lento que las LAN's que están cableadas. El margen de error es mucho más alto también y la transmisión entre distintas computadoras puede inferir con las demás.

Pero claro, existen aplicaciones inalámbricas como las de gente caminando alrededor de una tienda con un PDA haciendo inventario. En muchos aeropuertos saturados, los empleados del estacionamiento trabajan con

computadoras portátiles. Ellos teclean el número de placa en sus computadoras, las cuales tienen impresora, llaman a la computadora principal, obtienen la información de la renta del automóvil y se imprime directamente en la caja.

Las redes inalámbricas se presentan en distintas formas. Algunas universidades están instalando antenas alrededor del campus, que les permitan a los estudiantes consultar el catalogo de libros. En este caso, las computadoras se comunican directamente con la LAN inalámbrica de manera digital. Otra posibilidad es usando un celular el cuál es un teléfono con un MODEM análogo.
El sistema celular digital directo llamado CDPD (*Cellular Digital Packet Data)* esta siendo disponible en muchas ciudades.

1.3 Modelo de referencia OSI

A mediados de la década de 1970, cuando comenzaron a proliferar diferentes tipos de sistemas distribuidos (basados en redes tanto públicas como privadas), la industria de la computación reconoció las ventajas potenciales de los sistemas abiertos. El resultado fue la introducción de una serie de normas, la primera de las cuales se ocupaba de la estructura global de todo el subsistema de comunicación interno de cada computadora. Esta norma la introdujo la *Organización Internacional de Normas (ISO: Internacional Standard Organization)* y se conoce como el *modelo de referencia de la ISO (OSI: Open Systems Interconnection).* [Halsall, 1998]

El objetivo del modelo de referencia de la ISO es contar con un marco de referencia para coordinar el desarrollo de normas y permitir que las actividades de estandarización existentes y futuras tengan cabida dentro de dicho marco. Lo que se busca es que un proceso de aplicación en cualquier computadora que maneje un conjunto específico de normas pueda comunicarse con libertad con un proceso de aplicación de cualquier otra computadora que maneje las mismas normas, independientemente del origen de su fabricación.

La estructura lógica con que cuenta el modelo de referencia de la ISO esta constituida por siete capas de protocolos. Las tres capas inferiores (1 a 3 Ver Figura 1.6) dependen de la red y se ocupan de los protocolos relacionadas con la red de comunicación de datos que se esta usando para enlazar las dos computadoras. Las tres capas superiores (5 a 7 Ver Figura 1.6) están orientadas a las aplicaciones y se ocupan de los protocolos que permiten interactuar a dos procesos de aplicación de usuario final, casi siempre a través de una diversidad de servicios que ofrece el sistema operativo local. La capa de transporte intermedia (capa 4 Ver Figura 1.6) oculta a las capas superiores, orientadas a las aplicaciones, los detalles del funcionamiento de las capas inferiores, dependientes de la red. [Halsall, 1998]

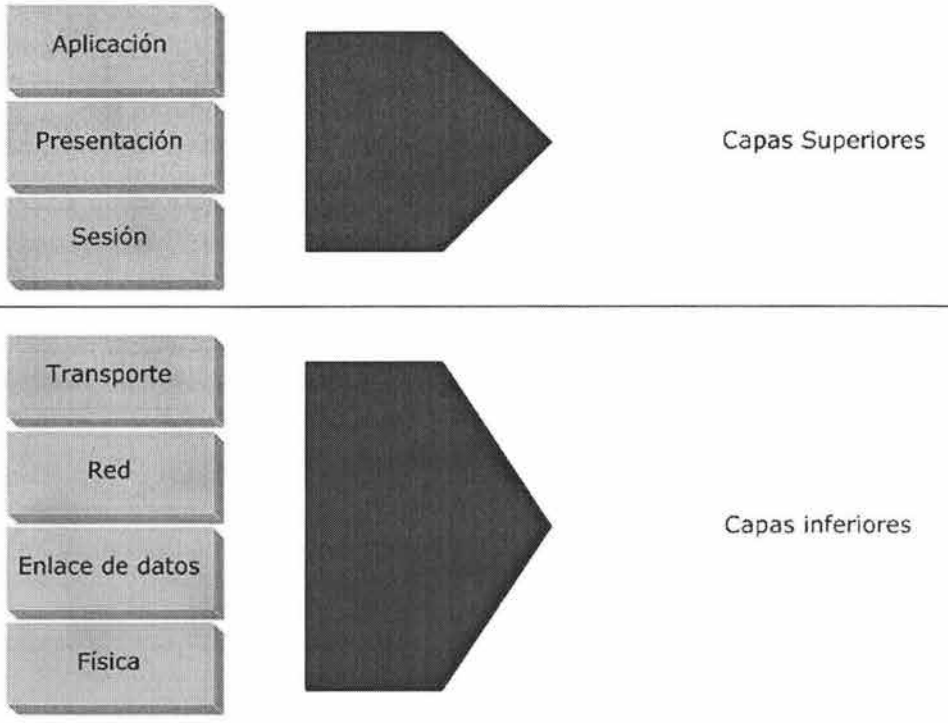


Figura 1.6: Modelo de referencia OSI.

Las capas dependientes de la red

Como las tres capas inferiores del modelo de referencia OSI dependen de la red, su funcionamiento peculiar varia de un tipo de red a otro. Sin embargo, en general, la capa de red se encarga de establecer y liberar una conexión entre dos entidades de protocolo de la capa de transporte que abarque toda la red. Entre otras, esta capa desempeña funciones de enrutamiento (direccionamiento) de red y, en algunas circunstancias, de control de flujo a través de la interfaz computadora-red. En el caso de la interconexión de redes, la capa de red realiza diversas funciones de armonización entre las redes interconectadas.

La capa de enlace utiliza la conexión física proporcionada por la red específica para ofrecer a la capa de red un recurso de transferencia de información confiable. La capa de enlace se encarga de funciones como la detección de errores y, en caso de haber errores de transmisión, de la retransmisión de mensajes. Por lo regular son dos tipos de servicios:

- Sin conexiones, que trata cada trama de información como una entidad autónoma que se transfiere según un enfoque "del mejor intento"; esto es, si se detectan errores en una trama, esta simplemente es desechada.
- Orientado a las conexiones, que procura proveer un recurso de transferencia de información libre de errores.

1.3.1 La capa física

La capa física define el tipo de medio, tipo de conector y tipo de señalización. Éste especifica los requisitos eléctricos, mecánicos, procedimentales y funcionales para activar, mantener y desactivar el vínculo físico entre sistemas finales. La capa física especifica también características tales como niveles de voltaje, tasas de transferencia de datos, distancias máximas de transmisión y conectores físicos.

Medios físicos y conectores

El medio físico y los conectores usados para conectar dispositivos al medio vienen definidos por estándares da la capa física.

Los estándares de Ethernet e IEEE 802.3 (CSMA/CD) definen una topología de bus para LAN que opera a una tasa de señalización de 10 megabits (Mbps). Los estándares de cableado de tres capas físicas, responden a las siguientes descripciones:

- **10Base2.** Conocido como Thinnet. Permite segmentos de red de hasta 185 metros sobre cable coaxial para interconectar o encadenar dispositivos.
- **10Base5**. Conocido como Thicknet. Permite segmentos de red de hasta 500 metros sobre grandes cables coaxiales con dispositivos en el cable para recibir señales.
- **10BaseT**. Transporta señales Ethernet hasta 100 metros de distancia en cable de par trenzado económico hasta un concentrador centralizado denominado hub. [McQuerry, 2001].

1.3.2 La capa de enlace

Antes de que el tráfico pueda entrar en la red, es necesario dar algunos detalles acerca de dónde ir y lo que se ha de hacer al llegar al destino. La capa de enlace de datos proporciona esta función.

La finalidad de esta capa es proporcionar las comunicaciones entre puestos de trabajo en una primera capa lógica que hay por encima de los bits del cable. El direccionamiento físico de los puestos finales se realiza en la capa de enlace de datos con el fin de facilitar a los dispositivos de red la determinación de si deben subir un mensaje a la pila de protocolo. También hay campos en esta capa para indicar al dispositivo cual es la pila de la capa superior donde deben pasar los datos (como IP, IPX, Apple Talk, etc.). La capa de enlace de datos da soporte a servicios basados en la conectividad y no basados en ella, y proporciona la secuencia y control de flujo.

Para proporcionar estas funciones, la capa de vínculo de datos IEEE está definida mediante dos subcapas:

- **Subcapa de control de acceso al medio (MAC) (802.3).** La subcapa de control de acceso al medio es la responsable de determinar cómo han de ser transportados los datos a través del cable físico. Ésta es la parte de la capa de vínculo de datos que se comunica hacia abajo con la capa física. En ella se definen funciones tales como el direccionamiento físico, topología de la red, disciplina

de la línea, notificación de errores, distribución ordenada de tramas u control óptimo de flujo.

- **Subcapa de control de enlace lógico (LLC) (802.2).** La subcapa de control de enlace lógico es la responsable de la identificación lógica de los distintos tipos de protocolos y el encapsulado posterior de los mismos para ser transmitidos a través de la red. Un identificador de código de tipo o punto de acceso al servicio (SAP) es el encargado de realizar la identificación lógica. El tipo de la trama LLC utilizado por un puesto final depende del identificador que espera el protocolo de la capa superior. Entre las opciones LLC adicionales figuran el soporte para conexiones entre aplicaciones que se ejecutan en la LAN, el control de flujo a la capa superior y la secuencia de bit de control. Para algunos protocolos, LLC define servicios fiables y no fiables para la transferencia de datos, en lugar de la capa de transporte.

Éstas son las definiciones de los campos de la subcapa MAC:

- La trama IEEE 802.3 comienza con un patrón alternado de unos y ceros llamado **preámbulo.** El preámbulo avisa a los puestos receptores de la llegada de una trama (Ver Figura 1.7).

- Inmediatamente a continuación del preámbulo se encuentran los campos de **dirección física de origen** y **destino.** Dichas direcciones se conocen como **direcciones de la capa MAC**. Éstas son únicas para cada dispositivo de la **interconexión** de redes. En la mayoría de las tarjetas LAN, la dirección MAC se graba en la ROM, lo que explica el término burned-in-address (BIA). Cuando sé inicializa la tarjeta de red, esta dirección se copia en la RAM para identificar el dispositivo en la red (Ver Figura 1.7).

La dirección MAC consta de 48 bits y viene expresada en 12 dígitos hexadecimales. Los primeros 24 bits, o 6 dígitos hexadecimales, de la dirección MAC contienen un código de identificación del fabricante o vendedor. Otro nombre por el que se conoce a esa parte de la dirección es Organizationally Unique Identifier (OUI). Los últimos 24 bits, o 6 dígitos hexadecimales, están administrados por cada fabricante y presentan, por lo general, el número de serie de la tarjeta. La dirección de origen es siempre una dirección de unidifusión (nodo simple), mientras que la dirección de destino puede ser una unidifusión, multidifusión (grupo de nodos) o difusión (todos los nodos) (Ver Figura 1.7).

En las tramas IEEE 802.3, el campo de dos bytes que sigue a la dirección de origen es el campo **longitud**, e indica el número de bytes de datos que siguen a este campo y preceden al campo de secuencia de verificación de trama (FCS) (Ver Figura 1.7).

A continuación del campo longitud se encuentra el campo **datos**, que incluye la información de control LLC, además de otra información de control de capa superior y los datos del usuario (Ver Figura 1.7).

Por último, a continuación del campo de datos hay un campo de 4 bytes FCS que contiene un valor de verificación de redundancia cíclica (CRC). La CRC se crea por el dispositivo emisor y se vuelve a calcular por el dispositivo receptor para comprobar si ha habido daños en la trama durante su tránsito (Ver Figura 1.7).

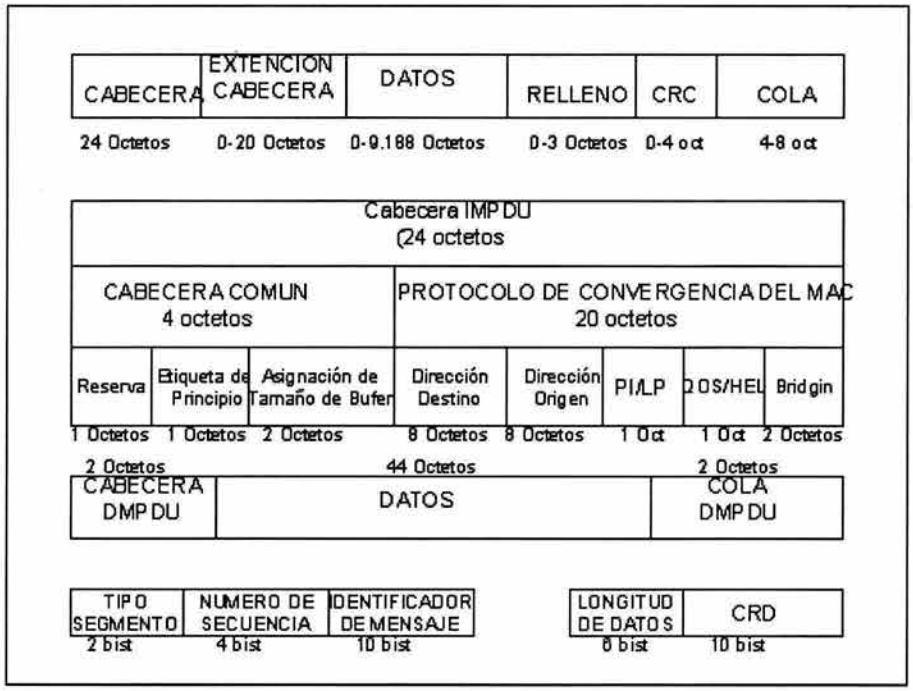


Figura 1.7: Campos de la Subcapa MAC.

Dispositivos de la capa de enlace

Los bridges y switches de la Capa 2 son dispositivos que funcionan en la capa de enlace de datos de la pila del protocolo. La conmutación de la Capa 2 se basa en el puenteado por hardware. En un switch, el reenvío de tramas se controla por medio de un hardware especial llamada circuitos integrados específicos de aplicaciones (ASIC). La tecnología ASIC permite que un chip de silicio pueda ser programado para realizar una función específica durante el proceso de fabricación del mismo. Esta tecnología permite que las funciones puedan llevarse a cabo a una velocidad mucho mayor que si el chip estuviese programado por software. Debido a la tecnología ASIC, los switches proporcionan escalabilidad a velocidades de gigabits con una latencia baja.

Una red puenteada/conmutada proporciona una excelente administración del tráfico. La finalidad del dispositivo de Capa 2 es reducir las colisiones al asignar a cada segmento su propio dominio de colisión. Cuando hay dos o más paquetes que necesitan entrar en un segmento, quedan almacenados en memoria hasta que el segmento esté disponible.

Las redes punteadas/conmutadas poseen las siguientes características:

- Cada segmento posee su propio dominio de colisión.
- Todos los dispositivos conectados al mismo bridge o switch forman parte del mismo dominio de difusión.
- Todos los segmentos deben utilizar la misma implementación al nivel de la capa de enlace de datos como, por ejemplo, Ethernet o Token Ring. Si un puesto final concreto necesita comunicarse con otro puesto final a través de un medio diferente, se hace necesaria la presencia de algún dispositivo, como puede ser un router o un bridge de traducción, que haga posible al diálogo entre los diferentes tipos de medios.
- En un entorno conmutado, puede haber un dispositivo por segmento, y todos los dispositivos pueden enviar tramas al mismo tiempo, permitiendo de este modo que se comparta la ruta primaria.

1.3.3 La capa de red

La capa de red define cómo tener lugar el transporte de tráfico entre dispositivos que no están conectados localmente en el mismo dominio de difusión. Para conseguir esto se necesitan dos elementos de información:

- Una dirección lógica asociada a cada puesto de origen y de destino.
- Una ruta a través de la red para alcanzar el destino deseado.

Los esquemas de direccionamiento lógico se utilizan para identificar redes en una interconexión de redes y la ubicación de los dispositivos dentro del contexto de dichas redes. Estos esquemas varían en función del protocolo de capa de red que se utilice.

Direcciones de la capa de red

Las direcciones de la capa de red (denominadas direcciones lógicas o virtuales) se sitúan en la Capa 3 del modelo de referencia OSI. A diferencia de las direcciones de la capa de vínculo de datos, que suelen residir en un espacio de direcciones plano, las direcciones de la capa de red poseen habitualmente una estructura jerárquica en la cual se definen primero las redes y después los dispositivos o nodos de cada red.

Las capas orientadas a las aplicaciones

1.3.4 La capa de transporte

Para poder conectar dos dispositivos en la construcción de una red, es necesario establecer una conexión o sesión. La capa de transporte define las directrices de la conexión entre dos puestos finales. Una sesión constituye una conexión lógica entre transporte iguales en los puestos de origen y destino.

Concretamente, la capa de transporte define las funciones que se describen a continuación:

- Permitir a los puestos finales ensamblar y desensamblar múltiples segmentos de capa superior en el mismo flujo de datos de la capa de transporte. Esto se consigue asignando identificadores de aplicación de capa superior. Dentro de la suite del protocolo TCP/IP, estos identificadores se conocen como **números de puerto**. El modelo de referencia OSI denomina a estos identificadores como puntos de acceso al servicio (SAP). La capa de transporte utiliza estos números de puerto para identificar elementos de la capa de aplicación como FTP O Telnet. Un ejemplo de número de puerto es el 23, que identifica la aplicación Telnet. Los datos con un número de puerto de transporte 23 serán destinados a la aplicación Telnet.

- Permitir a las aplicaciones solicitar transportes fiables de datos entre sistemas finales que están en comunicación. Los transportes fiables utilizan una relación orientada a la conexión entre los sistemas en comunicación para conseguir los siguientes objetivos:
  - Asegurar que los segmentos distribuidos serán confirmados al remitente.
  - Proporcionar la retransmisión de cualquier segmento que no sea confirmado.
  - Colocar de nuevo los segmentos en su orden correcto en el puesto receptor.
  - Proporcionar control y evitar congestiones.

En la capa de transporte, los datos pueden ser transmitidos de forma fiable o no fiable. Para IP, el protocolo TCP es fiable u orientado a conexión, mientras que UDP no es fiable, o independiente de la conexión.

1.3.5 La capa de sesión

La capa de sesión es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

Además, la capa de sesión proporciona varios servicios opcionales, entre ellos los siguientes:

- Gestión de interacciones. El intercambio de datos asociado a un dialogo puede ser duplex -bididireccional simultaneo- o semiduplex–bidireccional alternado-.
- Informe de excepciones. La capa de sesión puede notificar a la capa de aplicación la ocurrencia de excepciones no recuperables durante una transacción.

1.3.6 La capa de presentación

La capa de presentación proporciona diversas funciones de conversión y codificación que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que los datos enviados desde la capa de aplicación de un sistema podrán ser leídos por la capa de aplicación de otro sistema. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Otro ejemplo podrían ser los formatos de imágenes jpeg y gif que se muestran en páginas Web. Este formato asegura que todos los navegadores Web podrán mostrar las imágenes, con independencia del sistema operativo utilizado.

Otra función de la capa de presentación es la encargada de la seguridad de los datos. En algunas aplicaciones, antes de ser enviados, los datos se cifra una clave que solo conozca la capa de presentación del destinatario al que van dirigidos. Ésta descifra los datos recibidos con la clave correspondiente antes de pasarlos al destinatario.

1.3.7 La capa de aplicación

La capa de aplicación proporciona la interfaz de usuario normalmente un programa/ proceso de aplicación a una variedad de servicios de información distribuida que abarca toda la red. Entre ellos se cuentan transferencia y gestión de archivos, así como, servicios generales de intercambio de documentos y mensajes, como el correo electrónico.

Además de la transferencia de información, la capa de aplicación proporciona servicios como:

- Identificación del o los interlocutores buscados, por nombre o por dirección.
- Determinación de la disponibilidad actual de un interlocutor buscado.
- Establecimiento de la autorización para comunicarse.
- Acuerdo sobre mecanismos de confidencialidad.
- Verificación de la autenticidad de un interlocutor buscado.
- Selección de la disciplina de dialogo, incluidos los procedimientos de inicio y liberación.
- Acuerdo sobre quien se encargara de la recuperación de errores.
- Identificación de restricciones de la sintaxis de los datos.

1.4 TCP/IP

Las redes están compuestas generalmente por un pequeño número de máquinas localizadas en el mismo edificio, o incluso en una sola planta que están interconectadas para proporcionar un entorno de trabajo homogéneo. Es típico que se quiera compartir archivos entre estos nodos, o ejecutar aplicaciones distribuidas en diferentes máquinas.

Estas tareas requieren una aproximación completamente diferente a las redes. En lugar de reenviar archivos completos con una descripción del trabajo, todos los datos se fragmentan en pequeñas unidades (paquetes),

que se envían inmediatamente al nodo destino, donde son reensamblados. Este tipo de redes son llamadas redes de intercambio de paquetes. Entre otras cosas, esto permite ejecutar aplicaciones interactivas a través de la red.

La solución que han adoptado los sistemas es conocida como TCP/IP. El TCP/IP tiene sus orígenes en un proyecto de investigación fundado en Estados Unidos por el DARPA (*Defense Advanced Research Projects Agency, Agencia de Proyectos Avanzados de Investigación en defensa)* en 1969. Una vez comprobado el éxito, esta red ARPANET fue operativa en 1975. [Parker, 1996].

Si queremos definir TCP/IP, podemos decir que es un conjunto de protocolos de red que proporcionan comunicaciones a través de redes interconectadas de computadoras con diversas arquitecturas hardware y variados sistemas operativos. Las siglas significan: protocolo de Control de Transmisiones/ Protocolo Internet.

TCP/IP esta dividido en cuatro capas que definen el llamado Modelo DOD (Department of Defense), cada una de éstas, se encarga de realizar una función o tarea especifica dentro de una red y también puede incluir diferentes protocolos (Ver Figura 1.8).

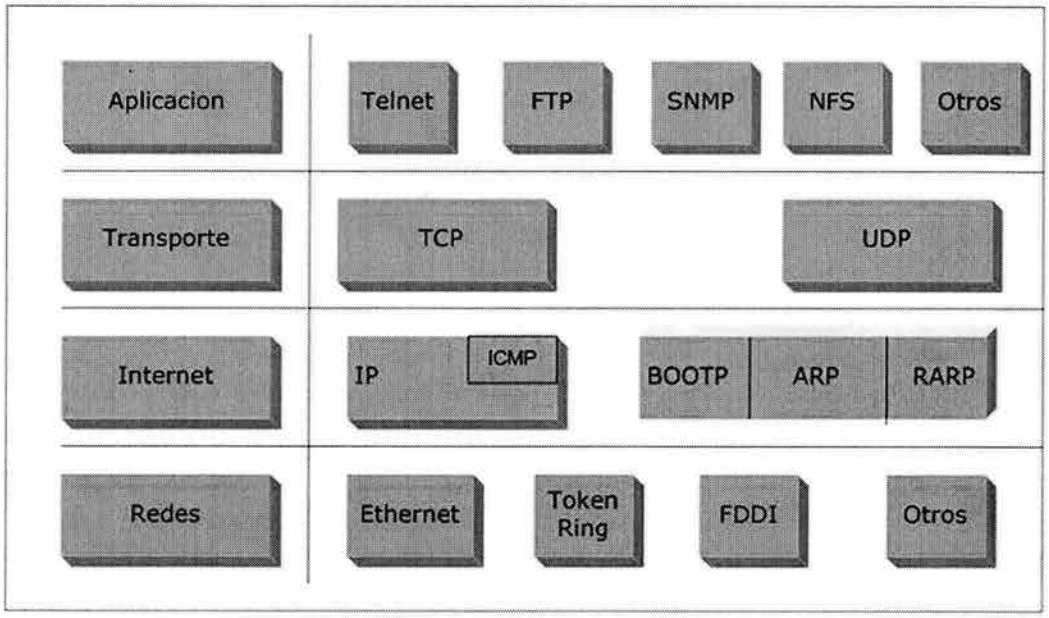


Figura 1.8: Descripción del modelo DOD y su referencia con TCP/IP.

1.4.1 Capas del protocolo

Capa Interfaz de Redes

Es la base del modelo y el nivel más bajo. Esta capa es responsable de poner los frames dentro de los cables y fuera de ellos; es decir, es

responsable de la transmisión de los datagramas sobre la capa física de la red y hasta el destino.

Cuando llega el paquete a esta capa, se agrega un CRC y un preámbulo; al recibirse en el host destino se descarga el preámbulo y se calcula el CRC si esta correcto la dirección MAC es examinada.

- CRC: (Cyclic Redundancy check), calculo matemático que se añade para verificar que no ha sido corrupto el paquete.
- Preamble: secuencia de bits que identifican el inicio del paquete.
- MTU: (Maxim Transfer Unit) cada tipo de medio físico tiene un tamaño máximo de trama que no se puede superar, el nivel de redes o el nivel de enlace (modelo OSI) es el responsable de obtener esta unidad y de informar a los protocolos situados por encima.

Cuando se establece una conexión, los dos hosts involucrados intercambian sus valores MSS (tamaño de segmento máximo), y que para la conexión se utiliza el valor más pequeño de los dos MSS, el calculo es el siguiente: MTU menos 40 bytes para los encabezados de IP y TCP.

Capa de Internet

Es el segundo nivel y es el responsable de proveer la comunicación host-to-host. Aquí es donde el paquete es encapsulado en un datagrama de Internet, los algoritmos de ruteo son cargados (ya sea estático o dinámico) y el datagrama es enviado a la capa de Redes para su transmisión. Los protocolos más importantes son:

- ARP: que es usado para obtener la dirección física de los hosts localizados en la misma red física.
- ICMP: envía mensajes y reportes de error de los paquetes.
- IP: es el principal responsable de la dirección y ruteo de los paquetes entre hosts y redes. IP para enviar un paquete le agrega su propio encabezado con las direcciones IP del host origen y del host destino, el protocolo que lo entrega, checkhsum y el TTL.

Capa de Transporte

Provee la comunicación entre computadoras. El método deseado para la entrega de paquetes lo define el protocolo, de los cuales tenemos:

- TCP que es orientado a conexión, establece comunicación para aplicaciones de transferencia larga y que requiere un mensaje de conocimiento de la información enviada.
- UDP no es orientado a la comunicación por lo que no garantiza que los paquetes hayan sido entregados. Las aplicaciones que utilizan UDP son pequeñas y es su responsabilidad la entrega de los paquetes.

Capa de Aplicaciones

Es la capa más alta, es donde las aplicaciones inician la cadena hacia el acceso por la red. Esta capa es la interfase con el usuario, contiene aplicaciones específicas. Entre las cuales tenemos: FTP, Telnet y SNMP, lo

que son transferencias de archivos y correos electrónicos, entre otras y varían de acuerdo al sistema operativo con el que estemos trabajando.

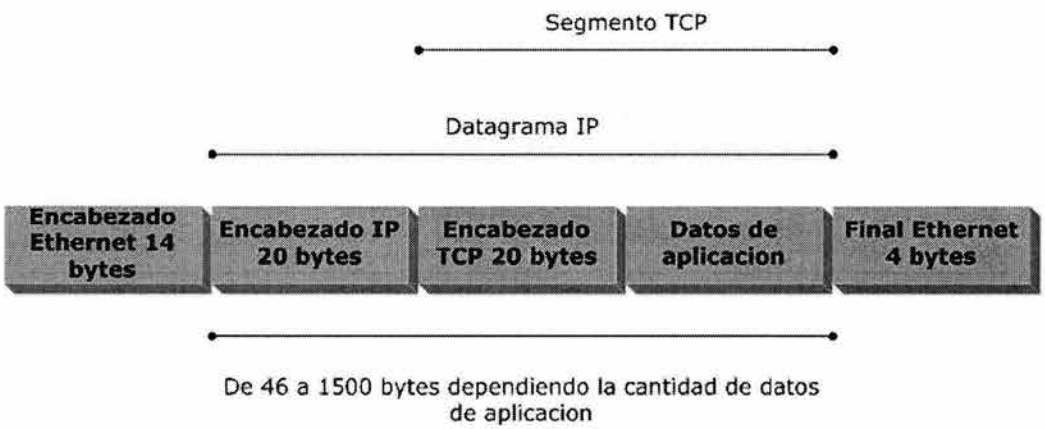
Terminología TCP/IP y protocolos

Llamamos paquete a la unidad de transmisión de tamaño máximo fijo que consta de información binaria que representa datos y una cabecera que contiene un número ID, direcciones origen y destino y datos de control de errores [Heywood, 1998].

Un paquete de datos se mueve de una capa a otra dentro del stack TCP/IP, cada protocolo agrega al paquete su propia información. El paquete con la información que se le va agregando recibe diferentes nombres técnicos como identificación a los protocolos. Estos nombres son:

- Segmento: un segmento es la unidad de transmisión en TCP. Este contiene un encabezado y datos de aplicación [Heywood, 1998].
- Mensaje: un mensaje es una unidad de transmisión de protocolos no-fiables como: ICMP, UDP, IGMP. Este contiene un encabezado del protocolo y datos de aplicación [Heywood, 1998].
- Datagrama: es la unidad de transmisión IP. Contiene un encabezado IP acompañado de datos de la capa de transporte y también se considera como no fiable [Heywood, 1998].
- Frame: un frame es una unidad de transmisión en la capa de interfaz de redes y consiste de un encabezado agregado por la capa de interfaces de red acompañado de datos capa IP [Heywood, 1998].

El propósito de toda esta información que contienen estos encabezados es ayudar a la red a que dirija los paquetes desde el equipo origen hasta el equipo destino, permite a la computadora decidir si quiere aceptarlo. El encabezado IP específica que maquina debería recibirlo y el encabezado TCP especifica que aplicación de la computadora destino tomara los datos (Ver Figura 1.9).



Un Frame Ethernet con los encabezados de todos los componentes de un paquete TCP

Figura 1.9: Encabezados de un paquete TCP.

Componentes del Frame

Un frame que es el término para un paquete de datos en la capa de interfaz de redes contiene tres componentes principales: el encabezado, datos y trailer.

- Encabezado: incluye una señal de alerta para indicar que el paquete es transmitido, la dirección fuente y la dirección destino.
- Datos: esta es la información actual enviada por la aplicación. Este componente varía en tamaño despendiendo de los límites configurados por la red.
- Trailer: el contenido exacto varía dependiendo de la capa de interfaz de redes. Contiene un CRC (*Cyclical Redundancy Check)* que es un número que se produce de un cálculo matemático en la fuente. Cuando el paquete llega al destino, el calculo se hace de nuevo, si el resultado es el mismo indica que el paquete se ha mantenido estable.

1.4.2 ARP, Address Resolution Protocol

Para que los hosts de una red se puedan comunicar, es necesario que entre ellos se conozcan sus direcciones físicas, la resolución de direcciones es el proceso del mapeo entre las IP de los hosts y sus direcciones físicas [Heywood, 1998].

ARP, es el responsable de esta función y lo hace a través del envío de broadcast a los hosts si están en una red local o al ruteador si es remoto. Una vez que se obtiene un mapeo se guarda una entrada en su cache, así, cada vez que requiere de una dirección primero checa si no la ha resuelto ya.

El proceso ARP, incluye dos fases un ARP request y un ARP replay, y va de la siguiente manera:

1. Una petición ARP es iniciada cada vez que un host intente conectarse a otro host. Primero IP determina si esta en su mismo segmento de red para que el host cheque su cache y busque la dirección física del host.
2. Si no cuenta con el mapeo, ARP construye un mensaje solicitando "de quien es esta IP y cual es su dirección física". Es enviado como una señal de tipo broadcast y es para todos los hosts de la red.
3. Todos los hosts escuchan el mensaje y revisan si no es su dirección, en caso de no ser para ellos, ignoran la solicitud.
4. Cuando el host destino reconoce su IP entonces envía un replay (respuesta) directamente al host origen con su dirección MAC. Por supuesto, actualiza su cache con la información del host y al enviar su respuesta se establece la comunicación.

Si el host destino se encuentra en otra red, el proceso varia un poco porque el mensaje broadcast va dirigido al ruteador, él a su vez, envía un datagrama al host destino.

La cache ARP

La cache ARP mantiene entradas estáticas y dinámicas, las dinámicas se crean y se borran automáticamente cuando estamos resolviendo a direcciones IP y tienen un tiempo de vida de diez minutos.

Las entradas estáticas se ingresan manualmente y se conservan hasta que la maquina es re-iniciada, o cuando se borran manualmente y cuando ARP recibe una dirección diferente, entonces se convierte en dinámica y reemplaza la anterior.

1.4.3 ICMP, Internet Control Message Protocol

El protocolo de mensajes de control de Internet es un protocolo de mantenimiento especificado en el RFC 792. Los mensajes ICMP se encapsulan dentro de los datagramas de IP para que puedan encaminarse entre varias redes interconectadas [Heywood, 1998]. Se utiliza para:

- Construir y mantener tablas de ruteo.
- A descubrir la Unidad de Transferencia (MTU); se basa en los mensajes del destino no alcanzables RFC 1191.
- Diagnosticar problemas.
- Ajustar el control de flujo para prevenir la saturación de enlace de encaminadotes.

1.4.4 IP, Internet Protocol

Es el protocolo primeramente responsable del direccionamiento y ruteo de los paquetes entre los hosts. Protocolo de mensajeria, proporciona un sistema de envió de mínimo esfuerzo [Heywood, 1998].

No esta orientado a la conexión, lo que quiere decir es que no establece una sesión antes del intercambio de datos. No garantiza la entrega de paquetes.

Si el IP identifica en una red remota, entonces IP checa la tabla de ruteo para enviarlo al router que corresponde el host remoto.

1.4.5 TCP, Transmission Control Protocol

Es un protocolo de Internet orientado a conexión responsable de fragmentar los datos en paquetes que el protocolo IP envía a la red. Este protocolo proporciona un flujo de comunicación fiable y secuenciado para la comunicación de red [Heywood, 1998].

El protocolo de control de transmisión suministra a los programas un servicio orientado a conexión, fiable y de flujos de bytes. Los servicios de red se basan en el transporte TCP para iniciar la sesión, compartir archivos e impresión, duplicar la información entre controladores de dominio, transferencia de listas de examinadores y otras funciones comunes. Sólo puede utilizarse TCP para comunicaciones de uno a uno. TCP utiliza una suma de comprobación en ambas cabeceras y en los datos de cada segmento para reducir las probabilidades de corrupción que no se detecte en los datos.

Un mensaje de ACK (*Acknowledgment)* es usado para verificar que los datos hayan sido recibidos por los otros hosts. Por cada segmento enviado, el host que recibe debe enviar un ACK.

Cuando no se recibe el mensaje de ACK, la información es retransmitida, igualmente, cuando un segmento es dañado se vuelve a enviar.

1.4.6 UDP, User Datagrama Protocol

El protocolo de datagramas de usuarios suministra un servicio no orientado a conexión y no fiable. Se utiliza frecuentemente en comunicaciones de datagramas IP de difusión. Puesto que no esta garantizada la recepción de los datagramas UDP, los programas que lo utilizan deben elaborar sus propios mecanismos de fiabilidad [Heywood, 1998].

UDP Ports: para uso de UDP, la aplicación debe contar con la dirección IP y el número de puerto de la aplicación destino. Un port es la entrada por donde se reciben los mensajes. Por mencionar algunos tenemos Netstat, 15, 53; TFTP, 69; SNMP, 161.

1.4.7 Clases de redes

La comunidad de Internet decidió que las direcciones IP se dividieran en diferentes clases de redes, (A, B, C, D y E); de los cuales trabajamos con tres nada mas ya que los otros rangos están asignados a usos experimentales e investigaciones [Heywood, 1998].

Para organizar mejor las clases de red, se decidió desde los primeros días de vida de IP, que los primeros bits deberían decidir la clase a la que pertenecían. Esto quiere decir que el primer octeto de la dirección IP específica la clase.

TCP/IP soporta las clases A, B y C; las clases de redes se definen por el número de bits que son utilizados para identificar la red (Network ID) y los bits restantes son asignados a los dispositivos que componen la red. Igualmente define los posibles números de redes que hay dentro de cada clase y los números de hosts que puede haber para cada red.

Redes Clase A

En una red clase A, el primer octeto identifica la red y los tres octetos últimos el número de nodo.
El primer bit debe ser 0xxxxxxx
Valor mínimo: 00000000 Decimal: 0
Valor máximo: 01111111 Decimal: 127
Rango: 1-126

Hay 126 redes de clase A, cada una tiene 16,777,214 hosts.

Redes Clase B

En redes clase B. Los dos primeros octetos son para identificar la red y los demás para el número de host.
Los primeros bits deben ser: 10xxxxxxxx
Valor mínimo: 10000000 Decimal:128
Valor máximo: 10111111 Decimal:191
Rango: 128-191
Hay 16,384 redes de clase B. Cada una tiene 65,534 hosts.

Redes Clase C

Los primeros bits deben ser: 110xxxxxxx
Valor mínimo: 11000000 Decimal:192
Valor máximo: 11011111 Decimal:223
Rango: 192-223
Hay 2,091,152 redes de clase C y cada una tiene 254.

Redes Clase D

Las direcciones de las redes clase D están dentro del rango de 224.0.0.0 al 239.255.255.255 son usadas para paquetes multicast.

Los paquetes multicast usan muchos protocolos para alcanzar el grupo de hosts. IGMP Router Discovery es un ejemplo de un protocolo que utiliza paquetes multicast.

Redes clase E

Igualmente, las direcciones de esta clase se encuentran dentro del rango 240.0.0.0 al 255.255.255.255 y están reservadas para futuros nodos de direcciones. Direcciones de las clases D y E no están asignadas a hosts individuales y mas bien son para fines de investigación.

Se cuentan con ciertas reglas que debemos tener siempre en cuenta:

- El ID de una red no puede ser 127, ya que esta reservada para funciones de Loopback.
- El ID de la red y el ID del host, nunca pueden ser todos 0's o sea que no puede ser 0 porque se considera como en esta red nada mas.
- El ID de la red y el ID del host, nunca pueden ser todos 1's o sea que no puede tener el valor de 255 ya que se considera como un broadcast a la dirección.
- El número ID de un host debe ser único en una red local.
- Todos los hosts incluyendo interfaces como routers, requieren una dirección única dentro de la red.

1.4.8 Mascara de Red

Las direcciones IP se dividen en dos partes, la dirección de red y la dirección de la maquina. Dependiendo de la clase de la dirección hay 254 a 16 millones de direcciones disponibles para los hosts de la red.

Una mascara de red, es una dirección de 32 bits, que:

- En primer lugar le dice al sistema que bits de la dirección IP corresponden al componente de red y que bits corresponden al componente maquina.
- Sirve para bloquear una porción de la dirección IP para distinguir el ID de la red del número de los hosts.
- Especificar cuando un host destino esta en una red local o remota.
- Cada host en una red basada en TCP/IP requiere de una mascara, ya sea una mascara por defecto cuando la red no esta subdividida o una personalizada de acuerdo a los segmentos en que se haya dividido la red.

1.5 VLAN's

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub. Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.
Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma. Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, logramos, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios. Además, al poder distribuir a los usuarios en diferentes segmentos de la red, podemos situar puentes y encaminadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, podemos mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo [Palet, 1995].

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde/hacia otras redes. Pero aún se puede llegar más lejos. Las redes virtuales nos permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o

MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

Existen tres aproximaciones diferentes que pueden ser empleadas como soluciones válidas para proporcionar redes virtuales: conmutación de puertos, conmutación de segmentos con funciones de bridging, y conmutación de segmentos con funciones de bridging/routing.

Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones válidas, sólo la última, con funciones de bridge/router, ofrece todas las ventajas a las VLAN.

- Conmutadores de puertos. Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden ser dinámicamente asociados a cualquiera de los segmentos, mediante comandos software. Cada segmento se asocia a un "backplane", el cual a su vez, equivale a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden ser asignadas y reasignadas a diferentes grupos de trabajo o redes virtuales.

Podemos definir a los conmutadores de puertos como "software patch panels", y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo; sin embargo, tienen graves limitaciones.

Dado que están diseñados como dispositivos compartiendo un backplane físico, las reconfiguraciones de grupo de trabajo están limitadas al entorno de un único concentrador, y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos, padecen de conectividad con el resto de la red. Al segmentar sus propios backplanes, no proporcionan conectividad integrada entre sus propios backplanes, y por tanto están "separados" de la comunicación con el resto de la red. Para ello requieren un bridge/router externo. Ello implica mayores costos, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red.

Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, y por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.

- Conmutadores de segmentos con bridging: A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Para ello, se emplean los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos, para proporcionar conectividad entre varios segmentos a la "velocidad del

cable" o velocidad máxima que permite la topología y protocolos de dicha red [Palet, 1995].

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane, sino grupos lógicos de nodos que pueden ser conectados a cualquier número de segmentos de red físicos. Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, mediante comandos software se puede reconfigurar y modificar la estructura de la VLAN, con la ventaja añadida del ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aún así, comparten el mismo problema con los conmutadores de puertos en cuanto a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red precisan de routers (encaminadores), con las consecuencias de las que ya hemos hablado en el caso anterior respecto del costo y la reconfiguración de la red.

- Conmutadores de segmentos con bridging/routing: Son la solución evidente. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además, con funciones añadidas de routing (encaminamiento), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de red.

Además, sus funciones de routing facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales, podemos crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiéndonos así asignar el ancho de banda requerido por el nuevo grupo de trabajo sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de routing, la comunicación con el resto de la red se puede realizar de dos modos diferentes: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de routing multiprotocolo integradas, que facilitan el tráfico incluso entre varias VLAN's.

Los dispositivos con funciones VLAN nos ofrecen unas prestaciones de "valor añadido", suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLAN.

Al igual que en el caso de los grupos de trabajo "físicos", las VLAN permiten a un grupo de trabajo lógico compartir un dominio de broadcast. Ello significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física. Por ello, las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos broadcast no son recibidos por otras estaciones situadas en otras VLAN.

Las VLAN no se limitan solo a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica. Además las redes virtuales pueden solaparse, permitiendo que varias de ellas compartan determinados recursos, como backbones (troncales) de altas prestaciones o conexiones a servidores.

Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales, es la administración de las redes y subredes. Las VLAN tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones.

Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred; por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico puede soportar varias subredes.

Asimismo, hay que tener en cuenta que los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que nos permiten determinar con gran precisión las características del tráfico y de la seguridad que deseamos en cada dominio, segmento, red o conjunto de redes. Todo ello se realiza en función de algoritmos de bridging, y routing multiprotocolo.

Vamos a intentar esquematizar los puntos en que las redes virtuales pueden beneficiar a las redes actuales:

- Movilidad: Como hemos visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.
- Dominios lógicos: Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.
- Control y conservación del ancho de banda: Las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.
- Conectividad: Los modelos con funciones de routing nos permiten interconectar diferentes conmutadores y expandir las redes virtuales

a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

- Seguridad: Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.
- Protección de la inversión: Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costos adicionales.

Como se ha venido observando, es importante tener en cuenta muchos aspectos en el momento de diseñar o implementar una red ya que de ello dependerá el buen funcionamiento de esta en el futuro, asimismo, es necesario hacer un análisis correcto, con un enfoque dirigido para satisfacer las necesidades de la empresa como las necesidades de la misma red de datos. Es por ello que en el siguiente capitulo analizaremos la red de la Institución Educativa y propondremos un nuevo diseño de la misma.

Capítulo 2

2.1 Análisis de la red

Hasta este momento nos hemos limitado a definir conceptos generales de redes, el objetivo de definir estos conceptos es poder tener una base formal sobre la cual poder enfocarnos a la optimización de la red.

Sin embargo, debemos tener presente que no existe una respuesta única a este problema. Es mas, tras cada cuestión y tras cada posible respuesta se esconden multitud de soluciones que también tendremos que ir considerando a medida que avancemos en el desarrollo de este trabajo.

Primeramente nos enfocaremos a dar una descripción general de la red de la Institución Educativa, para posteriormente proponer una solución concreta y definir un nuevo diseño de esta red.

2.1.1 Descripción de la Red

La Institución Educativa cuenta con varios servidores que se encuentran protegidos por un firewall en una zona conocida como DMZ (De-Militarized Zone) (Ver figura 2.1). Dichos servidores proporcionan diferentes servicios de información tanto a usuarios internos de la Institución como a usuarios externos que navegan en Internet. Ejemplos de los servicios que ofrecen son: Correo Electrónico, Servidores con plataformas Web para consultar cursos, el propio servicio de Intranet y el servicio de resolución de nombres para ser resueltos hacia Internet.

Los servidores de la DMZ están configurados con direcciones IP no homologadas, es decir, no visibles desde Internet, pero hacen uso del servicio de NAT (Network Address Translation), que es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. NAT es necesario cuando la cantidad de direcciones IP que nos haya asignado nuestro proveedor de Internet (ISP) sea inferior a la cantidad de computadoras que queramos que accedan a Internet. NAT se describe en el RFC 1631 [http://www.faqs.org/rfcs/rfc1631.html]. NAT nos permite aprovechar los bloques de direcciones reservadas que se describen en el RFC 1918. Generalmente, una red interna se suele configurar para que use uno o más de estos bloques de red para que les sea posible intercambiar información hacia el exterior.

Actualmente, las direcciones homologadas a través de las cuales estos servidores pueden ser accesados desde Internet son direcciones que pertenecen al ISP (Una de las dos conexiones actuales de la Institución Educativa). Sin embargo, al interior de la Institución Educativa, estas direcciones no son visibles debido a la forma en que se están traduciendo por el proceso de NAT.

Nota.- Por cuestiones de seguridad y privacidad de la Institución Educativa mostraremos las direcciones IP públicas e internas modificadas.

La sección llamada DMZ cuenta con el siguiente equipo:

- Server DNS, IP pública 200.69.105.12 IP interna (NAT) 172.16.10.16 y corre bajo Linux.
- Server Educación Virtual, IP pública 200.69105.11 IP interna (NAT) 172.16.10.22, corre bajo Linux.
- Server MAIL, IP pública 200.69.105.10 IP interna (NAT) 172.16.10.10, corre bajo Linux.
- Server INTRANET, IP pública 200.69.105.14, 200.69.105.13 IP interna (NAT) 1a 172.16.10.12, 2a 172.16.10.18, utiliza Windows 2000 Server.

Estos dispositivos están conectados a un HUB 3COM a 10Mbps y tiene un Default Gateway 200.69.105.10/27, que le permite comunicarse con la interfaz correspondiente en el firewall DMZ.

La parte llamada MZ (Militarized zone) es una red LAN, y su primordial función es la de brindar servicios cliente/servidor, el término cliente/servidor, describe un sistema en el que una máquina cliente solicita a una segunda máquina llamada servidor que ejecute una tarea específica. El cliente suele ser una computadora personal común conectada a una LAN, y el servidor es, por lo general, una máquina anfitriona, como un servidor de archivos PC, un servidor de archivos de UNIX o una macrocomputadora o computadora de rango medio. El programa cliente cumple dos funciones distintas: por un lado gestiona la comunicación con el servidor, solicita un servicio y recibe los datos enviados por aquél. Por otro, maneja la interfaz con el usuario: presenta los datos en el formato adecuado y brinda las herramientas y comandos necesarios para que el usuario pueda utilizar las prestaciones del servidor de forma sencilla. El programa servidor en cambio, básicamente sólo tiene que encargarse de transmitir la información de forma eficiente. No tiene que atender al usuario. De esta forma un mismo servidor puede atender a varios clientes al mismo tiempo. Es en esta parte de la red es donde nos enfocaremos a realizar la optimización planteada en esta tesis.

Esta parte de la red (MZ) al igual que los otros segmentos de la red cuentan con un Firewall Nokia IP330, 64 Mb de memoria RAM y 30Gb de disco duro, maneja tres interfaces: WAN, MZ y DMZ estas interfaces están configuradas a una velocidad de 10 Mbps (Ver figura 2.1).

En la interfaz MZ que maneja el firewall antes descrito esta conectado un Switch: SmartStack Fast Ethernet con dirección Gateway 172.16.1.50 y dirección IP 172.16.5.240, a este switch llega también el enlace al Plantel Anexo Bachillerato con dirección IP 172.16.3.254; por otra parte, también están conectados los demás switches que se utilizan para el enlace de las comunicaciones, así como, los servidores que a continuación se describen (Ver figura 2.1):

- Server VOZ, IP 172.16.1.94, mascara de subred 255.255.0.0 y utiliza Windows 2000 Professional.
- Server Base de Datos, IP 172.16.1.1, mascara de subred 255.255.0.0, HP-UX 11.0.
- Server Aplicaciones, IP 172.16.2.241, mascara de subred 255.255.0.0, Windows 2000 Server.

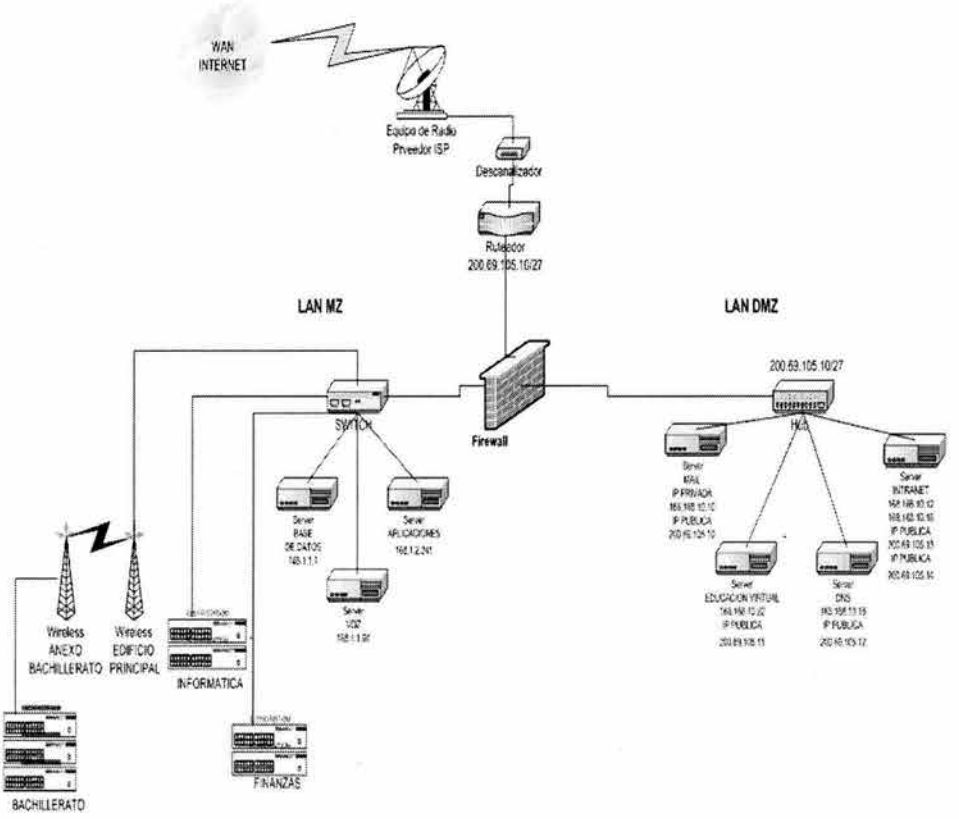


Figura 2.1: Red Anterior de la Institución.

Podemos observar que la comunicación entre los equipos no es eficiente ya que los equipos conectados en la red DMZ cuentan con tarjetas de red de 100Mbps, sin embargo, al llegar al Hub, la salida de éste, es solo a 10Mbps, esto hace que estemos restringiendo la salida a mayor velocidad de los dispositivos.

El siguiente problema que observamos fue el crecimiento de las necesidades de Institución, ya que la demanda de utilizar el canal de comunicación se fue incrementando, la red MZ tenia mayor demanda en las aplicaciones de bases de datos, por otra parte, la red DMZ sufría del mismo problema, ya que la demanda de la Intranet se fue incrementando debido a nuevas aplicaciones como lo son:

- Historial Académico
- Horarios de materias Inscritas
- Historial Financiero

Estas aplicaciones como cualquier otra Institución Educativa centralizan la información en un servidor de bases de datos, cualquier petición que se haga a los servidores colocados en la parte de la red expuesta hacia Internet (DMZ), necesariamente tendrá que ser permitida por el firewall.

El incremento en la matrícula de alumnos también se vio reflejada en la red, ya que se tuvieron que adquirir nuevos equipos de computo, tanto para personal administrativo como para personal académico, originando así, más tráfico en la red debido a las peticiones que se realizaban en la Intranet, mencionadas anteriormente, así como, plataforma académica en Web y correo en apoyo de tareas (mail).

Este crecimiento de personal (académico y administrativo) y de equipo de cómputo originó problemas en la red. Debido a las peticiones que se hacían sobre ella, el canal de comunicación cada vez se fue haciendo mas lento, la velocidad de transmisión y recepción de las aplicaciones no tenia el tiempo de respuesta adecuado, aunado a esto teníamos una red plana donde el dominio de broadcast era escuchado por todos los equipos originando así más tráfico y el número de colisiones iba en aumento.

La confiabilidad tanto en las aplicaciones, en la información, el crecimiento sin una planeación de administración adecuada, la organización de la red y la seguridad (la manera en que se iba conectando al ir creciendo la red) fueron los principales problemas que originaron el planteamiento para rediseñar la red y crear una red segmentada, con esto lograríamos una red más segura y con una velocidad mayor en el canal de comunicación.

2.1.2 Análisis del comportamiento de la Red

En esta parte se mencionará la importancia de realizar una administración preventiva, que es el monitoreo y análisis permanente de las condiciones de la red y que esto nos servirá para saber si nuestra red necesita ser segmentada. La mayoría de las herramientas de administración pueden monitorear las estadísticas de la red y permite ver el comportamiento del tráfico por medio de estas, pero el administrador debe realizar un trabajo bastante laborioso de análisis de estos datos para entender lo que significan.

Podemos mencionar diferentes paquetes comerciales que ayudan al administrador a realizar este proceso de análisis entre los que se encuentran Sniffer de Network´s Associates, Netasyst WLX Versión 1.0.003, Ether peek NX de Wild packets entre otros. Específicamente, el producto Sniffer de Network´s Associates (Sniffer Technollogies), utiliza un modulo el cual conjuntamente con un sistema experto y basado en capacidades analíticas proporciona un monitoreo distribuido en tiempo real, de salud de la red a través, de toda la infraestructura de la misma. El resultado de este monitoreo es una lista que se actualiza automáticamente, con prioridades asignadas a los problemas potenciales de la red. Así, los administradores de la red podrán ver los problemas antes de que se desarrollen. Asimismo, el software presenta un análisis detallado de las causas del problema, permitiendo al administrador de la red prevenir una degradación del servicio o puntos de falla de la red.

2.1.3 Analizadores y Monitores de la red

Entre las Herramientas que auxilian en la administración de la red, encontramos analizadores de la Red, que básicamente consisten en obtener la información que viaja en la red, y mostrarla al administrador. Una fuerte limitación de estas herramientas es que la información se muestra paquete a paquete por lo que el administrador necesita de antemano saber lo que esta buscando, de otra manera esta herramienta es inútil.

En el mercado existen diferentes Analizadores de la red, pero uno de los más importantes es Sniffer pues nos permite analizar la red en las diferentes capas de la misma, auxiliándose de un hardware especial con el cual es posible ver la información a un nivel más bajo (Modelo de referencia OSI), esto solo un experto en el área es capaz de analizarlo. Dentro de las muchas herramientas que contiene sniffer, cabe resaltar a un sistema experto, el cual nos muestra algunos síntomas de la red, es decir una vez que se analizo la red, el producto es capaz de decirnos algunos problemas de red, por ejemplo un tiempo de respuesta muy alto. Este tiempo de respuesta fue una de las causas en la que se puso más atención en diferentes puntos de nuestra red LAN como se muestra en la figura 2.2.

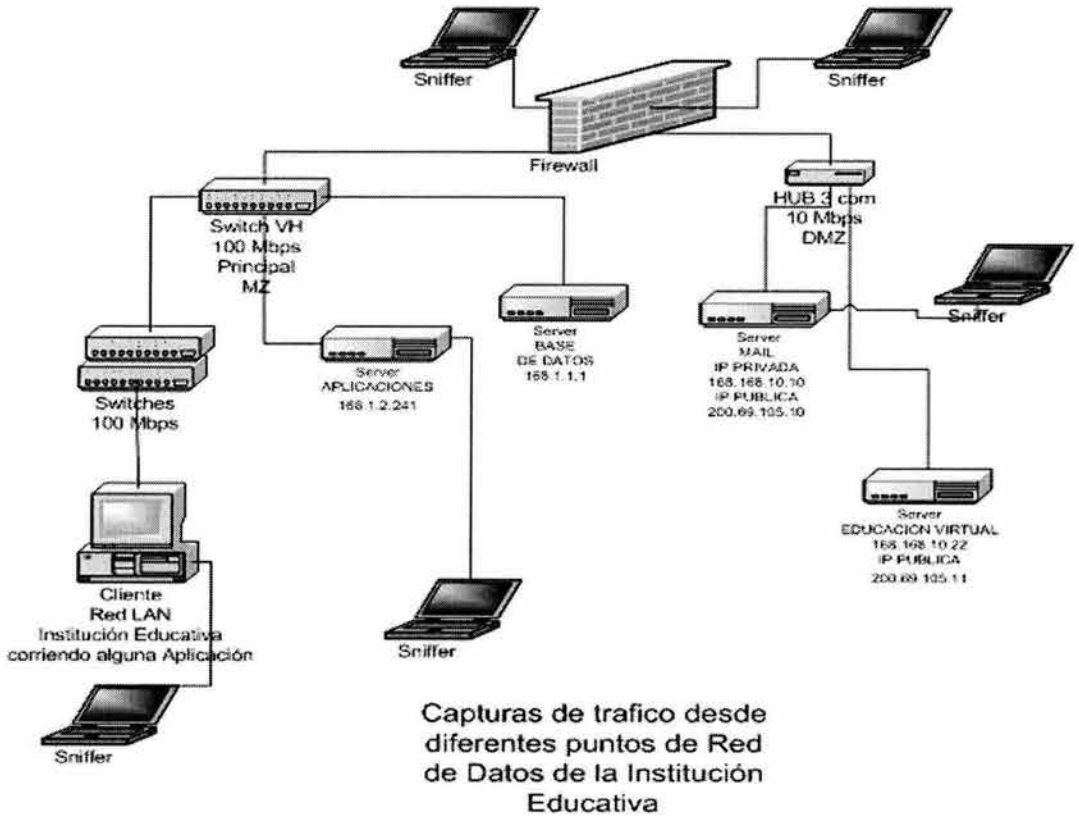


Figura 2.2: Capturas de tráfico desde diferentes puntos de la Red de la Institución.

A continuación presentamos las graficas que nos arrojo el sniffer de Network's Associates, colocado en el equipo frontera, es decir, analizamos el trafico que pasa por el firewall, para poder observar el comportamiento de la red.

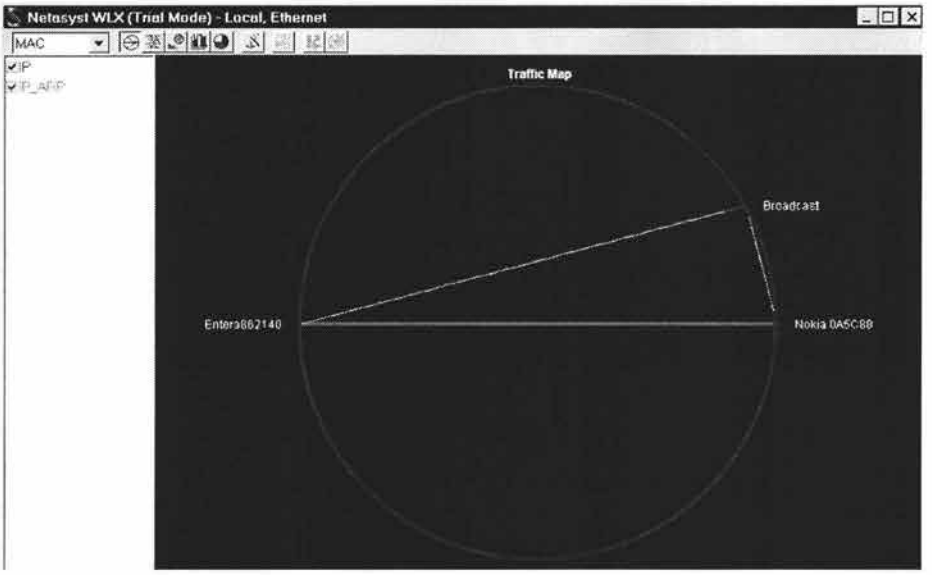


Figura 2.3: Tráfico de MAC.

En la figura 2.3 podemos observar el tráfico de broadcast que circula desde un switch vh hacia el firewall, y el tráfico que éste también genera.

En la figura 2.4 observamos el tráfico IP que generan los diferentes equipos de la red, aquí observamos que teniendo una red "plana", un equipo puede comunicarse con todos los demás equipos sin ningún orden esto a la larga provoca colisiones que pueden disminuir el performance de la red.

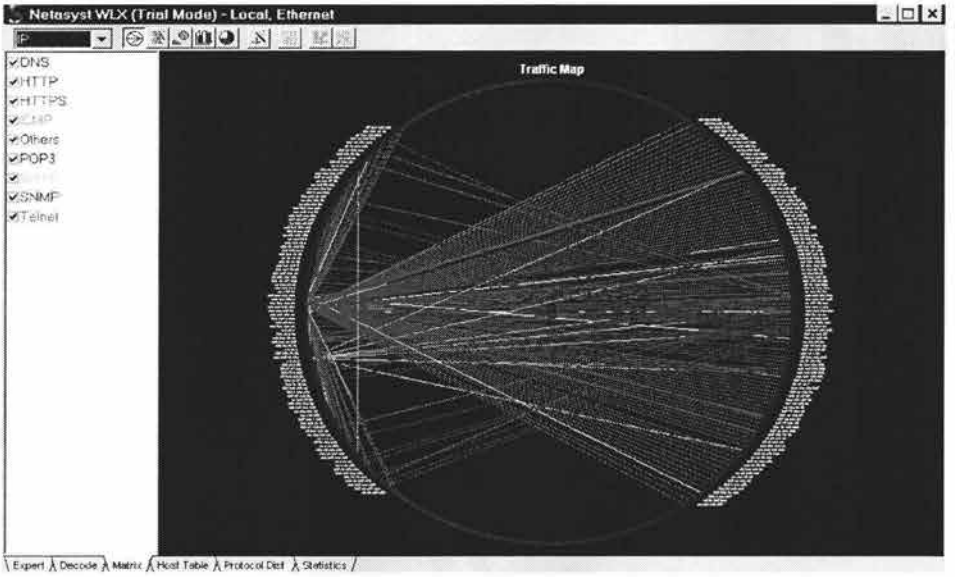


Figura 2.4: Tráfico IP.

Con el análisis de estas capturas y también con el análisis realizado en el diseño de la red (parte MZ), se decidió optimizar la red y la solución que tomamos fue hacer una red segmentada y así tener una red más eficiente en cuanto a comunicación de datos, tener el menor tráfico posible y disminuir las colisiones que se producen en la red.

2.2 Planificación de la nueva red

El desarrollo tecnológico plantea el flujo de la información más allá de las instalaciones físicas, pero en ellas es donde se deben tomar las medidas necesarias para garantizar la integridad de los datos y evitar que lleguen a manos de extraños con intenciones de dañar a la empresa.

La inseguridad que existe al contar con redes abiertas bloquea la confianza de transmitir información relevante para la industria. Los mensajes y datos pueden ser interceptados e incluso modificados y la información puede llegar a personas no autorizadas con la posibilidad siempre latente de que haga mal uso de ella.

Definitivamente, el tema de la seguridad de la información se ha convertido en uno de los aspectos más conflictivos en el uso de tecnologías de información. De hecho, la falta de una política global de seguridad dificulta el desarrollo de algunas de las nuevas tecnologías.

Cada vez son más las empresas que trabajan en el desarrollo de nuevas tecnologías de redes y telecomunicaciones debido a que proveen canales efectivos, fáciles de utilizar y de bajo costo para la transmisión masiva de información que hoy en día se refleja como una realidad conocida por propios y extraños como Internet.

Sin embargo, la inseguridad que existe al contar con redes abiertas bloquea la confianza de transmitir información relevante para la industria.

Es claro tener presente que las necesidades de crecimiento y de seguridad de una red trae muchos beneficios, es necesario tener claro también las exigencias de reconocer tres grupos de controles con los que se debe contar a fin de establecer un programa integral.

Controles operacionales y de producción. Aquellos que son ejecutados por el personal para mejorar la operación de un proceso o un sistema o bien un conjunto de ellos. Estos surgen por las necesidades de crecimiento de la misma empresa.

El aumento de equipos que nos ayudaran al desarrollo tecnológico al cual queremos llegar, lleva también el aumento de una mayor administración y supervisión de estos para que el control técnico se encuentre también bajo control.

Control Técnico. Se refiere a los que son ejecutados por los sistemas de cómputo y dependen de un adecuado funcionamiento de los mismos. Su operación siempre requiere de consideraciones funcionales y deben ser consistentes con los procesos productivos establecidos. Son de vital

importancia los Métodos y procedimientos que se tocaran mas adelante para tener un Control administrativo.

Control Administrativo. Técnicas enfocadas a la administración de los programas de seguridad e incremento de tráfico en la red y al manejo de los riesgos que esto implica para la empresa, para tener una visión clara del crecimiento que puede tener su red a un corto, mediano y largo plazo.

Hace algunos años era impredecible la evolución que las comunicaciones, en el mundo de la informática, iban a tener: no se podía prever que fuese necesaria la interconexión ya no sólo de varias computadoras sino de cientos de ellas. No basta con tener las computadoras en una sala conectadas, es necesario conectarlas a su vez con las computadoras del resto de las salas de una empresa, y con el resto de las sucursales de una empresa situadas en distintos puntos geográficos.

La interconexión de redes permite, si se puede decir así, ampliar el tamaño de una Intranet. Sin embargo, el término interconexión se utiliza para unir redes independientes, no para ampliar el tamaño de una.

El número de computadoras que componen una Intranet es limitado, depende de la topología elegida, (recuérdese que en la topología se define el cable a utilizar) aunque si lo único que se quisiera fuera sobrepasar el número de computadoras conectadas, podría pensarse en simplemente segmentar la Intranet. Sin embargo existen otros factores a tener en cuenta.

Cuando se elige la topología que va a tener una Intranet se tienen en cuenta factores, como son la densidad de tráfico que ésta debe soportar de manera habitual, el tipo de aplicaciones que van a instalarse sobre ella, la forma de trabajo que debe gestionar, etc.; esto debe hacer pensar en que, uno de los motivos por el que se crean diferentes topologías es por tanto el uso que se le va a dar a la Intranet. De aquí se puede deducir que en una misma empresa puede hacerse necesaria no la instalación de una única Intranet, aunque sea segmentada, sino la implantación de redes independientes, con topologías diferentes e incluso arquitecturas diferentes y que estén interconectadas.

Habitualmente la selección del tipo y los elementos físicos de una Intranet, se ajusta a las necesidades que se tiene; por este motivo pueden encontrarse dentro de un mismo edificio, varias intranets con diferentes topologías, y con el tiempo pueden surgir la necesidad de interconectarlas.

2.3 Propuesta de plan de acción

Se puede ver que por diferentes razones se hace necesaria tanto la segmentación como la interconexión de intranets, y que ambos conceptos a pesar de llevar a un punto en común, parte de necesidades distintas.

La tabla 2.1 refleja a grandes rasgos diferentes casos en los que se plantea la necesidad de segmentar y/o interconectar intranets, dando la opción más idónea para cada uno de los casos planteados.

NECESIDAD	SOLUCIÓN
Debido a la necesidad de manejo de aplicaciones que producen una carga importante de información aumenta el tráfico en la red; esto lleva a que baje el rendimiento de la misma.	Dividir la red actual en varios segmentos: segmentar la red.
Se tiene que ampliar el número de puestos que forman la Intranet, pero se necesita mantener el rendimiento de la red.	Crear un nuevo segmento de red en el que se pondrán los nuevos puestos e incluso al que se pueden mover puestos, que por disposición física pueda ser conveniente que pertenezcan al nuevo segmento creado en la misma.
Se tiene la necesidad de unir dos intranets exactamente iguales en la empresa.	Se puede optar por definir una de ellas como un segmento de la otra y unirlas de esta forma; o bien, interconectar las dos intranets con un dispositivo de nivel bajo.
Se tiene la necesidad de unir dos o más redes con diferentes topologías pero trabajando con los mismos protocolos de comunicaciones.	Es necesario la interconexión de ambas redes a través de dispositivos de nivel medio
Se tiene la necesidad de unir dos o más redes totalmente diferentes, es decir, de arquitecturas diferentes.	Es necesaria la interconexión de ambas redes a través de dispositivos de nivel alto.

Tabla 2.1: Necesidades de interconectividad y su solución.

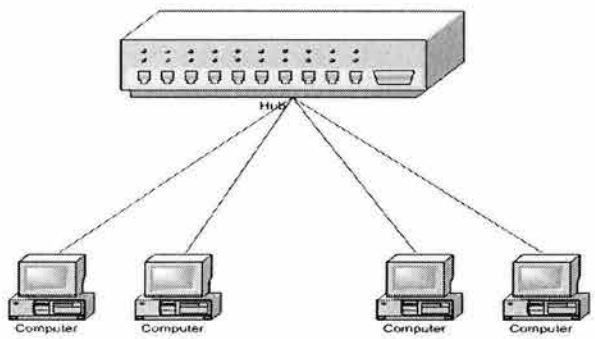


Figura 2.5: Red inicial con topología lógica en bus y física en estrella a través de un hub.

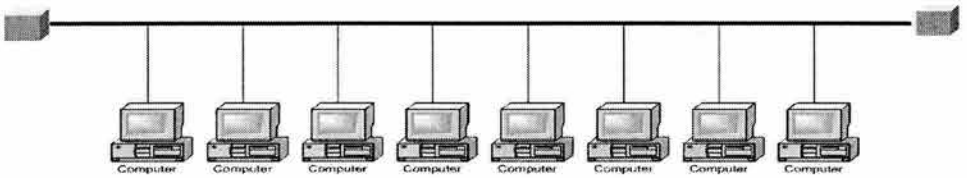


Figura 2.6: Si se necesita ampliar la red, una solución puede ser esta, pero no mejora el rendimiento de la red porque lógicamente está vista como una única red.

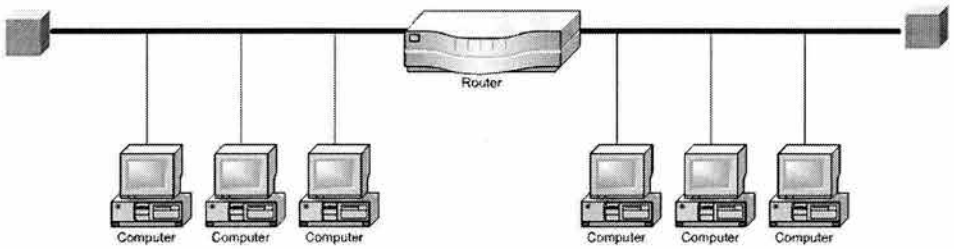


Figura 2.7: Una solución para ampliar la red puede ser esta, y en esta situación mejora el rendimiento de la red.

2.3.1 Concepto de segmento

Un segmento es un bus lineal al que están conectadas varias estaciones y que termina en los extremos. Las características son:

- Cuando se tiene una red grande se divide en trozos, llamados segmentos a cada uno de ellos.
- Para interconectar varios segmentos se utilizan bridges o routers
- El rendimiento de una red aumenta al dividirla en segmentos.
- A cada segmento junto a las estaciones a él conectadas se las llama subred.
- Cada segmento maneja su propio ancho de banda.
- Cada segmento tiene su propio default gateway, esto para que el tráfico circulante solo corresponda al segmento correspondiente.

2.3.2 Segmentación: sus necesidades

Segmentar una Intranet consiste en dividirla en subredes para así poder aumentar el número de computadoras conectadas a ella y/o el rendimiento de la misma.

Cuando se segmenta una Intranet, lo que se esta haciendo es crear subredes pequeñas que, por decirlo de alguna manera, se autogestionan, de forma que la comunicación entre segmentos se realiza cuando es necesario, es decir, cuando un nodo de un segmento quiere comunicarse con un nodo del otro segmento; mientras tanto cada segmento de la Intranet está trabajando de forma independiente por lo que en una misma Intranet se

están produciendo varias comunicaciones de forma simultánea; evidentemente esto mejora el rendimiento de la Intranet.
La tabla 2.2 refleja las longitudes máximas de los segmentos dependiendo de las diferentes topologías de red [González Fernández, 1998].

TOPOLOGÍAS	LONGITUD
Ethernet gruesa	500 metros
Ethernet fina	185 metros
Ethernet de par trenzado	100 metros
Ethernet de fibra óptica	2.000 metros
Token-Ring de par trenzado	100 metros

Tabla 2.2: Topologías utilizadas y la longitud máxima de segmentación.

El dispositivo que se utiliza para segmentar una red debe ser inteligente ya que debe ser capaz de decidir hacia qué segmento debe enviar la información llegado a él: si hacia el mismo segmento desde el que la recibió o hacia otro segmento diferente.

Abstrayéndose de algunos detalles, es fácil pensar que segmentar una Intranet, ya que se habla de subredes, es como interconectar intranets diferentes. Sin embargo, cuando se habla de segmentar se hace referencia a una única Intranet; esto lleva asociado lo siguiente: una única topología, un único tipo de protocolo de comunicaciones, un único entorno de trabajo; cuando se habla de interconectar intranets, en la mayoría de los casos, las intranets tienen como mínimo topologías diferentes. No obstante, sí debe destacarse que los dispositivos que se utilizan para segmentar redes coinciden con algunos de los dispositivos que son utilizados para interconectar redes diferentes.

Dependiendo del tipo de protocolos que se utilicen en la Intranet segmentada, así como, de dispositivos que se utilicen para realizar esta segmentación puede hacerse necesario o no el atribuir a cada segmento una dirección de red diferente. Cuando se trabaja con protocolos TCP/IP esto no es necesario, basta con que cada estación tenga su propia dirección IP, y que no aparezcan dos estaciones con la misma dirección, independientemente de si están o no en el mismo segmento de la Intranet.

Existen diferentes motivos por los que se puede hacer necesaria la segmentación de una Intranet, como pueden ser:

- **Necesidad de sobrepasar el número de nodos que la topología permite.** La limitación del número de nodos en una Intranet vienen impuesta por varios factores, como son el método de acceso al medio que se utiliza, el tipo de cable, el ancho de banda, etc.
- **Mejorar el rendimiento de una Intranet en la que ha aumentado el tráfico.** En ocasiones, una Intranet que inicialmente funciona bien, con un tiempo de repuesta aceptable, empieza a perder prestaciones; el motivo es claro: de forma paulatina se ha ido

incrementando el número de comunicaciones que la Intranet debe gestionar, por diferentes motivos como que los usuarios comienzan a conocer la red y la aprovechan más, o que se han ido instalando más aplicaciones.

Existen diferentes formas de atacar este problema: Una de ellas, la más drástica es cambiar algún elemento físico de la Intranet: por ejemplo sustituir el cable que implementa la Intranet por uno que pueda soportar velocidades mayores, cambiar las tarjetas de red por otras más rápidas, e incluso cambiar la topología empleada. Una solución menos concluyente consiste en segmentar la Intranet. Dividirla estratégicamente en dos subredes, reduciendo de esta forma el tráfico en cada una de ellas.

La interconexión de intranets se puede establecer a varios niveles: desde el nivel físico, a través de un dispositivo llamado hub (concentrador) hasta niveles más altos (niveles del modelo OSI) a través de dispositivos como un puente (Bridge) o un router (encaminador).

La tabla 2.3 muestra el nivel en el que trabajan los diferentes dispositivos.

DISPOSITIVO	NIVEL
repetidor	físico
concentrador	físico
puente	enlace
Router	red

Tabla 2.3: Dispositivos de interconexión y su referencia con el modelo OSI.

Para la segmentación de intranets, y teniendo en cuenta que uno de los motivos por el que se realiza esta operación es mejorar el rendimiento de la red, es necesario emplear dispositivos inteligentes, como pueden ser un router o un puente.

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz.

Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host. Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 (modelo de referencia OSI) de dirección MAC destino, los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la

totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.
Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionarían rápidamente con tráfico y colisiones y virtualmente no ofrecerían ningún ancho de banda.

Al dividir redes de gran tamaño en unidades autónomas, los puentes y los switches ofrecen varias ventajas. Un puente, o switch, reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico. Los puentes y los switches amplían la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

Aunque los puentes y los switches comparten los atributos más importantes, todavía existen varias diferencias entre ellos. Los switches son significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

De forma genérica existen varias maneras de ampliar las intranets:

- Hubs: Para unir hosts dentro de una red.
- Repetidores: conexión a nivel físico, en el mismo segmento.
- Bridges: Conexión a nivel de enlace entre dos segmentos (iguales o distintos).
- Routers: Conexión a nivel de red.
- Gateways: Conexión a nivel de presentación, entre dos redes distintas.

Es por ello que en la planificación de la nueva red para esta Institución decidimos hacer de la red original una red segmentada, con esto lograremos una mejor comunicación entre los dispositivos, el rendimiento en cuanto a la velocidad de transmisión de datos será mejor, por último la seguridad quedará mejor implementada con la segmentación.

2.4 Diseño de la nueva red

Derivado del diagnostico efectuado se propone el desarrollo de un esquema de comunicación de datos ruteada, por medio del cual se pueda realizar el intercambio de servicios entre el edificio principal, edificio Anexo Bachillerato y por último el edificio Anexo Posgrado, además de realizar en un futuro cercano, filtrado de contenido y control absoluto de usuarios.

De acuerdo a las necesidades en materia de transferencia de datos, en cada punto requerido de los closets de comunicaciones en los edificios de la

Institución se estructurará una red de datos segmentada y apoyada por redes virtuales (VLAN's).
A continuación describiremos los cambios que se realizaron, para empezar a dar forma al diseño de la nueva red.

Con la finalidad de integrar una red libre de broadcast y tráfico indeseado en todos los equipos y closets, se contemplo instalar un Switch Ruteador marca Enterasys Networks modelo SSR-2000-B-128, o X-Pedition 2000, (se decidió utilizar este equipo por cuestiones económicas y por las principales necesidades que presenta ahora y para el progresivo incremento de estas necesidades de la Institución, lo que nos arrojo esta evaluación se muestra en el Apéndice A), el cual controlara toda la segmentación de los IDF o closets de comunicaciones, de los edificios remotos como los son Anexo Bachillerato y Anexo Posgrado (Ver figura 2.8).

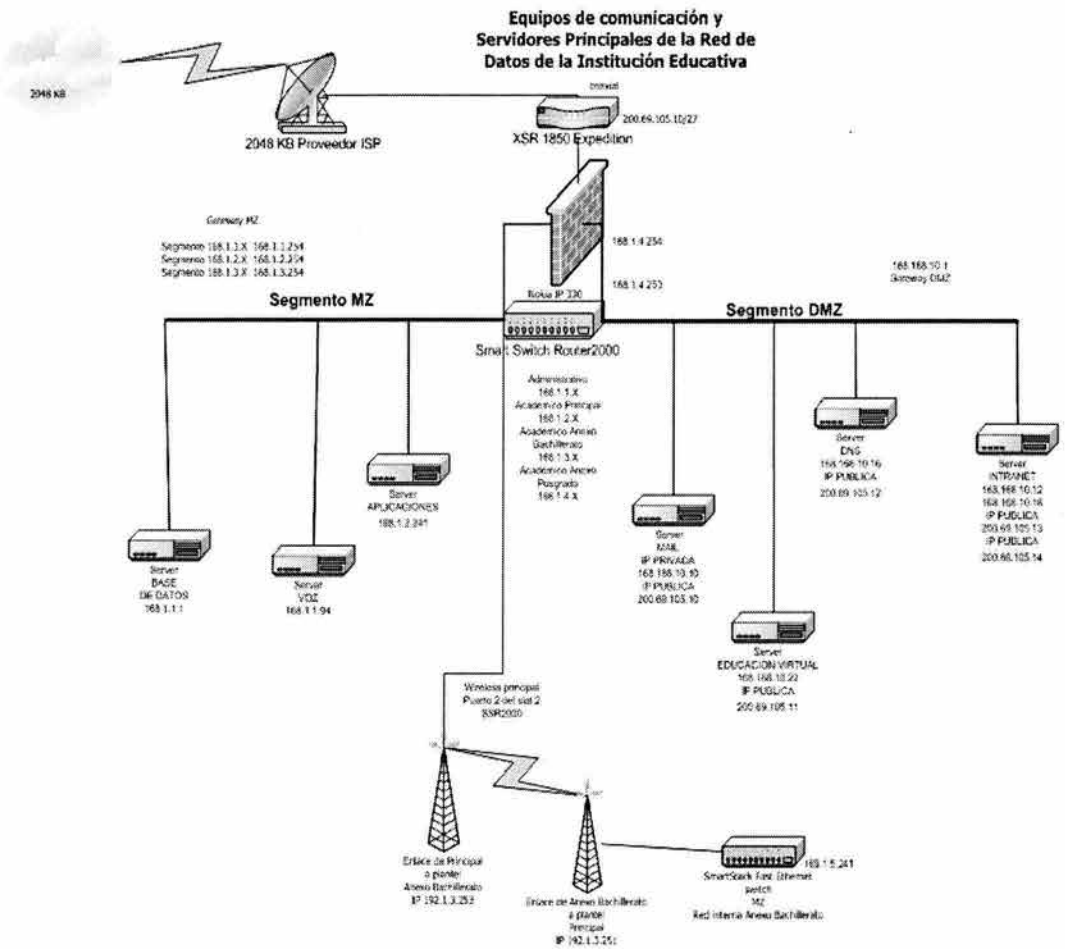


Figura 2.8: Red con el nuevo ruteador.

El Switch Ruteador cuenta con 24 puertos 10/100 BaseTx (Ver figura 2.9).

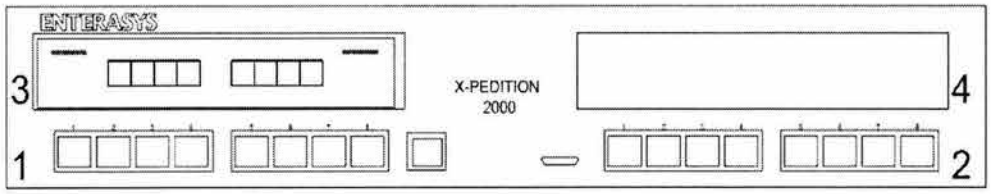


Figura 2.9: Panel frontal del equipo SSR-2B-128 o X-PEDITION 2000

2.4.1 Switch secundario de distribución DMZ VH-2402SM

Con la finalidad de contar con la conectividad de equipos servidores de servicios de la Extranet o Internet, se agregó un Switch marca Enterasys Networks modelo VH-2402SM de 24 puertos 10/100 BaseTx, en la barra del Firewall DMZ, (El Apéndice A muestra el comparativo que se realizo para decidir porque utilizar este equipo tomando en cuenta precio, rentabilidad y necesidades de la Institución Educativa), el cual permitirá la comunicación de la granja de servidores del Site principal de computo (Ver figura 2.10 y 2.11).

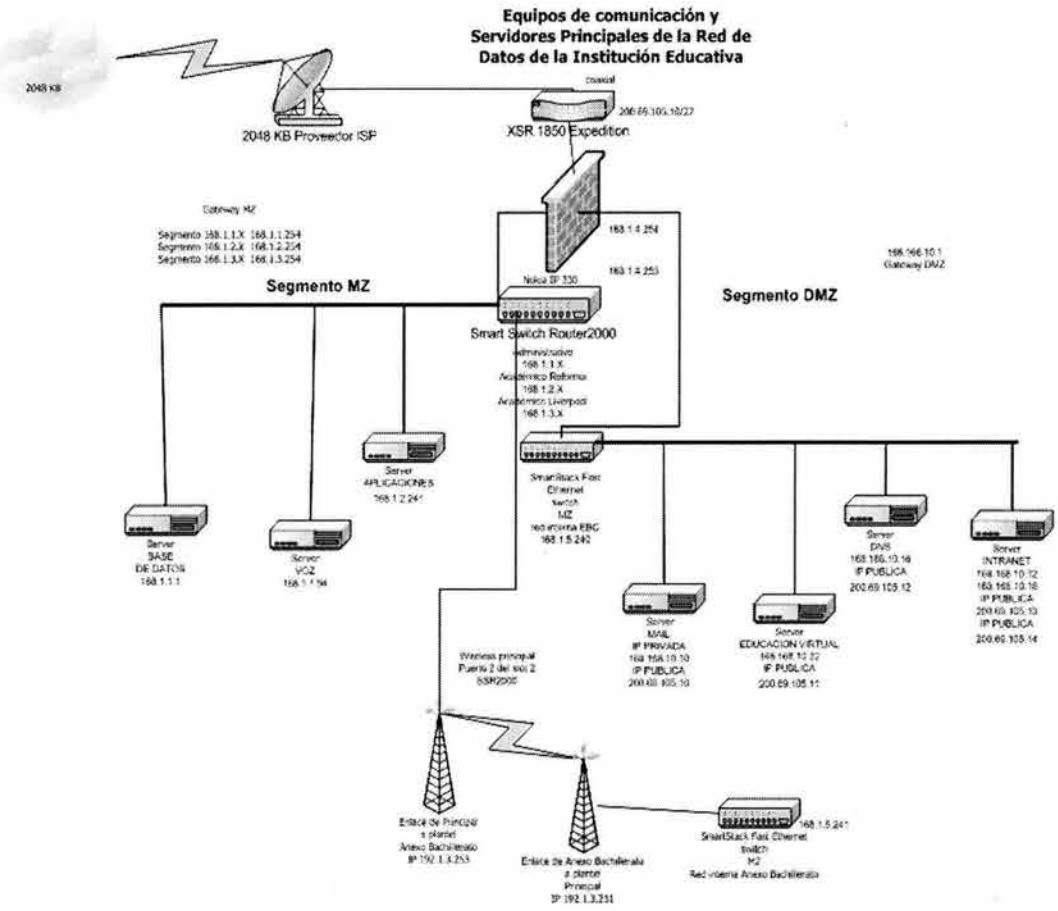


Figura 2.10: Diseño con el Switch VH-2402SM.

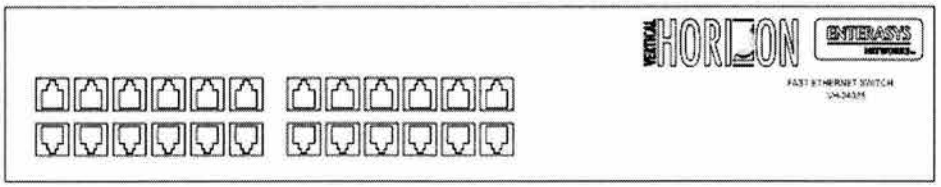


Figura 2.11: Panel frontal del equipo VH-2402SM.

2.4.2 Equipos de enlace de microondas de 11 Mbps.

Con la finalidad de mantener comunicado a los edificios de la Institución, se adecuó la solución existente, agregando un equipo RoamAbout marca Enterasys Networks modelo R2 en el edificio Principal, el cual cuenta con un segundo modulo Mezanine, éste a su vez, enlazará a los edificios de Anexo Bachillerato y Anexo Posgrado (Ver figura 2.12).

La solución para intercomunicar la red de computo entre los edificios Anexo Bachillerato, Anexo Posgrado hacia el edificio Principal, es un enlace de 11 Mbps Bi-direccional, utilizando tecnología 802.11b, el cual podrá comunicar las redes de datos en el ámbito privado y permitiendo la segmentación de las redes existentes en ambos inmuebles y manejar las VLAN's que se irán creando para éstos, y que serán controladas por el Switch Ruteador Central "Core" (Ver figura 2.12).

Vamos a describir un poco las características de las tecnologías 802.11a y 802.11b para justificar el porque utilizamos la tecnología 802.11b para esta optimización.

Las tecnologías 802.11a y 802.11b definen cada una capa física diferente. Los radios 802.11b transmiten a 2.4 GHz y envían datos a tasas tan altas como 11Mbps usando modulación DSSS (Espectro Disperso de Secuencia Directa); mientras que los radios 802.11a transmiten a 5 GHz y envían datos a tasas de hasta 54 Mbps usando OFDM (Orthogonal Frequency Division Multiplexing o en español Multiplexación de División de Frecuencia Ortogonal).

Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a, sino en las 802.11g, en comunicaciones de alta velocidad por vía telefónica como las ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia.

Claro que el desempeño superior de 802.11a ofrece un excelente soporte para aplicaciones que requieren un gran ancho de banda, pero la frecuencia de operación más alta se traduce en un rango de alcance bastante más corto. En la vida real se pueden ver radios 802.11a enviando 54Mbps con distancia de cerca de 20 metros, lo cual es mucho menos que los 100 metros que se obtienen en promedio con sistemas 802.11b equivalentes. En cuanto a los access points, se necesita un número mucho mayor de éstos funcionando con la tecnología 802.11a para proporcionar cobertura de radiofrecuencia a un local, especialmente si es uno grande.

802.11b es la tecnología preponderante en este momento entre los fabricantes de dispositivos de identificación automática para ser utilizada en equipos como terminales portátiles. Las marcas más importantes han apostado por esta tecnología debido a su gran confiabilidad y apropiado desempeño en la gran mayoría de aplicaciones reales.

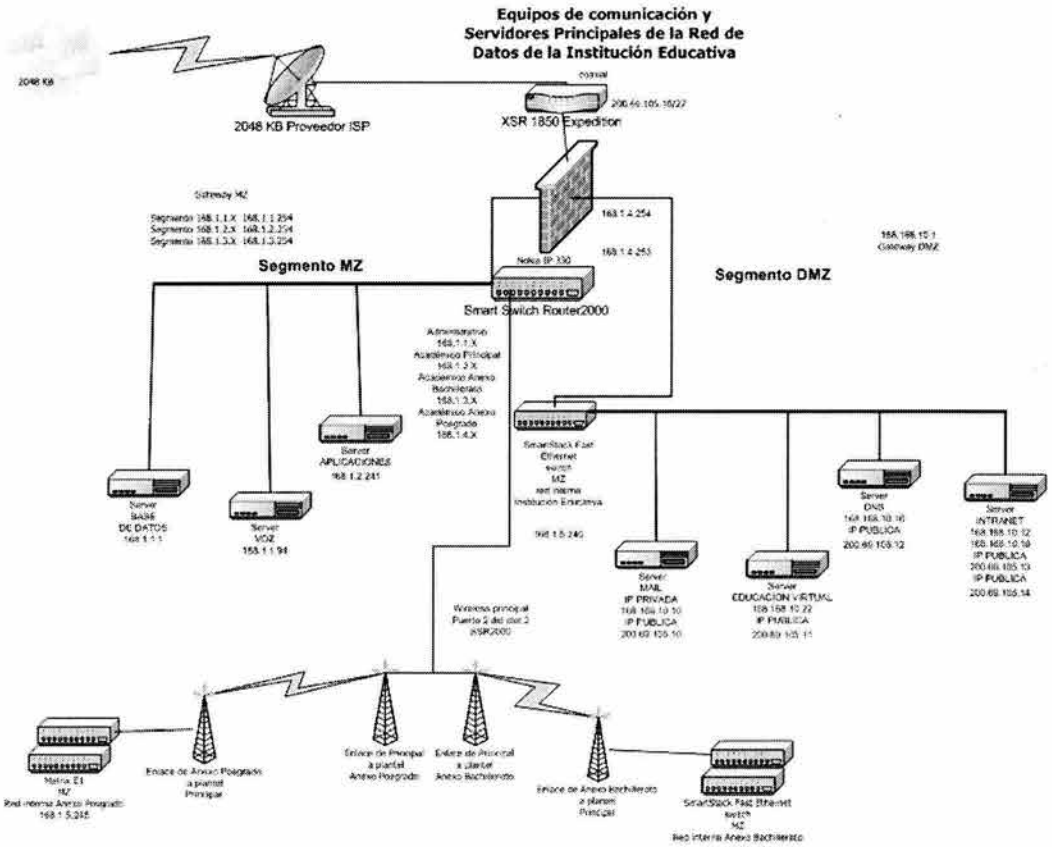


Figura 2.12: Red Institución Educativa con equipos de enlace de microondas de 11 Mbps.

2.4.3 Equipo de seguridad Firewall IP330

Se contemplo actualizar el equipo marca Nokia modelo IP330 (la Institución Educativa ya contaba con este equipo de seguridad, para esta optimización), en la parte del software Checkpoint, así como, de la memoria, con esto pretendemos manejar de manera más eficiente los accesos hacia Internet o la Intranet de la Institución, todo esto con la finalidad de optimizar la carga de procesos de las consultas.

Esta solución consta de un Firewall IP330 Nokia y una consola de administración la cual contendrá la última versión del FG Checkpoint (Ver figura 2.13).

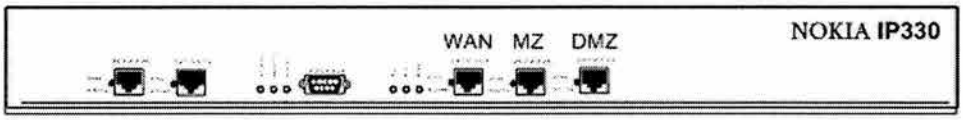


Figura 2.13: Vista frontal del Firewall Nokia IP330.

La figura 2.14 muestra el diseño final de la red.

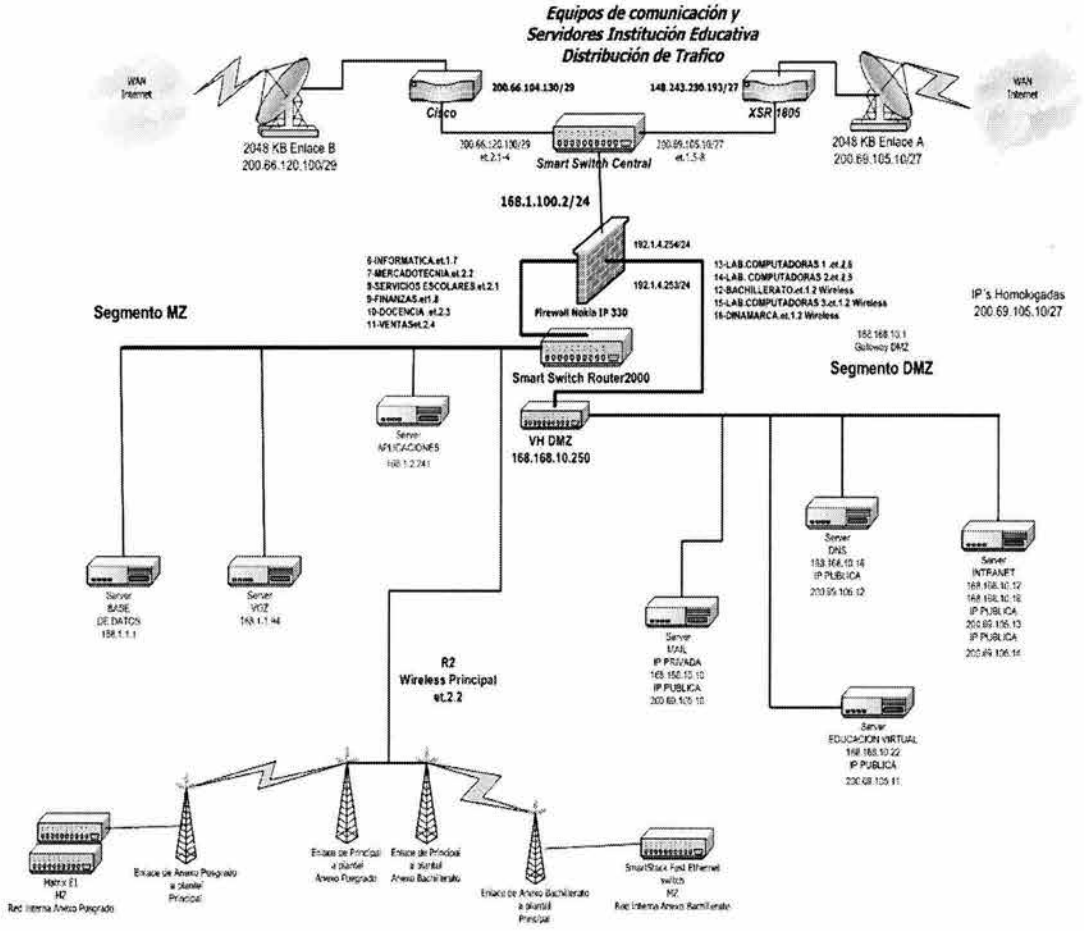


Figura 2.14: Diseño final.

2.5 Posibles fallas en el diseño

Una falla que observamos al diseñar esta nueva red, radicaba en la necesidad de implementar un servidor WINS para los equipos que aun cuentan con Windows 95 y que tenían el problema de resolución de nombres.

El Servicio de Nombres de Internet de Windows, o "Windows Internet Name Service" (WINS) es la implementación de Microsoft de un servidor de nombres NetBIOS (NBNS). Como tal, WINS hereda muchas de las características de NetBIOS. Primero, WINS funciona con nombres simples o llanos; sólo se pueden tener máquinas llamadas Pedro o grupos de trabajo como CANADA o USA.

En suma, WINS es dinámico: cuando un cliente aparece en la red, se envía su nombre de máquina, su dirección y su grupo de trabajo al servidor WINS local. Este servidor WINS retendrá la información mientras el cliente periódicamente refresque su registro WINS, lo cual indica que todavía está conectado a la red. Cabe mencionar que los servidores WINS no son específicos de un grupo de trabajo o dominio; pueden aparecer en cualquier lugar y servir a cualquiera.

El servidor WINS activo es conocido como el servidor WINS primario. También es posible instalar un servidor WINS secundario, el cual entrará en acción en el caso de que el primario falle o se vuelva inaccesible. Hay que hacer notar que no hay un proceso de elección para determinar qué máquina se convierte en servidor WINS primario o de seguridad, la elección de servidores WINS es estática. Tanto el servidor WINS primario como el de seguridad sincronizarán sus bases de datos de direcciones cada cierto período determinado de tiempo.

Normalmente la resolución de nombres en una red Microsoft Windows se realiza mediante el envío de paquetes de difusión. Por ejemplo en Windows 95, cuando se utiliza el protocolo Netbeui, se necesita obtener el nombre de todos los equipos registrados en la red, se envía una llamada de difusión (broadcast). A esta llamada responden todos los equipos configurados como examinadores de red. Este mecanismo permite a las diferentes computadoras de la red anunciarse sin necesidad de emplear servidores de nombres dedicados. Sin embargo, el uso de paquetes de difusión (broadcast) debe ser evitado por dos motivos fundamentales:

- Se consume un ancho de banda importante y obliga a todos los equipos a procesar paquetes broadcast.
- La presencia de gateways (routers) aíslan las diferentes subredes ya que los paquetes broadcast no se reenvían entre ellas. Para acceder a equipos remotos son necesarios mecanismos no basados en la difusión de paquetes. El modelo de capas TCP/IP compatible Netbios que usa tanto NT como el resto de sistemas de red de Microsoft trabaja normalmente en modo difusión para la resolución de nombres Windows. Los ruteadores incorporados en Windows trabajan examinando las peticiones de registro de los clientes que envían mediante difusión. Este mecanismo es sencillo pero utiliza difusión.

Desde NT 4.0 Server Microsoft introdujo un nuevo servicio: el Servidor de Nombres de Internet para Windows, conocido habitualmente como WINS. Este servicio no trabaja en modo difusión, sino que cuando un equipo desea registrar un nombre u obtener una lista de los nombres registrados en el

servidor, contacta utilizando el protocolo TCP con el servidor WINS directamente, sin utilizar difusión.

El servicio WINS se comporta de un modo parecido al servicio DNS, es decir, los clientes WINS solicitan al servidor WINS la dirección IP para cada nombre. El servidor de nombres WINS registra en su base de datos varios tipos de nombres:

- Nombres de equipos
- Nombres de grupos de trabajo
- Nombres de dominios
- Examinadores de red.
- Controladores primarios y de reserva del dominio
- Usuarios (utilizado por el servicio de mensajería)

Pero hay una diferencia fundamental entre el servicio WINS y el DNS. Los servidores WINS crean su base de datos dinámicamente, utilizando la información que les envían los clientes WINS.

El servicio WINS tiene grandes ventajas:

1. Se instala en minutos y prácticamente no necesita configuración y administración.
2. En una misma subred pueden existir múltiples servidores WINS, de manera que en caso de fallo de uno de ellos la red siga trabajando.
3. Las bases de datos se pueden duplicar automáticamente entre servidores, lo que facilita la administración de los servidores WINS.

2.6 Ventajas y desventajas del nuevo diseño

Es evidente que hay muchas soluciones para optimizar una red y cada solución tendrá defensores y detractores y que cada uno de ellos argumenta su posición según determinadas características de la solución que se haya determinado tomar. A continuación presentaremos las principales desventajas (Ver tabla 2.4) y ventajas (Ver tabla 2.5) argumentadas en cada caso.

DESVENTAJAS	
Servidor WINS	Tuvimos que utilizar un nuevo servidor para este servicio.
Switch-Ruteador	Para que la comunicación entre las VLAN's sea eficiente, se tuvo que adquirir nuevo equipo, es decir, un gasto económico para la empresa.

Tabla 2.4: Desventajas de optimizar una red utilizando la segmentación.

VENTAJAS	
Disminución del dominio de colisión	Cuando utilizamos un switch podemos separar los dominios de colisión.
Disminución del dominio de broadcast	Al utilizar VLAN's el dominio de broadcast es independiente para cada VLAN.
Velocidad estándar de los equipos de comunicación.	Si utilizamos VLAN's, éstas solo corren sobre fast ethernet es decir a una velocidad de 100 Mbps. Además cada VLAN maneja su propio ancho de banda.
Reducción de la carga de la red.	La independencia de cada segmento hace que la comunicación sea mucho más rápida.

Tabla 2.5: Ventajas de optimizar una red utilizando la segmentación.

Una vez hecho el análisis de cómo estaba conformada la red, tomando en cuenta las necesidades que presentaba la Institución y con los resultados obtenidos por las capturas del sniffer, la decisión final para resolver el problema planteado en la introducción de este trabajo de Tesis, fue hacer una red segmentada con la finalidad de brindar un servicio eficiente tanto en la comunicación de datos como en seguridad. En el siguiente capitulo nos enfocaremos a detallar los aspectos técnicos necesarios para llevar a cabo dicha segmentación, asimismo, hablaremos de cómo se fueron creando las redes virtuales (VLAN's) y las implicaciones que estas conllevan.

Capítulo 3

3.1 Reconfiguración de la red

Con el análisis realizado en el capitulo 2 de este trabajo de investigación comenzaremos a detallar los cambios realizados para la optimización de la red de la Institución.

Primeramente describiremos el procedimientos a seguir para realizar el cambio en los equipos frontera.

Uno de los principales objetivos en esta parte de reestructuración es el cambio de las interfaces de nuestro equipo frontera más critico que es el firewall, ya que hasta el momento de este cambio, estas interfases transmiten a 10 Mbps half-duplex y se pretende que trabajen a 100 Mbps full-duplex.

Con este cambio aumentara considerablemente la velocidad de transmisión y se evitaran colisiones y cuellos de botella en las interfases de este equipo frontera (Firewall), como son las interfaces del equipo que centraliza la red MZ, el equipo que centraliza la red DMZ y el equipo que da salida al tráfico interno hacia la red WAN.

Pasos a seguir para cambios en Interfases Firewall - WAN

1.-Cambio de velocidad en la interfase del Firewall al ruteador WAN

1.1.-Modificar configuración en el FW

Configuration

Interface Configuration

Interfaces

Physical Interface eth-s3p1

Link Speed

10 Mbps half-duplex por 100 Mbps full-duplex

2.- Cambio de velocidad en la interfase del ruteador WAN al Firewall

2.1.-Desde la interfaz fast-Ethernet 0:speed 100Mbps duplex full

Pasos a seguir para cambios en Interfaces Firewall – SSR (MDF de toda la LANMZ)

1.-Cambio de velocidad en la interfase del Firewall al SSR (MDF de toda la LANMZ)

1.1.-Modificar configuración en el FW

Configuration

Interface Configuration

Interfaces

Physical Interface eth-s4p1

Link Speed

10 Mbps half-duplex por 100 Mbps full-duplex

2.- Cambio de velocidad en la interfaz del SSR (MDF de toda la LANMZ) al Firewall

2.1.-Desde la interfaz fast-ethernet 0:speed 100Mbps duplex full

2.2- Desde modo configuración: port et.1.1 auto-negotiation off speed 100Mbps duplex full

Pasos a seguir para cambios en Interfaces Firewall – Switch VH (MDF de la LANDMZ)

1.-Cambio de velocidad en la interfaz del Firewall al Switch VH (MDF de la LANDMZ)

1.1.-Modificar configuración en el Firewall

Configuration

Interface Configuration

Interfaces

Physical Interface eth-s5p1

Link Speed

10 Mbps half-duplex por 100 Mbps full-duplex

2.- Cambio de velocidad en la interfaz del Switch VH (MDF de la LANDMZ) al Firewall

2.1.-Desde la interfaz fast-Ethernet 0:speed 100Mbps duplex full

2.2-Situado en el modulo y el puerto del VH que comunica ambos equipos:

Vertical Horizon Stack Local Management

Vertical Horizon Stack Local Management

Port Information : Unit 1 Port 1-12

Port	Type	Operational	Link InUse	FlowControl Duplex	Speed and InUse
1	10/100TX	YES	UP	NONE	100_FULL

Con estos puntos quedarían configuradas las interfaces frontera en los cuatro equipos involucrados, esto definitivamente ayudara al rendimiento de las transacciones entre servidores del segmento DMZ y clientes del segmento MZ, así como, clientes que vengan de la red WAN al segmento de DMZ.

3.1.1 Diseño DNS Split

En la figura 3.1 que se muestra a continuación, se pueden observar todos los componentes que intervienen de alguna manera en el diseño de la resolución de nombres. En esta misma imagen, se observan también en donde están conectados los servidores en donde se encuentran corriendo los servidores de DNS. Su configuración se explicará en la siguiente sección.

Podemos observar también en la figura 3.1 que todos los usuarios tanto de Internet como los internos, tienen que pasar a través del firewall para acceder a los servicios de la DMZ, sin embargo no lo hacen haciendo referencia a las mismas direcciones IP. En realidad, los usuarios que accesan de Internet lo hacen a través de direcciones del ISP (200.69.105.xx) y los usuarios internos los pueden acceder por sus direcciones reales (168.168.10.xx). Esto sucede precisamente porque el proceso de NAT está corriendo en el SSR Central que conecta a los ruteadores de frontera, los que tienen las conexiones seriales a los ISP's. Esta configuración se decidió conservar debido a que ese mismo switch/router es el encargado de realizar el balanceo de cargas hacia Internet.
En este punto ya podemos deducir que la configuración de DNS va a ser la conocida como DNS Split Horizon.

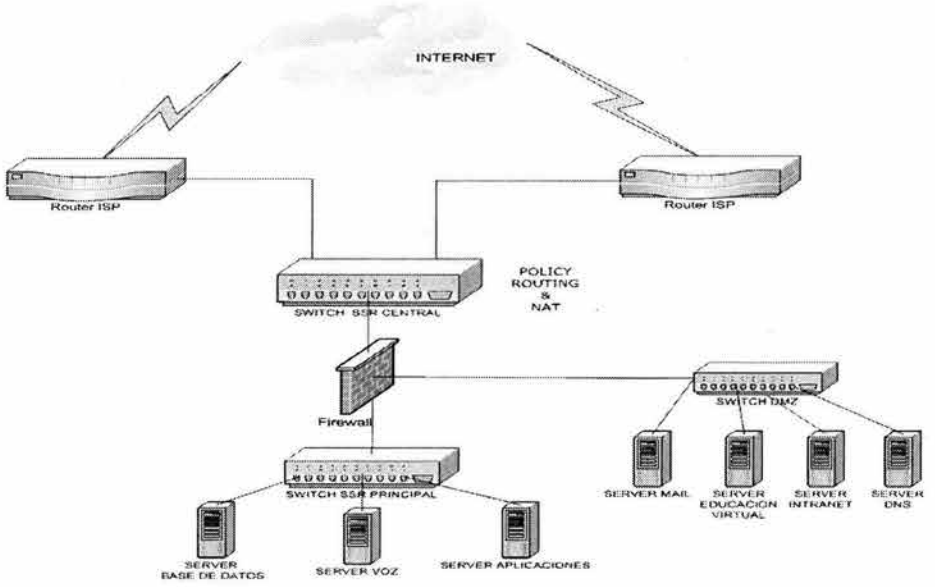


Figura 3.1: Resolución de nombres DNS.

La arquitectura del DNS Split consiste de un servidor DNS externo que provee la resolución de nombres para los clientes de Internet y un servidor DNS interno, que resuelve los nombres para los usuarios internos de la red. La figura 3.2 muestra una visión general de cómo el DNS interno y externo funcionan.

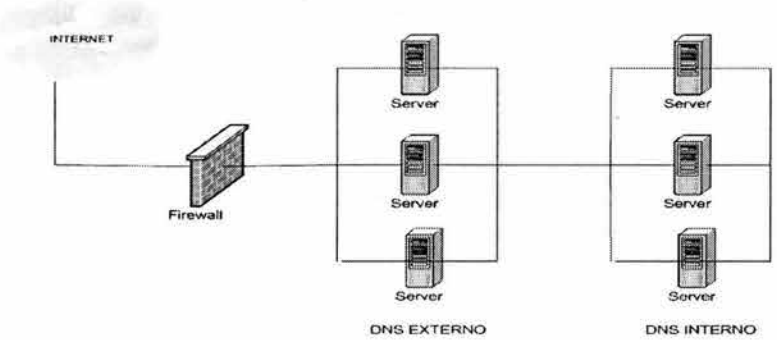


Figura 3.2: Configuración del DNS Split.

A continuación describiremos un poco más la implementación del DNS interno y externo.

Servicios DNS externo.

La zona de transferencias esta configurada para tomar lugar entre el DNS externo primario y secundario, esto del lado interno de la granja de servidores. Esto previene cualquier exposición de datos hacia Internet por el lado de los servidores.

La zona de transferencias no esta permitida entre el servidor DNS interno y externo. Esta separación o configuración DNS Split permite que la información de resolución de nombres permanezca aislada e inaccesible hacia Internet.

Bajo ninguna circunstancia puede haber búsquedas en el DNS desde Internet permitiendo pasar hacia la red interna para la resolución de nombres. En limitados casos, se requiere transmitir datos del DNS externo hacia el servidor DNS de nuestro ISP, para agregar redundancia. Si se implementa, los servidores DNS tienen que ser configurados solo para permitir la transmisión de datos entre los servidores DNS de nuestro ISP y nuestros servidores externos.

Servicios DNS interno.

El conjunto de servidores DNS internos localizados en la infraestructura VLAN, son usados para soportar Active Directory (herramienta de Microsoft), y soportan la resolución de nombres para los servidores en la red DMZ, y para la administración de datos de las VLAN's.

Para propósitos de escalabilidad y redundancia, múltiples servidores son configurados para soportar esta arquitectura. Por economía y simplicidad los servidores DNS son instalados con el controlador de dominios en el Active

Directory y también son configurados para integrar la zona de datos de los servidores con la base de datos del Active Directory. Por configurar el DNS en el Active Directory, las zonas de datos de ambos servidores DNS son replicadas automáticamente por el Active Directory, y ambos servidores DNS estarán disponibles para administrar los mismos dominios estáticos por actuar como servidores DNS primarios. Todos los miembros del dominio están configurados para apuntar hacia ambos servidores DNS como primario y secundario. Todos los servidores pueden registrar los nombres "amistosos" hacia el servidor DNS automáticamente, a través de un DNS dinámico (DDNS). En la mayoría de las configuraciones incluyen la arquitectura de Internet Data Center, los sistemas internos deben ser capaces de comunicarse con los sistemas hacia fuera de la Intranet. Para conseguir la resolución de nombres de Internet, los servicios internos del DNS están configurados para reenviar todas las búsquedas del DNS hacia los servidores DNS externos para la resolución. [http://www.microsoft.com]

3.2 Direccionamiento

En esta parte del capitulo se van a describir los pasos a seguir para llevar a cabo la migración de la red de datos actual de la Institución a un nuevo direccionamiento que permita realizar la segmentación en redes virtuales VLAN´s

Actualmente como hemos visto en el capitulo anterior la red de datos de la Institución cuenta con tres segmentos de red que hasta ese momento dan servicio: 168.1.1.X, 168.1.2.X y 168.1.3.X estas reciben enlaces hacia las distintas áreas de la Institución Educativa.

El objetivo principal de esta migración es la segmentación de la red en distintas redes virtuales (VLAN´s), que además de contener el tráfico de broadcast en secciones, faciliten la administración y el performance de la red de datos.

Para lograr el objetivo anterior, se plantearon dos opciones, las cuales se describen a continuación, para este propósito llamaremos IDF a la pila de switches en los cuales están conectados cada unos de los clientes de esta red de datos y MDF al equipo que concentrara cada uno de los enlaces.

OPCIÓN 1

En esta opción se plantea realizar redes virtuales por cada uno de los IDF´s que se conectan al SSR.
La información que se tiene se muestra en la tabla 3.1:

	Nombre del IDF	Descripción	Tipo de Switch	Enlaces al SSR
1	**Informática**	**Pila de 2 switches**	**VH**	**1**
2	**Mercadotecnia**	**Pila de 2 switches**	**ELS**	**1**
3	**Servicios Escolares**	**Pila de 2 switches**	**1 VH y 1 ELS**	**1**

4	Finanzas	Pila de 2 switches	VH	1
5	Docencia	Pila de 2 switches	ELS	1
6	Ventas	Pila de 3 switches	ELS	1
7	Bachillerato	Pila de 2 switches	1 VH y ELS	1
8	Lab.Computadoras 1 Lab.Computadoras 2	Pila de 3 switches y Pila de 4 switches	ELS	2
9	Lab.Computadoras 3	Pila de 6 switches	3 VH y 3 ELS	1
10	Posgrado	Pila de 2 switches	Matrix E1	1

Tabla 3.1: IDF's que se conectan al Switch SSR.

Tomando en cuenta que se tienen 10 IDF´s, se plantea hacer 10 redes virtuales (VLAN´s), una por IDF y a su vez se asignarán segmentos de red a cada una de las redes virtuales (Ver tabla 3.2).

IDF	SEGMENTO DE RED
Informática	172.16.6.X/24
Mercadotecnia	172.16.7.X/24
Servicios Escolares	172.16.8.X/24
Finanzas	172.16.9.X/24
Docencia	172.16.10.X/24
Ventas	172.16.11.X/24
Bachillerato	172.16.12.X/24
Lab.Computadoras 1	172.16.13.X/24
Lab.Computadoras 2	172.16.14.X/24
Posgrado	172.16.16.X/24

Tabla 3.2: Segmentos de red para los IDF's.

3.2.1 Procedimiento de Migración (OPCIÓN 1)

Esta migración se deberá llevar a cabo en varias etapas en las cuales se puede migrar uno o varios IDF´s.
A continuación describiremos los pasos que se siguieron para llevar a cabo la migración:

1. Asignar direccionamiento de IP nuevo a cada unos de los clientes de la red de datos, dependiendo de la red virtual que corresponda, es recomendable dejar bloques específicos por tipo de usuarios que estén trabajando en este IDF, es decir, se debe procurar asignar direccionamiento IP consecutivo a usuarios del mismo tipo.

2. Verificar que estén creadas las redes 168.168.XXX.XXX hasta la 168.168.XXX.XXX como secundarias en el SSR2000 (SSRLAN).
3. Configurar en el Firewall los objetos con el direccionamiento nuevo de la red virtual que se vaya a trabajar.

Nota.- Esta migración o estos cambios tienen que ser transparentes para el cliente ya que esta configuración se realizará cuando la red este en producción.

4. Realización del cambio de dirección IP y Default Gateway a cada cliente involucrado en la red virtual a cambiar. Este cambio no representará corte en el servicio ya que los usuarios seguirán operando normalmente debido a las configuraciones realizadas con anterioridad en el Firewall y en el SSR2000.
5. Quitar de la red virtual existente para la red LAN, el o los puertos involucrados según la etapa de migración, para reasignarlos a sus redes virtuales especificas.
6. Se crea la red virtual, se le asigna un nombre que identifique al IDF.
7. Se crea una interfase lógica a la cual se le asignara una dirección IP. Esta dirección es la última dirección utilizable del segmento asignado para cada IDF.
8. Se asigna el o los puertos a la red virtual creada.
9. Se asigna un Default Gateway a la red virtual en el SSR2000
10. Se lleva a cabo un script de pruebas previamente realizado con las necesidades de red que tenga el cliente.

En el caso de que se requieran pasar usuarios de un IDF a otro después de la migración se realizara lo siguiente:

1. Se deberá asignar al usuario una dirección IP correspondiente a la VLAN donde se desea mover.
2. Se deberá editar el objeto en el Firewall para modificar la IP anterior a la IP nueva.
3. En el caso de que el usuario que se desea mover este dentro de alguna ACL creada, se deberá modificar la línea en el SSR2000 correspondiente a ese cliente.

OPCIÓN 2

Esta opción plantea el realizar las redes virtuales por área de trabajo.
Actualmente en la Institución se tienen aproximadamente de 35 a 40 áreas de trabajo diferentes, por lo que se tendría que crear una red virtual por cada unos de los grupos que se tenga.
Existen usuarios que pertenecen a distintas áreas de trabajo en cada IDF, por lo que de inicio se deberán configurar todas las redes virtuales de las áreas existentes dentro de los IDF´s

3.2.2 Procedimiento de Migración (OPCIÓN 2)

1. Asignar direccionamiento de IP nueva a cada unos de los clientes de la red de datos dependiendo del área que corresponda.
2. Verificar que estén creadas las redes 168.168.XXX.XXX hasta la 168.168.XXX.XXX como secundarias en el SSR2000 (SSRLAN)
3. Configurar en el Firewall los objetos con el direccionamiento nuevo de la red virtual que se vaya a trabajar.

Nota.- Esta migración o estos cambios tienen que ser transparentes para el cliente ya que esta migración se realizará cuando la red este en producción.

4. Realización del cambio de dirección IP y Default Gateway a cada cliente involucrado en la red virtual a cambiar. Este cambio no representara corte en el servicio ya que los usuarios seguirán operando normalmente debido a las configuraciones realizadas con anterioridad en el Firewall y el SSR2000.
5. Se crea la red virtual y se le asigna un nombre que identifique el área.
6. Se deben configurar los puertos que reciben los enlaces de los IDF´s como Qtrunk.
7. Se crean las redes virtuales correspondientes en las pilas de switches de cada IDF. El número de redes virtuales que se crearán dependerá del número de áreas que se encuentren en ese IDF.
8. Se corre un script de pruebas en el área cambiada.

En el caso de que se requieran pasar usuarios de un área a otra después de la migración se realizará lo siguiente:

1. Se deberá verificar que en el IDF al que se moverá exista la red virtual a la cual pertenece el usuario, de lo contrario se deberá crear en los switches la VLAN correspondiente.
2. Se deberá editar el objeto en el Firewall para modificar la dirección IP anterior a la dirección IP nueva.
3. Se deben modificar las redes virtuales en la pila de switches de tal forma que el puerto al que se va conectar el cliente nuevo pertenezca a la red virtual correcta.
4. En el caso de que el usuario que se desea mover este dentro de alguna ACL creada, se deberá modificar la línea en el SSR2000 correspondiente a ese cliente.

3.3 Segmentación

El aprovechamiento adecuado de las innovaciones tecnológicas en el área de comunicaciones (que se han mencionado en el capitulo 2) permitirá a la Institución modernizar sus esquemas de operación y reducir los costos actuales.

Establecer un esquema técnico y económicamente viable para desarrollar una red de datos, por medio de la cual sea posible el intercambio de información entre los edificios que componen a la Institución, la comunicación con instancias externas, el acceso a redes públicas y optimizar el uso de los recursos informáticos que se encuentren conectados a la misma.
Del diagnostico puntualizado en el capitulo 2 efectuado para el análisis del comportamiento de la red (Ver Figuras 2.3 y 2.4, que es el análisis del sniffer), se propone el desarrollo de un esquema de comunicación de datos ruteada por medio del cual se pueda realizar el intercambio de servicios entre los edificios que conforman esta red de datos.

Y de acuerdo a lo mencionado anteriormente, la opción viable para realizar la segmentación, será la opción 1 presentada en el tema anterior, esta decisión fue tomada ya que representa una fácil administración y también se tomaron factores como las necesidades que presenta la Institución (cambios de área).

3.4 Creación VLAN's

En esta parte presentamos el equipo de comunicaciones en el cual se llevan a cabo la configuración de las VLAN's, esto es como complemento de lo presentado con anterioridad en el capítulo 2 de este trabajo de investigación.

SWITCH RUTEADOR CENTRAL CORE SSR-2-B-128 O X-PEDITION 2000.

Este switch router provee un link del backbone hacia el escritorio de trabajo, esta diseñado para desempeño de un workgroup, soporta velocidades de 10/100/1000 Mbps de switcheo y ruteo aplicando throughput. Desempeña switcheo para las capas 2 (data-link), 3 (Network) y 4 (transport) del modelo de referencia OSI.

Adicionalmente el X-Pedition 2000 provee aplicaciones de control pinpoint y tiene una capacidad superior para el ruteo de paquetes. Este tipo de switch router tiene interoperabilidad con modelos anteriores a este. Finalmente el X-Pedition 2000 proporciona ruteo de unicast y multicast para full-function IP/IPX (Ver tabla 3.3).

CANTIDAD	UNIDAD	NO. PARTE	DESCRIPCIÓN
1	PZA	SSR-2-128-B	SWITCH ROUTER 16 PORTS 10/100 BASETX AND 3 SLOTS FOR UPLINK AND SWITCH MODULES.
1	PZA	XP-2-TX-AA	X-PEDITION 2400 8 PORT 10/100 TX MODULE
1	PZA	XP-2-RKMT	RACKMOUNT KIT FOR XP-2400 & XP2100

Tabla 3.3: Especificaciones Switch ruteador.

Las líneas de configuración del Smart Switch Router (SSR) 2000 se encuentran dentro del Apéndice B de este trabajo de investigación.

3.5 Implicaciones

Comunicación en los clientes del Red de datos de la Institución

Como en cualquier otra red plana los clientes de la red de la Institución Educativa basan toda su comunicación en recursos compartidos por nombre de los equipos cliente-cliente y cliente servidor, por lo que de primera instancia se da la solución de abrir estos puertos que permiten la comunicación por Netbios. En Microsoft, NetBIOS empezó como interfaz de lenguaje de programación de alto nivel para programas MS-DOS utilizados en los equipos compatibles con IBM PC de los últimos años de la década de 1980. Para construir LAN basadas en el hardware y software de red disponibles para aquellos equipos, Microsoft y otros fabricantes estandarizaron el uso de la interfaz NetBIOS para diseñar los componentes de sus sistemas operativos y sus programas de red. Dicha interfaz utiliza nombres con una única parte, limitados a 16 caracteres de longitud, para identificar los recursos de la red.

El espacio de nombres de NetBIOS es plano, lo que significa que dichos nombres sólo se pueden utilizar una vez dentro de una red. Estos nombres se registran dinámicamente cuando se inician los equipos, los servicios o cuando los usuarios inician la sesión. Los nombres NetBIOS se pueden registrar como nombres únicos o nombres de grupo. Los nombres únicos tienen una dirección asociada al nombre. Los nombres de grupo tienen más de una dirección asignada al nombre.

La solución propuesta en las últimas líneas de configuración (Ver Apéndice B) no fue la mas adecuada ya que por una parte se tendrían que configurar estos puertos para cada una de las redes virtuales, por otra parte, y la más importante es la implicación que tendría el dejar estos puertos abiertos para la comunicación entre clientes de diferentes VLAN's en este equipo de comunicación. Tener un puerto "abierto" permitiría la entrada de ataques de virus, que a últimas fechas se han propagado de manera importante y

han cambiado su forma de atacar a la red, ahora estos virus ya no se enfocan en dañar el equipo físicamente (como borrar archivos o provocar daños irreversibles en los discos duros), sino que ahora estos virus se enfocan mas a dejar puertos abiertos para ataques de hackers o la entrada de más virus en la red.

3.6 Resolución de Problemas

3.6.1 WINS

Con la finalidad de proporcionar la resolución de nombres de la plataforma de Windows en las versiones de Windows 9x, windows200 profesional y Windows 2000 Server, se implemento un servidor de nombres WINS, el cual ayudara a toda las computadoras o clientes de las **diferentes redes virtuales en las cuales quedo segmentada la red de la Institución** a encontrarse en la red por su alias o dirección IP y ayudando a evitar los esquemas de consulta por IP.

En redes con servidores Windows 2000 Server y los demás equipos con Windows 2000 Professional, ya no es necesario NetBIOS si la red se basa en TCP/IP. Como consecuencia de este cambio, WINS es necesario para la mayoría de las redes, pero puede haber casos en que no lo sea. Para decidir si necesitamos usar o no WINS, debemos plantearnos antes las siguientes cuestiones:

- *¿Hay algún equipo heredado en la red que necesite usar nombres NetBIOS?*

Hay que recordar que todos los equipos en red que utilicen alguna versión anterior de los sistemas operativos de Microsoft, por ejemplo versiones de MS-DOS, Windows o Windows NT, necesitan los nombres NetBIOS. Windows 2000 es el primer sistema operativo de Microsoft que ya no necesita los nombres NetBIOS. Por eso, los nombres NetBIOS pueden seguir siendo necesarios en la red para ofrecer servicios básicos de archivos e impresión y asegurar la compatibilidad con muchas aplicaciones heredadas aún en uso.

- *¿Están configurados y preparados todos los equipos de la red para permitir el uso de otro tipo de sistema de nombres de red, como puede ser DNS?*

El sistema de nombres de red es aún un servicio crucial para encontrar equipos y recursos en la red, incluso en el caso de que ya no sean necesarios los nombres NetBIOS. Antes de decidirnos a eliminar la compatibilidad con WINS o los nombres NetBIOS, debemos asegurarnos de que todos los equipos y programas pueden operar con otro servicio de nombres, por ejemplo DNS.

En general, los sistemas operativos Windows son compatibles con dos de los sistemas principales existentes para resolver nombres en red. Son los siguientes:

- **Resolución de nombres de host.** Se trata de un sistema de resolución de nombres basado en Windows Sockets que usa la API gethostbyname () para buscar la dirección IP de un host a partir de su nombre. Este método se basa en un archivo Hosts o en consultas DNS para realizar la resolución del nombre.

- **Resolución de nombres NetBIOS.** Este tipo de resolución de nombres utiliza el redirector NetBIOS para buscar una dirección en función del nombre NetBIOS consultado. Este método se basa en un archivo Lmhosts o en consultas WINS para realizar la resolución del nombre.

Los clientes WINS que usan Windows 2000 están configurados de forma predeterminada para usar, en primer lugar, DNS para la resolución de nombres de más de 15 caracteres de longitud o que incluyan puntos (".") en el nombre. Para los nombres de menos de 15 caracteres y que no incluyen puntos, DNS es la última opción cuando no se obtienen resultados de la consulta WINS, siempre que el cliente esté configurado para usar un servidor DNS.

Evitar el uso de entradas estáticas en WINS.

Las entradas estáticas en WINS precisan de otras acciones administrativas para garantizar el uso para el que fueron creadas. Sin embargo, las entradas estáticas pueden resultar útiles en determinados casos, como puede ser para impedir el registro WINS de los nombres utilizados por servidores de importancia crítica.

Por ejemplo, una entrada estática en WINS podría usarse para impedir que otros equipos lleguen a apropiarse del nombre de un servidor mientras éste no se encuentra disponible.

El mayor inconveniente que tiene el uso de entradas estáticas en WINS son las complicaciones que se producen en la administración de los cambios de nombres y direcciones en la red. Por ejemplo, si la dirección IP o el nombre de un equipo de una entrada estática WINS cambian, puede que también sea necesario actualizar manualmente otras configuraciones, como las de los servidores DHCP, servidores DNS, sistemas finales y archivos Lmhosts.

Si se decide utilizar entradas estáticas WINS, debemos tener en cuenta las siguientes sugerencias para configurar otras propiedades de los servicios DHCP y WINS de forma que se eviten problemas habituales:

- Para cada dirección IP utilizada en la asignación WINS estática, debemos pensar en utilizar una reserva de direcciones de cliente para reservar la dirección IP en el servidor DHCP.

- Si utilizamos entradas WINS estáticas sólo para permitir cambios temporales en la red, debemos mantener seleccionada la opción predeterminada **Migración activada** en la consola WINS.

Al seleccionar **Migración activada**, las entradas estáticas temporales únicas o múltiples que se agreguen los clientes las pueden actualizar y cambiar de forma dinámica. Cualquier intento posterior de un cliente para registrar dinámicamente una entrada de nombre único o múltiple, cuando

ya existe una entrada estática con el mismo nombre, da lugar a un proceso de desafío.

En el desafío, la dirección IP de la asignación estática se compara con la dirección IP que el cliente en cuestión trata de registrar dinámicamente en WINS. Si las dos direcciones son diferentes y se determina que la dirección estática ya no está activa ni en uso, la asignación IP puede migrar (de una asignación estática a una dinámica) y actualizarse la dirección IP en WINS.

Si utilizamos de forma permanente entradas WINS estáticas, podemos deshabilitar **Migración activada**. De esta forma, se impide que una entrada WINS dinámica llegue a suplantar una entrada WINS estática asignada al nombre y dirección de un servidor crítico de la red.

Programar la comprobación de coherencia para que se ejecute en un período de poco tráfico.

En el caso de Windows 2000 Server, la comprobación de coherencia WINS se realiza mediante el complemento de WINS. Periódicamente debe utilizar esta característica para comprobar la coherencia de la base de datos WINS. Sin embargo, la comprobación de coherencia consume muchos recursos del equipo servidor WINS y sobrecarga la red. Por eso, las comprobaciones de coherencia WINS deben realizarse en períodos de poco tráfico, como son las horas nocturnas o el fin de semana.

Usar sólo los servidores WINS que sean necesarios.

Si hay demasiados servidores WINS en una red, se pueden complicar los problemas que se presenten. Tenemos que ser austeros a la hora de agregar nuevos servidores WINS a la red y utilizar el menor número posible de servidores WINS para dar servicio a todos los clientes y mantener un rendimiento aceptable en cada servidor.

El tráfico de red WINS que se produce en el registro de clientes puede ser mucho menor que el de DHCP, ya que éste usa difusiones de cliente para encontrar a los servidores. De forma predeterminada, la mayoría de los clientes WINS tratan en primer lugar de comunicar con los servidores WINS configurados como primarios empleando mensajes de datos punto a punto. Un servidor WINS es suficiente para dar servicio a una red interna pequeña. Sin embargo, es aconsejable utilizar al menos dos servidores WINS para que la instalación sea tolerante a fallos.

Supervisar y realizar operaciones de compactación periódicas y sin conexión.

Aunque las operaciones manuales de compactación de la base de datos del servidor WINS no son tan importantes en Windows 2000 Server como lo han sido en versiones anteriores, siguen siendo todavía útiles. Para eliminar la fragmentación del disco del servidor y mejorar su rendimiento, debemos realizar una compactación periódica de WINS (mensual o semanal). A continuación, debemos supervisar los cambios que se produzcan en el tamaño del archivo de la base de datos, Wins.mdb, que se encuentra en la carpeta *raízSistema*\System32\WINS\.

En cada compactación sin conexión, resulta útil comparar el tamaño del archivo Wins.mdb antes y después de la compactación, para medir su tasa de crecimiento y reducción. Esta información puede ser de utilidad para determinar las ventajas que supone la operación de compactación sin conexión. Según esta información, podemos determinar con qué frecuencia debemos repetir la compactación sin conexión para obtener ventajas apreciables.

Usar NBTSTAT -RR para registrar y solucionar problemas de conectividad de clientes.

En el caso de Windows 2000, la opción de la línea de comandos NBTSTAT -RR permite purgar nombres remotos de la caché de nombres NetBIOS locales y fuerza la renovación y nuevo registro de los nombres de clientes locales. Podemos utilizar esta opción de la línea de comandos para actualizar las entradas de clientes en WINS y duplicarlas en otros asociados de duplicación, sin que sea necesario reiniciar el cliente.

Configurar cada equipo de servidor WINS de forma que se apunte a sí mismo.

Cada servidor WINS que se instale en la red debe registrar en WINS su propio conjunto de nombres únicos y de grupo NetBIOS. Para evitar los problemas del servicio WINS que pueden presentarse cuando un registro WINS se divide (es decir, cuando los nombres registrados para un servidor WINS determinado pasan a ser propiedad de distintos servidores WINS), cada equipo de servidor WINS sólo debe apuntar a su propia dirección IP mientras se configuran sus propiedades TCP/IP.

Por lo general la resolución de nombres en una red Microsoft Windows se realiza mediante el envió de paquetes de difusión. Por ejemplo cuando se utiliza el protocolo Netbeui, se necesita obtener el nombre de todos los equipos registrados en la red, se envía una llamada de difusión (broadcast). A esta llamada responden todos los equipos configurados como examinadores de red. Este mecanismo permite a los diferentes clientes de la red anunciarse sin necesidad de emplear servidores de nombres dedicados, pero esta tarea como se mencionó anteriormente no puede ser posible debido a que hasta este punto de la optimización de la red los clientes únicamente pueden consultarse por dirección IP.

Una de las primordiales tareas de esta segmentación y por ende de la optimización de la red es reducir el uso de estos paquetes de difusión (broadcast) por todos los clientes que forman parte de esta red de comunicación. Esta difusión como lo hemos tocado en el resto de los capítulos debe ser evitado por dos motivos fundamentales:

Se consume un ancho de banda importante y obliga a todos los equipos a procesar paquetes broadcast.

En el caso de esta segmentación parte de la concentración de todos los clientes de la red LAN de la Institución Educativa en un equipo que es capaz de hacer tareas de switcheo y ruteo, solo que a diferencia de la definición anterior la difusión será únicamente para los clientes que pertenezcan a su

misma red virtual , esto es, que los clientes que pertenezcan a una red virtual solo harán difusión de estos paquetes hasta donde el tamaño de su propia red se lo permita , recordemos que el tamaño de cada red virtual es de /24 , y es por eso que cada nodo tendrá configurado su default gateway y será configurado a cada nodo

Finalmente para dar solución al problema que se presento en las últimas líneas de configuración de los puertos decidimos bloquear los puertos que eran utilizados, con esto logramos negar el paso de ataques de virus. La nueva configuración de estas líneas pueden ser vistas dentro del Apéndice B.

Una vez establecida estas nuevas líneas y tomando en cuenta lo planteado tanto en el capitulo 2 como en este capitulo 3 de este trabajo de investigación, el diseño de la red de la Institución que actualmente esta funcionando es el siguiente (Ver figura 3.3):

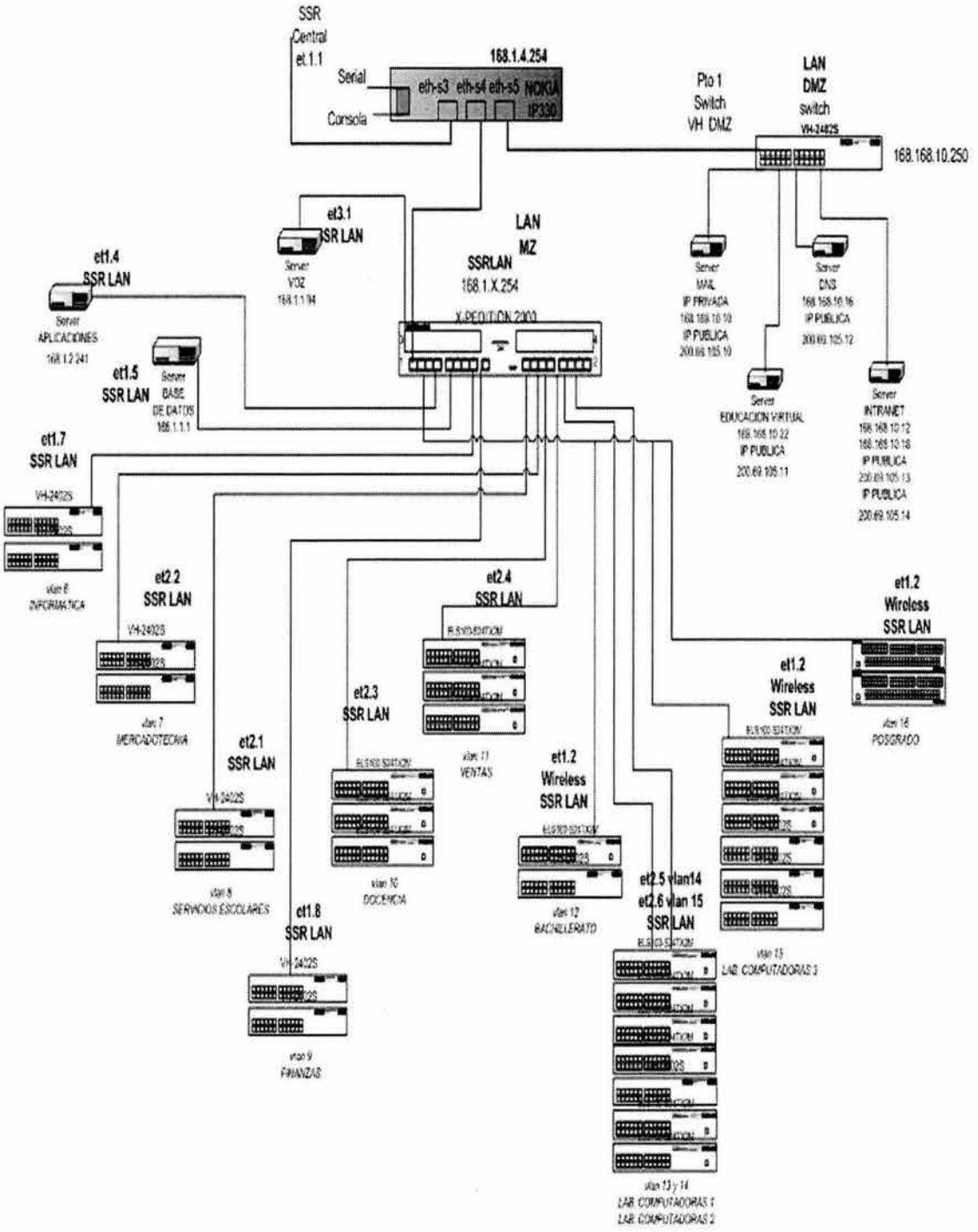


Figura 3.3 Red Actual de la Institución

En el siguiente capitulo nos enfocaremos a definir la manera en la cual se esta trabajando la parte administrativa de la red. Así como, presentaremos los scripts de administración, monitoreo y de respaldo para los planes de emergencia.

Capítulo 4

4.1 Monitoreo y administración

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.

- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.

- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.

- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

El sistema de administración de red opera bajo los siguientes pasos básicos:

- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.

- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.

- Transportación de la información del equipo monitoreado al centro de control.

- Almacenamiento de los datos coleccionados en el centro de control.

- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

4.1.1 Operaciones de la administración de red

Las operaciones principales de un sistema de administración de red son las siguientes:

- Administración de fallas: La administración de fallas maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

  - Detección de fallas.
  - Diagnóstico del problema.
  - Darle la vuelta al problema y recuperación.
  - Resolución.
  - Seguimiento y control.
  - Control de fallas.

Esta operación tiene que ver con la configuración de la Red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

- Administración de cambios: La administración de cambios comprende la planeación, la programación de eventos e instalación.
- Administración del comportamiento: Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye: El número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

- Servicios de contabilidad: Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

  - Tiempo de conexión y terminación.
  - Número de mensajes transmitidos y recibidos.
  - Nombre del punto de acceso al servicio.
  - Razón por la que terminó la conexión.
  - Control de Inventarios.

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

- Seguridad: La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

  - Identificación y autentificación del usuario, una clave de acceso y un password.

  - Autorización de acceso a los recursos, es decir, solo personal autorizado.

  - Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración, rendimiento, seguridad e inventarios.

4.1.2 Funciones de administración definidas por OSI

OSI define las cinco funciones de administración básicas siguientes:

- Administración de Configuración
- Administración de Fallas
- Administración de acceso
- Administración de desempeño
- Administración de Seguridad.

La configuración comprende el proceso de mantener a través de varios parámetros de los dispositivos e instalaciones para mantener operativa la red [Joachim, 1992].
Así mismo, la administración de configuración se encarga de configurar a los elementos de red desde una terminal remota. En general es la encargada de las funciones de monitoreo y mantenimiento del estado de la red.

La administración de fallas incluye la detección, el aislamiento y la corrección de fallas en la red. El objetivo es determinar lo más rápido posible el lugar de la red donde se encuentra la falla, para que ésta sea corregida lo más rápido posible. Para localizar una falla en la red se siguen los siguientes pasos:

- Encontrar exactamente donde se encuentra la falla.
- Aislar el área donde se encuentra la falla, del resto de la red, para que ésta pueda seguir funcionando.
- Determinar el origen o las posibles causas del problema.
- Corregir o reparar la falla si es posible.

Es importante entender que muchos problemas que se presentan en la red pueden ser resueltos inmediatamente. Muchos otros problemas requieren ser tratados por personal capacitado para resolver tales problemas, cabe la pena mencionar, que estos problemas pueden ser resueltos en algunos minutos o talvez en algunas horas, también cabe la posibilidad que estos problemas tengan que ser monitoreados periódicamente para dar una solución adecuada.

La función de administración de acceso, permite el establecimiento de cargos a usuarios por uso de los recursos de la red. Es decir, es el seguimiento de la utilización de los recursos de la red por los usuarios. En esta parte el administrador de red puede observar:

- El uso ineficiente de la red.
- Que los usuarios tengan uso de los recursos necesarios de la red.
- Del abuso de los privilegios en los accesos a usuarios.

Finalmente, en esta administración es donde se planea el crecimiento de la red, en base a las actividades de los usuarios como puede ser: uso de periféricos, espacio de almacenamiento, procesamiento de datos, etc.

La función de la administración de desempeño, es mantener el comportamiento de la red en niveles aceptables. Se deben tomar en cuenta los siguientes aspectos:

- Cantidad de errores
- Tiempo de respuesta para los usuarios finales
- Porcentaje de utilización
- Tráfico
- Capacidad disponible con la que cuenta la red

En la administración de seguridad, se proveen mecanismos para autorización, control de acceso, confidencialidad y manejo de claves. También se debe incluir prevención de virus, continuidad en los procedimientos de operación y la planeación e implementación de métodos cuando algún desastre ocurra.

4.1.3 Normas para la administración de la red

El Comité Asesor de Internet (Internet Advisory Board, IAB) ha elaborado normas para la administración de la red. Un grupo de trabajo Internet, responsable de las normas para la administración de la red, adopto un enfoque de dos cuestiones para cubrir las necesidades actuales.

La primera consiste en el uso del protocolo SNMP (Simple Network Management Protocol), este protocolo actualmente es utilizado en muchas redes Internet. Conforme ha pasado el tiempo este protocolo ha venido mejorando y se ha convertido en un protocolo mas completo.

La segunda cuestión hace referencia a las normas OSI para administración de redes llamados CMIS (Common Management Information Services), éste es el servicio para la colección y transmisión de información de administración de red a las entidades de red que lo soliciten, y CMIP (Common Management Information Protocol), es el protocolo de OSI que soporta a CMIS, y proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones [Joachim, 1992].

4.1.4 Protocolos de administración

Para el desarrollo de la gestión de redes en Internet basadas en TCP/IP, el IAB (Internet Activities Board) decidió seguir una estrategia en la cual a corto plazo se usaba el Simple Network Management Protocol (SNMP) para gestionar los nodos, y se proponía para largo plazo la estructura de gestión de redes OSI. Se escribieron entonces dos documentos para definir la gestión de la información: RFC 1065 que definía la Estructura de la Información de Gestión (Structure of Management Information, SMI), y RFC 1066, que definía la Base de Información de Gestión (Management Information Base, MIB). Ambos documentos fueron diseñados para ser compatibles con la estructura SNMP y la de gestión de redes OSI. Posteriormente se observó que los requerimientos de SNMP y los de gestión

de redes OSI diferían más de lo esperado en un principio, por lo que los requerimientos de compatibilidad entre el SMI y el MIB y ambas estructuras fueron suspendidas.

La IAB ha designado al SNMP, a la SMI, y a la Internet MIB inicial como "Protocolos Estándar", con status de "Recomendado". Por medio de esta acción, la IAB recomienda que todas las implementaciones de IP y TCP sean gestionables por la red, y que las implementaciones que son gestionables por red se espera que los adopten e implementen.

Así pues, la actual estructura para gestión de redes basadas en TCP/IP consiste en:

- Estructura e Identificación de la Información de Gestión para redes basadas en TCP/IP, que describe cómo se definen los objetos gestionados contenidos en el MIB tal y como se especifica en la RFC 1155.
- Protocolo de Gestión de Redes Simples, que define el protocolo usado para gestionar estos objetos, según se expone en la RFC 1157.

4.1.5 MIB (Management Information Base)

La MIB define los objetos de la red operados por el protocolo de administración de red, y las operaciones que pueden aplicarse a cada objeto. Una variable u objeto MIB se define especificando la sintaxis, el acceso, el estado y la descripción de la misma. La MIB no incluye información de administración para aplicaciones como Telnet, FTP o SMTP, debido que es difícil para las compañías fabricantes instrumentar aplicaciones de este tipo para el MIB.

Estas bases de datos contienen cuatro datos:

- Sintaxis: Especifica el tipo de datos de la variable, entero, cadena dirección IP, etc.
- Acceso: Especifica el nivel de permiso como: Leer, leer y escribir, escribir, no accesible.
- Estado: Define si la variable es obligatoria u opcional.
- Descripción: Describe textualmente a la variable.

La MBI-1 define solo 126 objetos de administración, divididos en los siguientes grupos:

- Grupo de Sistemas: Se usa para registrar información del sistema el cual corre la familia de protocolos [Vázquez, 2000], por ejemplo:
  - Compañía fabricante del sistema.
  - Revisión del Software.
  - Tiempo que el sistema ha estado operando.
- Grupo de Interfaces: Registra la información genérica acerca de cada interfaz de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados, MTU del aparato, etc. [Vázquez, 2000].

- Grupo de traducción de dirección: Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar, como la tabla ARP, que relaciona direcciones IP con direcciones físicas de la red LAN. [Vázquez, 2000].

- Grupo IP: Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc. También contiene información de variables de control que permite aplicaciones remotas puedan ajustar el TTL (Time To Live) de omisión de IP y manipular las tablas de ruteo de IP. [Vázquez, 2000].

- Grupo TCP: Este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activas como dirección IP, puerto o estado actual. [Vázquez, 2000].

- Grupo de ICMP y UDP: Mismo que el grupo IP y TCP. [Vázquez, 2000].

- Grupo EGP: En este grupo se requieren sistemas (ruteadores) que soporten EGP. [Vázquez, 2000].

Como se observa, el agente y la MIB residen dentro del aparato que es monitoreado y controlado. La estación administradora contiene software que opera los protocolos usados para intercambiar datos con los agentes, y software de aplicación de administración de red que provee la interfaz de usuario para a fin de habilitar a un operador para saber el estado de la red, analizar los datos recopilados e invocar funciones de administración.

4.1.6 SNMP (Simple Network Management Protocol)

El protocolo Snmpv1 fue diseñado a mediados de los 80 por Case, McCloghrie, Rose, and Waldbusser, como una solución a los problemas de comunicación entre diferentes tipos de redes.

En un principio, su principal meta era el lograr una solución temporal hasta la llegada de protocolos de gestión de red con mejores diseños y más completos. Pero esos administradores de red no llegaron y SNMPv1 se convirtió en la única opción para la gestión de red.

El manejo de este protocolo era simple, se basaba en el intercambio de información de red a través de mensajes (PDU's). Además de ser un protocolo fácilmente extensible a toda la red, debido a esto su uso se estandarizo entre usuarios y empresas que no querían demasiadas complicaciones en la gestión de sus sistemas informáticos dentro de una red.

No obstante, este protocolo no era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo. Para subsanar sus carencias surgió la versión 2 (SNMP v2). Las mayores innovaciones respecto a la primera versión son:

Introducción de mecanismos de seguridad, totalmente ausentes en la versión 1. Estos mecanismos protegen la privacidad de los datos, confieren autentificación a los usuarios y controlan el acceso.

Mayor detalle en la definición de las variables.

Se añaden estructuras de la tabla de datos para facilitar el manejo de los datos. El hecho de poder usar tablas hace aumentar el número de objetos capaces de gestionar, con lo que el aumento de redes dejo de ser un problema.

Realmente esta versión 2, no supuso mas que un "parche", es más hubo innovaciones como los mecanismos de seguridad que se quedaron en pura teoría, no se llegaron a implementar.

Mensajes SNMP
El administrador de red de la estación de control y los agentes instalados en los aparatos manejados se comunican enviando mensajes SNMP. Sólo hay 5 mensajes:

- Get request: Contiene una lista de variables que el administrador desea leer de una MIB; es decir, el administrador pregunta a un agente sobre el estado de un objeto.

- Get Next request: Este comando provee un modo de leer secuencialmente una MIB.

- Set request: El administrador usa este comando para ordenar un cambio en el valor de una o más variables.

- Get response: El agente envía este mensaje como réplica a un mensaje de Get request, Get next request o Set request.

- Trap: El agente usa este mensaje para informar que ha ocurrido un hecho significativo:

    - falla de un enlace local.
    - otra vez funciona el enlace.
    - mensaje recibido con autentificación incorrecta.

SNMP maneja los siguientes tipos de datos:

- Enteros: Para expresar, por ejemplo, el MTU (Maximum Transfer Unit).

- Dirección IP: Se expresa como cuatro bytes. Recuérdese que cada elemento de red se configura con al menos una dirección IP.

- Dirección física: Se expresa como una cadena de octetos de longitud adecuada; por ejemplo, para una red Ethernet o Token Ring, la dirección física es de 6 octetos.

- Contador: Es un entero no negativo de 32 bits, se usa para medir, por ejemplo, el número de mensajes recibidos.

- Tabla: es una secuencia de listas.

- Cadena de Octetos: Puede tener un valor de 0 a 255 y se usa para identificar una comunidad.

4.1.7 Monitoreo de la red

El monitoreo de red consiste en observar y analizar el estado y comportamiento de cada elemento de la red. El objetivo de este monitoreo es obtener la mayor información posible del comportamiento de la red, para tal propósito, la información obtenida se clasifica en:

- Información dinámica. Esta información esta relacionada con los eventos que suceden en la red como la transmisión de paquetes. Esta información es guardada por el nodo que la genera y puede ser observada desde un nodo remoto.
- Información estática. Esta información de refiere a como esta configurado cada elemento en la red. Por ejemplo los nombres de dispositivos asociados a una partición de disco.
- Información estadística. Es la información generada por la información dinámica, como el promedio del número de paquetes por unidad de tiempo por cada computadora. También puede ser consultada desde un nodo remoto.

Para dar soporte a lo antes planteado, la Institución utiliza algunos programas de software para apoyo en las tareas de administración de la red, a continuación indicaremos las características de estos programas.

Para el apoyo en la seguridad, se cuenta con un programa llamado Dragon Intrusion Detection System, que es un software de la compañía Enterasys Networks y cuenta con las siguientes características:

- Alta velocidad en la detección de intrusos.
- Provee una completa detección de intrusos.
- Soporta desde una red pequeña, hasta redes corporativas.
- Monitorea firewalls, servidores Web y aplicaciones.
- La administración se maneja desde un sistema central.

Esta herramienta es de gran ayuda para la Institución ya que nos provee de soluciones para detectar ataques a través de toda la infraestructura de la red, así mismo, nos proporciona un nivel alto de protección contra intrusos, ya que hace un análisis completo en los host, firewall, servidores y aplicaciones, así como, un monitoreo en tiempo real.

Por otra parte, nos apoyamos en una herramienta llamada Netsight Atlas Console, que es una herramienta para administrar listas de control de accesos (ACL, Access List Control), este software cuenta con las siguientes características:

- Provee herramientas graficas de fácil uso para definir ya aplicar control en las ACL's para equipos X-Pedition, como los que maneja la INSTITUCION EDUCATIVA.
- Reduce el tiempo de configuración al compararse con el CLI, proporcionando configuración grafica y wizard-driven ACL.
- Fácil verificación del estatus de las ACL's y el estatus de los iconos de las ACL's.
- Duplica la regla de verificación, usando el menú para verificar reglas de duplicación dentro de las ACL's.
- Interfaces lógicas para recuperar la IP, IP secundaria, información MAC y VLAN, así como, información del ruteador.

Usando esta herramienta, el Dragon Intrusion Detection System y el sniffer visto en el Capitulo 2 de este trabajo, son de gran utilidad para garantizar la seguridad de la red, y nos brinda una gran ayuda para la administración de la red, ya que cuentan con herramientas graficas que son fáciles de administrar y con esto podemos encontrar más rápidamente problemas dentro de la red, y así, brindar una solución rápida y eficiente.

4.2 Métodos y Procedimientos

En esta parte y en el Anexo B presentaremos los scripts de administración, monitoreo y actualización de firmware, ya que estos scripts son de gran ayuda para mantener congruencia con la parte antes mencionada en este capitulo, así como, nos permiten tener un mejor desempeño de la red de la Institución.

Nota. Las direcciones IP y los nombres de usuarios han sido omitidos o cambiados para seguridad y privacidad de la Institución.

4.2.1 Script para el monitoreo de tráfico de cualquier interfaz en Equipos de Comunicación (LAN o WAN)

Para este caso utilizaremos una herramienta libre para que nos ayude a monitorear el tráfico que pase por la interfaz de nuestro equipo.

Herramienta .- PRTG Paessler Router Traffic Grapher, (Ver Figura 4.1).
Características.- Herramienta de tipo Freeware, si se necesita graficar más de una interfaz se requiere pagar un upgrade.
Es capaz de graficar interfaces desde cualquier equipo de comunicación de switcheo o ruteo.

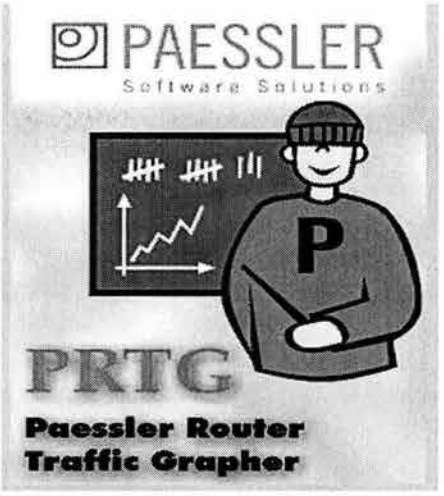


Figura 4.1: PRTG Paessler Router Traffic Grapher.

Alta de Interfaz

Una vez ejecutado daremos de alta la interfase a monitorear con ayuda de la opción: Add Sensor (Ver Figura 4.2)

Se agregara la dirección IP del equipo que contenga la interfaz que requiere ser monitoreada.

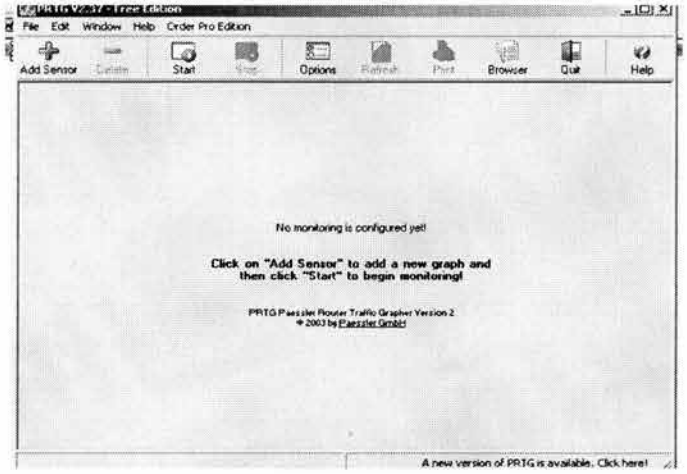


Figura 4.2: Alta de Interfaz.

Configuración de IP y Comunidad SNMP

Para el caso de nuestro equipo (y por razones de seguridad) escribiremos la IP que le corresponde así como la palabra de la Comunidad SNMP previamente configurada en el equipo, para este ejemplo será "pumas". (Ver Figura 4.3)

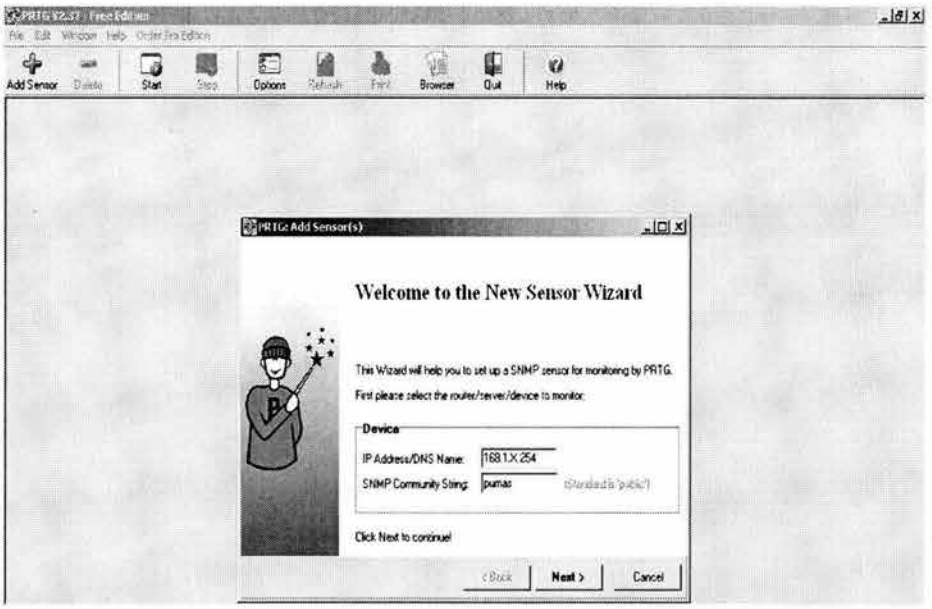


Figura 4.3: Configuración de IP y comunidad SNMP.

Conexión Establecida

Una vez que establece la comunicación con nuestro equipo, la herramienta manda todas las características del equipo con el que estamos estableciendo comunicación. (Ver Figura 4.4)

Figura 4.4: Conexión establecida.

Interfaz a Monitorear

Ahora se tendrá que escoger la interfaz de la cual se quiera monitorear el tráfico de entrada y de salida (bits de entrada y bits de salida). (Ver Figura 4.5)

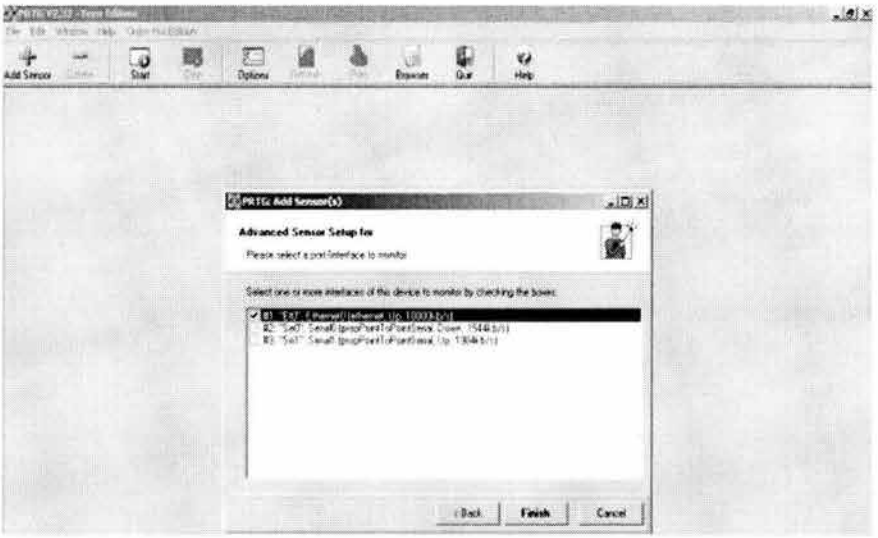


Figura 4.5: Interfaz a monitorear.

Envío de Mensajes Importantes

A esta Herramienta se le puede configurar una cuenta de correo para que de aviso de alguna caída de la interfase, que puede ser por alguna falla en el equipo, por alguna saturación e inclusive por alguna problema eléctrico. Esta cuenta puede ser las del Administrador de la Red. (Ver Figura 4.6)

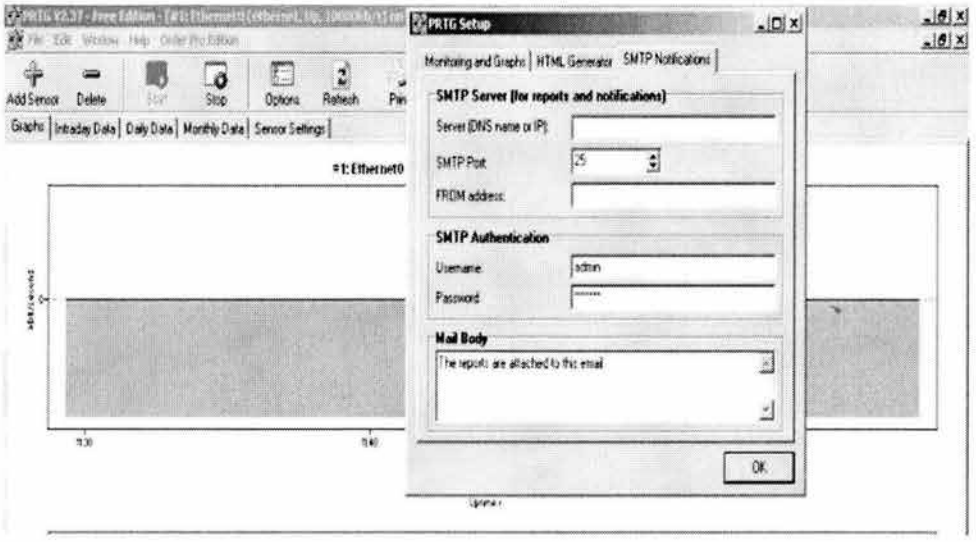


Figura 4.6: Envío de mensajes importantes.

Intervalos de Tiempo para las Gráficas

En esta opción habilitaremos los intervalos de tiempo, en los cuales deseamos que grafique nuestro tráfico (bits de entrada y bits de salida) por la interfase previamente seleccionada. (Ver Figura 4.7)

Estos intervalos pueden ser cambiados en base al día que se esta graficando, a la semana e inclusive al mes.

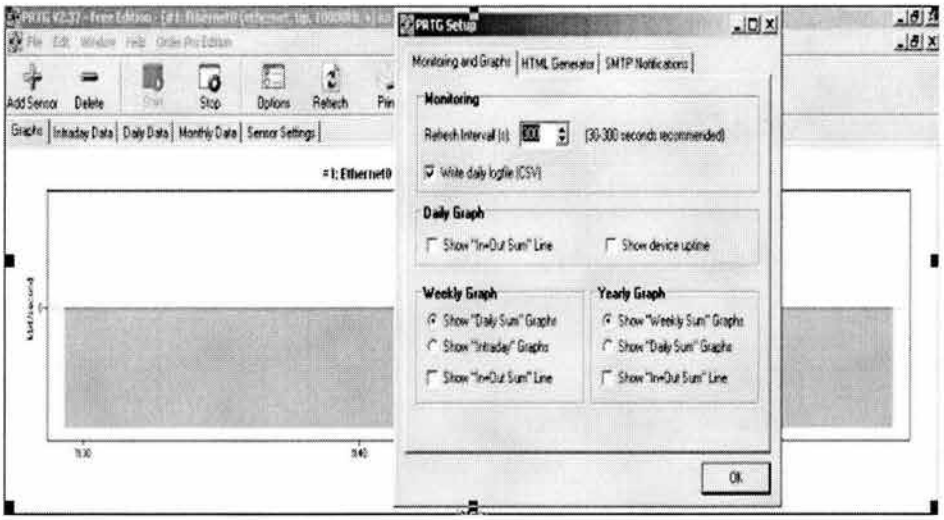


Figura 4.7: Intervalos de tiempos.

Gráficas obtenidas

Estas son las graficas que se obtienen y que fueron previamente configuradas en los puntos anteriores. Es importante mencionar que estas graficas se obtienen en tiempo real, por lo que el programa se debe mantener abierto mientras se hace la captura. (Ver Figura 4.8)

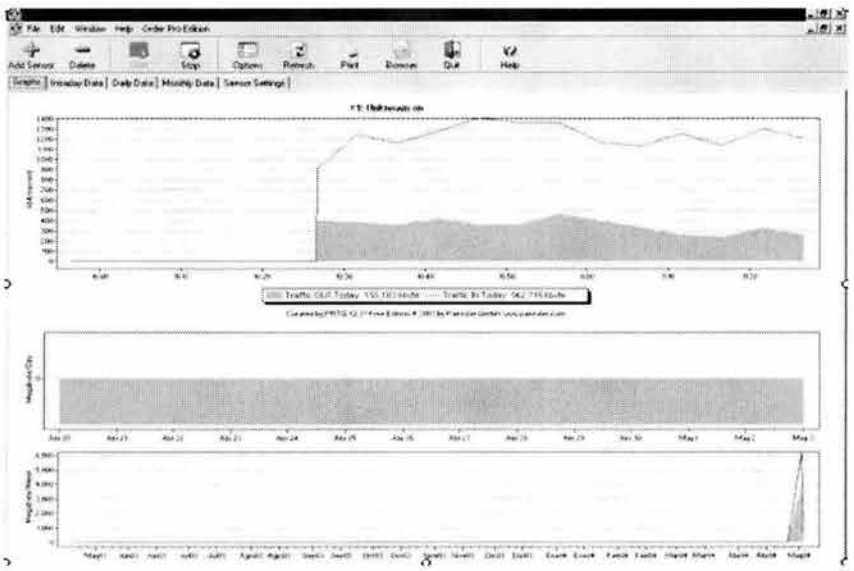


Figura 4.8: Gráficas obtenidas.

Otras Interfases que se apoyan en esta Herramienta

Aquí se muestran otras capturas de interfases monitoreadas con esta Herramienta.
Interfaz de Ruteo WAN (Ver Figura 4.9)
Interfaz Wireless Outdoor (Ver Figura 4.10)

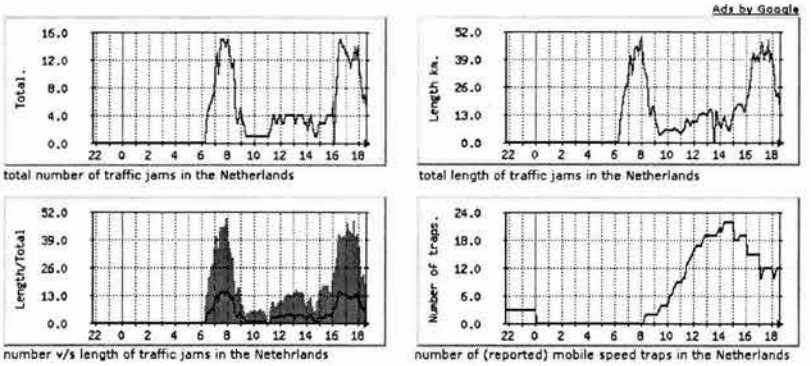


Figura 4.9: Interfaz de Ruteo WAN.

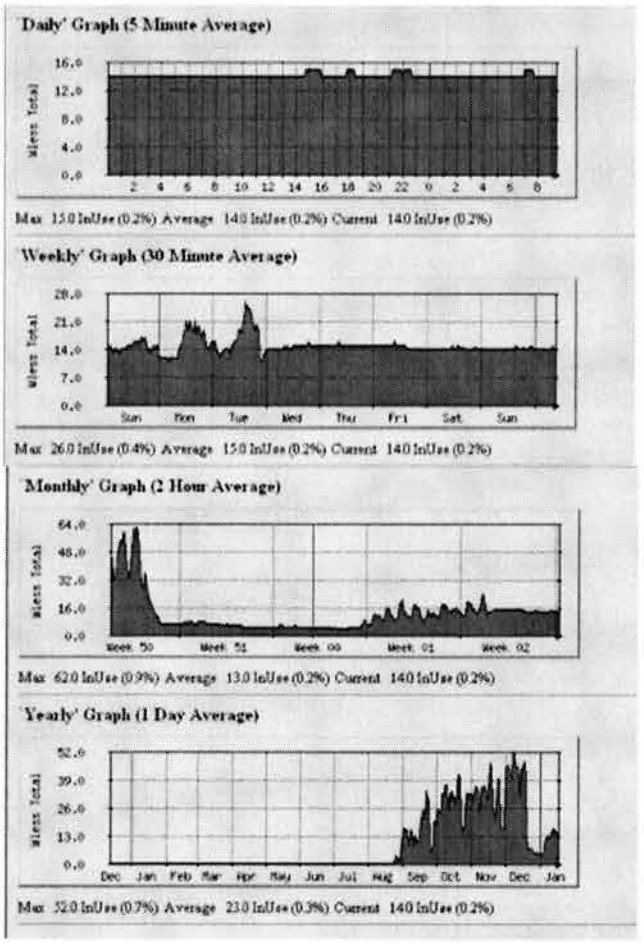


Figura 4.10: Interfaz Wireless Outdoor.

Los Scripts para la creación de un puerto espejo y el de actualización del Firmware y configuración de VLAN's se encuentran descritos dentro del Apéndice C.

4.3 Respaldos y planes de emergencia

4.3.1 Monitoreo de fallas

El monitoreo de fallas, deberá detectar y reportar fallas. El agente deberá mantener un archivo log o un archivo resumen donde se encuentren los errores que se generen, así como, los eventos significativos, esta información deberá estar disponible para aquellos nodos autorizados para recibir esta información.

Un buen monitor de fallas, tiene que anticiparse a dichas fallas, esto puede lograrse definiendo valores de umbral o frontera. Estos valores son límites preestablecidos que están cerca de ser una falla, cuando los resultados de un evento rebasan los valores de umbral definidos, se genera una alarma, de esta manera se detectan situaciones que puedan terminar en una falla para dispositivos de interconexión de red y/o servidores.

Monitoreo de desempeño

Un requisito importante para la administración de redes es la posibilidad de medir el desempeño de esta. Primeramente tenemos que monitorear el desempeño de la red, ya que sin esto no podemos administrar y controlar la red.

El monitoreo de desempeño tiene dos funciones básicas:

- Medición del desempeño: obtiene estadísticas acerca de los elementos de la red.

- Análisis del desempeño: en el se analizan los datos estadísticos. La medición del desempeño es casi siempre llevada a cabo por agentes dentro de los dispositivos de la red. Estos dispositivos están en posición de observar la cantidad de tráfico de paquetes dentro y fuera de un elemento de la red, el número de conexiones en las capas del protocolo, esto provee un detallado esquema del comportamiento de un elemento de dentro de la red.

Para medir el apropiado desempeño de la red se utilizan indicadores de desempeño, debemos conocer los indicadores apropiados para esta tarea. Los indicadores de desempeño se dividen en dos categorías: los orientados a eficiencia y los orientados a servicios.

Los indicadores orientados a eficiencia se basan en el rendimiento de la velocidad, en la cual un evento de aplicación (transferencia de archivos, mensajes) ocurre. Éste puede verse afectado por un mal funcionamiento de los elementos de la red a los cuales la aplicación este asociada, por ejemplo al transferir un archivo se detecta que la velocidad de transferencia es

lenta, probablemente el canal de comunicaciones no sea el adecuado o bien, puede existir un cuello de botella en alguna parte de la red.

Los indicadores orientados a servicios son aquellos que se relacionan con la satisfacción de las necesidades de los usuarios por medio de los servicios que nos proporciona la red: correo electrónico, almacenamiento de datos, impresión, etc.

En esta parte del capitulo, como su nombre lo dice, nos enfocaremos a mencionar la manera en que trabajamos los respaldos de configuración de los equipos de comunicación.

Primeramente los archivos son guardados en dos partes:

- BootFlash: guarda la configuración interna (archivos de usuario) en el directorio: /int-flash/cfg/.
- PC-Flash: almacena archivos del sistema operativo en el directorio: /pc-flash/boot/

Para poder visualizar la información que contienen estos archivos utilizamos el comando file dir <location>, ejemplo:
Ruteador#file dir bootflash.

Para copiar nuestras configuraciones o algún archivo lo realizamos con el comando copy, de la siguiente manera:
Copy <source> to <destination>, en el siguiente ejemplo copiamos el archivo startup en el archivo test_file:
Ruteador# copy startup to test_file, con este ejemplo observamos que el archivo test_file se ha copiado en bootflash, para comprobar esto tenemos que observar el contenido de bootflash, como se hizo anteriormente.

Igualmente el comando copy nos ayuda para mandar la configuración de startup, hacia un servidor TFTP, esto lo hacemos de la siguiente manera:
Ruteador#copy startup to tftp-server
TFTP server? 168.1.15.30
Destination filename? C:/tftp/startup.bak

Con estos comandos estaremos haciendo un back-up de la información de nuestros equipos de comunicación. Esto nos ayuda en gran medida por cualquier tipo de emergencia que se nos presente.

4.4 Pruebas y análisis

En esta parte del capitulo analizaremos las graficas que obtuvimos después de hacer la optimización de la red. Esto es en comparación con las graficas 2.3 y 2.4 del capitulo 2 de este trabajo de investigación.

La grafica 4.30 muestra el broadcast que obtuvimos colocando un sniffer en el mismo lugar que lo colocamos antes de hacer la optimización (Ver Figura 2.2), solo hubo una variante para que los resultados fueran más representativos hicimos "mirroring" de nuestro switch SSR 2000 con nuestro Firewall.

En esta grafica (4.11) observamos que el broadcast ha disminuido en forma considerable en comparación con la grafica 2.3, esto se debe a que los dominios de broadcast y de colisión se separaron al momento de usar VLAN's y switches respectivamente, ahora la red esta segmentada y esto nos permite obtener un mejor performance de la red, ya que la velocidad de transmisión se aumento cuando utilizamos una velocidad Fast Ethernet, cabe notar que aun cuando tuvimos un incremento de usuarios y equipos en la red, obtuvimos un mejor desempeño de la misma.

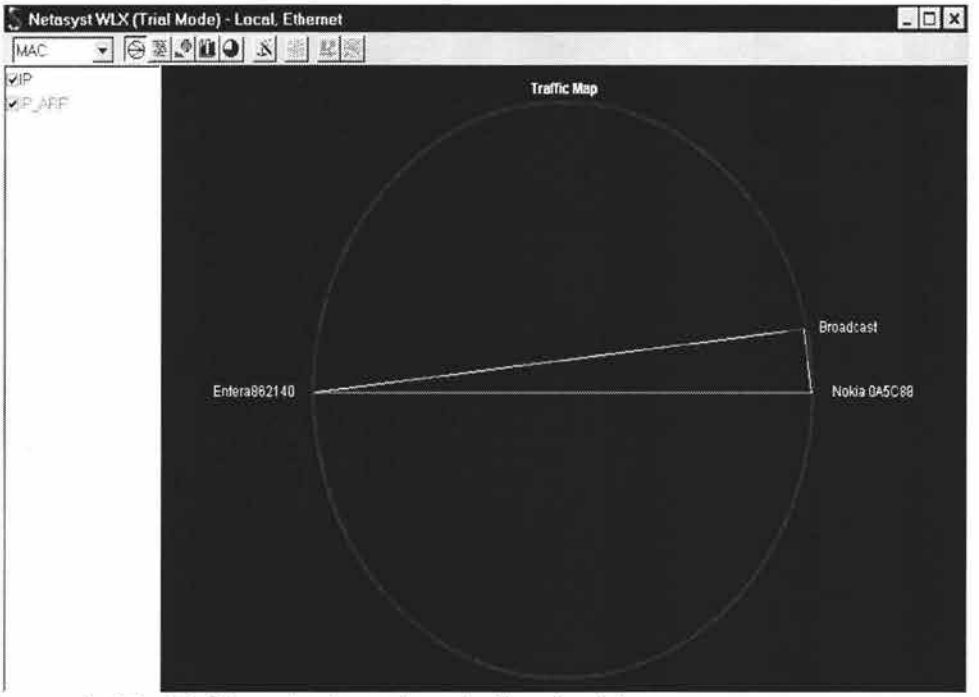


Figura 4.11: Tráfico de broadcast disminuido.

En la figura 4.12, podemos observar en comparación con la figura 2.4 del capitulo 2, que ahora las peticiones a los servidores provienen del switch central (hay que recordar que para que fuera más representativa esta grafica utilizamos "mirroring"), nuevamente comprobamos que los equipos conectados en el switch SSR central solo tienen acceso a los servidores por medio de este switch y ya no es necesario que generar tráfico de broadcast innecesario.

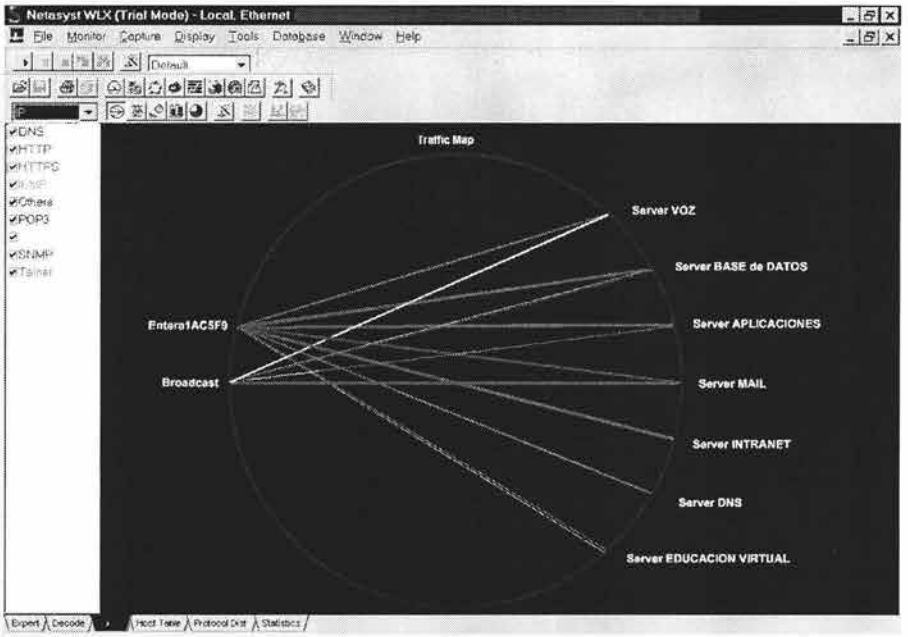


Figura 4.12: Tráfico IP después de la optimización.

Con esta parte presentada procederemos a concluir este trabajo de investigación en el capitulo número 5, asimismo, presentaremos las líneas de continuación surgirán, para este trabajo.

Capítulo 5

5.1 Conclusiones

En esta tesis se ha realizado una investigación detallada sobre los problemas que presenta una red de datos en el momento en que ésta empieza a crecer en cuanto a las necesidades de comunicación o transferencia de datos, centrada fundamentalmente en la segmentación de la red y una nueva estructura, por así decirlo, de los componentes que la integran. El principal resultado de este trabajo ha sido proponer una alternativa efectiva en lo que se refiere a optimizar una red, esto con el fin de evitar tráfico dentro de la misma para que el usuario final tenga resultados óptimos en cuanto a comunicación de datos se trate. En lo concreto, la aportación ha consistido en el diseño de la red y la realización de una red segmentada, apoyándonos en VLAN's, logrando una red funcionando eficientemente.

5.2 Aportaciones

La principal aportación desde el plano general ha sido el modelo conceptual basado en varias configuraciones dentro de la red para llegar a una red libre de tráfico y/o broadcast innecesario.

El marco que resulta, proporciona una apreciable coherencia al proceso: especificación, planeación, diseño, realización y verificación.

Con la doble intención de que sirva como ejemplo de aplicación y, a su vez, como investigación concreta, la optimización de la red de datos de la Institución Educativa aporta una línea de solución al problema de una red congestionada de tráfico y pone de manifiesto el potencial de contar con una red segmentada con una velocidad de transferencia de datos uniforme entre sus componentes. Análogamente, permite crear subredes divididas en diferentes VLAN's, separando el tráfico que circula por ésta, así mismo, logra una comunicación eficiente hacia el exterior de la red LAN, es decir, la comunicación con Internet. De esta forma mantenemos una comunicación coherente entre los equipos y servicios que proporciona la red de datos.

Los siguientes apartados muestran las aportaciones de la investigación de una forma ordenada, conforme a los distintos capítulos en las que aparecen.

Capítulo 1. Aspectos teóricos.

- Este capítulo nos aporta un conocimiento general acerca de las redes de comunicación, esto nos ayuda a comprender el funcionamiento de una red de datos y también es de utilidad para entender las diferentes tecnologías que se presentan dentro de una red de comunicaciones, específicamente, una red LAN.

Capítulo 2. Planificación de la nueva red.

- En esta parte comprendemos el funcionamiento de la red de datos LAN de la Institución Educativa, así como, el diseño inicial con el que empezamos este proyecto.
- Hacemos un análisis de los problemas que se presentan en la red y que son críticos para la comunicación entre los dispositivos, por ejemplo, la velocidad de transferencia de datos.
- Planteamos una solución adecuada a las necesidades de la red, y especificamos la manera en como se va a trabajar para lograr los objetivos.
- Hacemos un nuevo diseño de la red, esto nos permite identificar los principales componentes de la red y sus capacidades de operación.
- Finalmente identificamos las ventajas y desventajas que acarrea este nuevo diseño, así como, visualizar posibles problemas que se nos puedan presentar en el futuro.

Capítulo 3. Reconfiguracion de la red

- Especificación formal de cambios de configuración en los diferentes equipos de comunicación "frontera", esto nos permite tener una comunicación heterogénea cuando nos referimos a la velocidad de transmisión de datos.
- Propuesta de utilización de un diseño de servidores denominado DNS Split, que permite la comunicación eficiente entre la red de datos interna (LAN) hacia Internet, por medio del servidor DNS.
- Planteamos dos alternativas de "migración", esto con el fin de optar por la más adecuada para nuestro propósito.
- Especificación y configuración de las VLAN's en el equipo de comunicación SSR 2000, detallando el significado de cada línea de configuración.
- Evaluación de lo que implica haber optado por la solución que establecimos, así como, la solución de los problemas que se nos presentaron a lo largo de esta optimización.

Capítulo 4. Monitoreo y administración

- Especificamos los aspectos necesarios para la correcta administración de la red, definidos para el modelo de referencia OSI.
- Estudio de diversos campos dentro del monitoreo de una red de datos, así como, los protocolos más utilizados para la administración y monitoreo.
- Presentamos los diferentes scripts, que utilizamos para la administración y monitoreo de la red, esto con el fin de poder hacer el trabajo más eficiente y organizado.
- Finalmente presentamos un análisis de las pruebas que realizamos para este proyecto de investigación, donde observamos el comportamiento de la red actual.

5.3 Líneas de continuación

La optimización de una red de datos, abre diversas vías encaminadas a la profundización en aspectos concretos. Es por ello que, vemos la necesidad de utilizar Redes Privadas Virtuales (VPN) en un futuro cercano para poder intercomunicar los planteles que se encuentran en la Cd. De México con el Plantel Regional. Asimismo, creemos en la necesidad de dar alta importancia en el aspecto de seguridad de la red.

Finalmente, como se ha venido observando a lo largo de este trabajo de investigación, podemos concluir que los objetivos planteados al inicio del mismo, se han cumplido en su totalidad, esperando que el desarrollo de este trabajo sea una fuente de desarrollo para otras instituciones que pretendan llevar acabo una optimización similar a la planteada en esta tesis.

Apéndice A

I.I Tabla de comparación del switch principal

En esta tabla A.1 encontramos la comparación que se realizó para optar por la mejor opción en el momento de adquirir el Switch principal, esta comparación se realizó entre las marcas Enterasys Networks, Cisco y 3Com, tres de las principales marcas en el mercado.

	Enterasys SSR 2000	Cisco Catalyst 6500 Family	3Com SuperStack 3 Switch 3200 Family
Performance	- Ruteo complete para IP/IPX para tráfico de unicast y multicast. --8 Gbps non-blocking switching fabric; 9.2 Mpps routing throughput --Arriba de 16 10/100/1000 puertos operando con en modo full-duplex. --Listo para aplicaciones multicast de voz y video. -- QoS para fiabilidad punto a punto --Aplicación para balanceo y verificación de contenido.	--*Scalable performance*— Provee más de 400 Mpps performance con una arquitectura de forwarding distribuida **--Enhanced Data Voice, and Video Services** • Provee comunicacion IP a través de toda la plataforma de Cisco Catalyst 6500. • Provee puertos a una velocidad de 10/100 y 10/100/1000 • Soporta estándares de la IEEE y los propios de Cisco desarrollados con anterioridad • Soporta velocidades T1/E1 y foreign Exchange Station (FXS) de voz sobre IP (VoIP) para redes públicas switcheadas • Tiene un alto performance para aplicaciones de video y audio multicast sobre IP • Provee una administración eficiente necesaria para una escalabilidad posterior.	Capacidad de switcheo: SuperStack 3 Switch 3226, 8.8 Gbps; Switch 3250, 13.6 Gbps Forwarding rate: Switch 3226, 6.6 Mpps; Switch 3250, 10.1 Mpps Store-and-forward switching; latency <12 µs -- IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex Supports Broadcast Storm Suppression (3,000 pps threshhold)

Seguridad	--Contiene un arquitectura segura que provee filtros de capa 2/3/4 del modelo de referencia OSI	• Gigabit firewall—provee protección de acceso • Alto-performance para detección de intrusos(IDS)	IEEE 802.1X autenticación de usuarios • Autenticación RADIUS • Modo seguro (locks MAC address) Puertos basados en ACLs • Filtrado de destino IP address / mask • Una ACL por puerto • 32 únicas ACLs por switch • 32 réglas por ACL (10/100 ports) Telnet • SSH v1 (56bit DES)
Administración	El X-Pedition prove abundante funcionalidad ya que es de fácil administración a través de aplicaciones de NetSight, el cual provee una extensa configuración y monitorización de la red. NetSight esta basado en Javabased, permitiendo a los administradores de redes cualquier estación-cliente para una administración remota cualquier X-Pedition. NetSight Puede "corer" bajo los ambientes: Solaris, Windows NT and Windows 95/98/2000.	• El Modulo Gigabit Network Analysis provee una mayor infraestructura de manejabilidad y un complete monitoreo remoto de la red ya que soporta Remote Monitoring (RMON)	-- SNMP v1 -- Configuración TFTP: upload/download TFTP agent: upload -- administración remota 3Com Network Supervisor (se prove una copia con el producto) • Descubre la topología de la red • Reporte de cambios en la administración. • Capacidad de planificación. • Eventos Log • Problemas con la identificación de usuarios y troubleshooting para resolverlos • Monitoreo de utilización
Capa 3 Switching	--Best-selling modular Layer 3 --Alta velocidad en el performance con todo con todas las características	Soporta Multiprotocolos tradicionales de capa 3 para el ruteo de y provee un mecanismo de transición	Ruteo basado en Hardware para 2000 rutas IP 1,990 dinámicas y 10 estáticas para entradas de ARP (Address Resolution

	funcionando -- El primero en soportar interfaces WAN -- Control en la aplicación Pinpoint del escritorio hacia la WAN -- Filtros de seguridad Multicapa que no disminuyen el performance. --Award-winning, time-tested solution --Altamente manejable y fácil de configurar.	transparente en la empresa • Provee un soporte de hardware para la empresa y tablas de ruteo escalables • Provee soporte para IPv6 en hardware (usando Supervisor Engine 720) • Soporta MPLS en harware para permitir servicios de VPN para la empresa y facilita la integración transparente para altas velocidades para infraestructuras en el core y para hacer uso de Metro Ethernet	Protocol) Ruteo IP : 32 interfaces IP Multi-netting (multiple IP interfaces por VLAN) RIP (Routing Information Protocol), v1 and v2 • Split Horizon • Split Horizon con envenenamiento inverso • Triggered updates • MD5 autenticación de paquetes RIP • Password autenticado para paquetes RIP • Advertencias de rutas Host --Filtrado para 64 grupos multicast IGMP (Internet Group Management Protocol) snooping en interfaces de capa 2 Layer 2 IGMP v1 and v2 IGMP Querier. Protocolo de red: DHCP (Dynamic Host Configuration Protocol) Helper/Relay UDP Helper ARP, ARP Proxy
Soporte para Vlan's	Mas de 4,000 VLANs, 2,000 filtros de seguridad. Adicionalmente el X-Pedition 2000 provee capacidades mayores a muchas soluciones de switcheo en capa 3 disponibles hoy en día, soporta arriba de 50,000 rutas, 256,000 aplicaciones flows y 240,000 direcciones MAC de capa 2. El X-Pedition 2000 puede	802.1Q and 802.1Q tunneling (QinQ) provee point-to-point y multipoint Servicios Ethernet • EoMPLS en MPLS backbones para una mayor escalabilidad en la red proveyendo LAN Virtual(VLAN) capacidad de traducción	Soporta más de 2,000 rutas externas, permitiendo que el switcheo crezca conforme la red va incrementando su tamaño–ideal para crecimiento en la frontera de la red. Soporta más de 255 VLANs y estándares basados en el IEEE 802.3ad trunking (LACP).

	también ser posicionado en capa 2/3/4 para un servicio de balanceo en el switcheo. Los servidores pueden ser conectados vía 1000Base-SX, extendiendo así el control en las aplicaciones y proveyendo un balanceo a través de múltiples servidores.		
Estándares soportados	IEEE 802.1p IEEE 802.1Q IEEE 802.1d Spanning Tree IEEE 802.3 IEEE 802.3u IEEE 802.3x IEEE 802.3z RFC 1213 - MIB-2 RFC 1493 - Bridge MIB RFC 1573 - Interfaces MIB RFC 1643 - Ethernet-like Interface MIB RFC 1163 - A Border-Gateway Protocol (BGP) RFC 1267 - BGP-3 RFC 1771 - BGP-4 RFC 1657 - BGP-4 MIB RFC 1058 - RIP v1 RFC 1723 - RIP v2 Carrying Additional Information RFC 1724 - RIP v2 MIB RFC 1757 - RMON RFC 1583 - OSPF Version 2 RFC 1253 - OSPF v2 MIB RFC 2096 - IP Forwarding MIB RFC 1812 - Router Requirements RFC 1519 - CIDR RFC 1157 - SNMP RFC 2021 - RMON2 RFC 2068 - HTTP RFC 1717 - The PPP Multilink Protocol RFC 1661 - PPP (Point to Point Protocol) RFC 1634 - IPXWAN RFC 1662 - PPP in HDLC Framing RFC 1490 - Multiprotocol	**IEEE Compliance** 802.1d Bridging 802.1p, q VLAN tagging 802.1s Per-VLAN Group Spanning Tree Protocol 802.1w Rapid Spanning Tree Protocol 802.1x 802.3 10BASE-T, 10BASE-FL 802.3ad Link aggregation 802.3ab 1000BASE-T 802.3ae 10 Gigabit Ethernet 802.3af Power over Ethernet (PoE) 802.3u 100BASE-TX, 100BASE-FX 802.3x Flow control 802.3z 1000BASE-SX, 1000BASE-LX **RFC Compliance** 1483, 2584 Protocol encapsulation over ATM AAL-5 768 User Datagram Protocol (UDP) 783 Trivial File Transfer Protocol (TFTP) 791 IP 792 Internet Control Message Protocol (ICMP) 793 TCP 826 Address Resolution Protocol (ARP) 854 Telnet	IEEE 802.1p (CoS) IEEE 802.1Q (VLANs) IEEE 802.1w (RSTP) IEEE 802.1X (Security) IEEE 802.3ab (Copper Gigabit) IEEE 802.3ad (Link Aggregation) IEEE 802.3i (10BASE-T) IEEE 802.3u (Fast Ethernet) IEEE 802.3x (Flow Control) IEEE 802.3z (Fiber Gigabit) RFC 1812 (IPv4) RFC 1518, 1519 (CIDR) RFC 826 (ARP) RFC 783 (TFTP) RFC 768 (UDP) RFC 791 (IP) RFC 793 (TCP) RFC 2474 (DiffServ) RFC 2131 (DHCP) RFC 1058 (RIP v1) RFC1723 (RIP v2) RFC 2138 (Radius Authentication) RFC 2139 (Radius Accounting) RFC 1157 (SNMP v1/v2c) RFC 1213 (MIB II) RFC 1398 Ethernet MIB RFC 1493 (Bridge MIB) RFC 1573 (Private IF MIB) RFC 1724 (RIP V2 MIB Extension) RFC 1757 RMON MIB RFC 2011 IP-MIB RFC 2012 TCP-MIB RFC 2013 UDP-MIB RFC 2037 Entity MIB RFC 2618 (RADIUS Authentication Client MIB) RFC 2665 Ethernet-MIB RFC 2674P P-BRIDGE-MIB RFC 2674Q Q-BRIDGE-MIB RFC 2737 Entity MIB RFC 2819 RMON MIB RFC 2863 IF-MIB IEEE8021-PAE-MIB (IEEE) (Network Login) Router MIB

	Interconnect Over Frame Relay	894 IP over Ethernet 903 Reverse Address Resolution Protocol (RARP) 782 VLAN Trunking Protocol (VTP) 783 TFTP 1157 Simple Network Management Protocol (SNMP)v1 2613 RMON analysis for switched networks (SMON) MIB 2668 802.3 media attachment unit (MAU) MIB 2787 VRRP MIB 2925 Ping/Traceroute/NS Lookup MIB 1492 Terminal Access Controller Access Control System Plus (TACACS+) 2138 Remote Authentication Dial-In User Service (RADIUS) authentication

Tabla A.1: Comparación de Switch principal.

I.II Tabla de comparación de Switch secundario

En la tabla A.2 encontramos la comparación de equipos de comunicaciones (Switch secundario), donde encontramos las principales características de estos equipos de las siguientes marcas: Enterasys, Alcatel y Extreme Networks.

	Enterasys Vertical Horizon 2402S	**Alcatel OmniStack 6024**	**Extreme Networks Summit 24/48/48i**
Características Físicas			
Tamaño	2.5" (1.5 RU) H x 17.37" W x 11.22" D	2.53" (1.5 RU) H x 17.37" W x 11.22" D	Summit24 & 48: 3.50" (2.0 RU) H x 17.32" W x 17.42" D; Summit48i: 3.50" (2.0 RU)

			H x 17.25" W x 20.0" D
Performance			
Raw Switching Capacity (Gbps)	4.8 Gbps	4.8 Gbps	17.5 Gbps
Switching Throughput (Gbps)	2.4 Gbps	2.4 Gbps	8.75 Gbps
Forwarding Rates (Mpps)	6.55 Mpps	8 Mpps	Summit 24: 5.1 Mpps, Summit 48, Summit 48i: 10.1 Mpps
Backplane Width (Gbps)	16 Gbps	10 Gbps	17.5 Gbps
64 Byte capa 2 Packet Latency	10/100 to 10/100 L2 Latency is 7 microseconds; 1000 Mbps to 1000 Mbps is <1 microsecond	8 us	3 us
Administración			
RMON/SMON	Statistics, History, Alarm, and Event	Statistics, History, Alarm, and Event	Statistics, History, Alarm, and Event
Interfaz de administración	Single Logical Unit	Single Logical Unit	Single Logical Unit
Capacidades para Port Mirroring	Soporta un grupo mirror hacia otro puerto, pero no acepta mirroring remoto	Soporta un grupo mirror hacia otro puerto, pero no acepta mirroring remoto	No hay limite para el número de puertos físicos que pueden ser direccionados como Puertos sencillos.
Code Flash Memory	2 MB of flash memory	2 MB of flash memory	4 MB of flash memory

Code Images Supported	1	1	2
Opciones para administracion	SNMP, An Embedded Web HTTP Server, Telnet y administración vía un Puerto de la consola.	SNMP, Web-based, Telnet, Serial	SNMP, Web-Based, Telnet, Serial, SSH2, RADIUS, TACACS+

Tabla A.2: Comparativo del Switch secundario de distribución DMZ.

I.III Tabla de ventajas y desventajas del switch secundario

A continuación, en la tabla A.3 mostramos las ventajas y desventajas del equipo de comunicaciones switch secundario.

	Desventajas	Ventajas
Enterasys Vertical Horizon 2402S	• The Vertical Horizon 2402S no soporta ATM uplinks.	• El objetivo del 2402S son redes Ethernet. La carencia de soporte para ATM significa una disminución considerable del producto.
	• Vertical Horizon 2402S no soporta inteligencia para capa 3.	• El switch Vertical Horizon 2402S puede ser conectado a un dispositivo de capa 3 en el core. Esto minimiza los costos.
Alcatel OmniStack 6024	• El precio del OmniStack 6024 es alto; los usuarios deben pagar por módulos de stackeo y también para slots de expansión.	• El OmniStack 6024 puede ser estackeable, soporta 24-96 puertos en incrementos de 24 puertos. El estaqueo esta disponible mientras se deje un puerto libre para expansión.
	•El precio del OmniStack	•El precio del OmniStack

	6024 se eleva especialmente cuando se añaden gigabit uplinks.	6024 has tiene un elevado costo por Puerto, pero considerando las características y funcionalidad el precio es mucho mejor en comparación con otros productos del mismo calibre.
	• El switch OmniStack 6024 no soporta inteligencia para capa 3 del modelo OSI.	• El switch Vertical Horizon 2402S puede ser conectado a un dispositivo de capa 3 en el core. Esto minimiza los costos.
Extreme Networks Summit 24/48/48i	• Los switches Summit 24/48 y 48i son demasiado caros en comparación con otros desktop switches.	• El precio que se paga por este equipo puede es justo ya que este switch soporta funcionalidad para la capa 3 del modelo OSI incrementando el performance.
	• Los switches Summit 24/48 and 48i no tienen funcionalidad para expansión o estaqueo.	• Los productos Summit pueden ser expandibles por medio de puertos GBIC. Los puertos GBIC incrementan la funcionalidad y el performance el equipo.
	• La serie Summit series requiere un costo adicional para añadir la funcionalidad para capa 3 del modelo OSI.	•Si el usuario no requiere funcionalidad para capa 3 no tienen que pagar un costo adicional.

Tabla A.3: Ventajas y Desventajas de los switches secundarios de distribución DMZ.

Apéndice B

II Líneas de configuración de los equipos de comunicación

Proceso de configuración del Smart Switch Router (SSR) 2000 de la red de la Institución

Este documento presenta la descripción de las líneas de configuración actuales contenidas en el equipo central Smart Switch Router 2000 de la red de datos de la Institución plantel Principal

Esto es un primer proceso de migración en el cual se describen las líneas más importantes de configuración.

Running system configuration:

```
    !
    !  Last modified from Telnet (172.16.1.16) on 2003-10-18 14:46:59
    !
1 : port set et.1.5 speed 10Mbps duplex half auto-negotiation off
    !
 2 : vlan create LANDMZ ip id 30
 3 : vlan create INTERNA ip id 31
 4 : vlan create WANINTERNET ip id 32
 5 : vlan add ports et.3.(1-8) to LANDMZ
 6 : vlan add ports et.1.1 to WANINTERNET
 7 : vlan add ports et.1.(2-8),et.2.(1-6) to INTERNA
    !
 8 : interface create ip WANINTERNET address-netmask 172.16.4.253/24
vlan WANINTERNET up
 9 : interface create ip INTERNA address-netmask 172.16.254/24 vlan
INTERNA up
10 : interface add ip INTERNA address-netmask 172.16.254/24
11 : interface add ip INTERNA address-netmask 168.16.3.254/24
12 : interface add ip INTERNA address-netmask 172.16.5.254/24
13 : interface add ip INTERNA address-netmask 172.16.6.254/24
14 : interface add ip INTERNA address-netmask 172.16.7.254/24
15 : interface add ip INTERNA address-netmask 172.16.8.254/24
16 : interface add ip INTERNA address-netmask 172.16.9.254/24
17 : interface add ip INTERNA address-netmask 172.16.10.254/24
18 : interface add ip INTERNA address-netmask 172.16.11.254/24
19 : interface add ip INTERNA address-netmask 172.16.12.254/24
20 : interface add ip INTERNA address-netmask 172.16.13.254/24
21 : interface add ip INTERNA address-netmask 172.16.14.254/24
22 : interface add ip INTERNA address-netmask 172.16.15.254/24
    !
23 : ip add route default gateway 168.1.4.254
    !
24 : port mirroring monitor-port et.2.8 target-port et.3.1
```

!
25 : ip helper-address interface INTERNA 172.16.2.241 135
26 : ip helper-address interface INTERNA 172.16.2.241 137
27 : ip helper-address interface INTERNA 172.16.2.241 139
28 : ip helper-address interface INTERNA 172.16.2.241 445
29 : ip helper-address interface INTERNA 172.16.2.241 138

Descripción de las líneas de configuración.

Running system configuration:
!
! Last modified from Telnet (172.16.1.16) on 2003-06-18 14:46:59

Estas primeras líneas hacen referencia a dos puntos importantes: el primero de ellos corresponde al tipo de configuración que se esta desplegando. Cabe mencionar que existen dos tipos de configuraciones la que se encuentra corriendo y funcionando en el equipo actualmente (running) y la que se encuentra guardada en el archivo de configuración y que es con la que inicia al encenderse el equipo (startup).

El segundo punto para tomar en cuenta es que la configuración corriente se encuentra almacenada en una memoria RAM y cuando se modifica algo de la configuración y se teclea el comando ***save active*** los cambios se aplicarán instantáneamente y se podrán ver en la configuración corriente con el comando ***show***. Los cambios que se realicen no se grabaran en la configuración startup hasta que se teclee el comando ***save startup***, que reemplazara el archivo de configuración antiguo por el que se acaba de modificar y lo almacenará en una memoria de tipo NVRAM.

Por lo anterior, la primera línea nos representa que la configuración que se va a utilizar corresponde a la running.

A su vez, podemos observar que el equipo nos presenta información en la línea siguiente acerca de los últimos cambios que se realizaron.

Podemos observar que la última modificación en el equipo se hizo vía telnet, la dirección IP desde donde se realizó, la fecha y la hora del cambio.

1 : port set et.1.5 speed 10Mbps duplex half auto-negotiation off

La línea anterior "amarra" el Puerto Ethernet 1.5 10Mbps en half-duplex además de apagar la auto negociación en el puerto. Esto se colocó debido a problemas con uno de los servidores para realizar la autonegociación y "engancharse" a 100Mbps.

2 : vlan create LANDMZ ip id 30

La línea 2 crea un VLAN con nombre LANDMZ y con un identificador 30. El nombre y el identificador son aleatorios.

3 : vlan create INTERNA ip id 31

Crea una VLAN con el nombre INTERNA y con el identificador 31.

4 : vlan create WANINTERNET ip id 32

Crea una VLAN con el nombre WANINTERNET con el identificador 32

5 : vlan add ports et.3.(1-8) to LANDMZ

Agrega los puertos Ethernet del 3.1 al 3.8 a la VLAN llamada LANDMZ

6 : vlan add ports et.1.1 to WANINTERNET

Agrega el puerto Ethernet 1.1 a la VLAN llamada WANINTERNET

7 : vlan add ports et.1.(2-8),et.2.(1-6) to INTERNA

Agrega los puertos Ethernet del 1.2 al 1.8 y del 2.1 al 2.6 a la VLAN denominada INTERNA.

8 : interface create ip WANINTERNET address-netmask 172.16.4.253/24 vlan WANINTERNET up

Crea una interfase lógica llamada WANINTERNET a la cual se le asigna una dirección ip 168.1.4.253 con máscara de 24 bits.

Esta interfaz es la que permite la comunicación entre el SSR y el Firewall Nokia, de ahí el nombre de WANINTERNET.

9 : interface create ip INTERNA address-netmask 172.16.1.254/24 vlan INTERNA up

Crea una interfase lógica llamada INTERNA a la cual se le asigna una dirección ip 172.16.1.254 con máscara de 24 bits.

Esta interfaz es la correspondiente a la red LAN de la Institución.

10 : interface add ip INTERNA address-netmask 172.16.2.254/24
11 : interface add ip INTERNA address-netmask 172.16.3.254/24
12 : interface add ip INTERNA address-netmask 172.16.5.254/24
13 : interface add ip INTERNA address-netmask 172.16.6.254/24
14 : interface add ip INTERNA address-netmask 172.16.7.254/24
15 : interface add ip INTERNA address-netmask 172.16.8.254/24
16 : interface add ip INTERNA address-netmask 172.16.9.254/24
17 : interface add ip INTERNA address-netmask 172.16.10.254/24
18 : interface add ip INTERNA address-netmask 172.16.11.254/24
19 : interface add ip INTERNA address-netmask 172.16.12.254/24
20 : interface add ip INTERNA address-netmask 172.16.13.254/24
21 : interface add ip INTERNA address-netmask 172.16.14.254/24
22 : interface add ip INTERNA address-netmask 172.16.15.254/24

De las líneas 10 a la 22 se asignan direcciones secundarias a la interfaz lógica INTERNA creada anteriormente. Esto permite que el equipo maneje 15 segmentos de red distintos con máscara de 24 bits.

23 : ip add route default gateway 172.16.4.254

La línea 23 es la correspondiente al default gateway del equipo. Esta línea establece que todas las peticiones que el equipo desconozca serán enviadas a esta dirección ip que corresponde a la interfaz que interconecta al firewall con el SSR.

24 : port mirroring monitor-port et.2.8 target-port et.3.1

Esta línea realiza un puerto "espejo" en el puerto 2.8 del tráfico que pasa por el puerto 3.1. Esta configuración se colocó con la finalidad de "montar" un sniffer y llevar a cabo un análisis del tráfico que pasa por ese punto de la red.

25 : ip helper-address interface INTERNA 172.16.2.241 135
26 : ip helper-address interface INTERNA 172.16.2.241 137
27 : ip helper-address interface INTERNA 172.16.2.241 139
28 : ip helper-address interface INTERNA 172.16.2.241 445
29 : ip helper-address interface INTERNA 172.16.2.241 138

Las últimas líneas de la configuración permiten que todas las peticiones de capa 2 (modelo de referencia OSI data-link) de puertos específicos sean enviadas a una dirección IP. Esto permite el "mapeo" de direcciones IP con los nombres del servidor de aplicaciones de la Institución.

Los puertos especificados se refieren a:

135	TCP	epmap	loc-srv	DCE endpoint resolution
135	UDP	epmap	loc-srv	DCE endpoint resolution
137	TCP	netbios-ns	nbname	NETBIOS Name Service
137	UDP	netbios-ns	nbname	NETBIOS Name Service
138	UDP	netbios-dgm	nbdatagram	NETBIOS Datagram Service
139	TCP	netbios-ssn	nbsession	NETBIOS Session Service

445	TCP			Microsoft CIFS
445	UDP			Microsoft CIFS

Estas líneas de configuración son creadas para permitir la comunicación entre los clientes de la red de la Institución, ya que debido a la segmentación los clientes no pueden comunicarse en capas superiores a la 3 (Network layer) del modelo de referencia OSI.

Líneas de configuración para dar solución al problema que se presento en el capitulo 3.

```
switch(config)# show
Running system configuration:
    !
    ! Last modified from Telnet (172.16.6.4) on 2004-02-21 10:58:29
    !
 1 : port set et.1.5 speed 10Mbps duplex half auto-negotiation off
 2 : port set et.1.1 auto-negotiation off speed 100Mbps duplex full
 3 : port set et.3.7 duplex full speed 100Mbps
 4 : port set et.3.8 duplex full speed 100Mbps
    !
 5 : vlan make trunk-port et.1.2
 6 : vlan create LANDMZ ip id 30
 7 : vlan create INTERNA ip id 31
 8 : vlan create WANINTERNET ip id 32
 9 : vlan create INFORMATICA ip id 106
10 : vlan create test ip id 200
11 : vlan create MERCADOTECNIA ip id 107
12 : vlan create DOCENCIA ip id 110
13 : vlan create FINANZAS ip id 109
14 : vlan create LAB. COMPUTADORAS 1_1 ip id 113
15 : vlan create LAB. COMPUTADORAS 2_2 ip id 114
16 : vlan create SERVICIOS ESCOLARES ip id 108
17 : vlan create VENTAS ip id 111
18 : vlan create CONTA bridged-protocols id 214
19 : vlan create POSGRADO ip id 116
20 : vlan create BACHILLERATO ip id 115
21 : vlan create BACHILLERATO ip id 112
22 : vlan create internet port-based id 100
23 : vlan add ports et.1.1 to WANINTERNET
24 : vlan add ports et.2.7 to WANINTERNET
25 : vlan add ports et.1.3 to INTERNA
26 : vlan add ports et.1.4 to INTERNA
27 : vlan add ports et.1.5 to INTERNA
28 : vlan add ports et.1.6 to INTERNA
29 : vlan add ports et.1.7 to INFORMATICA
30C: !!vlan add ports et.3.6 to LANDMZ
31C: !!vlan add ports et.3.7 to LANDMZ
32C: !!vlan add ports et.3.8 to LANDMZ
33 : vlan add ports et.2.2 to MERCADOTECNIA
34 : vlan add ports et.2.3 to DOCENCIA
35 : vlan add ports et.1.8 to FINANZAS
36 : vlan add ports et.2.6 to LAB. COMPUTADORAS 1
```

37 : vlan add ports et.2.5 to LAB. COMPUTADORAS 2
38 : vlan add ports et.2.1 to SERVICIOS ESCOLARES
39 : vlan add ports et.2.4 to VENTAS
40 : vlan add ports et.1.2 to POSGRADO
41 : vlan add ports et.1.2 to BACHILLERATO
42 : vlan add ports et.1.2 to BACHILLERATO
43 : vlan add ports et.2.5 to CONTA
44 : vlan add ports et.2.8 to WANINTERNET
45 : vlan add ports et.3.6 to internet
46 : vlan add ports et.3.7 to internet
47 : vlan add ports et.3.8 to internet
48 : vlan add ports et.3.5 to INFORMATICA
49 : vlan add ports et.3.1 to INTERNA
50 : vlan add ports et.3.2 to INTERNA
51 : vlan add ports et.3.3 to INTERNA
52 : vlan add ports et.3.4 to WANINTERNET
!
53 : interface create ip WANINTERNET address-netmask 172.16.4.253/24 vlan WANINTERNET up
54 : interface create ip INTERNA address-netmask 172.16.1.254/24 vlan INTERNA up
55 : interface create ip INFORMATICA address-netmask 172.16.6.254/24 vlan INFORMATICA
56 : interface create ip test address-netmask 172.16.200.254/24 vlan test
57 : interface create ip MERCADOTECNIA address-netmask 172.16.7.254/24 vlan MERCADOTECNIA
58 : interface create ip DOCENCIA address-netmask 172.16.10.254/24 vlan DOCENCIA
59 : interface create ip FINANZAS address-netmask 172.16.9.254/24 vlan FINANZAS
60 : interface create ip PRINCIPAL address-netmask 172.16.13.254/24 vlan LAB. COMPUTADORAS 1
61 : interface create ip LAB. COMPUTADORAS 1 address-netmask 172.16.14.254 /24 vlan LAB. COMPUTADORAS 1
62 : interface create ip SERVICIOS ESCOLARES address-netmask 172.16.8.254/24 vlan SERVICIOS ESCOLARES
63 : interface create ip VENTAS address-netmask 172.16.11.254/24 vlan VENTAS
64 : interface create ip POSGRADO address-netmask 172.16.16.254/24 vlan POSGRADO
65 : interface create ip BACHILLERATO address-netmask 172.16.15.254/24 vlan BACHILLERATO
66 : interface create ip BACHILLERATO address-netmask 172.16.12.254/24 vlan BACHILLERATO
67 : interface add ip INTERNA address-netmask 172.16.2.254/24
68 : interface add ip INTERNA address-netmask 172.16.3.254/24
!
69 : system set syslog server 172.16.6.4 level info buffer-size 200
!
70 : ip add route default gateway 172.16.4.254
!
71 : port mirroring monitor-port et.3.6 target-port et.3.8
!

```
72 : ip helper-address interface test 172.16.241 1759
73 : ip helper-address interface INFORMATICA 172.16.2.241 1759
74 : ip helper-address interface LAB. COMPUTADORAS 1 172.16.2.241 1759
75 : ip helper-address interface LAB. COMPUTADORAS 1 172.16.2.241 1759
   !
76 : system set hashed-password login
77 : system set hashed-password
78 : system set name INSTEDU-LAN
   !
79 : snmp set community  privilege read
80 : snmp set community adm privilege read-write
   !
81 : rmon set ports et.1.2
82 : rmon set standard default-tables yes
83 : rmon set lite default-tables yes
84E: rmon set memory 20
85 : rmon enable
   !
86 : port description et.1.1 WANINTERNET
87 : port description et.2.7 WANINTERNET
88 : port description et.1.7 INFORMATICA
89 : port description et.2.2 MERCADOTECNIA
90 : port description et.2.3 DOCENCIA
91 : port description et.1.8 FINANZAS
92 : port description et.2.6 LAB. COMPUTADORAS 1
93 : port description et.2.5 LAB. COMPUTADORAS 1
94 : port description et.2.1 SERVICIOS ESCOLARES
95 : port description et.2.4 VENTAS
96 : port description et.1.3 VH(WINS-VOZ)
97 : port description et.1.2 ANEXO POSGRADO-ANEXO
BACHILLERATO(SCA-LISTAS)
98 : port description et.2.8 WANINTERNET_Websense
99 : port description et.3.4 WANINTERNET_Websense
LAN(config)# search ?
 [search-string]         - String to search for
                       requires a value of this type:
  character string      - A character string
LAN(config)# search et.3.1
49 : vlan add ports et.3.1 to INTERNA
LAN(config)# search et.3.2
50 : vlan add ports et.3.2 to INTERNA
LAN(config)# search et.3.3
51 : vlan add ports et.3.3 to INTERNA
switch(config)#
```

Apéndice C

En esta sección presentamos los Scripts de configuración de los equipos de comunicación, esto es de utilidad para mantener una administración eficiente y optima.

III.I Script para creación de puerto espejo Comandos en el equipo SSR2000

1.- Desde un equipo de la red 6 Rack de sistemas, abrir una ventana de comando y hacer un telnet a la dirección XXX.XXX.XXX.XXX. Este es el default Gateway de cualquier equipo de la red 6 ejemplo: XXX.XXX.XXX.XXX (Ver Figura C.1).

Figura C.1: Telnet al default gateway.

2.- Nos pedirá un password para entrar como usuario de consulta. Este usuario nos permitirá ver la configuración del equipo, algunos parámetros, pero no permitirá hacer modificaciones a la configuración. El prompt de este usuario es > (Ver Figura C.2)

Figura C.2: Pantalla donde es requerido un password y un login.

3.-Después de estar con el usuario > tecleamos el comando enable o solo en, y le damos enter, nos pedirá un password para entrar como usuario de administración. Con este usuario nos aparecerá el prompt #, este usuario tiene más privilegios que el primer usuario, pero no los suficientes para modificar la configuración.

4.-Con el prompt # (usuario de administración) le damos la palabra configure y pulsamos enter, nos aparecerá el prompt (config) #, en esos momentos estaremos como usuario de configuración y podremos modificar la configuración del equipo. (Ver Figura C.3).

Figura C.3: Sesión para configurar el equipo.

5.- Con el comando show y enter dentro de este usuario nos mostrará la configuración del equipo.
Es importante ubicar el número de la parte izquierda, ya que ese número indica la línea de configuración.
Nota.- si este número no se tiene bien ubicado se podría afectar otro servicio (servidor o algún enlace) (Ver Figura C.4).

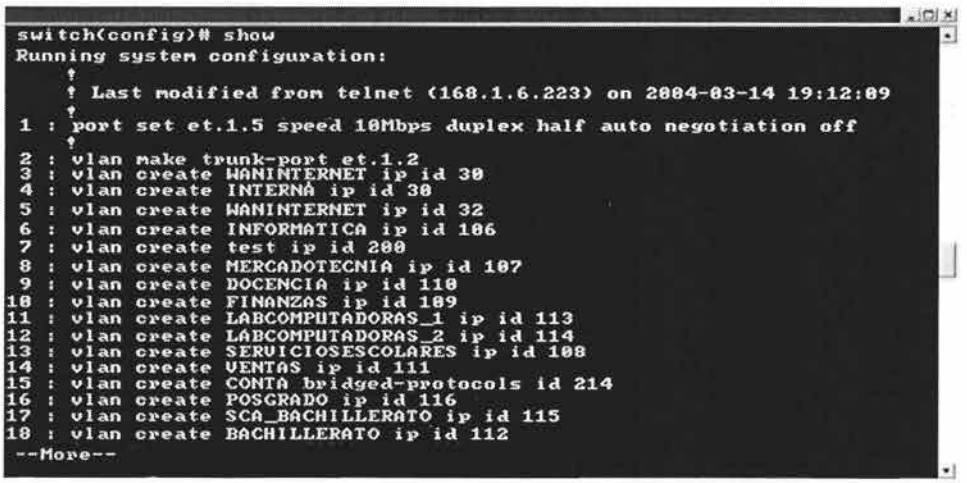


Figura C.4: Líneas de configuración.

6.-Con el comando search podemos identificar la línea de configuración que contenga el puerto al cual queremos hacer "espejo" (mirroring). Ejemplo: (config) #search et.2.4. Esto quiere decir que nos identifique la línea donde se encuentre declarado el puerto 4 del slot 2.

7.-De la misma forma buscamos el puerto del cual se quiere ser espejo. Ejemplo: (config) #search et.1.1. Esto quiere decir que nos identifique la línea donde se encuentre declarado el puerto 1 del slot 1. Puerto del que se quiere ser espejo (Ver Figura C.5)

Figura C.5: Comando Search.

8.-Ahora invalidaremos la línea de configuración del puerto que haremos espejo. Esto por que ahora le daremos la tarea de ser espejo de otro. (config) #negate 40. (Donde 40 es el número de la línea de configuración) (Ver Figura C.6)

Figura C.6: Invalidación de las líneas de configuración.

9.-Después de que neguemos la línea, y en general cuando hagamos cualquier tipo de modificación a la configuración del equipo tendremos que verificar que lo que hicimos esta correcto. Ejemplo: (config) #show scrachtpad
Este comando nos desplegará lo que estamos a punto de modificar, es una manera de confirmar estas modificaciones. (Ver Figura C.7)

Figura C.7: Comando: show scrachtpad.

10.- Ahora, para que el cambio tenga efecto en el equipo, esto es, se grabe en RAM se utiliza el comando save active: (configure) #save active
En el momento que demos este comando y le demos enter, nuestra configuración tomará efecto (Ver Figura C.8)

Figura C.8: Grabamos los cambios.

11.- Ahora si, después de tener el puerto que haremos espejo sin ningún servicio, es decir, libre, configuramos de quien será el puerto espejo.
Ejemplo: (config) #port mirroring monitor-port et.2.4 target-port et.1.1
Esto quiere decir que el puerto 2.4 será espejo de todo el tráfico que pase por el puerto 1.1 (Ver Figura C.9)

Figura C.9: Puerto espejo configurado.

12.-Después de que declaremos la línea de configuración del puerto espejo, repetiremos el punto 9 verificaremos nuestros cambios con show scrachtpad.
Ejemplo: (config) #show scrachtpad
Este comando nos desplegará lo que estamos a punto de modificar, es una manera de confirmar estas modificaciones.

13.- Estando seguros de nuestra configuración, repetiremos el punto 10, para se grabe en RAM se utiliza el comando save active:
(configure) #save active
En el momento que demos este comando y le demos enter, nuestra configuración tomará efecto.

14.- Para este ejemplo nuestro puerto et.2.4 será espejo del tráfico del puerto et.1.1.

III.II Actualización de Firmware y Configuración de VLAN's y Qtrunk

Equipos de Comunicación Anexo Bachillerato.

1.-Management Menú.

1.1.-Nos conectaremos a los equipos en los cuales se actualizara el firmware vía consola, esto es, al modulo de administración directamente con ayuda de un cable DB9, también se necesitara de una terminal grafica ("Tera Term"), o basta con una conexión de Hyperterminal.

Una vez conectados al modulo de administración de los equipos entraremos al menú "**Management Setup Menu**" . Escogemos la opción **TFTP Download Agent F/W** como se muestra en la figura C.10.

Figura C.10: Management Setup Menu.

2.-Dentro del menú **TFTP Download Agent F/W**

2.1.- **En** la opción Download Server IP, daremos de alta el servidor que servirá para bajar el firmware, en este caso será la computadora en la cual previamente se habrá bajado el firmware, a ésta computadora le configuraremos una dirección IP del mismo segmento del equipo al cual se le actualizara el firmware, ejemplo:
Equipo que hará la función de Servidor : **168.1.15.30**
Equipo al cual se le actualizara el Firmware : **168.1.15.252**

2.2.-En el servidor copiaremos el nombre exacto del firmware para posteriormente pegarlo en la opción Download Filename dentro de este mismo menú. (Ver Figura C.11)

Figura C.11: Nombre del Firmware.

3.-TFTP Server

3.1.-Para la Actualización del Firmware es necesario tener instalado un servidor TFTP ("Solar Winds"), en el equipo que servirá como servidor, así como, también una terminal grafica amigable como se menciono en el punto número 2 para que podamos observar el momento en el cual el firmware esta siendo instalado y el equipo esta reiniciando. (Ver Figura C.12)

Figura C.12: Servidor TFTP.

4.-Encendido y apagado del equipo

4.1.-Al término de la actualización del firmware, tendremos que ir al menú principal "Main Menu"y nos iremos a la opción: **System Restart Menú** (Ver Figura C.13)

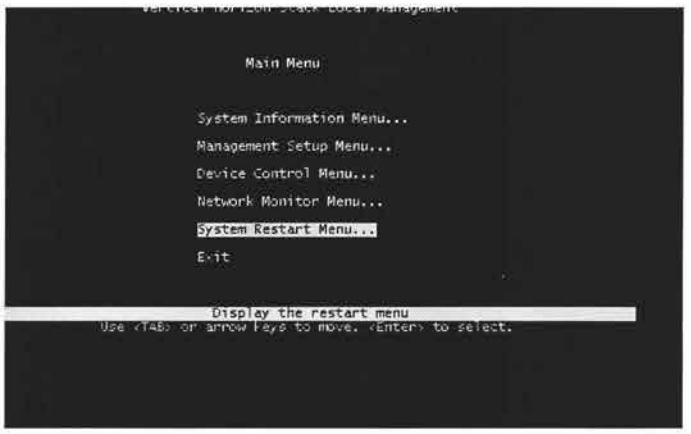


Figura C.13: System Restart Menu.

5.-Opciones Para el Encendido y Apagado del equipo, con el Nuevo Firmware

5.1.- Se habilitaran con la palabra **YES** las opciones **POST** y **Reload Factory Defaults**, esto para que los equipos tomen sus valores de fábrica y el equipo sea configurado nuevamente. (Ver Figura C.14)

Figura C.14: Restart System.

6.-Reconfiguración del equipo.

6.1.-En este punto comenzara la reconfiguración de los equipos, para lo cual, nos iremos al menú principal **"Main Menu"**, posteriormente escogeremos el submenú **"Device Control Menu"**, como se muestra en la figura C.15.

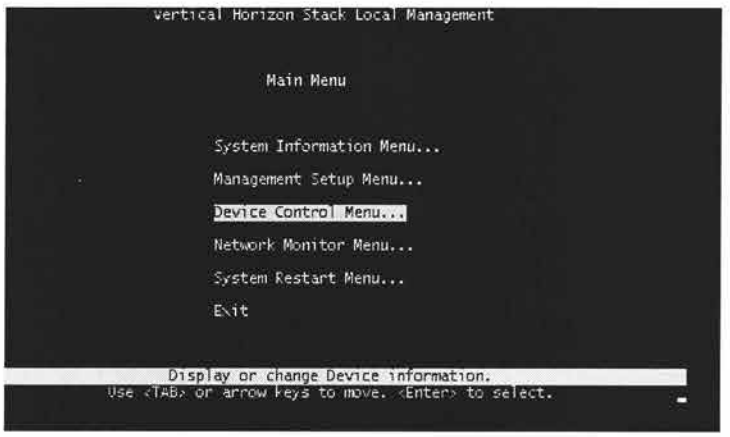


Figura C.15: Main Menu.

6.2.- Dentro del submenú: **Device Control Menú** escogeremos la opción: **Port Assignment VLAN Configuration** (Ver Figura C.16).

Figura C.16: Device Control Menu.

7.-Declaración de VLAN's

7.1-En esta sección se declararan todos los puertos con la vlan que le corresponde, en este caso, a estos equipos se les declara un PVID 115, esto por que es una vlan 15, es importante resaltar que esto se tiene que declarar para cada uno de los puertos en los cuales se a alojar esta vlan. (Ver Figura C.17)

Figura C.17: Declaración de VLAN's.

8.-Declaración de Puertos Qtrunk

8.1.-En estos equipos se tienen que declarar puertos 802.1Qtrunk, esto porque, por esos puertos pasara tráfico de más de una vlan ejemplo: en el Switch 1 puerto 24 es un puerto al cual se conecta otra vlan, que en este caso, es otro grupo de equipos de comunicación con la vlan 12. (Ver Figura C.18).

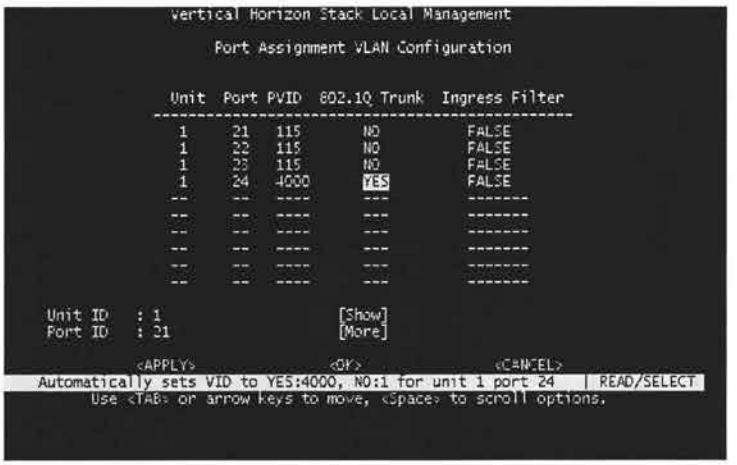


Figura C.18: Declaración de puertos 802.1qtrunk.

8.2.-Ahora se declarará el puerto 802.1Qtrunk por el cual pasara tráfico de ambas vlans, y el cual nos ayudara para enlazarnos al IDF principal, pasando previamente por una comunicación wireless Outdoor. (Ver Figura C.19).

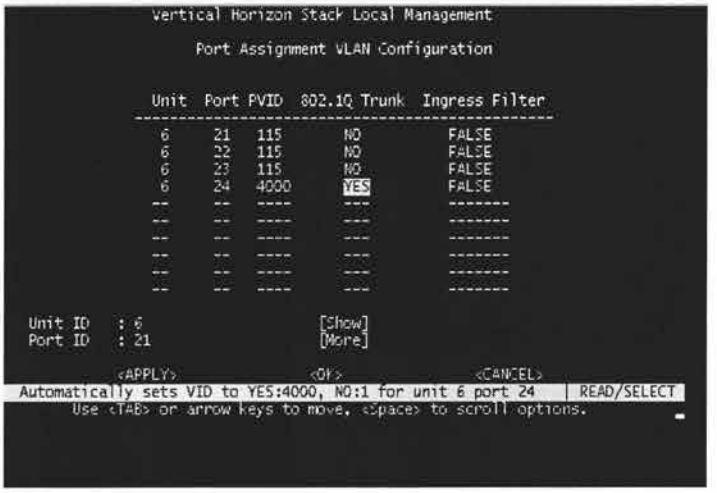


Figura C.19: Declaración de puerto por el cual nos enlazamos al IDF principal.

Estos ejemplos de scripts, son solo algunos de los muchos que manejamos dentro de la red de la Institución, como se menciono anteriormente esto nos permite una administración confiable y de una manera sistemática y no centralizada.

Referencias Bibliograficas

(Apachon D, 2003)
Ing. Álvaro Apachon D, La Evolución en la Arquitectura de las Redes, Sistemas y Telemática Universidad ICESI Revista No. 1. pp 89-100. Enero - Junio de 2003

(BLACK, 1995)
BLACK, Uyless REDES DE COMPUTADORES Protocolos, Normas e Interfaces Coedición: Alfaomega-Rama , 2ª Ed. 1995.

(González Fernández, 1998)
Jonathan González Fernández, Teoría de Redes Informáticas, 26 de diciembre de 1998.

(Halsall, 1998)
Fred Halsall, Comunicación de Datos, Redes de computadoras y Sistemas Abiertos. University of Wales, Swansea, UK (Addison Wesley) 1998; 4ª edición.

(Held, 1992)
Gilbert Held, Network Management, Techniques, Tools and Systems; John Wiley & Sons 1992.

(Heywood, 1998)
Drew Heywood, Networking with Microsoft TCP/IP, 3rd Edition, Ed Sams, 1998.

(Joachim, 1992)
Franz Joachim Kauffels, Network Management; Problems, Standards and Strategies, Addison Wesley 1992.

(Madron, 1992)
Thomas W. Madron, Redes de Área Local, REDES DE ÁREA LOCAL. LA SIGUIENTE GENERACIÓN. Limusa, México, 1992.

(McQuerry, 2001)
Steve McQuerry, Interconexión de dispositivos de red de Cisco; Cisco Press, 2001.

(Merilee Ford, 1998)
Merilee Ford ,Tecnologías de Interconectividad de Redes". Ed. Prentice-Hall. 1998

(Oppenheimer Priscilla, 1999)
Oppenheimer Priscilla, Top Down Network Design, Cisco Press; 1st edition (August 15, 1999).

(Palet, 1995)
Jordi Palet, Publicado UNIX Systems junio 1995.

(Parker, 1996)
Parker, Aprendiendo TCP/IP en 14 días, Prentice Hall; (June 1996)

(Raya, 1997)
José Luis Raya Redes Locales y TCP/IP, Coedición: Alfaomega-Rama, 1997.

(RAYA, 2001)
José Luis y RAYA, Cristina; TCP/IP PARA WINDOWS 2000 SERVER Coedición: Alfaomega-Rama, 1ª edición 2001.

(Siyan, 1997)
Karanjit S. Siyan. Inside TCP/IP". Third edition. Ed. New Riders. 1997.

(Switched Networks, 2000)
Building Cisco Multilayer, Switched Networks *Cisco Press.; 1st edition (May 15, 2000).*

(Tanenbaum, 1996)
Andrew S. Tanenbaum Computer Networks". Ed. Prentice-Hall. 1996.

(Vázquez, 2000)
Alejandra Vázquez Zúñiga, administración de Redes MIB, Universidad de Guadalajara (México), Diciembre 2000.

Páginas Web Consultadas

http://www.uv.es/ciuv/cas/vpn/
http://www.cisco.com/
http://www.vpnc.org/vpn-standards.html
http://www.vpnc.org/
http://www.ieee.com/portal/index.jsp
http://www.icesi.edu.co/es/publicaciones/publicaciones/contenidos
/sistemas _ telemática/1/apachon_evoluc-redes.pdf
http://www.windows.com/resources/documentation/msa/idc/all/solution/en
-us/rag/ragc02.mspx]

Glosario de términos

802.11
Familia de Estándares de la IEEE para redes Wireless

ACK
Acknowledgment
Confirmación

ANSI
American National Standards Institute
Instituto Nacional Estadounidense de Normas

ARP
Address Resolution Protocol
Protocolo de resolución de direcciones

ARPA
Advanced Research Projects Agency
Agencia de Proyectos de Investigación Avanzados

ARQ
Automatic Repeat Request
Solicitud de Repetición Automática

ASCII
American Standards Committee for Information Interchange
Comité Estadounidense de Normas para el Intercambio de Información

ATM
Asynchronous Transfer Mode
Modo de Transferencia Asíncrono

BROADCAST MESSAGE.
Mensaje que es transmitido por la red hacia todos los componentes de esta.

BROADCAST STORM
Cuando varias computadoras transmiten mensajes de tipo Broadcast, inundando la red y provocando que el performance de la misma se vea disminuido.

BRI
Basic Rate Interface
Interfaz de Tasa Básica

CD
Carrier Detect/Collision Detect
Detección de Portadora/Detección de Colisiones

CDMA
Code Division Múltiple Access
Acceso Múltiple por División de Código

CSMA
Carrier Sense Múltiple Access
Acceso Múltiple por Detección de Portadora

CSMA/CA
CSMA with Collision avoidance
CSMA con Evitacion de Colisiones

CSMA/CD
CSMA with Collision Detection
CSMA con Detección de Colisiones

DARPA
Defense Advanced Research Projects Agency
Agencia de Proyectos de Desarrollo para Defensa. Organismo dependiente del Departamento de Defensa Norteamericano (DoD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET

DCE
Data Circuit-Terminating Equipment
Equipo Terminal del Circuito de Datos

DNS
Domain Name Server
Servidor de Nombres de Dominio

DTE
Data Terminal Equipment
Equipo Terminal de Datos

DU
Data Unit
Unidad de Datos

EIA
Electrical Industries Association
Asociación de Industrias Eléctricas

ETSI
European Telecommunications Standards Institute
Instituto Europeo de Normas de Telecomunicaciones

FCS
Frame Check Sequence
Secuencia de Verificación de Tramas

FDDI
Fiber Distributed Data Interface
Interfaz de Datos Distribuida por Fibra

FTP
File Transfer Protocol
Protocolo de Transferencia de Archivos

Host
Utilizamos este término para referirnos a una computadora que actúa como principal con respecto a un sistema computador

ICMP
Internet Control Message Protocol
Protocolo de Mensaje de Control de Internet

IEEE
Institute of Electrical and Electronics Engineers
Instituto de Ingenieros en Electricidad y Electrónica

IP
Internet Protocol
Protocolo de Internet

ITU-T
International Telecommunications Union – Telecommunications (Sector)
Unión Internacional de Telecomunicaciones – (Sector) Telecomunicaciones.

LAN
Local Area Network
Red de Área Local

MAC
Médium Access Control
Control de Acceso al Medio. Es el encargado de la gestión de las tramas de la red: ensamblado de los datos en tramas con campos de dirección y detección de errores, desensamblado de tramas, reconocimiento de direcciones y control de acceso al medio de transmisión LAN.

MAN
Metropolitan Area Network
Red de Área Metropolitana

MIB
Management Information Base
Base de Información de Gestión

NC
Network Connection
Conexión de Red

NIC
Network Interface Card
Tarjeta Adaptadora de Red

NT
Network Termination
Terminación de Red

OSI
Open Systems Interconnection
Interconexión de Sistemas Abiertos

PDU
Protocol Data Unit
Unidad de Datos de Protocolo

QoS
Quality of Service
Calidad de Servicio. El termino calidad de servicio se usa habitualmente para describir propiedades similares de sistemas.

RARP
Reverse Address Resolution Protocol
ARP Inverso

Red de Computadoras
Sistema de comunicación de datos que interconecta computadoras que se encuentran físicamente en lugares distintos. Puede estar compuesta por una combinación de LANs, MANs o WANs.

RIP
Routing Information Protocol
Protocolo de Información de Enrutamiento

SNMP
Simple Network Management Protocol
Protocolo Simple de Gestión de Red

STP
Shielded Twisted Pair
Par Trenzado Blindado

TCP
Transmission Control Protocol
Protocolo de Control de Transmisión

TFTP
Trivial File Transfer Protocol
Protocolo Trivial de Transferencia de Archivos

UDP
User Datagram Protocol
Protocolo de Datagrama de Usuario

UTP
Unshielded Twisted Pair
Par Trenzado no Blindado

VPN
Virtual Private Network
Red Privada Virtual

WAN
Wide Area Network
Red de Area Extensa

WIRELESS
Sistemas que permiten la comunicación de teléfono o datos a través del aire sin una conexión física.