

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CREACIÓN DE UN LABORATORIO PARA EL ÁREA DE REDES

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TÍTULO DE

I N G E N I E R O E N C O M P U T A C I Ó N

PRESENTAN:

ARTEAGA RICCI TANYA ITZEL
MARTÍNEZ LAGUNAS CAROLINA
ZÚÑIGA MEDEL MARÍA ALEJANDRA

DIRECTOR: M.C. MA. JAQUELINA LÓPEZ BARRIENTOS



MÉXICO, D. F. **ENERO 2006**



A la Universidad Nacional Autónoma de México, nuestra máxima casa de estudios, por brindarnos la oportunidad de estudiar y superarnos, por ofrecernos día a día el potencial de ser autónomos y del descubrimiento.

A la Facultad de Ingeniería por ser un hogar durante estos años, por dejar una huella en nosotras y nosotras dejamos el corazón en ella.

A nuestra directora de tesis M.C. Ma. Jaquelina López Barrientos, por su paciencia, por sus consejos, por su apoyo en la realización de este proyecto, pero sobre todo por creer en nosotras.



A todos nuestros profesores que durante toda la carrera fueron siempre una guía, un apoyo. Por compartir sus conocimientos y experiencias, por darnos siempre ánimos para seguir adelante y continuar por el camino del éxito.

Alejandra Zúñiga Medel
Carolina Martínez Lagunas
Tanya Itzel Arteaga Ricci

... A Dios por haberme permitido estar aquí, por darme la capacidad necesaria para ser lo que soy, por brindarme su regazo cuando más triste estaba y por reglarme su sonrisa y alegrar mi corazón.

… A mi mami que siempre me ha apoyado, que ha estado conmigo en las buenas y en las malas, que me da su amor incondicional y que ahora estamos disfrutando juntas de este sueño que ya es una realidad.

… A mi familia, Madito, Esme, Liz, Mimi, Ale, Nacho, Jorge, Viri, Omar y mi consentido Carlitos, que han estado conmigo en mis múltiples alegrías y noches de desvelo, que me apoyan incondicionalmente y me ofrecen todo su amor.

… A mis mejores amigas Ale, Caro, Dulce y Lore que compartimos juntas las alegrías y triunfos de este proyecto, que me apoyaron mucho para no dejarme caer, y me alentaron a seguir adelante.

… A todos mis amigos que con sus constantes ánimos y porras me mostraron todo su cariño y compresión, que con mucha paciencia soportaron mis cambios de ánimo y nunca me dieron la espalda.

… A todos ellos GRACIAS.

Tanya Itzel Arteaga Ricci

A Dios
Por haberme dado la vida,
por darme una familia, amigos
y muchos motivos para salir adelante.
Por siempre llenarme de bendiciones.

A Mis Padres
Por ser mis guías, mis compañeros,
Por ser mi apoyo siempre
y darme todo su amor y comprensión.
Por que nunca me han dejado sola
y gracias a ellos he podido llegar
a cumplir todas mis metas.
Los amo.

A Mi Hermana
Por ser mi amiga y confidente,
apoyarme en los momentos buenos
y no tan buenos.
Por ser la mejor hermana.
Te quiero mucho hermanita.

A Mis Amigos:
Por hacerme pasar muchos ratos de alegría
y enseñarme todo lo que vale la amistad,
por su ayuda, su compañía y honestidad.
Por compartir conmigo parte de su vida
y dejarme compartir la mía con ustedes.

Gracias Ale y Tanya por estar conmigo
en este momento tan importante y permitirme
ser participe de sus logros también.

Muchas GRACIAS a todos!

Carolina Martínez Lagunas

A Dios

Por darme la oportunidad de vivir
Por ponerme en el camino a las mejores personas
porque sin ellas no sería nada

A mi madre

Por tu amor
Por darme la vida
Por apoyarme cuando más lo necesite
Por reprenderme, ahora soy más fuerte
Por tus sacrificios, pues serán recompensados
Por tu paciencia infinita

A mi madrina

Por educarme y cuidarme
Por tu paciencia y apoyo
Por tu cariño

A mi familia

Que siempre me impulsó para ser mejor
Que nunca hizo distinciones

A mi novio

Por ser parte de mi vida
Por no dejarme caer
Por tus desvelos
Por las largas esperas

A mis amigos

Por todas las palabras de apoyo
Por todas las aventuras
En especial a Kro y Tanya
Por soportarme, por su paciencia y
por nuestra amistad que sobrevivió

Ma. Alejandra Zúñiga Medel

ÍNDICE TEMÁTICO

INTRODUCCIÓN. 1
CAPÍTULO 1 ANTECEDENTES
1.1 Antecedentes de las redes de computadoras..... 4
1.1.1 Topologías..... 4
1.1.1.1 Topología Bus..... 4
1.1.1.2 Topología Estrella..... 5
1.1.1.3 Topología Anillo..... 6
1.1.1.4 Topología Malla..... 6
1.1.2 Cobertura geográfica..... 7
1.1.2.1 Redes LAN..... 7
1.1.2.2 Redes WLAN..... 8
1.1.2.3 Redes MAN..... 8
1.1.2.4 Redes WAN..... 8
1.2 Antecedentes de Sistemas Operativos..... 9
1.2.1 UNIX..... 9
1.2.1.1 Características Principales..... 10
1.2.2 LINUX..... 10
1.2.2.1 Características Principales..... 11
1.2.3 Windows..... 11
1.3 Antecedentes del Laboratorio de Redes..... 12
1.4 Condiciones actuales del Laboratorio..... 15

CAPÍTULO 2 DISEÑO

2.1 Organismos de estandarización..... 19
2.1.1 ISO..... 19
2.1.2 IEEE..... 19
2.1.2.1 IEEE Sección México..... 20
2.1.3 ANSI..... 20
2.1.4 TIA/EIA..... 22
2.1.4.1 Estándar ANSI/TIA/EIA-568-A de alambrado de telecomunicaciones para edificios comerciales..... 23
2.1.4.2 Estándar ANSI/TIA/EIA-569 de rutas y espacios de telecomunicaciones para edificios comerciales 24
2.1.4.3 Estándar ANSI/TIA/EIA-570 de alambrado de telecomunicaciones residencial y comercial liviano..... 27
2.1.4.4 Estándar ANSI/TIA/EIA-606 "Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales"..... 27
2.1.4.5 Estándar ANSI/TIA/EIA-607 "Requisitos de aterrizado y protección para telecomunicaciones en edificios comerciales" 27
2.1.5 Instituto Mexicano de Normalización y Certificación (IMNC)..... 27
2.2 Modelo OSI..... 28
2.2.1 Capa Física..... 29
2.2.1.1 Cableado Estructurado 31
2.2.1.2 Importancia del Cableado Estructurado..... 31
2.2.1.3 Normas para el Cableado Estructurado..... 32
2.2.2 Capa de enlace..... 32
2.2.2.1 Tarjetas de interfaz de Red..... 33
2.2.2.2 Direcciones MAC..... 34
2.2.2.3 Protocolo de acceso al medio CSMA/CD..... 35
2.2.3 Capa de red..... 36
2.2.3.1 Direcciones IP..... 37
2.2.3 Capa de transporte..... 39

2.2.5 Modelo de referencia TCP/IP..... 40
2.2.5.1 Capas del modelo de referencia TCP/IP..... 41
2.2.5.1.1 Capa Física..... 42
2.2.5.1.2 Capa de Internet..... 42
2.2.5.1.3 Capa de Transporte..... 42
2.2.5.1.4 Capa Aplicación..... 43
2.2.6 Capa de sesión..... 43
2.2.7 Capa de presentación..... 43
2.2.7.1 Compresión..... 44
2.2.7.2 Cifrado..... 44
2.2.8 Capa de aplicación..... 44
2.3 Comparación entre los modelos de referencia OSI y TCP/IP..... 45

CAPÍTULO 3 DESARROLLO

3.1 Cableado..... 47
3.1.1 Cableado horizontal..... 47
3.1.2 Rutas y espacios horizontales..... 47
3.1.3 Roseta..... 48
3.1.4 Conectores RJ45..... 50
3.1.5 Rack..... 51
3.1.6 Panel de parcheo..... 52
3.2 Dispositivos de conectividad..... 53
3.2.1 Switch..... 53
3.2.1.1 Encapsulamiento..... 54
3.2.1.2 Segmentación..... 55
3.2.1.3 Colisión..... 55
3.2.2 Router..... 56
3.2.3 Puente..... 57
3.2.4 Hub..... 58
3.3 Configuración de Red..... 58
3.3.1 Configuración de red en Windows XP..... 59
3.3.2 Configuración de la tarjeta de red en Fedora 3.0..... 62
3.4 SAMBA..... 66
3.4.1 Características de SAMBA..... 66
3.5 Difusión..... 68
3.5.1 Logotipo..... 68
3.5.2 Sitio Web..... 69

CAPÍTULO 4 PRUEBAS Y MANTENIMIENTO

4.1 Equipo..... 73
4.1.1 Dificultades..... 73
4.1.2 Pruebas..... 75
4.2 Pruebas de usuarios..... 81
4.2.1 Tesistas..... 81
4.2.1.1 Dificultades..... 81
4.2.2 Alumnos..... 82
4.2.2.1 Dificultades..... 82
4.3 Soluciones..... 83
4.3.1 Equipo..... 83
4.3.2 Usuarios..... 83
4.4 Programa de Mantenimiento..... 84
4.5 Errores frecuentes y soluciones..... 85

CONCLUSIONES Y COMENTARIOS FINALES..... 88

GLOSARIO..... 90

BIBLIOGRAFÍA..... 100

ANEXOS..... 102

Las computadoras son ahora las mejores herramientas para poder llevar a cabo los trabajos diarios, en ellas guardamos la información para poder después manipularla y que nos sea útil. Y en la actualidad la computadora no puede faltar en la realización de cualquier tipo de proyecto.

Es por esto que el desarrollo de la computación y su integración con las telecomunicaciones han propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas.

Las nuevas formas de comunicación a las que nos referimos son las redes de datos, las cuales su principal objetivo es el de poder tener la información siempre disponible, verás y segura, resulta difícil de definir que la información es relevante, tanto, que poniendo un ejemplo simple, para las empresas se ha convertido en uno de los activos más importantes, para el manejo de información, inventarios, producción y sobre todo la toma de decisiones.

No es posible entender el estado actual de las telecomunicaciones y la transmisión de datos sin conocer cuál ha sido su evolución histórica y la sucesión de avances tecnológicos en la materia. Un poco de su historia, que en realidad se remonta hasta la invención del telégrafo (1834) que es donde parte la comunicación electrónica, sin embargo dado un salto hasta alrededor de 1920 se habían establecido los principios básicos de telecomunicaciones, conmutación de mensajes y control de línea. Los sistemas se construyeron con base en comunicación a través de la voz y transmisión de datos. Luego de la Segunda Guerra Mundial comenzó el desarrollo comercial de la computadora. Como estas primeras máquinas eran orientadas a lotes, no existía la necesidad interconectarse con el sistema de comunicación que abarcaba toda la nación. Sin embargo, más adelante la industria tomó conciencia de la conveniencia de que máquinas y gente se comunicaran entre sí. Dado que el único sistema de comunicación disponible era el telefónico, naturalmente, las computadoras que estaban en evolución, habrían de desarrollarse siguiendo vías que les permitieran usar este servicio. El crecimiento del uso de la comunicación fue simultáneo al crecimiento de la tecnología de las computadoras y en parte, favorecido por él. Las redes de conmutación de mensajes, reservación y transacciones financieras de los años 50 y 60 usaban computadoras centralizadas comparativamente sofisticadas para controlar grandes poblaciones de dispositivos y terminales primitivas. A medida que esas redes crecían en lo que se refiere a volúmenes de tráfico y poblaciones de terminales, el aspecto no controlado de la operación de las terminales se volvió inaceptable. Luego de muchos estudios, los arquitectos del sistema finalmente determinaron que las terminales destinadas a la operación de redes basadas en computadoras debían permitir un grado de control más depurado que el alcanzado por los primeros métodos basados en electromecánica.

En 1969 surge ARPANET, era una red de telecomunicaciones militarizada y consistía entre otras cosas en un intento de hacer una red que sobreviviese a un ataque militar grande, y que es el precursor del Internet. La tecnología que incluía ARPANET era la conmutación de paquetes y la arquitectura de malla, lo que dio origen a un control distribuido.

Después de ARPANET, las primeras redes de computadoras que se constituyeron, tanto comerciales como militares, utilizaban sus propias normas de diseño y funcionamiento. Han llegado a existir compañías que utilizaban normas de comunicación diferentes para sus propios productos, lo que se convertía en un gran problema cuando necesitaron comunicarse entre ellas, ya que, los sistemas de transmisión no eran compatibles y era necesario deshacerse de todo lo instalado hasta la fecha y montar redes nuevas, todas ellas del mismo tipo. La otra solución

consistía en desarrollar equipos capaces de convertir y adaptar las señales de comunicación entre redes, pero era una opción demasiado cara.

A partir de ese momento se comenzó a estudiar la idea de que todas las redes deberían contar con un conjunto de normas que estandaricen y coordinen a todos los fabricantes y proveedores.

Así, la estandardización internacional comenzó en el campo electrotécnico: la Comisión Electrotécnica Internacional (IEC *International Electrotechnical Commission*) fue establecida en 1906. Iniciando el trabajo en otros campos fue realizada por la Federación Internacional de la Asociación Nacional de Estandarización (ISA *International Federation of the National Standardizing Associations*), que fue instalado en 1926. El énfasis dentro de ISA fue puesto fuertemente en la ingeniería industrial. Las actividades de ISA acabaron en 1942. En 1946, representantes de 25 países convocados en Londres decidieron crear una nueva organización internacional, cuyo objeto sería el facilitar la coordinación internacional y la unificación de los estándares industriales. La nueva organización, ISO, comenzó oficialmente operaciones el 23 de febrero de 1947.

La ISO es una red de los institutos nacionales de los estándares de 156 países, de un miembro por país, con una secretaría central en Ginebra, Suiza, que coordina el sistema. Para enfrentar el problema de incompatibilidad de redes, la ISO investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes, y el resultado de este esfuerzo en 1984 dio como resultado la creación de un Modelo de Referencia Interconexión de Sistemas Abiertos, llamado Modelo OSI.

En la actualidad y teniendo como referencia al modelo OSI podemos mantener una comunicación directa entre redes, eso las hace indispensables en empresas, hospitales, instituciones públicas y gubernamentales así como en bancos, escuelas, etc., y es necesario que éstas sean manejadas, administradas y mantenidas por gente especializada ya que de no ser así se pone en riesgo su buen funcionamiento y por ende la propia información. Esta gente especializada y capacitada en el ramo, debe poder hacer que estas tecnologías funcionen a la perfección y exploten toda la capacidad que estas ofrecen, y esto se logra desde su educación profesional en donde antes las instituciones educativas tenían el tiempo suficiente para ir cambiando y para adaptarse a las nuevas necesidades de la sociedad. Ahora, estas corren el riesgo de convertirse en instituciones obsoletas si no adoptan nuevas formas de trabajo que les permitan cambiar al ritmo que la sociedad le demanda. Es aquí donde entra la importancia de este laboratorio de redes y seguridad para la Facultad de Ingeniería, donde su principal objetivo es formar a los futuros ingenieros en computación en el ámbito de las redes, y que al egresar tengan un perfil idóneo y completo para poder competir en el mundo laborar que los aguarda.

Cuando decidimos aceptar el reto de la creación de un nuevo laboratorio para el área de redes, nunca imaginamos el gran número de retos y oportunidades que nos brindaría el desarrollo de este proyecto para lograr nuestros objetivos. Al empezar a trabajar en la creación del laboratorio, el primer obstáculo al que nos enfrentamos fue la asignación de un espacio, pero gracias a la valiosa persistencia de la M.C. Ma. Jaquelina López B. para que se proporcionara un lugar digno, se asignó un espacio en la planta baja del edificio Luis G. Valdez Vallejo.

Es así que la presente tesis tiene una estructura de acuerdo a la evolución del laboratorio, pero siempre basándonos en los siguientes objetivos: proveer una plataforma de trabajo en hardware y software a los estudiantes y profesores del área de redes de computadoras de la Facultad de Ingeniería y apoyar al alumno en el desarrollo de habilidades analíticas y funcionales para la creación, implantación, mantenimiento y administración de redes de computadoras mediante el seguimiento de las prácticas de las distintas materias del área.

Así empezamos con el capítulo 1, explicando los conceptos teóricos, ya que debemos saber de qué estamos hablando al referirnos a las redes y qué es lo que se relaciona con las mismas, por ello explicamos el concepto de red, los diferentes tipos de redes, las topologías que existen, los diferentes sistemas operativos que serán manejados. En especial, se da un amplio panorama de los inicios del laboratorio, el material, el equipo de cómputo y los elementos con los que se contaba al principio del proyecto para terminar con lo adquirido recientemente y las condiciones actuales de lo que es ahora el Laboratorio de Redes.

Una vez que tenemos los conceptos básicos podemos comenzar con el estudio de los protocolos y normas que se deben seguir para armar una red, así, en el capítulo 2 se encuentra la información de las distintas organizaciones que han propuesto los estándares que ahora usamos, tales como la ISO, IEEE, ANSI y la TIA/EIA. También podemos conocer el llamado Modelo OSI para entender cómo fue posible la compatibilidad entre las distintas arquitecturas de computadoras para que pudieran comunicarse entre sí.

En el capítulo 3 se detalla el desarrollo del laboratorio, cómo fue evolucionando en cuanto a equipo, cableado y software se refiere, en el capítulo 4 se aborda el tema de pruebas y mantenimiento; es decir, cuáles fueron las pruebas realizadas al laboratorio, los problemas que se enfrentaron, las soluciones para los mismos así como unas recomendaciones a futuro para prever posibles contratiempos.

A medida que avanzamos, se ha dado una rápida convergencia computacional, y también las diferencias entre la captura, transporte, almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar, procesar y distribuir información, la demanda de más sofisticados tipos de procesamientos crece todavía con mayor rapidez. Esto da lugar al manejo de las redes.

1.1 Antecedentes de las redes de computadoras

Una red es una interconexión de dos o más computadoras con el propósito de compartir información de manera eficiente y confiable así como recursos a través de un medio de comunicación, como puede ser el cable coaxial, un cable UTP o Fibra Óptica los cuales abordaremos más adelante.

El propósito más importante de cualquier red es enlazar entidades similares al utilizar un conjunto de reglas que aseguren un servicio confiable. Estas normas podrían quedar de la siguiente manera:

- La información debe entregarse de forma confiable sin ningún daño en los datos.
- La información debe entregarse de manera consistente.
- La red debe ser capaz de determinar hacia dónde se dirige la información.
- Las computadoras que forman la red deben ser capaces de identificarse entre sí o a lo largo de la red.
- Debe existir una forma estándar de nombrar e identificar las partes de la red.

Para ello es necesario considerar varios aspectos que involucran todas estas características, entre las cuales podemos citar: la forma de interconectar los equipos (topología), las reglas de comunicación (protocolos), etc.

1.1.1 Topologías

La topología de una red es la forma de interconexión entre computadoras (llamados también nodos). Existe tanto la topología lógica que significa, la forma en que es regulado el flujo de los datos, como la física, que es simplemente la manera en que se interconectan las computadoras.

Las topologías son criterios determinantes para la elección de las redes, la reducción del costo de encaminamiento, la fiabilidad o tolerancia a fallos y su facilidad para localizarlos, y por último la facilidad de su instalación y reconfiguraciones futuras.

Las topologías más comunes son: bus, estrella, anillo y malla.

1.1.1.1 Topología Bus

Todas las computadoras están conectadas a un cable central, llamado **bus** (Ver figura 1.1). Las redes de bus lineal son las más fáciles de instalar y son relativamente baratas. Este tipo de topología se hizo famoso al principio de la historia de las redes, y usualmente era utilizado con cable coaxial para su conexión aunque también se usa el cable UTP (Unshielded Twisted Pair) ahora es utilizado en

todas las topologías, además de ser más económico a largo plazo. La ventaja de este tipo de topología bus es su simplicidad.

Una vez que las computadoras están físicamente conectadas al alambre, el siguiente paso es instalar el *software* de red en cada computadora. El lado negativo de una red Bus es que si uno de los enlaces en el bus entre cualquiera de las computadoras se rompe, la red deja de funcionar.

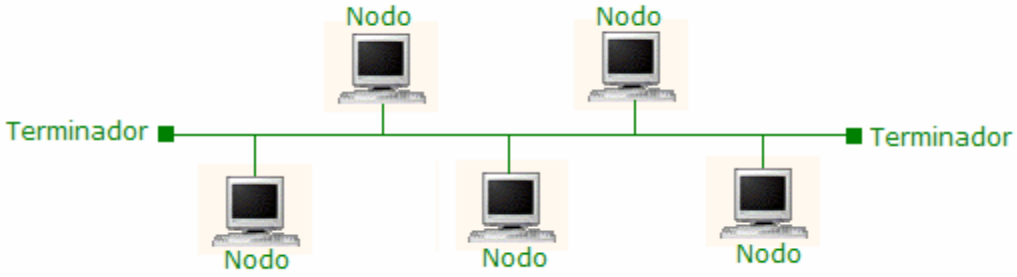


Figura 1.1 Topología tipo Bus.

1.1.1.2 Topología Estrella

En la topología en estrella (Ver figura 1.2) todas las computadoras están conectadas mediante enlaces bidireccionales a un concentrador (switch) o nodo central que controla la red. Este switch asume las funciones de gestión y control de las comunicaciones proporcionando un camino entre cada dos computadoras que deseen comunicarse.

La principal ventaja de la topología en estrella es que el acceso a la red, es decir, la decisión de cuándo una estación puede o no transmitir, se halla bajo control de la estación central. Además la flexibilidad en cuanto a configuración, así como la localización y control de fallos es aceptable al estar todo el control en el nodo central. El gran inconveniente que tiene esta topología es que si falla el nodo central. Toda la red queda desactivada. Otros pequeños inconvenientes de este tipo de red son el costo de las uniones físicas puesto que cada estación está unida a la unidad central por una línea individual.

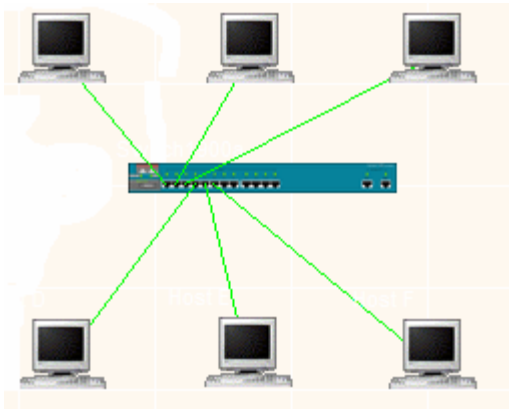


Figura 1.2 Topología tipo Estrella.

1.1.1.3 Topología Anillo

El **anillo** (Ver figura 1.3) consiste en que las computadoras están conectadas entre sí mediante un único enlace de transmisión que configura un camino cerrado.

La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información.

La información se transmite secuencialmente de una computadora a la siguiente a lo largo del anillo, de tal forma que cada computadora regenera la señal que recibe y la retransmite al siguiente, salvo que la información esté dirigida a él, en cuyo caso la recibe en su memoria.

Normalmente en las computadoras se encuentran repetidores, que hacen que la información no se vaya perdiendo durante el recorrido hasta llegar a su meta. Las redes en anillo permiten un control eficaz, debido a que, en cada momento, se puede conocer en qué trama está circulando la señal, puesto que se sabe la última estación por donde ha pasado y la primera a la que todavía no ha llegado. La desventaja fundamental es la falta de fiabilidad. Un fallo en el anillo inhabilitaría toda la comunicación.

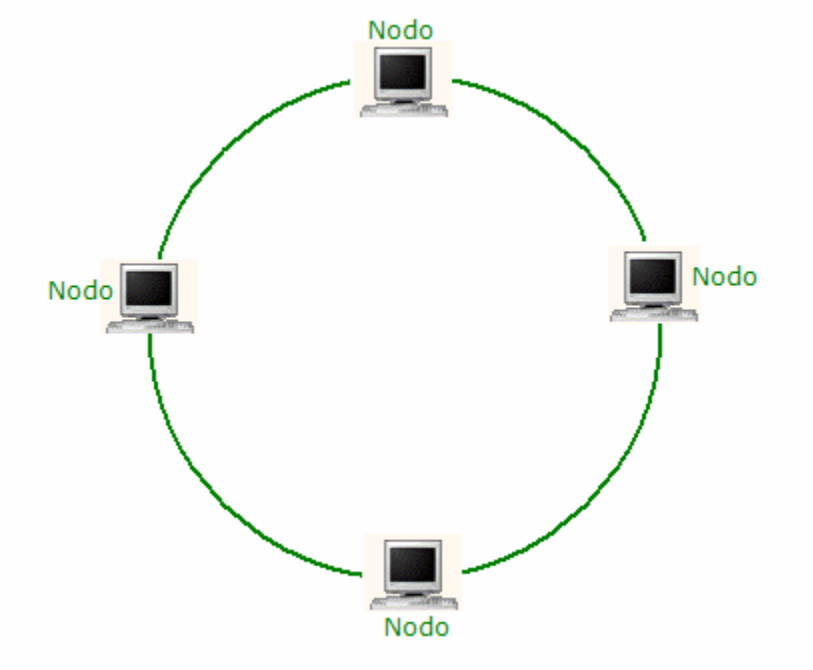


Figura 1.3 Topología tipo Anillo.

1.1.1.4 Topología Malla

Para la topología en **malla** (Ver Figura 1.4) se busca tener conexión física entre todas las terminales de la red. Utilizando conexiones punto a punto, esto permitirá que cualquier computadora se comunique con otras computadoras de forma paralela si fuera necesario. La principal ventaja es que este tipo de redes difícilmente falla, pues inclusive, si alguna de estas líneas fallara aún así se podrían encontrar otras rutas para lograr la transferencia de la información.

La desventaja de la topología en malla, es que se requiere demasiado cableado específicamente si existen n terminales en la red. Además cada computadora requiere n-1 puertos de comunicación. También el mantenimiento resulta costoso a largo plazo.

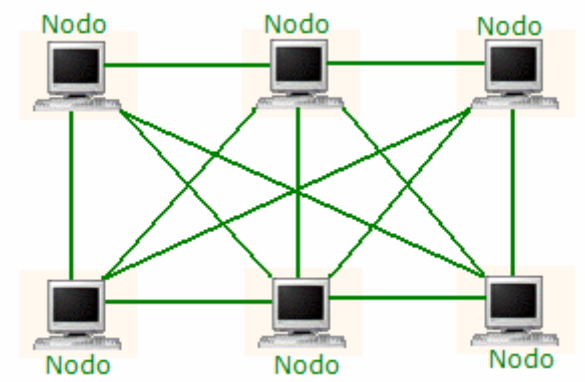


Figura 1.4 Topología en malla completa.

1.1.2 Cobertura geográfica

Según el lugar y el espacio que ocupen, esto es, por su cobertura geográfica las redes se pueden clasificar como LAN, WLAN, MAN y WAN:

1.1.2.1 Redes LAN

Las redes de área local (LAN Local Area Network) son aquellas que se expanden en un área relativamente pequeña. Comúnmente se encuentra dentro de un edificio o un conjunto de edificios contiguos. Asimismo, una LAN puede estar conectada con otras LAN a cualquier distancia por medio de una línea telefónica y ondas de radio. Aunque actualmente existen otros medios de enlace.

Una red LAN puede estar formada desde dos computadoras hasta cientos de ellas. Todas se conectan entre sí por varios medios y topologías. A la computadora (o agrupación de ellas) encargada de llevar el control de la red se le llama servidor y a las computadoras que dependen de éste, se les conoce como nodos o estaciones de trabajo.

Los nodos de una red pueden ser computadoras que cuentan con su propio CPU (Unidad Central de Proceso), disco duro y software. Tienen la capacidad de conectarse a la red en un momento dado o pueden ser computadoras sin CPU o disco duro, es decir, se convierten en terminales tontas, las cuales tienen que estar conectadas a la red para su funcionamiento.

Las LAN son capaces de transmitir datos a velocidades muy altas, algunas inclusive más rápido que por línea telefónica, pero las distancias son limitadas. Generalmente estas redes transmiten datos a 10 megabits por segundo (Mbps) que es el caso de Ethernet (la tecnología mas utilizada actualmente). En comparación, Token Ring opera a 4 y 16 Mbps, mientras que FDDI y Fast Ethernet a una velocidad de 100 Mbps o más. Cabe destacar que estas velocidades de transmisión no son caras cuando son parte de la red local.

1.1.2.2 Redes WLAN

Otro tipo de red que comienza a tomar mucha fuerza en estos días es la WLAN (Wireless Local Area Network; Red de Área Local Inalámbrica), que se basa en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

La velocidad de transmisión de las redes WLAN, surgidas experimentalmente a principios de los noventa, va de los 10 a los 100 Mbps, y son el complemento ideal para las redes fijas, por tener capacidad de enlazarse con las redes cableadas.

En esencia, responden al desarrollo del mercado de equipos portátiles (notebooks y handhelds) y de las comunicaciones móviles que han propiciado que los usuarios se mantengan en continuo movimiento, manteniendo comunicación constante con otras.

Las WLANs pueden ser la alternativa en aquellos negocios que no pueden instalar cables a través de un pasillo para tener acceso a otra de las oficinas (como es el caso de las oficinas en edificios de patrimonio nacional en donde no se puede alterar de ninguna forma la estructura física de dicho edificio), en escenarios diversos donde se requiera la instalación de redes, temporales (exposiciones, workshops, etc), o cuando el mismo cableado puede causar desórdenes y congestionamientos.

1.1.2.3 Redes MAN

Otro tipo de red que se aplica en las organizaciones es la red de área metropolitana o MAN (Metropolitan Area Network), una versión más grande que la LAN y que normalmente se basa en una tecnología similar a ésta.

La red MAN abarca desde un grupo de oficinas corporativas cercanas a una ciudad y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales.

1.1.2.4 Redes WAN

La red de área amplia (WAN Wide Area Network) es aquella comúnmente compuesta por varias LAN interconectadas, en una extensa área geográfica, por medio de fibra óptica o enlaces aéreos, como satélites.

Entre las WAN más grandes se encuentran: ARPANET, creada por la Secretaría de Defensa de los Estados Unidos y que se convirtió en lo que actualmente es la WAN mundial: Internet.

A diferencia de las LAN, las WAN casi siempre utilizan ruteadores. Debido a que la mayor parte del tráfico en una WAN se presenta entre las LAN que conforman ésta, los ruteadores ofrecen una importante función, pues aseguran que las LAN obtengan solamente los datos destinados a ellas.

1.2 Antecedentes de Sistemas Operativos

A través de la historia de la computación se han conocido muchos sistemas operativos y cada vez se ha deseado automatizar más los sistemas operativos y generarlos con más confiabilidad, seguridad y protección para los registros de los usuarios.

Los sistemas operativos se han convertido en una herramienta eficaz dentro del mundo de los negocios, académicos y personales. Con la ayuda de un buen soporte de hardware puede ser un patrón importante para el control de sus registros. De ahí que la importancia de los sistemas operativos radica en que se hizo evidente que el operar una computadora por medio de tableros podía mejorarse notoriamente, pues el usuario realizaba siempre una secuencia de pasos repetitivos, lo cual es una de las características contempladas en la definición de lo que es un programa, de ahí que nace uno de los primeros sistemas operativos con la filosofía de administrar una familia de computadoras: el OS/360 de IBM, pero siguió evolucionando con el paso de los años, y se fue volviendo mucho más amigable para atraer la atención del público, de esta manera se popularizó el Sistema Operativo MS-DOS y UNIX (del cual hablaremos de forma más específica más adelante), pero no se detuvo ahí sino que siguió con muchos cambios, además de empezar a establecer un ambiente mucho más gráfico para su fácil utilización.

Para mediados de los 80's, comienza el auge de las redes de computadoras y la necesidad de sistemas operativos en red y sistemas operativos distribuidos. Es entonces donde nos encontramos con el monopolio de Windows pero sin dejar a un lado los otros sistemas operativos. La red mundial Internet se va haciendo accesible a toda clase de instituciones y se comienzan a dar muchas soluciones (y problemas) al querer hacer convivir recursos residentes en computadoras con sistemas operativos diferentes. Para los 90's el paradigma de la programación orientada a objetos cobra auge, así como el manejo de objetos desde los sistemas operativos. Las aplicaciones intentan crearse para ser ejecutadas en una plataforma específica y poder ver sus resultados en la pantalla o monitor de otra diferente (por ejemplo, ejecutar una simulación en una máquina con UNIX y ver los resultados en otra con DOS). Los niveles de interacción se van haciendo cada vez más profundos.

Entre los sistemas operativos más utilizados en la actualidad son:

1. UNIX
2. LINUX
3. WINDOWS

1.2.1 UNIX

UNIX es un sistema operativo cuyo inicio se remonta a principios de los años setenta. No surgió como un producto comercial, sino más bien como un proyecto personal de Ken Thompson y Dennis Ritchie, que trabajaban en los Laboratorios Bell. La idea básica era crear un entorno de trabajo simple y, a la vez, agradable para el desarrollo de aplicaciones. Dotaron un nuevo sistema operativo con la capacidad de soportar multiprogramación o, lo que es lo mismo, permitir que hubiese en un mismo instante varios programas cargados en la memoria y la capacidad de tiempo compartido. De este modo, se puede tener a varias personas conectadas al mismo tiempo y desde distintas terminales a la misma computadora. Estas dos características hicieron que el sistema tuviese una buena aceptación, tanto en entornos universitarios como en laboratorios dedicados al desarrollo de software. Desde sus orígenes hasta la actualidad, UNIX ha sufrido multitud de modificaciones. Se le han ido añadiendo nuevas posibilidades, tales como el soporte para redes, los entornos de ventanas o extensiones para tiempo real.

1.2.1.1 Características Principales

- UNIX fue diseñado como un sistema multiusuario en tiempo compartido; es decir, un sistema en el que pueden trabajar varios usuarios simultáneamente compartiendo el CPU y todos los demás recursos del sistema. Cada usuario puede ejecutar varios procesos (programas en ejecución) a la vez.

- El sistema está escrito en un lenguaje de alto nivel (lenguaje C), lo cual propicia que fuera fácil de leer, entender, modificar y transportar a otras máquinas con una arquitectura completamente diferente.

- La interfaz de usuario (shell) es sencilla, potente y en cualquier momento puede ser reemplazada por otra si se desea.

- Proporciona primitivas que permiten construir grandes programas a partir de otros más sencillos.

- El sistema de archivos tiene una estructura de árbol invertido de múltiples niveles que permite un fácil mantenimiento y una implementación eficiente.

- Todos los archivos de usuario son simples secuencias de bytes (8 bits), no tienen ningún formato predeterminado.

- Los archivos de disco y los dispositivos de entrada y salida (E/S) se tratan de la misma manera. Las peculiaridades de los dispositivos se mantienen en el núcleo (kernel). Eso quiere decir que impresoras, discos, terminales, etc., desde el punto de vista del usuario se tratan como si fuesen ficheros normales.

- La arquitectura de la máquina es completamente transparente para el usuario, lo que permite que los programas sean fáciles de escribir y transportables a otras máquinas con hardware diferente.

1.2.2 LINUX



Tanto la creación de Linux como su desarrollo y popularización son acontecimientos relativamente recientes.

En 1985 Richard Stallman, actualmente uno de los mayores *gurús* de la informática, fundó la “Free Software Foundation” (Asociación para el Software Libre), con el ideal de que todo el software que se creara pudiera estar disponible para ser modificado por cualquiera según sus necesidades. Esto se oponía a la restricción de los sistemas propietarios (como es actualmente Windows), en los que el código fuente, requisito para modificarlo, no es accesible.

Unos años después, en 1991, la Asociación decide integrar en un sistema operativo libre creado por Stallman (GNU), otro diseñado por un estudiante de la Universidad de Helsinki, Linus Torvald, llamado Linux. Nació así un nuevo sistema informático libre, gratuito y de código fuente abierto, que se ha convertido en la base de los programas llamados de “software libre”: el sistema operativo GNU/Linux.

1.2.2.1 Características principales

- *Bajo costo en licencias*. Que muchas veces resulta cero. En la práctica esto no es 100% cierto puesto que existe un costo implícito que es el costo del aprendizaje, sobretodo para múltiples usuarios y computadoras. Habilidad para funcionar sobre máquinas antiguas.

- *Flexibilidad de configuración*. Es posible modificar el sistema operativo para los requerimientos propios. Linux se distribuye con el código fuente. En la práctica sólo es posible si se dispone de conocimientos suficientes para modificar el kernel.

- *No hay necesidad de Licencias*. Usuarios ilimitados, instalaciones ilimitadas. Sin embargo, los productos comerciales que se ejecutan en Linux, SI están sujetos a restricciones de sus licencias.

- *Estabilidad*. Linux tiene la experiencia de un cuarto de siglo de los sistemas Unix. El modelo de OpenSource de Linux asegura que los bugs sean detectados y corregidos rápidamente.

- En ambientes gráficos todavía hay mucho que realizar, sobretodo la integración con el kernel. Linux en el servidor no necesita interface gráfica.

- Linux nació en Internet; virtualmente garantiza que soporta todos los protocolos estándares de Internet. Fue el primero en soportar IPv6 y es muy usado como servidor en los proveedores de Internet. El servidor web más popular: Apache, se ejecuta en su mayoría sobre el Kernel de Linux y adicionalmente respecto a servicios de seguridad tiene entre otras, funcionalidades de firewall.

1.2.3 WINDOWS 

La diferencia entre Windows con el sistema operativo tradicional (en este caso DOS) está en la manera intuitiva mediante dibujos o iconos para comunicarse con la computadora en vez de teclear comandos.

Windows ha tenido numerosos cambios desde su primera aparición el 20 de Noviembre de 1985 hasta nuestros días. Comenzó como una extensión al sistema operativo DOS, por lo que necesitaba de este último para su correcto funcionamiento.

En la actualidad Windows casi ha monopolizado el mundo de las computadoras con Microsoft Windows, siendo éste un Sistema Operativo autónomo, que gracias a su interfaz gráfica, donde la base son “ventanitas”, ayuda al usuario a sentirse mucho más cómodo usando la computadora.

- Windows dispone de una interfaz gráfica que facilita el manejo de los procedimientos: cada comando puede ser visualizado en pantalla mediante una imagen que lo representa.

- Windows es el Sistema Operativo con mayor difusión en el mercado actual, y su imponente popularidad se torna elemento indispensable para la inserción de todo nuevo usuario al mundo informático.

- A su vez, dispone de la compatibilidad con los productos Microsoft, otro marco fundamental en el manejo de una PC: el paquete Office es el más utilizado en lo concerniente a las actividades de oficina, pues engloba todos los complementos necesarios para el trabajo de una secretaria.

- Los Servicios de actualización de software (SUS) de Microsoft ayuda a los administradores a automatizar las actualizaciones del sistema más recientes.

1.3 Antecedentes del Laboratorio de Redes

El área de Redes de Computadoras es una de las principales en el campo laboral, tanto que los Ingenieros en Computación son solicitados (contratados) para su planeación, diseño, instalación, mantenimiento y actualización. Por esto las asignaturas del Área de Redes son muy importantes para los alumnos de la carrera de Ingeniería en Computación y la falta de prácticas en dicha área tiene fuertes repercusiones al querer incorporarse al campo laboral, por lo que es imprescindible contar con un laboratorio en el cual los alumnos observen y practiquen lo que aprenden a lo largo del curso.

Esta área es sumamente interesante y de una utilidad incalculable debido a que su conocimiento y puesta en práctica puede traer grandes beneficios para las empresas e incluso para negocios particulares o fines personales ya que a través de las redes se mueve nuestra información, la cual en la actualidad se ha convertido en uno de los recursos más importantes para la humanidad. Este tema es muy extenso porque toca muchos puntos importantes relacionados con el cuidado y tratado de la información, pero también es un tema que hoy en día no podemos dejar de lado por que está en todas partes y tiene que ver con casi todas las actividades que realiza la humanidad.

Como se ha visto, las redes son un área muy importante en el medio laboral, y la Facultad de Ingeniería consciente de ello lo ha tomado en cuenta al determinar su objetivo como formadora de profesionales, ya que instruye, habilita y capacita ingenieros con una cultura científica, tecnológica y socio humanística, que contribuya con un espíritu crítico y participativo en el desarrollo integral del país. Además, el perfil del egresado, entre otros aspectos destaca que éste sabrá diseñar e instalar redes de teleinformática; planear, diseñar y construir sistemas de interfase máquina-máquina y hombre-máquina, etc., por lo que actualmente se encuentra en un proceso de revisión y actualización de los planes de estudio y se ha propuesto reforzar esta área, de manera que quedará conformada por dos asignaturas de carácter obligatorio: Redes de Datos, la cual es una actualización a la de Redes de Computadoras y la creación de una más: Administración de Redes. Lo anterior, con la finalidad de reforzar y mejorar la calidad de la enseñanza y la preparación de sus alumnos en esta área del conocimiento.

Así como es importante la adquisición del conocimiento teórico y científico también lo es el conocimiento práctico por lo que la creación de un laboratorio auxiliar es indispensable puesto que las materias que van a impartirse gracias a esta nueva propuesta requieren ser reforzadas con un laboratorio ex profeso para el área de redes donde los alumnos pongan en práctica sus conocimientos y adquieran las habilidades correspondientes en un medio controlado sin poner en riesgo las redes de la Facultad ni la información que transita por ellas.

Actualmente, en la Facultad de Ingeniería, ya se cuenta con un espacio destinado a la creación de un laboratorio para el Área de Redes y Seguridad el cual aun cuando funcionaba de manera virtual desde hace varios semestres, el espacio físico que ahora ocupa se proporcionó en noviembre de 2003. El primer problema

fue encontrar equipos de cómputo con los cuales iniciar. Sin embargo, tuvimos una gran ayuda con la donación de equipos que aminoró la problemática, sin embargo no fue suficiente para resolverla.

Cabe mencionar que el laboratorio fue provisto de equipo de cómputo y de algunos otros útiles para comenzar una pequeña red, donaciones que fueron hechas con la ayuda de ex-alumnos de la facultad que ahora sienten la necesidad de devolver algo a su Universidad. En 2003 se adquirió un equipo de cómputo por el departamento de computación mediante el presupuesto asignado a dicho departamento en el ejercicio de 2003. También tenemos que mencionar que adicionalmente la jefatura de la División (DIE) asignó tres equipos nuevos en agosto de 2004; y gracias a una donación importante de Hubbell ahora tenemos un cableado estructurado, sin embargo aún teníamos que hacer una selección de todo nuestro equipo, para poder montar el laboratorio lo más adecuadamente posible.

Ahora bien, como mucho del material donado es ya obsoleto, fue necesario revisar minuciosamente qué era lo que funcionaba para poder armar equipos completos, es decir, basándonos en todo lo que funcionaba correctamente buscamos CPU's, monitores, teclados y mouses que pudieran trabajar bien en conjunto. Es decir, que el CPU reconociera cada uno de los elementos, por ejemplo, el mouse, que pudiera ser compatible con el sistema operativo que la máquina puede soportar, que tenga las entradas adecuadas para conectarse al CPU, etc. Lo anterior debía hacerse porque no todas las piezas pueden acoplarse, ya que deben tener características similares entre sí.

Habiendo conformado el equipo que fue posible, tuvimos lo que podría denominarse la primera versión del laboratorio, con la cual otros tesistas comenzaron a trabajar en el diseño y desarrollo de prácticas de Redes, para, por una parte los estudiantes de Redes de Computadoras tengan la oportunidad de adquirir la práctica tan necesaria que se ha venido comentando en el documento, y además preparar el material que permitirá reforzar los planes de estudio que se encontraban en ese momento en proceso de revisión y actualización como ya se mencionó.

En estas circunstancias se llevó a cabo nuestra primera prueba, la cual fue la realización de un mini-taller en el cual desafortunadamente los equipos no soportaron la carga de trabajo a la que se vieron expuestos, sin embargo esto no nos desanimó, sino que ahora pudimos ver cuales habían sido las debilidades del laboratorio.

Finalmente obtuvimos un grupo de equipos con todo lo que había sido donado que soportarían la carga de trabajo adecuadamente.

Cada uno de los equipos cuenta con diferentes características tanto de procesamiento como de almacenamiento, pero todas están en un mantenimiento constante de actualización tanto de software como de hardware.

Hardware

A la fecha (noviembre de 2004) se cuentan con 6 equipos con las siguientes características:

Equipo1 JIMMY

Lanix
AMD K6 II a 400 Mhz

64 MB en RAM
2 tarjetas de red 3COM
Linux 9.0

Equipo2 PINKY

HP Compaq d220
Pentium 4
40 GB en disco duro
120 MB en RAM
Monitor de 15”
CD ROM
Unidad de 3½
Tarjeta de Red 10/100

Equipo3 MARVIN2

AMD – K6 3D Atlon
2 GB de disco duro
128 en RAM
Monitor AIMC – 1428 V45 15”
Tarjeta de red VIA VT 6105 RHINE III Fast Ethernet 10/100
CD ROM
Unidad de 3½

Equipo4 GARFIELD

HP EGA/VGA Genuine Intel Pentium (R)
4 GB de disco duro
64 MB en RAM
Tarjeta de red VIA VT 6105 RHINE III Fast Ethernet 10/100
Unidad de 3½
CD ROM

Equipo5 HOMERO

Pentium Pro 200
200 MB en disco duro
64 MB en RAM
Monitor DELL 15”
CD ROM
Unidad de 3½
Tarjeta de Red integrada en la Mother Board
Tarjeta de Red con cable coaxial

Equipo6 FELIX

Lanix
Pentium – S (586)
32 MB de RAM
Monitor EGA/VGA marca DTS de 13”
Tarjeta de Red
Unidad de 3½
CD ROM

Canaletas alrededor del laboratorio

Un switch de 12 puertos

Cable UTP categoría 5e y 6

Software

Windows 98 / XP
Linux 7.1/9.0
Norton Antivirus 2004
Panda Titanium
Office 2000 / 2003
Acrobat 6.0
WinZip 8.0

El equipo 1 JIMMY opera como servidor de nuestro laboratorio ya que es en el que se ha desarrollado el primer firewall.

Por las características antes mencionadas, se determinó que el resto de los equipos no podían funcionar adecuadamente bajo sistemas operativos que demandaran grandes capacidades de almacenamiento y/o procesamiento, por lo que los sistemas seleccionados fueron: Linux versiones de 7.1 a la 9 y Windows 98 al XP. Para la selección de los sistemas operativos se tuvieron que cubrir los requerimientos de las prácticas del laboratorio ya existentes. Y que con esto pretendemos tener dos miniredes funcionando en su totalidad, cada una con un sistema operativo diferente, esto es una con Windows y otra con Linux, esto porque sabemos que en el mundo laboral no siempre tenemos el mismo sistema operativo, así que si tenemos al menos conocimientos de 2 de los más importantes sistemas, aseguramos el pronto desarrollo de los recién egresados en el área de Redes.

1.4 Condiciones actuales del laboratorio

En el laboratorio se han presentado cambios significativos en cuanto a hardware se refiere, y se cuenta con nuevas máquinas que han sustituido a las que se tenían en un principio, gracias a la fructífera donación por parte del ISETI (Integradores de Soluciones Empresariales en Tecnología de Información) en donde el Ing. Agustín Calderón realizó una importante aportación de 2 equipos en enero de 2005, estas máquinas tienen más capacidad de almacenamiento y procesamiento y nos han permitido tener dos sistemas operativos en cada máquina, poder almacenar una mayor cantidad de información, etc.

También conservamos equipos que fueron donados recientemente y que nos son muy útiles por que sus características son las suficientes para dar un buen servicio.

El equipo que se tiene actualmente es:

Equipo 1 JIMMY

Lanix
AMD K6 II a 400 Mhz
64 MB en RAM
2 tarjetas de red 3COM

Linux 9.0

Equipo 2 PINKY

HP Compaq d220
Pentium 4
40 GB en disco duro
120 MB en RAM
Monitor de 15”
CD ROM
Unidad de 3½
Tarjeta de Red 10/100

Equipo 3 SPIDERMAN

Dell
Pentium 4
40 GB en disco duro
256 MB en RAM
Monitor de 17”
CD ROM
Unidad de 3½
Tarjeta de Red Intel(R) PRO/1000 MT

Equipo 4 SNOOPY

Dell
Pentium 4
40 GB en disco duro
256 MB en RAM
Monitor de 17”
CD ROM
Unidad de 3½
Tarjeta de Red Intel(R) PRO/1000 MT

Equipo 5 MICKEY

Dell
Pentium 4
40 GB en disco duro
256 MB en RAM
Monitor de 17”
CD ROM
Modem
Unidad de 3½
Tarjeta de Red Intel(R) PRO/1000 MT

Equipo 6 MANDY

Compaq
Pentium 4
80 GB en disco duro
256 MB en RAM
Monitor de 17”
CD ROM
Modem
Unidad de 3½
Tarjeta de Red

Equipo 7 EVA

Compaq
Pentium 4
80 GB en disco duro
256 MB en RAM
Monitor de 17”
CD ROM
Modem
Unidad de 3½
Tarjeta de Red

Equipo 8 KAKAROTTO

Dell
Pentium 4
80 GB en disco duro
512 MB en RAM
Monitor de 17” LSD
CD ROM
Unidad de 3½
Tarjeta de Red Intel(R) PRO/100 VE

Equipo 9 STICHT

Dell
Pentium 4
80 GB en disco duro
512 MB en RAM
Monitor de 17” LSD
CD ROM
Unidad de 3½
Tarjeta de Red Intel(R) PRO/100 VE

Equipo 10 SHAMPOO

Dell
Pentium 4
80 GB en disco duro
512 MB en RAM
Monitor de 17” LSD
CD ROM
Unidad de 3½

Tarjeta de Red Intel(R) PRO/100 VE

Equipo 11 BATMAN

Dell
Pentium 4
80 GB en disco duro
512 MB en RAM
Monitor de 17” LSD
CD ROM
Unidad de 3½
Tarjeta de Red Intel(R) PRO/100 VE

Equipo12 GARFIELD

Hp EGA/VGA Genuine Intel Pentium (R)
4 GB de disco duro
64 MB en RAM
Tarjeta de red VIA VT 6105 RHINE III Fast Ethernet 10/100
Unidad de 3½
CD ROM

El equipo 1, JIMMY, sigue conservándose como servidor del laboratorio, tarea que cumple desde los inicios del mismo. GARFIELD, que también es de los primeros equipos que se tuvieron, se conserva a pesar de que es un equipo con características reducidas en comparación con el resto por que es el utilizado para la realización de una de las prácticas que se llevan a cabo por algunos de los tesistas.

El diseño debe ser la base de toda red, ya que en él descansa el análisis de requerimientos en donde se instalará la red así como las aplicaciones que correrán en ella, su objetivo, usuarios, etc. Por esto, existen una serie de estándares desarrollados por diferentes organismos, los cuales ayudan a tener una red confiable y funcional.

2.1 ORGANISMOS DE ESTANDARIZACIÓN

2.1.1 ISO

ISO es una red de institutos nacionales estandarizados de 146 países, y su base es que haya un miembro por país, con una Secretaría Central en Geneva, Suiza, que coordina el sistema.

La ISO es una organización no gubernamental, los miembros no son delegaciones de gobiernos nacionales como en el caso de sistemas de Naciones Unidas. Sin embargo, la ISO ocupa una posición especial entre los sectores públicos y privados. Esto es porque, por un lado muchos de los institutos miembros de la ISO son parte de la estructura de sus países o es ordenada por sus gobiernos. Por otra parte otros miembros tienen sus raíces únicamente en el sector privado, siendo instalado por sociedades nacionales de las asociaciones de la industria.

Por lo tanto, la ISO actúa como una organización que establece una conexión sobre la cual un consenso puede alcanzar soluciones que resuelven los requisitos de un negocio y las necesidades más amplias de la sociedad, tales como las que existen entre consumidores y usuarios.

2.1.2 IEEE

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS INC

El Instituto de Ingenieros en Electricidad y Electrónica, Inc. (IEEE) fue fundado en 1884 donde su principal objetivo es que los profesionales y estudiantes de ingeniería desarrollen su potencial en campos de la ingeniería eléctrica.

La IEEE se preocupa porque en los sistemas de comunicación se asegure que los paquetes de información sean entregados confiablemente de una fuente a su destino, por lo que desarrolla una serie de estándares que aseguren lo anterior. Estos estándares se aplican a los cables coaxiales, de cobre y de fibra, así como a las interfaces en los diferentes medios de comunicación (terrestres o aéreos).

La IEEE es una organización mundial que atiende a más de 382,000 ingenieros, estudiantes de ingeniería, científicos y otros profesionistas en más de 175 países, dividido en:

- 10 Regiones
- 20 Consejos
- 304 Secciones (mas del 35 % fuera de U.S.A.)
- 49 Subsecciones
- 1384 Capítulos Técnicos
- 1450 Ramas Estudiantiles
- 323 Capítulos Técnicos de ramas estudiantiles

Cabe mencionar que en nuestro país existe una sección de este importante instituto denominada: IEEE Sección México.

2.1.2.1 IEEE Sección México

Ésta fue iniciada por el Sr. H. S. Foley, miembro y gran colaborador del Instituto, quien por primera vez en 1910, propuso la idea de establecer en México una Sección. El 29 de Junio de 1922 en las Cataratas del Niágara, Ontario y bajo el nombre de "MEXICO SECTION OF THE AMERICAN INSTITUTE OF ELECTRICAL ENGINEERS", se aprobó la primera sección mexicana, teniendo como Primer Presidente a el Sr. G. H. Paget

Su misión principal de esta sección es:

"Se empeña en actividades técnicas educacionales y profesionales que promueven la teoría y la práctica de la electrotecnología para el desarrollo personal y profesional de sus miembros.

Fomenta el conocimiento y los avances científicos y tecnológicos, los cuales, miembros del IEEE transforman en productos prácticos y seguros, y en procedimientos que engrandecen la calidad de vida."[1]

2.1.3 ANSI

ANSI American National Standards Institute

ANSI cuyas siglas significan American National Standards Institute es una organización privada no lucrativa que coordina la estandarización voluntaria a la conformidad de los estándares de Estados Unidos. Fue fundada el 19 de octubre de 1918. Según su página en el Internet www.ansi.org textualmente nos dice:

"... ANSI, ha mantenido como meta fundamental mejorar la competitividad global de las empresas de Estados Unidos así como la calidad de vida, promoviendo y facilitando estándares voluntarios y de consenso, y sistemas para las pruebas de conformidad, además de promover su integridad. El Instituto representa los intereses de sus casi 1.000 miembros entre compañías, organizaciones, agencias

[1] http://www.ieee.org.mx/

estatales y miembros institucionales e internacionales, a través de su oficina en Nueva York y de su sede central en Washington, D.C."

ANSI ayuda al desarrollo del American National Standards (ANS) ya que proporciona acreditaciones para las organizaciones que desarrollan los estándares (SDOs). Estos grupos trabajan en conjunto para obtener una acreditación del ANSI para sus estándares desarrollados y esto significa que cumplen los requisitos esenciales propuestos por el Instituto para su apertura al público, y que estos últimos tengan la certeza de que el estándar está en forma adecuada.

Hay muchos grupos, tal vez, centenares de organizaciones dedicadas a hacer estándares de forma tradicionalista, siendo las 20 mayores de estas organizaciones dedicadas al desarrollo de estándares (SDOs). Sin embargo, hay también organizaciones que elaboran estándares no tradicionalistas. Todo esto es referido a Estados Unidos en donde existen expertos que adecuan estos estándares específicamente para su área profesional.

Sin embargo, todas estas organizaciones de desarrollo de estándares para seguir siendo acreditadas por el ANSI deben estar en constante actualización con base en un conjunto de procedimientos conocidos como "ANSI Procedures for the Development and Coordination of American National Standards". El hecho de cumplir con estos procedimientos asegura que estos estándares se están desarrollando de manera igualitaria y accesible, y nos da pie a que podamos participar en el desarrollo de otros estándares.

Todo lo anterior es de suma importancia, ya que, la actualización en la tecnología informática demanda muchas adecuaciones a los estándares, esto nos lleva a una adaptación de los ya existentes, pero también sirve como parte fundamental para amparar ante público en general que el estándar que van a adoptar será accesible, útil y adecuado a sus necesidades.

El proceso de los American National Standards se distingue por[2]:

- Obtener el consenso en un estándar propuesto por un grupo, o bien "el cuerpo para el consenso" que incluye a los representantes de las partes materialmente afectadas e interesadas.

- Incluir revisiones y comentarios, abiertos a un público amplio, sobre los borradores de los estándares.

- Tener en consideración y dar respuesta a los comentarios propuestos por los miembros con voto del cuerpo pertinente del consenso y a los comentarios de las revisiones públicas.

- Incluir los cambios aprobados en un borrador de un estándar y salvaguardar el derecho a apelar por parte de los participantes que crean que no se respetaron suficientemente los principios debidos del proceso durante el desarrollo de los estándares, de acuerdo con los procedimientos acreditados por ANSI para el desarrollo de estándares.

Aunque ANSI es el único representante en Estados Unidos también se preocupa por que esta estandarización se internacionalice y que cada país resuelva de manera adecuada a las necesidades de la comunidad de usuarios. Además también es el encargado de estar al tanto de las organizaciones principales de estándares estas son la International Organization for Standardization (ISO), y, a

[2] www.ansi.org

través del U.S. National Committee (USNC), la International Electrotechnical Commission (IEC). Este último es supervisado por Technical Management Committee del USNC (TMC).

ANSI fue fundador de la primera organización para la estandarización y tiene un gran peso ante el gobierno, dado esto ANSI tiene un acceso inmediato a los procesos de desarrollo de los estándares ISO e IEC. Una de las partes de la cual también es responsable es la acreditación de los U.S. Technical Advisory Groups (U.S. TAGs) cuya finalidad es informar de los cambios y acreditaciones, además de las posiciones que toma el sector técnico internacional respecto a los desarrollos de los estándares.

ANSI juega un papel importante ya que obliga a las organizaciones desarrolladoras de estándares a llevar un patrón establecido y esto hace que no se monopolice por alguna institución en cierta región. Aunque ANSI no se encarga directamente de llevar a cabo la internacionalización de los estándares, tenemos voluntarios de la industria y el gobierno, y el éxito depende de lo dispuesto que estén estos portadores del ANSI para destinar los recursos requeridos para una participación técnica en el proceso de estandarización.

2.1.4 TIA/EIA



La TIA/EIA es creadora de estándares, bajo la aprobación de ANSI, y sus estándares están dirigidos a la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico, sin embargo para fines prácticos y avocado a nuestro trabajo, presentaremos solamente los cinco estándares principales de la ANSI/TIA/EIA relacionados con la infraestructura de las redes:

1. ANSI/TIA/EIA/568. Estándar de cableado de telecomunicaciones en edificios comerciales.

2. ANSI/TIA/EIA/569. Estándar para ductos y espacios de telecomunicaciones en edificios comerciales.

3. ANSI/TIA/EIA/570. Estándar de alambrado de telecomunicaciones residencial y comercio pequeño.

4. ANSI/TIA/EIA/606. Estándar de administración para la infraestructura de telecomunicaciones en edificios comerciales.

5. ANSI/TIA/EIA/607. Requerimientos de puesta a tierra para telecomunicaciones.

2.1.4.1 ESTÁNDAR ANSI/TIA/EIA-568-A DE ALAMBRADO DE TELECOMUNICACIONES PARA EDIFICIOS COMERCIALES.

Este estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán. La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.

Propósito del Estándar EIA/TIA 568-A:

- Establecer un cableado estándar genérico de telecomunicaciones que respaldará un ambiente multiproveedor.
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableado

ISO ha desarrollado un cableado estándar sobre una base internacional con el título: Cableado Genérico para Cableado de Establecimientos Comerciales ISO/IEC11801.

Campo del Estándar EIA/TIA 568-A

El estándar especifica:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina.
- Topología y distancias recomendadas.
- Parámetros de medios de comunicación que determinan el rendimiento.
- La vida productiva de los sistemas de telecomunicaciones por cable por más de 10 años (15 actualmente).

Subsistemas de la norma ANSI/TIA/EIA-568-A

La norma ANSI/TIA/EIA-568-A (Figura 2.1) especifica los requisitos mínimos para cableado de telecomunicaciones dentro de edificios comerciales, incluyendo salidas y conectores, así como entre edificios de conjuntos arquitectónicos. De acuerdo a la norma, un sistema de cableado estructurado consiste de 6 subsistemas funcionales, los cuales se aprecian en la figura 2.1:

1. **Instalación de entrada, o acometida**, es el punto donde la instalación exterior y dispositivos asociados entran al edificio. Este punto puede estar utilizado por servicios de redes públicas, redes privadas del cliente, o ambas. Este es el punto de demarcación entre el portador y el cliente, y en donde están ubicados los dispositivos de protección para sobrecargas de voltaje.
2. **El cuarto, local, o sala de máquinas o equipos** es un espacio centralizado para el equipo de telecomunicaciones que da servicio a los usuarios en el edificio.

3. **El eje de cableado central** proporciona interconexión entre los gabinetes de telecomunicaciones, locales de equipo, e instalaciones de entrada. Consiste de cables centrales, interconexiones principales e intermedias, terminaciones mecánicas, y puentes de interconexión. Los cables centrales conectan gabinetes dentro de un edificio o entre edificios.
4. **Gabinete de telecomunicaciones** es donde terminan en sus conectores compatibles, los cables de distribución horizontal. Igualmente el eje de cableado central termina en los gabinetes, conectado con puentes o cables de puenteo, a fin de proporcionar conectividad flexible para extender los diversos servicios a los usuarios en las tomas o salidas de telecomunicaciones.
5. **El cableado horizontal** consiste en el medio físico usado para conectar cada toma o salida a un gabinete. Se pueden usar varios tipos de cable para la distribución horizontal. Cada tipo tiene sus propias limitaciones de desempeño, tamaño, costo, y facilidad de uso.
6. **El área de trabajo**, sus componentes llevan las telecomunicaciones desde la unión de la toma o salida y su conector donde termina el sistema de cableado horizontal, al equipo o estación de trabajo del usuario. Todos los adaptadores, filtros, o acopladores usados para adaptar equipo electrónico diverso al sistema de cableado estructurado, deben ser ajenos a la toma o salida de telecomunicaciones, y están fuera del alcance de la norma 568-A

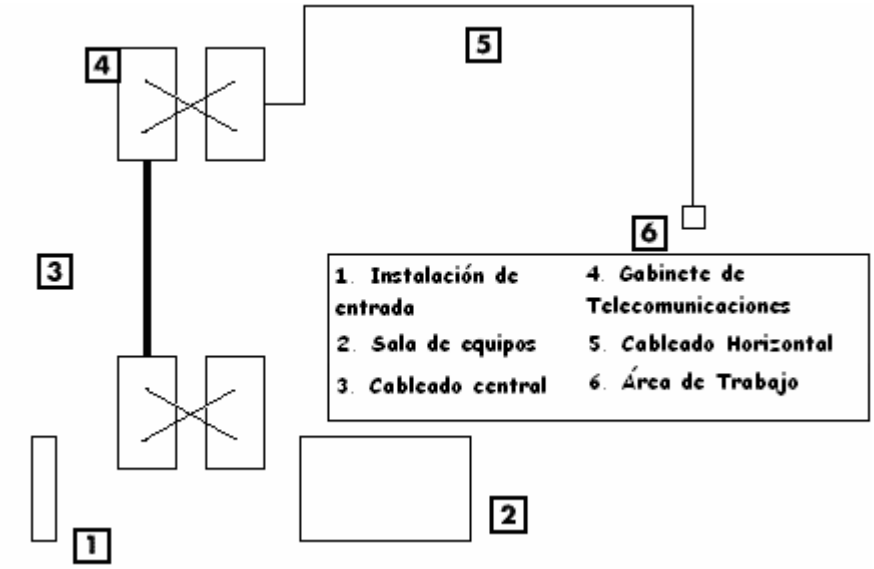


Figura 2.1 Subsistemas de la norma ANSI/TIA/EIA-568-A

2.1.4.2 ESTÁNDAR ANSI/TIA/EIA-569 DE RUTAS Y ESPACIOS DE TELECOMUNICACIONES PARA EDIFICIOS COMERCIALES

El Grupo de Trabajo de la Asociación de Industrias de Telecomunicaciones (TIA) TR41.8.3 encargado de Trayectorias y Espacios de Telecomunicaciones publicó la Norma ANSI/TIA/EIA-569-A ('569-A) en 1998.

Este estándar reconoce tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos.

- Los sistemas de telecomunicaciones y de medios son dinámicos.
- Las Telecomunicaciones son más que datos y voz.

Este estándar reconoce un precepto de fundamental importancia: De manera que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones, es imperativo que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

A continuación los rasgos sobresalientes de la Norma '569-A:

Objetivo

- Estandarizar las prácticas de construcción y diseño.
- Provee un sistema de soporte de telecomunicaciones que es adaptable a cambios durante la vida útil de la instalación.

Elementos

- Horizontal
- Cableado Maestro
- Área de Trabajo
- Habitáculo de Telecomunicaciones
- Sala de Equipo
- Espacio de Terminal Principal
- Instalación de Entrada

Provee especificaciones para el diseño de los espacios locativos y de las canalizaciones para los componentes de los sistemas de cableado para edificios comerciales y se definen 6 componentes:

Facilidades de Entrada

- Se define como la ubicación donde "entran" los servicios de telecomunicaciones al edificio.

Sala de equipos

- Se define como el espacio donde residen los equipos de telecomunicaciones comunes al edificio (PBX, Servidores centrales, Centrales de vídeo, etc.)
- Si un edificio es compartido por varias empresas, la sala de equipos puede ser compartida

Backbone

- Se dividen en: Canalizaciones entre edificios
- Vinculan las salas de facilidades de entrada de los edificios

Canalizaciones dentro del edificio

- Vinculan la sala de facilidades de entrada con la sala de equipos y la sala de equipos con los armarios de telecomunicaciones

Armarios de Telecomunicaciones

- Es el espacio que actúa como punto de transición entre la montante y las canalizaciones horizontales
- Se recomienda por lo menos un armario de telecomunicaciones por piso

Cuarto de Telecomunicaciones

- Es el área de trabajo exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. No debe ser compartido con instalaciones eléctricas.

Canalizaciones Horizontales

- Son las canalizaciones que vinculan las áreas de trabajo con los armarios de telecomunicaciones.

Áreas de Trabajo

- Son los espacios donde se ubican los escritorios, equipos activos o lugares habituales de trabajo (Figura 2.2)

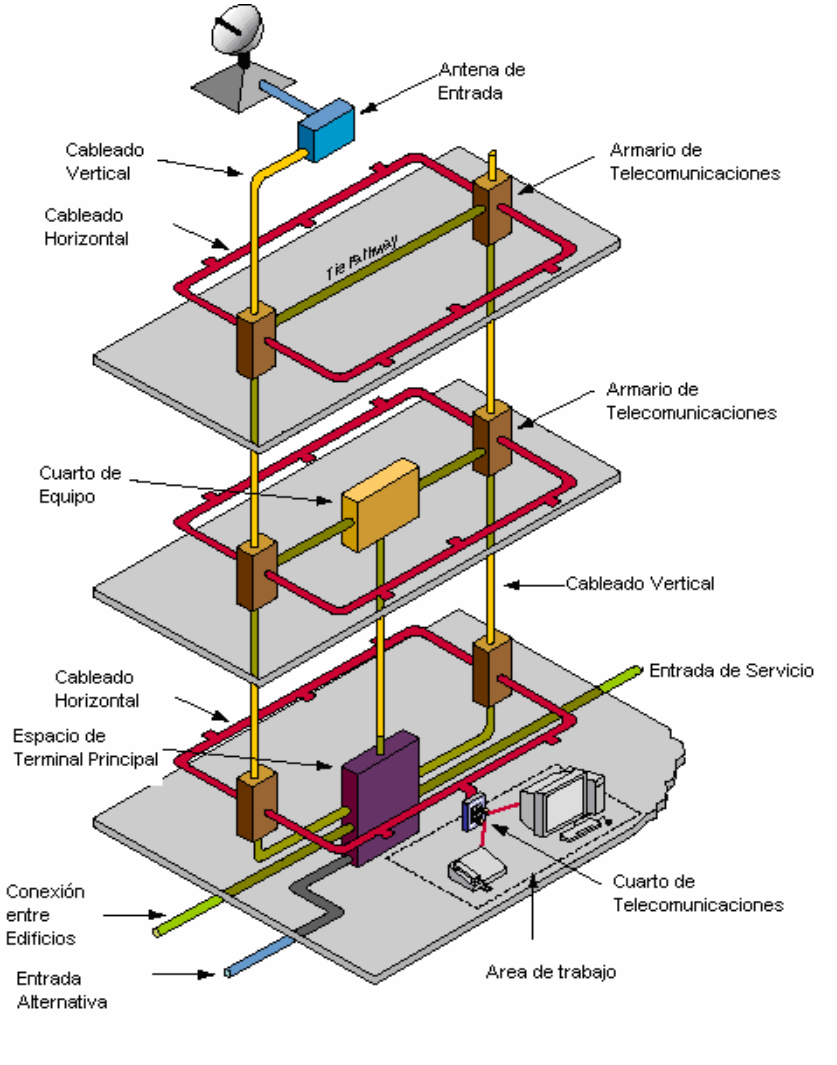


Figura 2.2 Áreas de trabajo

2.1.4.3 ESTÁNDAR ANSI/TIA/EIA 570 DE ALAMBRADO DE TELECOMUNICACIONES RESIDENCIAL Y COMERCIAL LIVIANO.

En este estándar están los requerimientos para tecnología existente y tecnología emergente. Especificaciones de cableado para voz, video, datos, automatización del hogar, multimedia, seguridad y audio están disponibles en este estándar. Este estándar es para nuevas construcciones, adiciones y remodelaciones en edificios residenciales.

Grados para cableado residencial:

- Grado 1 – provee un cableado genérico para el sistema telefónico, satélite y servicios de datos.
- Grado 2- provee un cableado genérico para sistemas multimedia básico y avanzado.
- 100 omhs 4 Pares trenzados (UTP).
- 62.5/125mm fibra óptica multi-modo
- 50/125mm fibra óptica multi-modo

2.1.4.4 ESTÁNDAR ANSI/TIA/EIA-606 "NORMA DE ADMINISTRACIÓN PARA LA INFRAESTRUCTURA DE TELECOMUNICACIONES EN EDIFICIOS COMERCIALES".

Proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado. Seguir esta norma, permite una mejor administración de una red, creando un método de seguimiento de los traslados, cambios y adiciones. Facilita además la localización de fallas, detallando cada cable tendido por características.

2.1.4.5 ANSI/TIA/EIA-607 "REQUISITOS DE ATERRIZADO Y PROTECCIÓN PARA TELECOMUNICACIONES EN EDIFICIOS COMERCIALES"

Dicta prácticas para instalar sistemas de aterrizado que aseguren un nivel confiable de referencia a tierra eléctrica, para todos los equipos.

Cada uno de estas normas funciona en conjunto con la 568-A. Cuando se diseña e instala cualquier sistema de telecomunicaciones, se deben revisar las normas adicionales como el código eléctrico nacional (NEC) de los E.U.A., o las leyes y previsiones locales como las especificaciones NOM (Norma Oficial Mexicana).

2.1.5 INSTITUTO MEXICANO DE NORMALIZACIÓN Y CERTIFICACIÓN (IMNC).

La Confederación de Cámaras Industriales de los Estados Unidos Mexicanos (CONCAMIN), la Confederación de Cámaras Nacionales de Comercio (CONCANACO) y el Consejo Nacional Agropecuario (CNA), decidieron crear una institución capaz de fortalecer el sistema mexicano de Normalización, Metrología y Evaluación de la

Conformidad; que tuviera como objetivo central y fundamental promover la Normalización, el uso de Sistemas de Gestión y desarrollo de tecnologías, como herramientas esenciales en la creación de una cultura de promoción de valores económicos, ecológicos y sociales.

Así es como, el 10 de agosto de 1993 nace IMNC, con el firme propósito de ayudar a las organizaciones mexicanas a enfrentar y defenderse en condiciones de igualdad con sus contrapartes extranjeras.

La actuación en la normalización nacional, regional e internacional de éste Instituto, se da a partir de que es un Organismo Nacional de Normalización registrado y reconocido por el Gobierno Mexicano por medio de la Dirección General de Normas de la Secretaría de Economía, en los términos que establece la Ley Federal sobre Metrología y Normalización y su Reglamento.

Hasta la fecha, tiene facultades para elaborar, revisar, modificar, emitir, publicar y cancelar normas mexicanas (NMX) en los siguientes ámbitos:

Número de registro	Ámbito de competencia
0002	Sistemas de calidad (en general)
0002/A	Turismo
0002/B	Metrología
0002/C	Sistemas de administración ambiental
0002/D	Grúas y dispositivos de elevación
0002/E	Artes gráficas
0002/F	Sistemas de administración de seguridad y salud en el trabajo

En Marzo de 2005 entro en vigor la última actualización de la norma para cableado estructurado denominada: NMX-I-248-NYCE-2005. Esta Norma Mexicana especifica un sistema de cableado estructurado genérico para telecomunicaciones en edificios comerciales que pueden implementarse con productos de uno o varios fabricantes, así como los requisitos de desempeño, distancias, configuraciones y topología del cableado estructurado genérico. Proporciona guías para la instalación, operación y verificación de cableados para tecnologías de la información. Así mismo, especifica el cableado estructurado genérico en edificios.

2.2 Modelo OSI

Las primeras arquitecturas de redes eran incompatibles entre sí, ya que cada proveedor tenía su propio formulismo dependían únicamente de estos.

Esto causó una dependencia hacia el fabricante. Pero para los años 70's se realizaron estudios para desarrollar una arquitectura que fuera compatible con todas las computadoras sin importar el proveedor o fabricante, esto con el fin de que la comunicación entre dichas computadoras fuera posible. Este objetivo originó que la Organización Internacional para Normalizaciones, ISO (International Organization for Standarization), desarrollara un modelo de referencia para la interconexión de sistemas abiertos, OSI (Open Systems Interconnection), y, por supuesto los protocolos estándar asociados. El modelo de referencia OSI proporcionó un entorno de trabajo para definir el proceso global de comunicaciones;

por tanto, su finalidad era facilitar el desarrollo de estándares. Este modelo incorporó gran parte del conocimiento disponible en la comunidad investigadora y ha desempeñado un papel muy útil en el diseño de redes durante más de dos décadas.

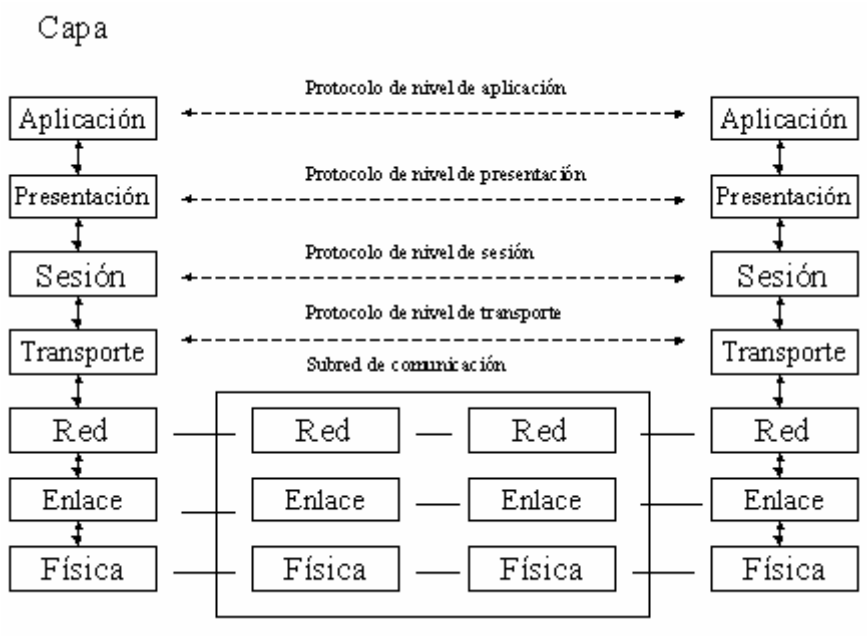


Figura 2.3 Arquitectura de red basada en el modelo OSI

El modelo OSI tiene varias características, una de ellas y a nuestro parecer la más importante, es la estructura multinivel (Figura 2.3), la cual nos ayuda a que cada nivel se dedique a una función en especifico y esto hace que en la resolución de problemas no tengamos todo englobado, sino que lo manejamos por partes o en este caso en niveles. Pero estos niveles utilizan servicios de un nivel arriba y un nivel abajo, es decir, aunque sus funciones son diferentes todos los niveles dependen de un nivel superior e inferior.

En cada nivel tenemos algo llamado “encabezados”, en donde su importancia radica que a cada mensaje le asigna un “encabezado” para que la computadora receptora se entere que la computadora emisora le esta enviando un mensaje, aunque esto parezca que al añadirle información al mensaje original lo robustece, al usuario final solamente le llega el mensaje original, esto dado que, al recibir el mensaje la computadora destino retira los encabezados en orden inverso a como fueron incorporados de la computadora origen.

El modelo OSI define en siete capas los protocolos de comunicación. Y como ya habíamos mencionado cada uno de los niveles tiene funciones definidas, que se relacionan con las funciones de las capas siguientes o anteriores. Los niveles inferiores se encargan de acceder al medio, mientras que los superiores, definen cómo las aplicaciones acceden a los protocolos de comunicación. Las cuales se describen a continuación:

2.2.1 Capa Física

En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación. Los aspectos de diseño implican asegurarse que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal, no como bit 0. Además

se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es unidireccional o bidireccional (simplex, duplex o full-duplex), además de los aspectos mecánicos de las conexiones y terminales, por ejemplo, de los estándares relacionados con el puerto serie RS-232C, presente en todos las computadoras actuales, es la forma común para realizar transmisiones de datos entre éstas.

El RS-232 consiste en un conector tipo DB-25 de 25 pines, aunque es normal encontrar la versión de 9 pines DB-9, donde su costo es menor e incluso mas extendido para cierto tipo de periféricos. En cualquier caso, las computadoras no suelen emplear más de 9 pines en el conector DB-25. Las señales con las que trabaja este puerto serie son digitales, de +12V (0 lógico) y -12V (1 lógico), esto para la entrada y salida de datos, y para las señales de control es a la inversa. El estado de reposo en la entrada y salida de datos es -12V. Dependiendo de la velocidad de transmisión empleada, es posible tener cables de hasta 15 metros.

Cada pin puede ser de entrada o de salida y cada uno de ellos tiene una función específica. Las más importantes son:

Pin	Función
TXD	(Transmitir Datos)
RXD	(Recibir Datos)
DTR	(Terminal de Datos Listo)
DSR	(Equipo de Datos Listo)
RTS	(Solicitud de Envío)
CTS	(Libre para Envío)
DCD	(Detección de Portadora)

Las señales TXD, DTR y RTS son de salida, mientras que RXD, DSR, CTS y DCD son de entrada.

En esta capa se lleva a cabo la transformación de un paquete de información binaria en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Cuando actúa en modo recepción el trabajo es inverso; se transforma estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

Estos impulsos pueden ser:

- Eléctricos
- Electromagnéticos
- Luminosos

Para cada tipo de impulso, tenemos un medio propio que lo propagará, así podemos tener dos grandes grupos:

- Medios aéreos: Aquí tenemos a los impulsos electromagnéticos, los cuales no necesitan cables para poder propagarse, simplemente el aire. Un ejemplo claro son las redes Wireless.

- Medios terrestres: Para el caso de los impulsos luminosos tenemos a la fibra óptica y para los eléctricos tenemos diferentes tipos de cable (par trenzado, cable coaxial, etc.)

Para cada tipo de medio se debe seguir ciertas normas para que la transmisión de los impulsos sea exitosa. Para el caso de los medios terrestres, el cable tiene características que a veces pueden ser una limitante para una transmisión satisfactoria. Para que esto no suceda, se siguen estándares que nos llevarán a tener un cableado genérico denominado “cableado estructurado”.

2.2.1.1 Cableado Estructurado

Antes de que surgiera el cableado estructurado existía el propietario (este tipo de cableado es sin un orden en específico, simplemente se cubre la necesidad de interconectar computadoras), pero provocó muchos problemas de desarrollo tecnológico ya que las empresas dejaron de invertir en tecnología al ver que cuando querían hacer cambios en su sistema tenían que cambiar el cableado.

Para solucionar este problema, dos asociaciones en Estados Unidos, la TIA (Telecommunications Industry Association; Asociación de Industrias de Telecomunicaciones) y la EIA (Electronic Industries Association; Asociación de Industrias Electrónicas), se pusieron de acuerdo para poder generar un cableado genérico al cual denominaron cableado estructurado.

Desgraciadamente los usuarios finales no contaban con ningún tipo de experiencia en el manejo de cableado estructurado y tenían distintas opciones: cableado coaxial grueso, cableado coaxial delgado, UTP (Unshielded Twisted Pair; Par trenzado sin blindaje), STP (Shielded Twisted Pair; Par trenzado blindado) y cable telefónico, entre otros, pero el problema al que se enfrentaban era saber cuál era la opción más viable para su empresa.

De esta forma el cableado estructurado vino a establecer una estandarización de medios de distribución con interfaces de conexión que cumplen con las normas internacionales.

2.2.1.2 Importancia del Cableado Estructurado

Como ya se mencionó anteriormente un cableado estructurado es muy útil para las empresas. Permite ahorrar costos significativos a diferencia del cableado propietario, con el cual se tendrían que hacer grandes inversiones a mediano plazo.

“El cableado estructurado sirve para soportar multimarcas y lo hace de una manera universal para que la forma de conectar los cables sea unificada y no existan variaciones.

La importancia que tiene el cableado estructurado es que hace más eficiente el trabajo de la red, facilita los MACs y hace más accesible la inversión. Aunque en un principio puede resultar más costoso que un cableado propietario, a la larga los costos se reducen sobre todo cuando se tienen que dar cambios en la red”, afirma Pedro Lerma, coordinador de Marketing para el área de Cableado Estructurado de Anixter México[3].

Dentro de las ventajas que tiene el cableado estructurado están:

- Mejor costo-beneficio
- Ahorro para las empresas
- Soporta cualquier tipo de aplicación
- Actualizaciones mínimas
- Costos accesibles por mantenimiento

[3] Redes de Computadoras, Adrew S. Tanenbaum Cuarta Edición

- Fácil administración de los servidores

2.2.1.3 Normas para el cableado estructurado

El cableado estructurado está diseñado para usarse en cualquier lugar y en cualquier momento; elimina la necesidad de seguir las reglas de un proveedor en particular, concernientes a tipos de cable, conectores, distancias, o topologías; Permite instalar una sola vez el cableado, y después adaptarlo a cualquier aplicación, desde telefonía, hasta redes locales Ehernet o Token Ring.

Estas normas deben estar basadas en cualquier estándar autorizado por las organizaciones mencionadas en el apartado 2.1, ya que, aunque tenemos la libertad de elegir la norma o estándar deseado, hay protocolos que nos limitan. Esto es para que al instalar nuestra red, se le pueda dar mantenimiento adecuado aunque no sean las mismas personas que la instalaron, también nos ayuda para que podamos aprovechar al 100% nuestra red.

2.2.2 Capa de enlace

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación efectiva que, al llegar a la capa de red, aparezca libre de errores de transmisión. La capa de enlace logra esta tarea haciendo que el transmisor fragmente o divida los datos de entrada en **tramas** de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción, si no fue enviada correctamente esta capa también se encarga de solucionar los problemas de reenvío, o mensajes duplicados cuando hay destrucción de tramas.

La capa de enlace puede considerarse dividida en dos subcapas:

1. Control lógico de enlace LLC ("Logical Link Control") define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores. Dentro de los protocolos comunes para la transmisión encontramos:

    - BSC: Usa código de 7 bits de la ISO completando el octavo bit con un 0. Orientado a transmisión de bytes, por lo que espera datos en número entero de octetos.
    - HDLC: Orientado al bit, delimitado por FLAGs

2. Control de acceso al medio MAC ("Medium Access Control"). Esta subcapa actúa como controladora del adaptador de red. La dirección física contenida en el hardware de la tarjeta de red es conocida como dirección MAC "MAC address" Su principal tarea consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo CSMA/CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa. El control de acceso MAC y el protocolo CSMA/CD serán retomados para una explicación más extensa en los siguientes aparatados.

De igual modo es necesario el control del tráfico, ya que, el controlar los diálogos entre dos computadoras que se estén comunicando y definir los mecanismos para hacer las llamadas a procedimientos remotos es tarea de esta capa, y debe hacerse en una perfecta sincronización,

Un problema, al cual también se debe poner atención, es en la transmisión bidireccional de los datos, el tema principal son los algoritmos para la comunicación confiable y eficiente entre dos máquinas adyacentes.

Dentro de los problemas que enfrenta esta capa como ya habíamos dicho, son los circuitos de comunicación pero tratemos más de cerca y más detalladamente estos problemas como sus velocidades finitas de transmisión, y el tiempo de propagación. Normalmente se parte de un flujo de bits en tramas, lo que se refiere a que el nivel de enlace detecte de manera confiable los errores, así se calcula un checksum o comprobación de datos para cada uno. Estas tramas contendrán información como: número de caracteres (un campo de encabezamiento guarda el número, pero si el número es cambiado en una transmisión, es difícil de recuperar) y caracteres de inicio y fin.

2.2.2.1 Tarjetas de interfaz de Red

Todas las computadoras que se conectan a una red lo tienen que hacer físicamente por un dispositivo de red, estos son conocidos como Network Interface Card, NIC (tarjetas de interfaz de red) o también como tarjetas adaptadoras LAN, sin embargo, la manera más fácil y conocida de llamarlas es simplemente tarjetas de red.

En la gran mayoría de los casos, esta tarjeta de red se conecta en alguna ranura de expansión de la computadora, sin embargo, tenemos algunas en las que se conectan externamente, como por un puerto paralelo o uno serial. Actualmente tenemos tarjetas de red externas que se conectan mediante un puerto USB (Figura 2.4) de la máquina y también tenemos las “tarjetas de red inalámbrica” (Figura 2.5), que de igual forma pueden ser externas o internas.



Figura 2.4 Tarjeta de red mediante el puerto USB



Figura 2.5 Tarjeta de red inalámbrica

La función de estas tarjetas es recopilar información de la computadora y la convierte en lenguaje adecuado para su transmisión, la envía a través del cable de conexión si la red es alámbrica o mediante ondas si es inalámbrica. Llegando esta señal a otra tarjeta de interfaz de red.

La tarjeta NIC dispone de un puerto que cumple las especificaciones de conector y de transmisión de los estándares de la capa física. La NIC también incluye una memoria de sólo lectura (ROM) que contiene las instrucciones que le permiten implementar protocolos MAC (de los cuales hablaremos más adelante) de un estándar LAN.

Las características con las que cuentan las NIC’s son las siguientes:

1. Comunicaciones de host a tarjeta
2. Buffering

3. Formación de paquetes
4. Conversión serial a paralelo
5. Codificación y decodificación
6. Acceso al cable
7. Saludo
8. Transmisión y recepción

Éstas son solamente algunas propiedades más representativas que ayudan a que la comunicación entre dos computadoras sea exitosa.

2.2.2.2 Direcciones MAC

Una dirección MAC (Médium Access Control) es un identificador exclusivo de cada tarjeta de interfaz de red, y en el modelo OSI la podemos ver trabajar en la capa 2 – Enlace, como se menciono en el apartado anterior.

Una MAC está formada por 48 bits, de los cuales los 24 primeros o los tres primeros octetos de la dirección identifican al fabricante, y los 24 siguientes son el número de referencia que el fabricante le ha asignado particularmente a esa NIC. Por ello se supone que no existen dos NIC con la misma MAC, o no deben de existir, aunque en el mercado existen tarjetas de red a las cuales se le pueden cambiar la MAC, esto quiere decir que han sido clonadas.

La forma de representar la dirección MAC es en hexadecimal:

1A-B2-CD-34-56-E7

También se pueden encontrar de la siguiente forma:

1AB2CD-3456E7, siendo la anterior la forma más común de representación.

Toda la información que es transmitida por la red, no importando el medio que se utilice, habrá sido encapsulada en la capa de enlace con una MAC destino y una MAC origen, lo que accede a que la información llegue a la MAC correcta.

También podemos tener tarjetas que operan de modo “promiscuo”, estas tarjetas aceptan toda la información que se transmita aunque no sea la MAC coincidente, para escuchar el tráfico de información, este modo es utilizado por administradores para poder tener un control sobre la red y resolver los problemas con mayor facilidad, para todo esto existe un nombre, “Sniffer”. Un *sniffer* es un programa que permite monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella. El sniffer también puede ser usado por los *hackers* para interceptar claves de acceso sin encriptar y otra información que pueda facilitar el acceso no autorizado a las computadoras de una red.

Al inicio de las redes locales, su desarrollo fue pensado para operar de manera privada, es por esto, que se pensó que existía cierta confianza entre todos los que tendrían contacto con la red, pero esta suposición en la actualidad, no es válida, por lo que se necesitan protocolos de seguridad de red.

Todo dispositivo que se quiere conectar a una red deberá de tener una MAC para que se pueda identificar a nivel capa de Enlace.

¿Pero porqué necesita identificase ante la capa de enlace? La capa de enlace se divide en dos subcapas, la de control de enlace lógico, LLC (*Logical Link Control*), y la de control de acceso al medio, MAC.

La subcapa MAC trata el problema de coordinación de acceso al medio físico, es por eso, que es tan importante una dirección MAC, ya que especifican las conexiones lógicas de las estaciones de trabajo a la red LAN. La principal tarea de las entidades MAC es ejecutar el protocolo MAC que decide cuándo transmitir las tramas a través del medio compartido.

Para la subcapa de control de enlace lógico, LLC, el cual funciona para todos los estándares de MAC, es parte de la cabecera LLC/SNAP del IEEE usada para identificar el tipo de un paquete. La cabecera completa es de 6 bits, de los que la parte LLC ocupa los primeros tres. LLC puede mejorar el servicio datagrama ofrecido por la capa MAC para ofrecer algunos servicios HDLC en la capa de Enlace. LLC también ayuda a intercambiar paquetes de información entre redes LAN que tienen diferentes protocolos MAC. La manera en que los datos son transferidos es a lo que se le llama tramas o frames, los formatos típicos para frames son los usados por los protocolos BSC y HDLC.

2.2.2.3 Protocolo de acceso al medio CSMA/CD

El protocolo CSMA/CD, cuyas siglas en ingles significan: “Carrier Sense Multiple Access with Collision Detection”, y que significan: “Detección de Portadora con Acceso Múltiple y Detección de Colisiones”, debe detectar la presencia de una señal portadora que se haya originado en una computadora lista para transmitir, y si el medio está libre, permite que dicha señal llegue su destino. Sin embargo, si además de la señal emitida, se detecta otra computadora que también quiere transmitir y libera su señal, se produce una colisión entre las señales. El protocolo CSMA/CD detecta dicha colisión y pide a las computadoras que retransmitan después de un tiempo aleatorio. Y ya que se trata de 2 tiempos aleatorios distintos, aseguramos que en la retransmisión de las señales no se presentará una nueva colisión.

La tecnología CSMA/CD se desarrolló por Digital Equipment Corporation e Intel, en cooperación con la compañía Xerox en el Centro de Investigación de Palo Alto en 1976. Utiliza topología de bus o estrella, soportando niveles de transferencia de datos de 10 Mbps y hasta 1 Gbps, es altamente usada en las LAN’s en la subcapa MAC. Pero no fue publicada oficialmente sino hasta 1980 por un consorcio de 3 empresas que crearon el estándar DIX (DEC- INTEL- XEROX), que dió vida al Ethernet experimental, liberándolo a una calidad de producción abierta que operaba a 10 Mbps, y posteriormente el Comité de Estándares LAN de la IEEE le otorgó el estándar 802 publicado para 1985 con el título formal de Especificaciones de Capa Física del Método de Acceso por Sensor de Portadora con Acceso Múltiple con Detección de Colisiones IEEE 802.3, y fue cuando la ISO la convirtió en un estándar mundial.

CSMA/CD, así como otros protocolos de LAN, utiliza un modelo como el que se presenta en la Figura 2.6 y en donde podemos explicar mucho mejor este protocolo.

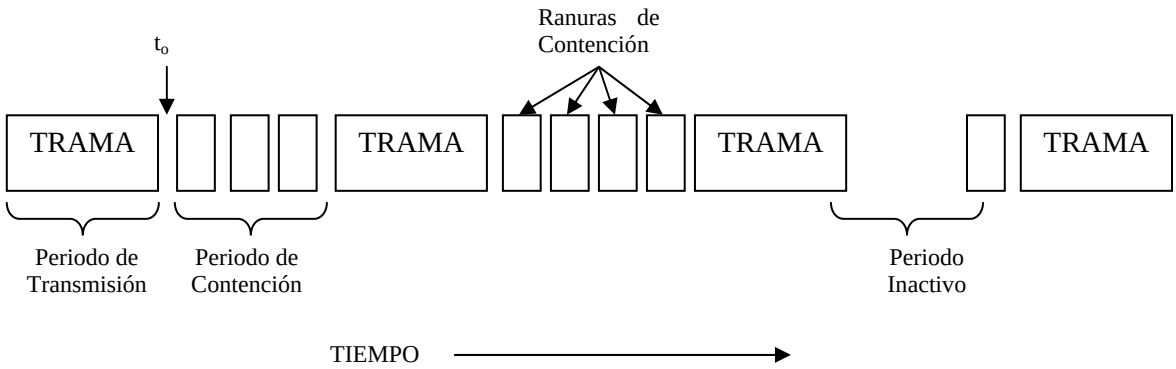


Figura 2.6 Protocolo CSMA/CD

En el punto t_0, es donde una computadora ha terminado su transmisión y da oportunidad a otra para poder transmitir. Sin embargo, al está el canal libre se puede dar el caso de una colisión, y entonces, comienza el proceso antes mencionado en donde se detiene la transmisión, esperando un tiempo aleatorio y comienza una nueva transmisión. Así, nuestro modelo CSMA/CD consistirá en periodos alternantes de contención y transmisión; pero también habrá periodos de inactividad en donde no se presentaran colisiones, pero tampoco se transmitirán señales en el canal.

Cabe mencionar que el estándar 802.3 no es el único otorgado por IEEE:Token Ring, también llamado IEEE 802.5, fue ideado por IBM y algunos otros fabricantes. Con operación a una velocidad de 4 Mbps o 16 Mbps, Token Ring emplea una topología lógica de anillo y una topología física de estrella. La tarjeta NIC de cada computadora se conecta a un cable que, a su vez, se hace lo mismo hacia un hub central llamado unidad de acceso a multiestaciones (MAU). Token Ring se basa en un esquema de paso de señales (token passing), es decir que pasa un token (o señal) a todas las computadoras de la red. La computadora que esté en posesión del token tiene autorización para transmitir su información a otra computadora de la red. Cuando termina, el token pasa a la siguiente computadora del anillo. Si la siguiente computadora tiene que enviar información, acepta el token y procede a enviarla. En caso contrario, el token pasa a la siguiente computadora del anillo y el proceso continúa. La MAU se salta automáticamente un nodo de red que no esté encendido. Sin embargo, dado que cada nodo de una red Token Ring examina y luego retransmite cada token, un nodo con mal funcionamiento puede hacer que deje de trabajar toda la red. Token Ring tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes con poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, Token Ring llega a ser más eficiente que CSMA/CD.

2.2.3 Capa de red

Los servicios de la capa de red deben estar dispuestos para ser utilizados por los procesos de niveles superiores a través de la interfaz entre las dos capas. Esos niveles no deben conocer el tipo de red sobre las que funcionan, y la capa de red debe ocultar todos esos detalles. Lo más importante es eliminar los cuellos de botella que se producen al saturarse la red de paquetes enviados, por lo que también es necesario encaminar cada paquete con su destinatario.

Al igual que en otras capas de la arquitectura, los servicios del nivel de red se pueden diseñar orientados o no orientados a conexiones y con control de errores o sin control de errores. Si se utilizan servicios orientados a conexión y fiables, es la red la que asume la complejidad, mientras que, si se utilizan servicios sin conexión

y no fiables, es el usuario el que asume la complejidad en los protocolos. Dentro de la capa existe una contabilidad sobre los paquetes enviados a los clientes.

Otro problema a solucionar por esta capa es la interconexión de redes heterogéneas, solucionando problemas de protocolos diferentes, o direcciones desiguales.

Este nivel encamina los paquetes de la fuente al destino final a través de encaminadores (routers) intermedios, para lo cual tiene que conocer la topología de la subred, evitar la congestión, y manejar saltos cuando la fuente y el destino están en redes distintas.

Por lo anterior, en este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta. Como consecuencia, esta capa puede considerarse dividida en dos:

- Transporte: Es la encargada de empaquetar los datos a transmitir (de usuario), utiliza los paquetes de datos. Es en esta categoría donde se encuentra el protocolo IP.
- Conmutación ("Switching"): Esta parte es la encargada de intercambiar información de conectividad específica de la red (su actividad es raramente percibida por el usuario). Los encaminadores son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. En esta categoría se encuentra el protocolo ICMP ("Internet Control Message Protocol"), responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante PING.

En esta capa como se mencionó, tenemos el protocolo **IP** (Internet Protocol), que es la base esencial de Internet, ya que, hace posible enviar datos de la fuente al destino. La capa de transporte parte del flujo de datos en datagramas, durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. Para que este protocolo funcione correctamente necesita el uso de direcciones IP, pero hablaremos más de esto en el siguiente apartado.

2.2.3.1 Direcciones IP

Cada host y cada dispositivo de enrutamiento tendrán una dirección única llamada dirección IP la cual tendrá una longitud de 32 bits; la cual se muestra en la Figura 2.7 y será utilizada en los campos “dirección de origen” y “dirección de destino” de la cabecera. Como ya dijimos la combinación es única: no hay 2 máquinas que tengan la misma dirección IP, ya que esto provocaría un error interno.

Una dirección IP no se refiere exactamente al host, sino que, se refiere a una interfaz de red, por lo que si un host está en dos redes, debe tener dos direcciones IP aunque sea la misma máquina, pero esto, en la práctica resulta muy poco común.

Esta dirección IP consta de un identificador de red y de un identificador de la computadora. La dirección está codificada para permitir una asignación variable de los bits utilizados al especificar la red y la computadora.

Las direcciones IP se dividieron en cinco categorías, las cuales se listan en la Figura 2.7. Está asignación se ha llamado direccionamiento con clase. Y aunque ya casi no se utiliza, es muy común encontrarla en los libros.

Clase A: Pocas redes, cada una con muchas computadoras. El rango de valores es de 1 hasta 126.

Clase B: Un número medio de redes, cada una con un número medio de computadoras. El rango de valores es de 128 hasta 191.

Clase C: Muchas redes, cada una con pocas computadoras. El rango de valores es de 192 hasta 233.

Clase D: Permite hacer multitransmisión en la cual el datagrama se dirige a múltiples computadoras. Podemos enviar un paquete IP a un grupo de máquinas que por ejemplo pueden estar cooperando de alguna manera mediante la utilización de una dirección de grupo. El rango de valores es de 224 hasta 239.
Clase E: Reservado, sin embargo el rango de valores es solamente del 240 hasta el 255.

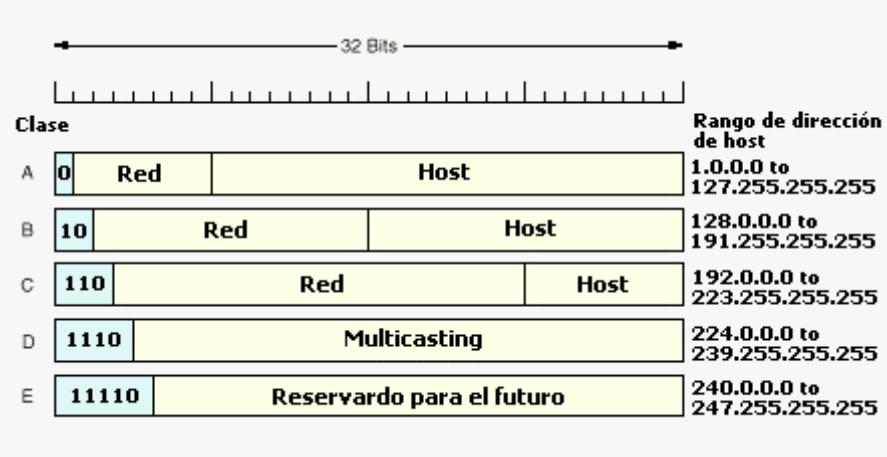


Figura 2.7 Clases de direcciones IP

Los formatos de clase A, B, C y D permiten hasta 128 redes con 16 millones de host cada una, 16,362 redes de hasta 64,000 host, 2 millones de redes de hasta 256 host cada una. También soportan la multidifusión, en la cual un datagrama es dirigido a múltiples host.

Una dirección IP consta de 2 partes principales, el NETWORK ID y el HOST ID, el Network ID es la primera parte de una dirección IP, el cual identifica el segmento de red en el cual la computadora esta localizado; y el Host ID es la segunda parte de la dirección IP, el cual identifica a la computadora, encaminador u otro dispositivo en el segmento, el Host ID para cada host debe ser único en un Network ID, esto nos lleva a tener un orden en las asignaciones de direcciones IP, ya que hay cerca de 500,000 redes conectadas al Internet, y la cifra se duplica cada año, es por esto que se crea una organización llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números) que controla toda la asignación de números y nombres para evitar conflictos. A su vez, la ICANN ha delegado partes del espacio de direcciones a varias autoridades regionales, las cuales han repartido direcciones IP a los ISPs y a otras compañías.

Estas direcciones IP, se escriben en notación decimal con puntos, en este formato, cada uno de los 4 bytes se escriben en decimal, de 0 a 255. Dentro de esta numeración tenemos 2 números en especial que es importante resaltar que son el 0 y el -1 (todos los 1s), el valor 0 se refieren a la red actual, estas direcciones permiten que las máquinas se refieran a su propia red sin saber el número (pero tiene que saber su clase para saber cuantos 0 hay que incluir). El valor -1 se usa como dirección de difusión para indicar todos los host de la red indicada, por lo común una LAN. También existen direcciones que no están consideradas dentro de las clases que ya habíamos mencionado, esta es la 127.xxx.yyy.zzz, esto es, porque se reservan para direcciones locales de prueba, es decir, los paquetes a esta dirección no se mandan por el cable, sino que se trabaja localmente.

SUBREDES

Cuando se trabaja con redes pequeñas, es decir, pocos equipos activos interconectados entre si, el administrador puede fácilmente configurar el rango de direcciones IP para conseguir un funcionamiento óptimo del sistema, pero cuando estas crecen y la red va aumentando, los dominios de colisión cada vez serán más grandes, llegando un momento en el que el rendimiento de la red se ve afectado seriamente.

La solución a este problema es permitir la división de una red en varias partes para uso interno, pero aún actuar como una sola red ante el mundo exterior, esto es, el número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. En la literatura sobre Internet, a estas partes de la red (en este caso Ethernets) se les llama “subredes”.

No debemos confundir el término de “subredes” con el de “subred” cuyo significado es el grupo de todos los enrutadores y líneas de comunicación de una red.

Para implementar subredes, el enrutador principal necesita una **máscara de subred,** concepto análogo al de máscara de red en redes generales, y que va a ser la herramienta que utilicen luego los routers para dirigir correctamente los paquetes que circulen entre las diferentes subredes.

Las máscaras de subred también se pueden escribir en notación decimal con puntos, o agregando a la dirección IP una diagonal seguida del número de bits usados para los números de red y subred.

2.2.4 Capa de transporte

La función principal es de aceptar los datos de la capa superior y dividirlos en unidades más pequeñas, para pasarlos a la capa de red, asegurando que todos los segmentos lleguen correctamente, esto debe ser independiente del hardware en el que se encuentre.

Sus servicios son muy semejantes a los de la capa de red. Las direcciones y el control de flujo son semejantes también. Sin embargo la razón por la cual necesitamos una capa de transporte es que el nivel de red es una parte de la subred y los usuarios no tienen ningún control sobre ella. El nivel de transporte permite que los usuarios puedan mejorar el servicio del nivel de red (que puede perder paquetes, puede tener routers que no funcionan a veces, etc.). Además el nivel de transporte permite que tengamos un servicio más confiable que el nivel de red. También, las funciones de la capa de transporte pueden ser independientes de

las funciones de la capa de red, las aplicaciones pueden usar estas funciones para funcionar en cualquier tipo de red.

Para bajar los costos de transporte se puede multiplexar varias conexiones en la misma red, esto es, que necesita hacer el trabajo de multiplexión transparente a la capa de sesión. La capa de transporte utiliza los servicios de la capa de red para proveer un servicio eficiente y confiable a sus clientes, que normalmente son los procesos en el nivel de aplicación. El hardware y software dentro de la capa de transporte se llama a la entidad de transporte y pueden estar en el corazón del sistema operativo, en un programa, en una tarjeta, etc.

Ya que la mayoría de las veces la capa de transporte tiene que multiplexar las conexiones como ya se dijo, si se desea una transmisión de datos muy rápida se abrirán varias conexiones y los datos se dividirán para hacerlos pasar por estas. Si solo se tiene una conexión pero se quieren pasar varios datos se deberá multiplexar el canal, de manera que por tiempos transmitirá una conexión u otra.

Si una parte de la subred se cae durante una conexión, el nivel de transporte puede establecer una conexión nueva y recuperar de la situación. Es así como entra el protocolo TCP (Transmition Control Protocol) que es el método usado por el protocolo IP (Internet Protocol) para enviar datos a través de la red. Mientras IP cuida del manejo del envío de los datos, TCP cuida el trato individual de cada uno de ellos (llamados comúnmente "paquetes") para el correcto enrutamiento de los mismos a través de Internet.

Cuando los datos van en salida, esta capa acepta los datos provenientes de las capas superiores, se dividen en unidades más pequeñas, si es necesario, se pasan a la capa de red y se asegura que todas las piezas lleguen correctamente al otro extremo. En llegada, los datos provienen de las capas superiores y la capa de transporte se encarga de reensamblar los bloques de datos a fin de conformar el mensaje y pasarlo al siguiente nivel superior; además, todo esto se debe hacer con eficiencia y de manera que se aíslen las capas superiores de los cambios en la tecnología del hardware. La capa de transporte también determina que tipo de servicio se debe proporcionar a la capa de sesión y, finalmente, a los usuarios de la red.

Un ejemplo típico de protocolo usado en esta capa es TCP, que con su homólogo IP de la capa de Red, configuran el modelo de referencia TCP/IP utilizado en Internet (este modelo será explicado más adelante), aunque existen otros como UDP ("Universal Datagram Protocol") una capa de transporte utilizada también en Internet por algunos programas de aplicación.

2.2.5 Modelo de referencia TCP/IP

TCP/IP surge de la necesidad de desarrollar un procedimiento estandarizado de comunicaciones que se utilizaría de manera inevitable en una variedad de plataformas. La necesidad de una norma, que además, estuviera disponible para todos, fue de vital importancia para el éxito de TCP/IP.

El uso de normas asegura que un protocolo como el TCP/IP sea igual en cada sistema. Esto significa que una computadora puede hablar con una microcomputadora que ejecuta TCP/IP sin rutinas de traducción o conversión especiales. Quiere decir que una red entera de hardware y sistemas operativos diferentes puede funcionar con los mismos protocolos de red.

Conocer las interacciones entre TCP/IP y los otros componentes de un sistema de comunicación es importante para la configuración y optimización

apropiadas, y para asegurar que todos los servicios que se necesitan están disponibles y funcionando interrelacionados en la forma debida.

Los trabajos en TCP/IP empezaron en la década de los 70, aproximadamente al mismo tiempo que se empezaban a desarrollar las redes de área local. El ejército americano gracias al proyecto ARPA (Advanced Research Projects Agency) invirtió muchos recursos en investigar el TCP/IP y en la interconexión de redes. Fueron unas de las primeras organizaciones que contaron con varias redes y por lo tanto de las primeras que se encontraron con la necesidad de tener servicios universales. La capacidad de conectar entre sí múltiples redes de manera transparente fue uno de los primeros objetivos de diseño.

Las principales características del protocolo TCP/IP son:

- Para que las computadoras interconectadas, se puedan comunicar unas con otras, y saber hacia dónde se deben dirigir los paquetes con la información, independientemente de dónde estén ubicadas físicamente y de los enlaces necesarios para alcanzarse.

- Para resolver de forma automática los problemas que se puedan dar durante el intercambio de información: fallos en los enlaces, errores, pérdidas o duplicación de datos información.

- Para tratar de resolver posibles incompatibilidades en la comunicación entre computadoras.

2.2.5.1 Capas del modelo de referencia TCP/IP

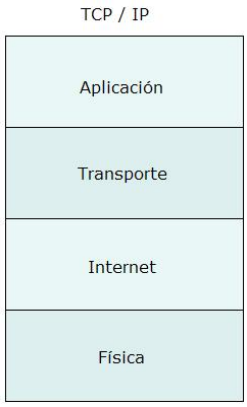


Figura 2.8 Capas del modelo TPC/IP

TCP/IP se suele confundir muchas veces con un protocolo de comunicaciones concreto, cuando, en realidad, es una compleja arquitectura de red que incluye varios de ellos, apilados por capas. Es, sin lugar a dudas, la más utilizada del mundo, ya que es la base de comunicación de Internet y también se utiliza ampliamente en las distintas versiones del sistema operativo Unix y Linux.

La arquitectura de TCP/IP, como se aprecia en la Figura 2.8 se construyó diseñando inicialmente los protocolos para, posteriormente, integrarlos por capas en la arquitectura. Por esta razón, a TCP/IP muchas veces se le califica como *pila de protocolos*.

El modelo de referencia TCP/IP consta principalmente de tres protocolos: IP, UDP y TCP. El protocolo básico es IP y permite enviar mensajes entre dos sistemas

de computadoras. UDP y TCP utilizan los mensajes del nivel IP para construir un diálogo más complejo entre las computadoras. En la Figura 2.9 se expresa de manera gráfica la transmisión dentro del modelo TCP/IP, desde el origen hasta el destino, y así como las etapas que recorre.

Un dato curioso y relevante en el modelo TCP/IP es que el uso de todas las capas no es obligatorio, por ejemplo, hay algunos protocolos de la capa de aplicación que operan directamente sobre IP.

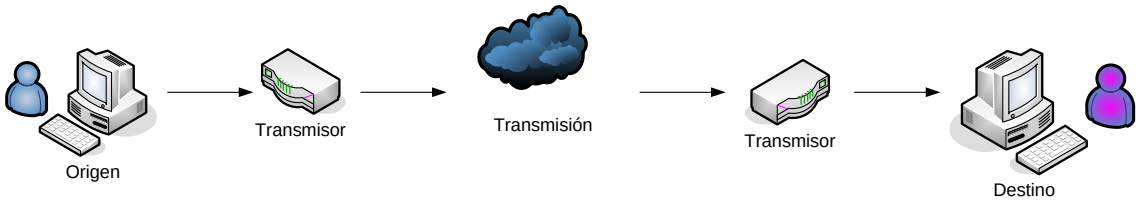


Figura 2.9 Transmisión en el modelo TCP/IP

2.2.5.1.1 Capa Física

El modelo no da mucha información de esta capa, y solamente se especifica que debe existir algún protocolo que conecte la estación con la red. La razón fundamental es que, como TCP/IP se diseñó para su funcionamiento sobre diferentes redes, esta capa depende de la tecnología utilizada y no se especifica de antemano.

2.2.5.1.2 Capa de Internet

Esta capa es la más importante de la arquitectura y su misión consiste en permitir que las estaciones envíen paquetes a la red y los hagan viajar de forma independiente hacia su destino. Durante ese viaje, los paquetes pueden atravesar redes diferentes y llegar desordenados. Esta capa no se responsabiliza de la tarea de ordenar de nuevo los mensajes en el destino sino de encontrar la mejor ruta para que los paquetes lleguen a su destino. El protocolo más importante de esta capa se llama IP, aunque también existen otros protocolos.

2.2.5.1.3 Capa de Transporte

Ésta cumple la función de establecer una conversación entre el origen y el destino, de igual forma que hace la capa de transporte en el modelo OSI. Puesto que las capas inferiores no se responsabilizan del control de errores ni de la ordenación de los mensajes, ésta debe realizar todo ese trabajo. Aquí también se han definido varios protocolos, entre los que destacan TCP (Transmisión Control Protocol o Protocolo de Control de Transmisión) que es un protocolo orientado a conexión, el cual además de encargarse de segmentar los bloques de datos en salida y reensamblarlos en llegada, se encarga de establecer la sesión con el host destino, mantener la sesión y liberarla cuando concluya la transferencia de información, y UDP (User Datagram Protocol o Protocolo de Datagrama de Usuario), es un protocolo no orientado a la conexión y se dice que por lo tanto es no fiable, sus principales aplicaciones están en arquitecturas cliente servidor donde por ejemplo se está solicitando una conexión al servidor y si no se logra se solicita nuevamente, algunas respuestas de aceptación o no, que no requieren haber establecido una sesión para ello.

2.2.5.1.4 Capa de Aplicación

Esta capa contiene, al igual que la capa de aplicación de OSI, todos los protocolos de ato nivel que utilizan los programas para comunicarse. Aquí se encuentra el protocolo de terminal virtual (TELNET[4]), el de transferencia de archivos (FTP[5]), el protocolo HTTP[6] que usan los navegadores para recuperar páginas en la World Wide Web.

2.2.6 Capa de sesión

La capa de sesión se encarga de la adecuada comunicación entre máquinas no importando si son dos o más, tiene la responsabilidad de asegurar la entrega correcta de la información detectando y corrigiendo los errores. También controla los diálogos entre dos entidades que se estén comunicando y define los mecanismos para hacer las llamadas a procedimientos remotos (Remote Procedure Control - RPC). A este nivel se proporcionan algunos servicios mejorados, como la reanudación de la conversación después de un fallo en la red o una interrupción, y podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.

Cabe destacar que el protocolo TCP ejecuta funciones importantes en la capa de sesión, así como lo hace el NCP de Novell[7].

2.2.7 Capa de presentación

A diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida, define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso “en el cable”. La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto. Algunos ejemplos de los servicios específicos que se podrían realizar en esta capa son los de compresión y cifrado de datos.

---

[4] **Telnet** es el nombre de un protocolo que sirve para acceder mediante una red a otra máquina. Sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.

[5] **FTP** es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Archivos) y es el ideal para transferir datos por la red.

6 **HTTP** es el protocolo de la Web, usado en cada transacción. Las letras significan Hyper Text Transfer Protocol, es decir, protocolo de transferencia de hipertexto. El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla.

[7] **Redes Novell** Su éxito se basa, entre otras cosas a no utilizar el software para vender el hardware sino darle soporte al hardware de distintos proveedores para vender software, es decir, es una tecnología que permite la interconexión de diferentes tipos de redes, sistemas y protocolos, además es potencia para el futuro, ya que no solo puede adaptarse a las tecnologías ya existentes sino que se actualiza cada cierto tiempo para estar preparada para las futuras tecnologías.

2.2.7.1 Compresión

La meta de la compresión de datos es representar un archivo, una señal de discurso, una imagen, o una señal video, lo más cercano a la realidad como sea posible con la menor cantidad de información. Una característica simple de la compresión de datos es que implica transformar de una cadena de caracteres a una cierta representación (tal como ASCII) en una secuencia nueva (de pequeños pedacitos de información) que contenga los mismos datos pero que su longitud sea lo más pequeña posible. La compresión de datos tiene uso importante en las áreas de la transmisión de datos y del almacenaje de datos que es el concepto principal detrás de las capas de OSI. Muchos procesos de datos requieren el almacenaje de grandes volúmenes de datos, y el número de tales procesos está aumentando constantemente, mientras que el uso de computadoras se extiende a las nuevas disciplinas. Cuando la cantidad de datos que se transmitirán se reduce, el efecto es el de aumentar la capacidad del canal de comunicaciones. Así mismo, la compresión de un archivo a la mitad de su tamaño original es equivalente a doblar la capacidad del medio de almacenaje. Puede entonces llegar a ser factible para almacenar mayor cantidad de datos de forma rápida y para reducir la carga en los canales de entrada-salida del sistema de información.

En la capa de presentación, se debe establecer el tránsito de datos, de manera que se acuerdan: el lenguaje que se utilizará en la transmisión, las características de seguridad para garantizar el aislamiento, la autenticación, el volumen de datos que se transmitirán y la compresión.

2.2.7.2 Cifrado

Otra función de la capa de presentación se encuentra en el cifrado o la protección de los datos ofrecidos a transmisiones dentro de las capas. Esto se puede alcanzar gracias a la criptografía. La Criptografía es la ciencia de la seguridad de la información que por medio de herramientas y métodos oculta el significado de un mensaje, siendo éste públicamente disponible. Por medio de ella se puede almacenar o transmitir información en una forma tal que permite ser revelada únicamente a aquellos que deben verla. Aunque hay varias formas de ocultar la información tales como el uso de palabras en combinación con imágenes, en el mundo de la computación se dedica gran parte al cifrado de texto.

Esta función no es exclusiva a la capa de presentación, también se aplica en otras capas del modelo OSI tales como la de sesión, red y transporte.

2.2.8 Capa de aplicación

Por la capa de aplicación se entiende el programa o conjunto de programas que generan una información para que ésta viaje por la red. Esta capa contiene varios protocolos que sirven directamente a los programas de usuario, navegador, e-mail, FTP, TELNET, etc.

Un protocolo de aplicación de amplio uso es HTTP (Protocolo de Transferencia de Hipertexto), que es la base de World Wide Web. Cuando un navegador desea una página Web, utiliza este protocolo para enviar al servidor el nombre de dicha página. A continuación, el servidor devuelve la página. Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico y noticias en la red.

Es la capa que está en contacto directo con los programas o aplicaciones informáticas de las estaciones y contiene los servicios de comunicación más

utilizados en las redes. Como ejemplos de servicios a este nivel se puede mencionar la transferencia de archivos, el correo electrónico, etc.

Es en esta capa donde se puede definir una computadora virtual de red abstracta, con el que los editores y otros programas pueden ser escritos para trabajar con él. Así, esta capa proporciona acceso al entorno OSI para los usuarios y también proporciona servicios de información distribuida.

Otra función de esta capa es la de transferencias de archivos, cuando los sistemas de archivos de las máquinas son distintos, ésta soluciona esa incompatibilidad, y se encarga del sistema de correo electrónico, y otros servicios de propósitos generales.

La capa de aplicación es siempre la más cercana al usuario, ya que la capa de aplicación, mediante la definición de protocolos, asegura una estandarización de las aplicaciones de red.

2.3 Comparación entre los modelos de referencia OSI y TCP/IP

El modelo OSI así como el TCP/IP (Figura 2.10) explicados anteriormente cuentan con una base muy parecida, de manera que la similitud en las capas que están arriba de la capa de transporte, están ahí para proporcionar un servicio de transferencia independiente de extremo a extremo de los procesos que desean comunicarse, y esto sucede en ambos modelos.

Sin embargo, vamos a comparar ambos modelos de referencia, no incluyendo los protocolos correspondientes en cada uno de los modelos, ya que, una de las aportaciones más importantes del modelo OSI es la distinción que hace entre tres conceptos básicos:

1. Servicios
2. Interfaces
3. Protocolos

Que originalmente el modelo TCP/IP no distinguía claramente entre estos tres conceptos, pero en la actualidad se ha adaptado para ser lo más semejante al modelo OSI.

Por ejemplo, inicialmente la capa de enlace de datos sólo trataba con redes de punto a punto. Cuando llegaron las redes de difusión, se tuvo que extender una nueva subcapa en el modelo. Cuando las personas empezaron a construir redes reales utilizando el modelo OSI y los protocolos existentes, se descubrió que estas redes no coincidían con las especificaciones de los servicios solicitados, por lo que se tuvieron que integrar subcapas convergentes en el modelo para proporcionar un espacio para documentar las diferencias. Por último, el comité esperaba en un principio que cada país tuviera una red, controlada por el gobierno y que utilizara los protocolos OSI, pero nunca pensaron en la interconectividad de redes. Para no hacer tan larga la historia las cosas no sucedieron como se esperaba.

Con TCP/IP sucedió lo contrario no había problemas para ajustar los protocolos al modelo, porque encajaban a la perfección. El único problema era que el modelo no aceptaba otras pilas de protocolos. Como consecuencia, no era útil para describir otras redes que no fueran TCP/IP.

Sin embargo, atendiendo a las diferencias más específicas, empezando por la que es evidente al visualizar los modelos de manera gráfica es el número de capas entre ellos. El modelo OSI cuenta con 7 capas mientras que el TCP/IP solamente

con 4 (Figura 2.10). Además, aunque algunas capas del modelo de referencia TCP/IP corresponden a las de referencia del modelo OSI, dentro de las capas del modelo OSI no tiene ninguna que corresponda con la capa “INTERNET” del modelo TCP/IP. Esto se debe a que el modelo OSI se definió antes de que se inventara el “Internetworking” por lo que este modelo no contiene ninguna capa para los protocolos de Internet.

Otro punto importante es que el modelo OSI dedica una capa completa para los protocolos de sesión, que han perdido mucha importancia a medida que las computadoras han cambiado, desde sistemas de tiempo compartido a estaciones de trabajo. Por este motivo, los desarrolladores que diseñaron TCP/IP inventaron un nuevo modelo de capas.

Otra diferencia más está en el área de comunicación no orientada a la conexión frente a la orientada a la conexión. El modelo OSI considera ambos tipos, pero en la capa de transporte donde es más importante, ya que es perceptible al usuario, lo hace únicamente con la comunicación orientada a la conexión. El modelo TCP/IP en la capa de red sólo tiene el modo sin conexión pero considera ambos modos en la capa de transporte, ofreciendo una alternativa a los usuarios. Esta elección es importante sobre todo para los protocolos simples de petición y respuesta.

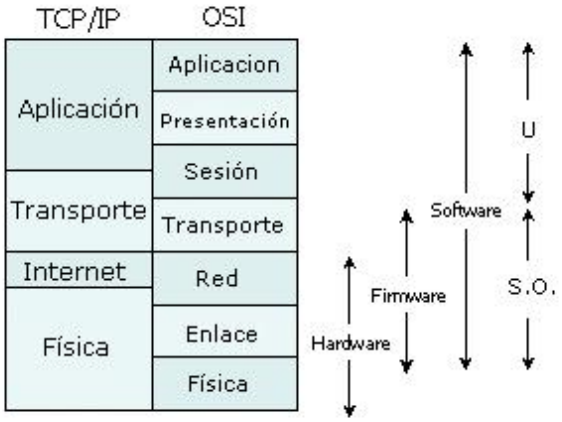


Figura 2.10 Comparación entre el modelo OSI y modelo TCP/IP

Para el desarrollo del Laboratorio de Redes y Seguridad, es necesario un fundamento teórico como el que se está presentado en los dos capítulos anteriores, ahora es el momento de enfocarnos un poco más a la capa 1 del modelo OSI, capa física, ya que en ésta se define el medio o medios físicos por los que va a viajar la información, se definen las características materiales (componentes y conectores mecánicos) y eléctricas, se especifica qué tipo de cables y conectores van a utilizarse, etc., es por eso que comenzaremos este capítulo mostrando la configuración del hardware básico con el que contamos en el laboratorio.

3.1 Cableado

La topología usada en el laboratorio es en estrella por las diferentes ventajas que ofrece (ya mencionadas en el capítulo anterior) y haremos referencia a las normas del cableado estructurado en especial a la norma EIA/TIA 568 que se comentó en el capitulo dos, para nuestros fines nos enfocaremos en este momento a dos elementos principales:

- Cableado horizontal
- Rutas y espacios horizontales.

3.1.1 Cableado horizontal

El sistema de cableado horizontal es la porción del sistema de cableado que se extiende del área de trabajo al cuarto de telecomunicaciones y consiste de dos elementos básicos: Cable Horizontal y Hardware de Conexión que proporcionan los medios para transportar señales entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales.

El cableado horizontal incluye: Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo. Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones. Páneles de parcheo (patch panel) y cables utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Se reconocen tres tipos de cables para el sistema de cableado horizontal: Cables de par trenzado sin blindar (UTP) de 100 ohms y cuatro pares. Cables de par trenzado blindados (STP) de 150 ohms y dos pares. Cables de fibra óptica multimodo de 62.5/125 μm y dos fibras. Para el laboratorio se utilizó cable UTP de 100 ohms categoría 5e ya que es el que se prefiere para la red del edificio en el cual se encuentra el laboratorio.

La norma EIA/TIA 568A hace las siguientes recomendaciones en cuanto a la topología del cableado horizontal: El cableado horizontal debe seguir una topología estrella. Cada toma/conector de telecomunicaciones del área de trabajo debe conectarse a una interconexión en el cuarto de telecomunicaciones.

3.1.2 Rutas y espacios horizontales

También llamado "sistemas de distribución horizontal", las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado Horizontal.

1.- Si existiera cielo raso suspendido se recomienda la utilización de canaletas para transportar los cables horizontales.
2.- Una tubería de ¾ de pulgada por cada dos cables UTP.
3.- Una tubería de 1 pulgada por cada cable de dos fibras ópticas.
4.- Los radios mínimos de curvatura deben ser bien implementados. En nuestro caso se utilizaron canaletas de tipo Media Trak 7 sin adhesivo como la que se muestra en la Figura 3.1

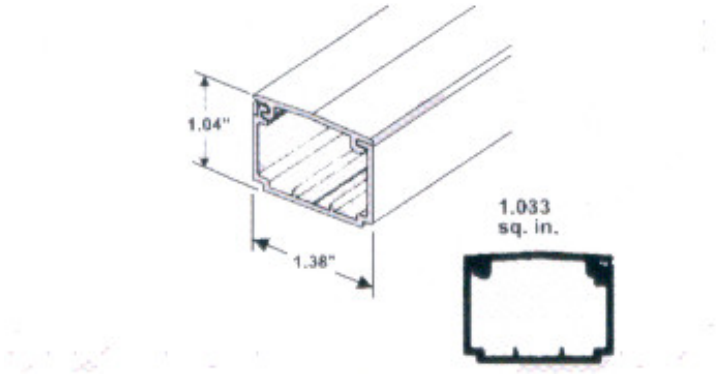


Figura 3.1 Canaleta

Sin importar el medio físico, la distancia horizontal máxima no debe exceder 90m. La distancia se mide desde la terminación mecánica del medio en la interconexión horizontal en el cuarto de telecomunicaciones hasta la toma/conector de telecomunicaciones en el área de trabajo.

El siguiente paso es realizar las conexiones del cableado, para esto se tienen dos configuraciones: T568A y T568B. Se pueden usar cualquiera de las dos configuraciones, siempre y cuando se use solo una para todas las conexiones.

Como parte del cableado también están las terminales que proveerán de señal a los equipos de cómputo, éstas son unas cajas denominadas rosetas (véase Figura 3.2).



Figura 3.2 Canaleta y roseta

3.1.3 Roseta

En las rosetas se encuentra una de las partes terminales del cable UTP, el cual debe estar provisto por un conector RJ45 de tipo hembra o también llamado “Jack” como el que se muestra en la Figura 3.3



Figura 3.3 Jack

En el laboratorio de Redes y Seguridad se utiliza la norma T568B, por lo que usamos la misma norma para el armado de los Jacks. Existe una herramienta especial para esto denominada pinzas de impacto las cuales se muestran en la Figura 3.4



Figura 3.4 Pinzas de impacto

El procedimiento es el siguiente:

Se quitan 10 cm del forro que cubre al cable UTP aproximadamente, se separan los pares trenzados y se comienzan a ordenar en el Jack conforme a la norma que estamos utilizando (Figura 3.5) Una vez puestos los cables en las ranuras se “ponchan” con las pinzas de impacto que fijan el cable, logran que el cobre haga contacto con las terminales del Jack y quitan el excedente de cable. Por último se acomodan los Jakcs dentro de la caja y se coloca la tapa que es etiquetada con el nombre o número de cable para llevar un orden (Figura 3.6).

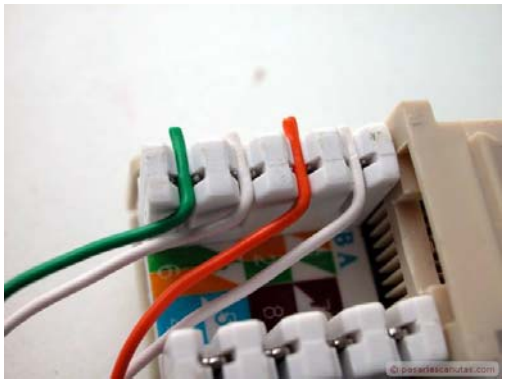


Figura 3.5 Cable UTP en Jack



Figura. 3.6 Roseta y Jack

3.1.4 Conectores RJ45

Como se dijo anteriormente, la roseta es la terminal que albergará la señal para los equipos, para esto se necesita un cable que vaya de la roseta al equipo, este cable debe estar provisto de unos conectores RJ45 de tipo macho en cada extremo del mismo (véase Figura 3.7)



Figura 3.7 Conector RJ45

Por lo tanto, se construyeron dichos cables de la siguiente forma:

Se quitan 10 cm del forro que cubre al cable UTP aproximadamente, se separan los pares trenzados y se comienzan a ordenar en el conector de acuerdo a la configuración T568B como se muestra a continuación en la Figura 3.8:

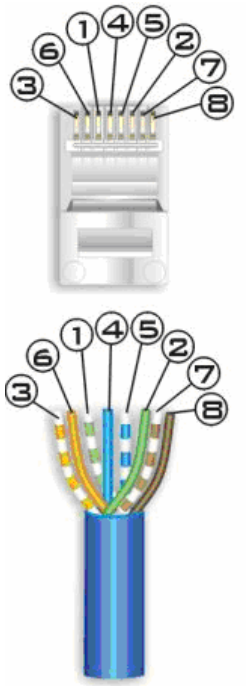


Figura 3.8 Configuración T568B

Es importante que los alambres hagan contacto con el extremo superior del conector, hecho lo anterior se prosigue a “ponchar” el cable con unas pinzas especiales como se muestra en la Figura 3.9.



Figura 3.9 Ponchado de cables

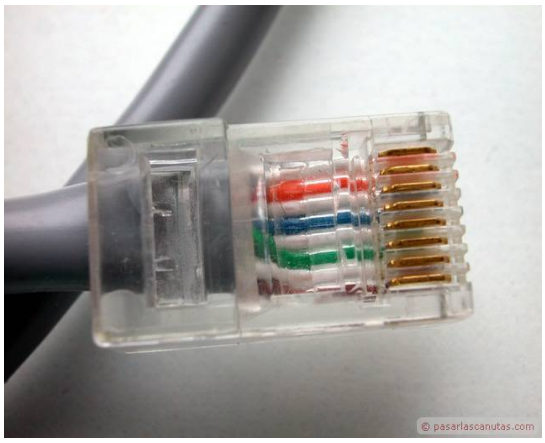


Figura 3.10 Conector en cable UTP

Finalmente, el cable terminado es como el mostrado en la Figura 3.10. Estos cables pueden ser utilizados tanto del equipo hacia la roseta como también de un dispositivo de conectividad (switch, hub, etc.) al panel de parcheo (estos serán explicados más adelante), los dispositivos deben estar sujetos por medio de una estructura especial llamada Rack.

3.1.5 Rack

Estructura de material resistente que soporta el cableado de tipo vertical. Este cableado es el que sale de la canaleta y sube sujeto por uno de los extremos del rack hasta el panel de parcheo para ser conectado. El rack esta fijo al piso y se encuentra en el cuarto de telecomunicaciones soportando también al dispositivo de conectividad (switch, hub, etc.) además del panel de parcheo. Es necesario tomar en cuenta diferentes aspectos antes de fijar el rack ya que debe haber el espacio suficiente para que una persona pase libremente por cada uno de los lados del mismo y contar con la orientación adecuada para facilitar la manipulación del cableado y los equipos.

El rack con el que se cuenta en el Laboratorio de Redes y Seguridad es de aproximadamente 1.30 m. de alto por 70cm. de ancho (véase Figura 3.11).



Figura 3.11 Rack

Ya se tiene armada una parte de la red que es del equipo de cómputo hacia la roseta y de allí, el otro extremo del cable debe ser conectado en un panel, llamado panel de parcheo.

3.1.6 Panel de parcheo

El panel está compuesto por estructuras metálicas con placas de circuitos que permiten interconexión entre equipos, éstos poseen una determinada cantidad de puertos (RJ45) donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores. El panel es recomendado en las características del cableado estructurado ya que nos brinda diferentes ventajas como:

- Fácil identificación de cada uno de los cables
- Fácil mantenimiento, modificación y ampliación de la red
- Rápida detección de posibles fallos
- Al ofrecernos un orden nos permite conservar en mejor estado el cableado

El panel usado es de la marca Hubell y cuenta con 24 puertos, tal como se muestra en la Figura 3.12.



Figura. 3.12 Panel de parcheo

Para realizar la conexión del cable UTP y el panel de parcheo se hizo lo siguiente:

Se cortan 10cm. de forro del cable UTP aproximadamente, se separan los pares trenzados y se introduce en cada una de las entradas de acuerdo con la configuración establecida (en nuestro caso T568B), después, se toman las pinzas de impacto, se “ponchan” y se quita el cable sobrante. Es recomendable que se vaya llenando el panel desde el centro hacia los lados para facilitar la expansión del mismo evitando que los cables se estorben entre si.



Figura. 3.14 Cable UTP en el panel

El panel contiene un etiquetado propio con la finalidad de identificar cada puerto, teniendo así una correspondencia puerto-máquina, ya que cada equipo esta identificado por un nombre y un número comenzando por el 1.

Como se había mencionado, el panel establece comunicación hacia los dispositivos de conectividad, los cuales serán comentados a continuación.

3.2 Dispositivos de Conectividad

3.2.1 Switch

Un Switch (Figura 3.15) es un dispositivo que se usa para la interconexión de redes de computadoras, opera en la capa 2 *Enlace de datos* del modelo OSI. Éste interconecta dos o más segmentos de red (Figura 3.16), funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra de acuerdo con la dirección MAC de destino de los datagramas[1] en la red. Funcionan como un filtro en la red, mejora el rendimiento y la seguridad de las Redes de Área Local.



Figura 3.15 Switch de 24 puertos

Los switches envían e inundan el tráfico con base en 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 una 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.

[1] Un datagrama es un fragmento de paquete de una computadora origen, que es enviado con la suficiente información como para que la red pueda simplemente llevar dicho fragmento hacia la computadora destino, de manera independiente a los fragmentos restantes.

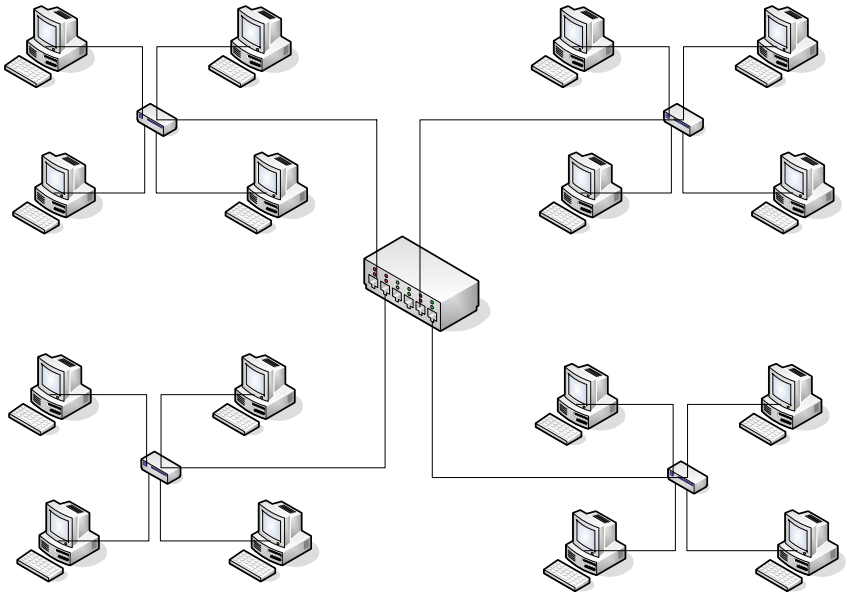


Figura 3.16 Switch interconectando 4 redes

3.2.1.1 Encapsulamiento

El encapsulamiento es el proceso por el cual los datos que se van a enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la misma. De las siguientes capas del modelo, la capa de transporte divide los datos en **segmentos**, a estos segmentos se les asigna números de secuencia para asegurarse de que los *hosts* receptores (computadora receptora) vuelvan a unir los datos en el orden correcto; luego la capa de red encapsula el segmento creando un **paquete**, a este paquete se le agrega una dirección IP de red, donde se conoce su origen y destino.

En la capa de enlace de datos continúa el encapsulamiento del paquete con la creación de algo más grande llamado **trama**. Le agrega a la trama la dirección local (MAC) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino; pero si se deben enviar los datos a otro host, a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia, esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos.

Las tres capas inferiores (red, enlace de datos y física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o Internet, la excepción principal a esto es un dispositivo denominado ***gateway***; este dispositivo ha sido diseñado para convertir los datos desde un formato, creado por las capas de aplicación, presentación y sesión, en otro formato, de modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.

3.2.1.2 Segmentación

La segmentación o *pipeline* como se le conoce en inglés, es un método por el cual se puede aumentar el rendimiento de algunos sistemas, esto se logra gracias a que podemos descomponer la ejecución de cada instrucción en varias etapas para poder empezar a procesar una instrucción diferente en cada una de ellas y trabajar con varias a la vez. En las redes LAN hay dos motivos fundamentales para que ésta sea dividida en segmentos, el primer motivo es aislar el tráfico entre segmentos y así poder obtener un ancho de banda mayor por el usuario, al crear dominios de colisión más pequeños, y esta es la parte importante, ya que si la red no fuera dividida en pequeños segmentos, podrían congestionarse rápidamente los canales de comunicación y se desencadenarían las colisiones y como resultado no ofrecería ningún ancho de banda. Así que para dividir estas redes de gran tamaño se utilizan los puentes o los switches, porque reducen el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo envía un determinado porcentaje de tráfico, además de que nos dan la oportunidad de ampliar la longitud activa de una LAN, permitiendo la conexión de estaciones distantes que anteriormente estaban inaccesibles.

Aunque estamos hablando de switches y puentes sin hacer evidente diferencia alguna, existen varias entre ellos. Sin embargo estas diferencias se explicarán con más detalle en los apartados siguientes.

3.2.1.3 Colisión

Estuvimos hablando de que una de las ventajas de la segmentación de Red es precisamente el evitar colisiones, pero ¿que es en verdad una colisión?

Una colisión se ocasiona cuando dos computadoras transmiten al mismo tiempo en una misma red. En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadoras envíen mensajes, cada una por turnos, esto significa que ambas pueden mandar mensajes, pero solamente una a la vez. El problema es que en las grandes redes hay muchas computadoras conectadas, cada una de las cuales desea comunicar miles de millones de bytes por segundo.

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo. Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

El área dentro de la red donde los paquetes se originan y colisionan, se denomina ***dominio de colisión***, e incluye todos los entornos de medios compartidos. Por ejemplo, un alambre puede estar conectado con otro a través de cables y paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la capa 1 forman parte del dominio de colisión.

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

Una cantidad determinada de colisiones es una función natural de un dominio de colisión, ya que una gran cantidad de computadoras intentan comunicarse entre sí simultáneamente usando el mismo cable. Los repetidores regeneran y retemporizan los bits, pero no pueden filtrar el flujo de tráfico que pasa por ellos. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. El uso de repetidor extiende el dominio de colisión, por lo tanto, la red a ambos lados del repetidor es un dominio de colisión de mayor tamaño.

La mejor solución para este problema es la utilización de switches para la correcta segmentación de una LAN.

3.2.2 Router



Figura 3.17 Router

Un router o mejor dicho encaminador (Figura 3.17) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa 3 del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Los routers toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los routers toman decisiones basándose en diversos parámetros. El más importante es la dirección de la red hacia la que va destinado el paquete (en el caso del protocolo IP esta sería la dirección IP). Otros serían la carga de tráfico de red en los distintos interfaces de red del router y la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

Los broadcast o difusiones se producen cuando una fuente envía datos a todos los dispositivos de una red. En el caso del protocolo IP, una dirección de broadcast es una dirección compuesta exclusivamente por números unos (1) en el campo del host.

Los protocolos de encaminamiento son aquellos protocolos que utilizan los routers para comunicarse entre si y compartir información que les permita tomar la decisión de cual es la ruta mas adecuada en cada momento para enviar un paquete. Los protocolos mas usados son RIP2 (v1 y v2), OSPF3 (v1, v2 y v3) y

[2] **R**outing **I**nformation **P**rotocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o **IGP** (**I**nternet **G**ateway **P**rotocol) utilizado por los routers (enrutadores), aunque también pueden actuar equipos, para intercambiar información acerca de redes IP.

BGP4 (v4), que se encargan de gestionar las rutas de una forma dinámica. Aunque no es estrictamente necesario que un router haga uso de estos protocolos, ya que se le puede indicar de forma estática las rutas (caminos a seguir) para las distintas subredes que estén conectadas al dispositivo.

Otra forma de adquirir un router es ya contactando con fabricantes que se dedique a desarrollar su propio software no libre y con su hardware especialmente hecho para tal fin, este es el caso de fabricantes como Cisco Systems.

3.2.3 Puente



Figura 3.18 Puente

Este dispositivo (Figura 3.18) divide una red en segmentos haciendo la transferencia de datos de una red para otra, con base en la dirección física de destino de cada paquete.

Funciona a través de una tabla de direcciones MAC detectadas en cada segmento al que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el puente copia el *frame* para la otra subred. Por utilizar este mecanismo de aprendizaje automático los puentes no necesitan configuración manual.

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 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. Éstos pueden soportar densidades de puerto más altas que los puentes. Algunos switches soportan la conmutación por el método cut-through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). 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.

---

[3] **O**pen **S**hortest **P**ath **F**irst es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Internet Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa *cost* como su medida de métrica. Además, construye una base de datos enlace-estado identica en todos los encaminadores de la zona.

[4] **B**order **G**ateway **P**rotocol es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un router que tenga conFigurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca. Se trata del protocolo mas utilizado para redes con intencion de conFigurar un EGP *(external gateway protocol)*

3.2.4 HUB



Figura 3.19 Hub del Laboratorio de Redes y Seguridad

El hub o concentrador (Figura 3.19) es un dispositivo que permite centralizar el cableado de una red. Funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta de forma que todos los puntos tienen acceso a los datos. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que las computadoras están conectadas en serie, es decir, a una línea que une a varias o todas las computadoras entre sí, antes de llegar a la computadora central. También puede ser llamado repetidor multipuerto y existen 3 clases.

- Pasivo: No necesita energía eléctrica.
- Activo: Necesita alimentación.
- Inteligente o smart hubs: Son hubs activos que incluyen microprocesador.

La principal diferencia entre un puente y un hub es que el segundo pasa cualquier frame con cualquier destino para todos los otros nodos conectados, en cambio el primero sólo pasa los frames pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

Ya que se tiene toda la estructura física de nuestra red, lo siguiente es trabajar a nivel software, es decir, configurar tarjetas y principalmente la máquina o equipo que hará las veces de servidor.

3.3 Configuración de Red

Ya que en el laboratorio manejamos dos sistemas operativos diferentes (Windows XP y Fedora 3.0) haremos los procedimientos para cada uno de ellos.

Para la configuración de la tarjeta de red primero debemos fijarnos qué tipo de ranuras (slots) tienen los equipos de cómputo, en específico en nuestra tarjeta madre, como podemos ver en la Figura 3.20 es entonces cuando podremos conectar la tarjeta.

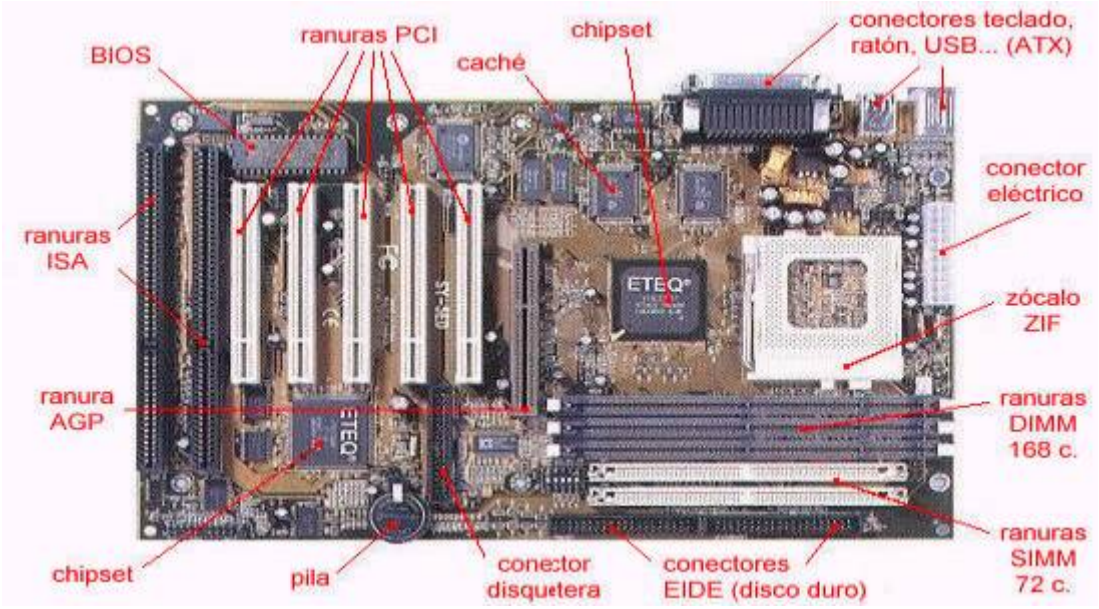


Figura 3.20 Partes de una tarjeta madre

Una vez que tenemos conectado todo el cableado y la tarjeta de red es reconocida por el sistema, se presentará en la pantalla un aviso que nos alertará que tenemos un nuevo hardware y que está listo para utilizarse. El siguiente paso será conectar el cable de red a la computadora para poder empezar con la configuración lógica de la red.

3.3.1 Configuración de red en Windows XP

Si la tarjeta de red no es configurada automáticamente tendremos que buscar el controlador adecuado para que el sistema lo reconozca; una vez hecho esto lo primero es dirigir el apuntador al icono donde se encuentran las conexiones de red, que es, por default, un apartado que trae Windows. En esta ventana se nos presentará un icono como se muestra en la Figura 3.21.

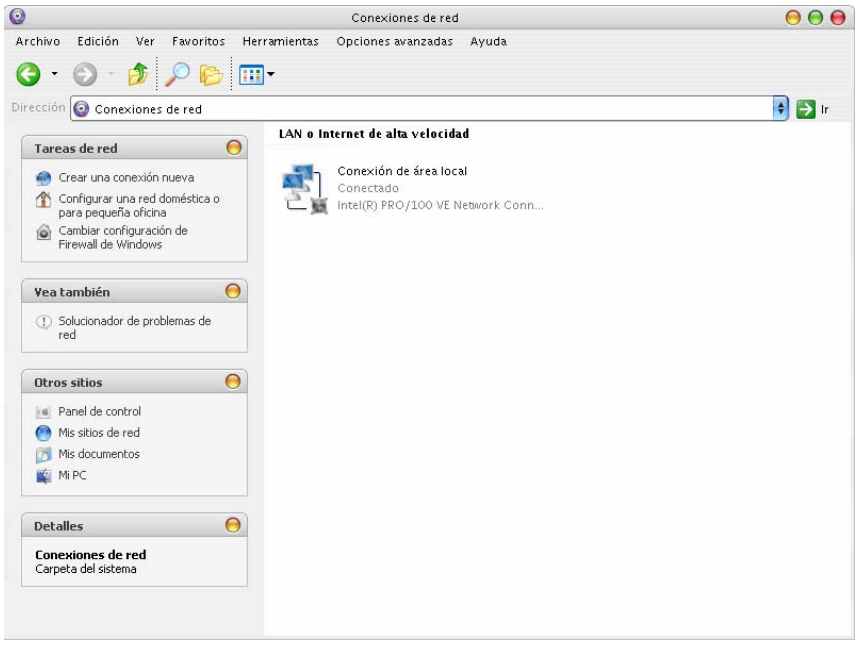


Figura 3.21 Conexión de área local

Ahora vamos a configurar la dirección IP, para ello, sobre este icono dando click con el botón derecho se nos desplegará un menú en donde elegiremos Propiedades (véase Figura 3.22).

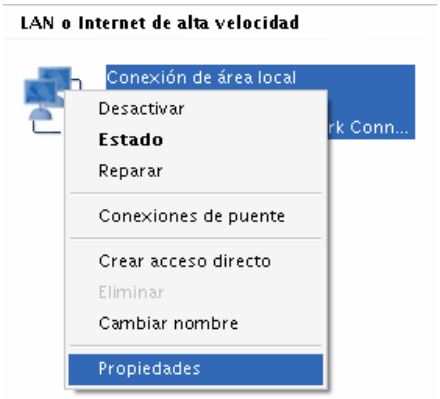


Figura 3.22 Selección de propiedades de Conexión de Área Local

Ya que tenemos abiertas las propiedades de conexión nos vamos a la pestaña de General (Figura 3.23)

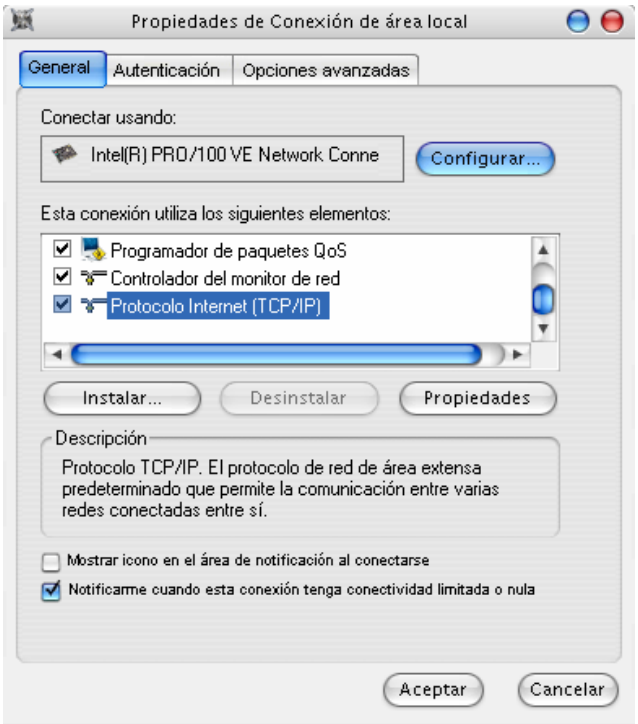


Figura 3.23 Selección de la opción del protocolo TCP/IP

Y presionamos el botón de propiedades (Figura 3.24)

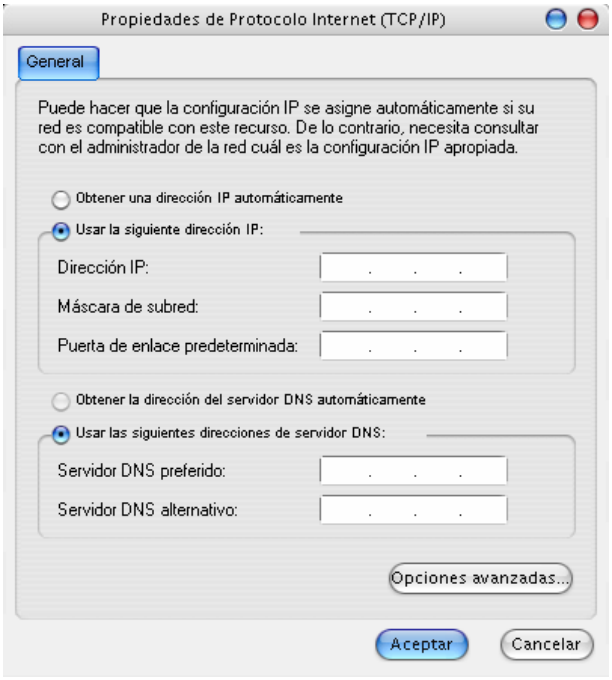


Figura 3.24 Propiedades del protocolo TCP/IP

Como se dijo en el capítulo anterior, para la organización de la red se utilizaron las normas de cableado estructurado, pero también es importante establecer el orden de las máquinas, dado el hecho de que en el Laboratorio no todas las máquinas cuentan con las mismas características, así, se les asignó un lugar en especial a cada una, situándolas por marca y modelo, este criterio se utilizó simplemente para tener un orden funcional y estético. Las direcciones IP se asignaron desde 192.168.2.2 hasta la 192.168.2.11, y los DNS asignados a todas las máquinas son pertenecientes a la DIE o a DGSCA (Figura 3.25).

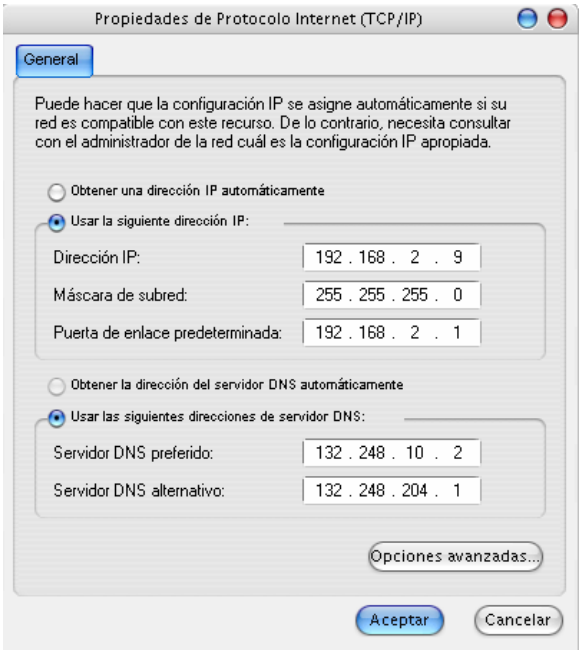


Figura 3.25 Configuración del protocolo TCP/IP

3.3.2 Configuración de la tarjeta de red en Fedora 3.0

En Linux podemos inicializar una NIC (Network Interface Card) o tarjeta de red de diversas formas. Fedora puede identificar y configurar automáticamente el hardware durante el arranque, si esta habilitado el demonio de hardware kudzu, pero si no utilizamos la detección y configuración automática del hardware, podemos inicializar el hardware de red siguiendo uno de los siguientes métodos.

- Modificar manualmente el archivo en /etc/modprobe.conf para pedir al sistema que reconozca y admita al nuevo hardware durante el arranque.
- Escribir una secuencia de comandos o insertar comandos en el archivo /etc/rc.d/rc.local para inicializar el nuevo hardware durante el arranque, teniendo cuidado de evitar las dependencias de servicios de software; es decir, no debe intentar montar conexiones remotas o el sistema de archivos hasta que no esté inicializado y configurado el hardware.
- Cargar o descargar manualmente el módulo del núcleo del nuevo dispositivo con el comando modprobe.

Aunque en nuestro caso todas las tarjetas de red fueron configuradas automáticamente, ya sea por kudzu, o porque teníamos el controlador en un disco.

Ahora configuramos las tarjetas de manera lógica de la siguiente forma:

Se pueden modificar siete archivos de configuración de red para realizar cambios en la interacción básica de la red y nuestro sistema. Estos archivos son:

- /etc/hosts
- /etc/services
- /etc/nsswitch.conf
- /etc/resolv.conf
- /etc/host.conf
- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-eth0

Nosotros utilizamos este último que es el encargado de las configuraciones de red para el dispositivo de red eth0, lo hacimos primero en modo texto y luego se presenta en modo gráfico. Primero editamos el archivo utilizando el comando ***vi***, dejando los valores como se presentan el Figura 3.26.

[root@BATMAN ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0

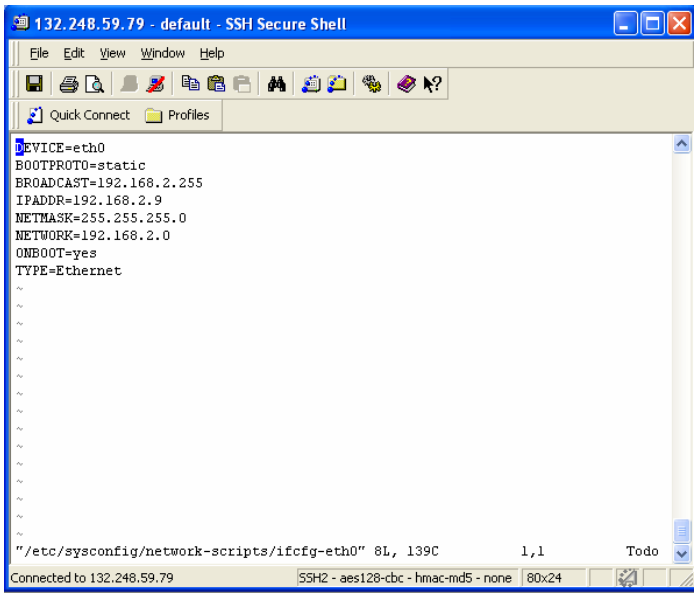


Figura 3.26 Archivo ifcfg-eth0

Ahora editamos el archivo /etc/sysconfig/network y colocamos la información como se presenta en la Figura 3.27

[root@BATMAN ~]# vi /etc/sysconfig/network

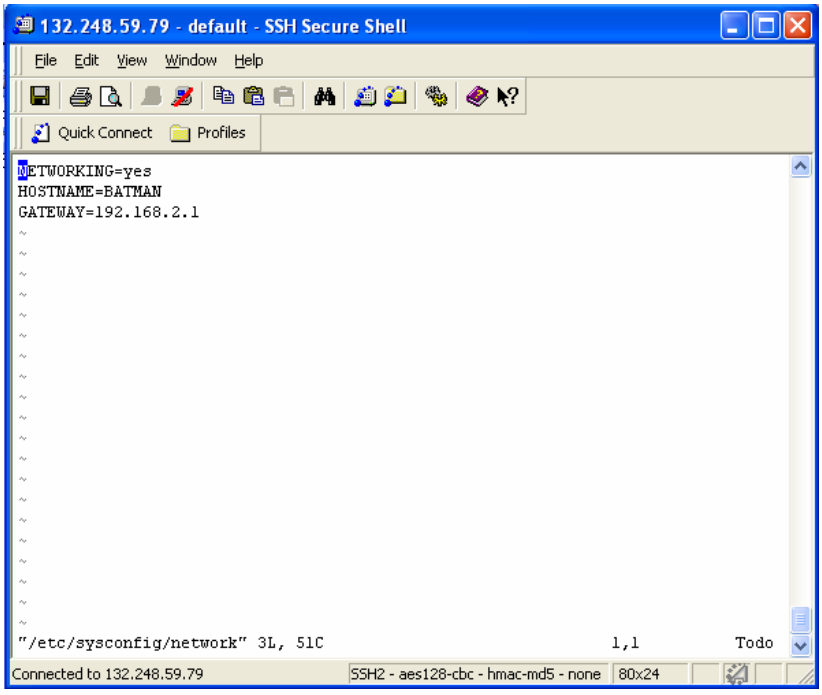


Figura 3.27 Configuración del archivo network

El archivo /etc/resolv.conf lo utiliza DNS, el Servicio de nombres de dominios el contenido de este archivo se establecerá automáticamente si utilizamos el Protocolo de configuración de host dinámico (DHCP). En nuestro caso configuramos el archivo de la siguiente forma (Figura 3.28).

[root@BATMAN ~]# vi /etc/resolv.conf

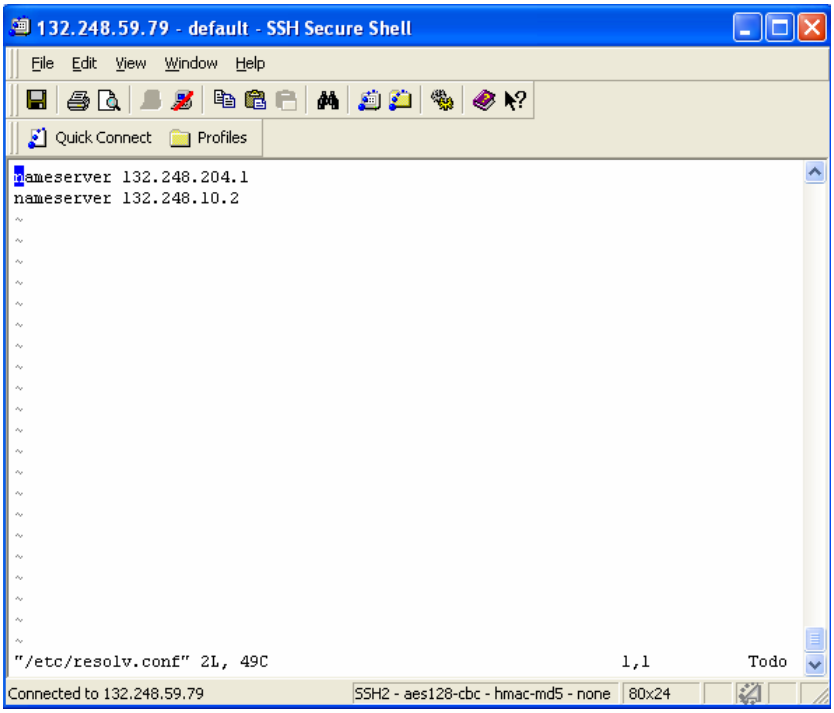


Figura 3.28 Configuración de los DNS

Finalmente tecleamos ifconfig eth0 up como se muestra en la Figura 3.29

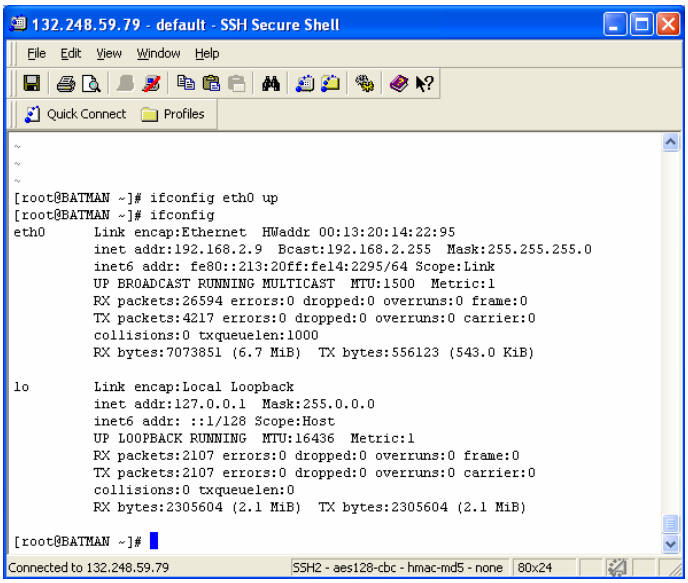


Figura 3.29 Visualización de la configuración de la tarjeta de red

Ahora haciéndolo de manera gráfica, que resulta mucho más fácil, igual que la mayoría de las herramientas gráficas, system-config-network nos permite rellenar espacios y hacer clic en los botones adecuados para que la herramienta modifique los archivos requeridos y envíe los comandos apropiados.

Lo primero que se hace es abrir la ventana de configuración de Red (Figura 3.30). Haciendo clic en la pestaña que dice DNS para configurar las distintas opciones, el nombre de la computadora

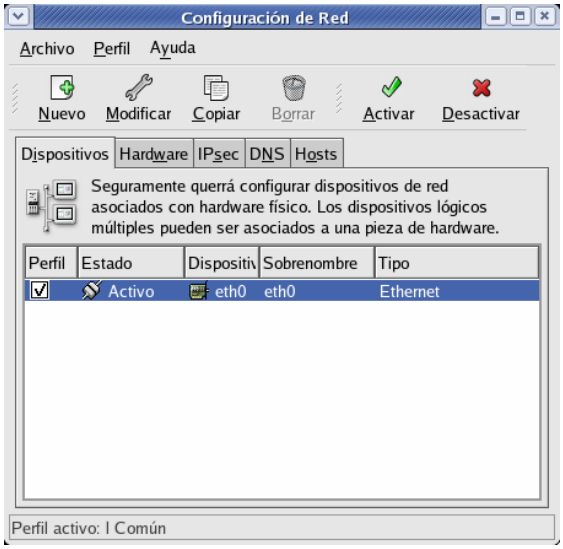


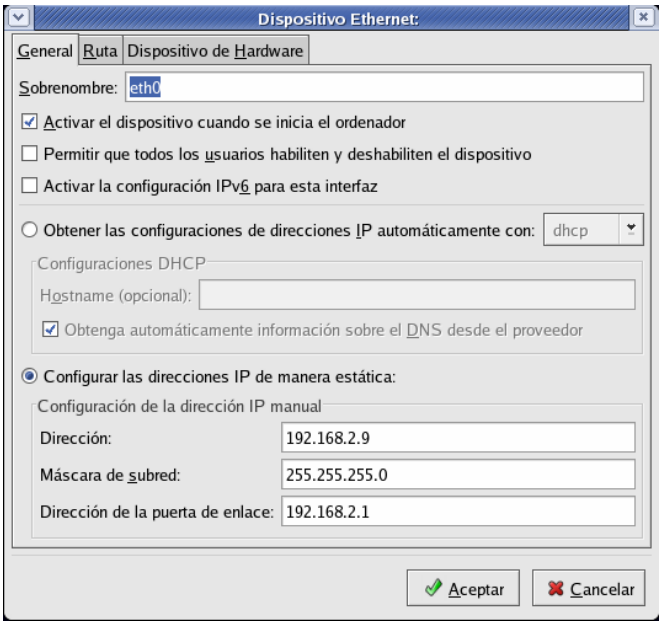
Figura 3.30 Configuración de Red

Asignamos los DNS tal como lo hicimos en modo texto (Figura 3.31)



Figura 3.31 DNS modo gráfico

Finalmente asignamos la IP, la puerta de enlace y la mascara de Red (Figura 3.32)



3.32 Asignación de IP

3.4 SAMBA

3.4.1 Características de SAMBA

La interconectividad entre equipos con diferentes sistemas operativos, en nuestro caso Linux y Windows es muy importante, sobre todo si hablamos de que nos encontramos en un Laboratorio de Redes, en donde compartir recursos es una de las características de este laboratorio. Esta interconectividad se consigue exitosamente a través de SAMBA.

SAMBA originalmente fue creado por Andrew Tridgell y actualmente es mantenido por The SAMBA Team, bajo la licencia pública de GNU.

El proyecto comenzó en 1991 como un servidor de archivos para su red casera. Es decir, SABMA es un conjunto de herramientas que nos permiten compartir recursos sobre una red TCP/IP utilizando el protocolo SMB (Server Message Block) para comunicar datos entre clientes Windows y servidores Unix.

Algunas de las ventajas que nos encontramos al contar con SAMBA son:

- Compartir archivos Linux a clientes Windows y viceversa
- Compartir impresoras instaladas en Linux a clientes Windows
- Proveer servicios de nombre (broadcast y WINS)
- Crear grupos o dominios Windows

Entre otras.

Esencialmente, SAMBA consiste en dos programas denominados smbd y nmbd. Ambos programas utilizan el protocolo NetBIOS para acceder a la red, con lo cual pueden conversar con sistemas Windows.

El programa smbd se encarga de ofrecer los servicios de acceso remoto a archivos e impresoras, así como de autenticar y autorizar a los usuarios, ofrece los dos modos de compartición de recursos existentes en Windows, basado en usuarios o basado en recursos. El modo basado en usuarios se realiza en función de

nombres de usuarios registrados en un dominio, mientras que en el modo basado en recursos a cada recurso se le asigna una contraseña, estando autorizado el acceso en función del conocimiento de dicha contraseña.

El programa nmbd permite que el sistema Linux anticipe en los mecanismos de resolución de nombre propios de Windows, lo cual incluye el anuncio en el grupo de trabajo, la gestión de la lista de computadoras del grupo de trabajo, la contestación a peticiones de resolución de nombres y el anuncio de recursos compartidos. De esta forma, el sistema Linux aparece en el "Entorno de Red" como cualquier otro sistema Windows publicando la lista de recursos que ofrece al resto de la red.

Adicionalmente a los dos programas anteriores SAMBA ofrece varias utilidades. Algunas de las más relevantes son las siguientes:

- smbclient: Una interfaz similar a la utilidad ftp que permite a un usuario de un sistema Linux conectarse a recursos SMB y listar, transferir y enviar archivos.
- swat: Samba Web Administration Tool. Esta utilidad permite configurar Samba de forma local o remota utilizando un navegador de web.
- Sistema de archivos SMB para Linux. Linux puede montar recursos SMB en su jerarquía, al igual que sucede con directorios compartidos vía NFS.
- winbind: Permite integrar un servidor SAMBA en un dominio Windows sin necesidad de crear usuarios Linux en el servidor SAMBA que correspondan con los usuarios del dominio Windows, simplificando así la labor de administración.
- smbtar: Una utilidad para respaldar datos compartidos a través de la red.
- nmblookup: Una utilidad para consultar nombres NetBIOS sobre TCP/IP.
- smbpasswd: Utilidad para contraseñas de SAMBA.
- smbstatus: Utilidad para listar las conexiones al servidor SAMBA.
- testparm: Utilidad para validar la conFiguración SAMBA
- testprn: Utilidad para validar las impresoras de SAMBA.

Finalmente todos los archivos de configuración para SAMBA se encuentran en el Anexo 1.

El laboratorio ya está listo para ser usado, pero aún el trabajo no ha terminado, si el laboratorio no cuenta con personas que lo usen de nada sirve el esfuerzo, por lo que existe la necesidad de dar a conocer nuestro trabajo y llamar la atención de estudiantes y personas que se interesen en el trabajo hecho hasta ahora y estén en posibilidades de ayudar para mejorarlo. Por lo anterior, se debe contar con una difusión adecuada en la comunidad, para que, en la medida de lo posible, se de a conocer el laboratorio.

3.5 DIFUSIÓN

El laboratorio necesita una imagen que mostrar hacia el exterior, por lo que se pensó en la idea de un logotipo que lo representara.

3.5.1 Logotipo

El primer logotipo es el que se muestra en la Figura 3.33 donde la idea principal era hacer ver que en el laboratorio existía una red de computadoras y que a partir de allí se podía hacer comunicación con cualquier parte del mundo.



Figura 3.33 Logotipo inicial

Aunque la idea no nos convencía del todo, pues se quería que a simple vista se lograra saber algo más del laboratorio, entonces se pensó en un logotipo más elaborado como el que se muestra a continuación en la Figura 3.34:

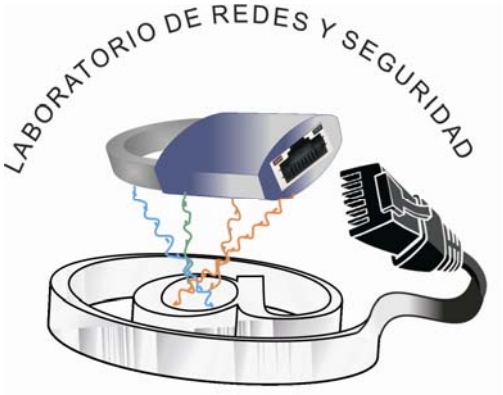


Figura 3.34 Logotipo actual

Cada parte que lo compone tiene una razón en específico que se muestra en la Tabla 3.5.1

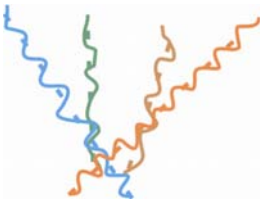
	**Arroba:** Es el símbolo más representativo y conocido para referirnos a Internet. El laboratorio cuenta con una comunicación entre otras redes incluyendo Internet
	**Conector RJ45:** Hasta ahora el medio más usado en el ámbito de redes es el cable UTP y aquí presentamos el conector usado con este cable a modo representativo de las redes alámbricas
	**Pares Trenzados:** Además de que el cable UTP es el medio más usado, es también el que se utiliza en el laboratorio.
	**Candado con entrada de Jack:** El candado es un símbolo de seguridad, el laboratorio es también de Seguridad Informática que aunque es una parte que no es tema central de esta tesis, sí lo es para el laboratorio mismo por lo que debía ser incluido en este logo. La entrada de Jack es para especificar que se trata de seguridad en redes principalmente.
	**Nombre:** En el laboratorio se harán prácticas tanto de Redes como de Seguridad informática, ya que están relacionadas, el nombre se compone de ambas

Tabla 3.5.1 Componentes del logotipo

Pero el logotipo no lo es todo, en nuestros días el principal medio de difusión es el Internet, por lo que hubo la necesidad de hacer un sitio web.

Así como hubo dos logotipos, también existen dos páginas distintas, que son las que se muestran a continuación.

3.5.2 Sitio Web

El primer sitio fue realizado en su totalidad en Flash, por lo que contaba con una entrada donde se mostraba el progreso de carga del mismo (Figura 3.35)

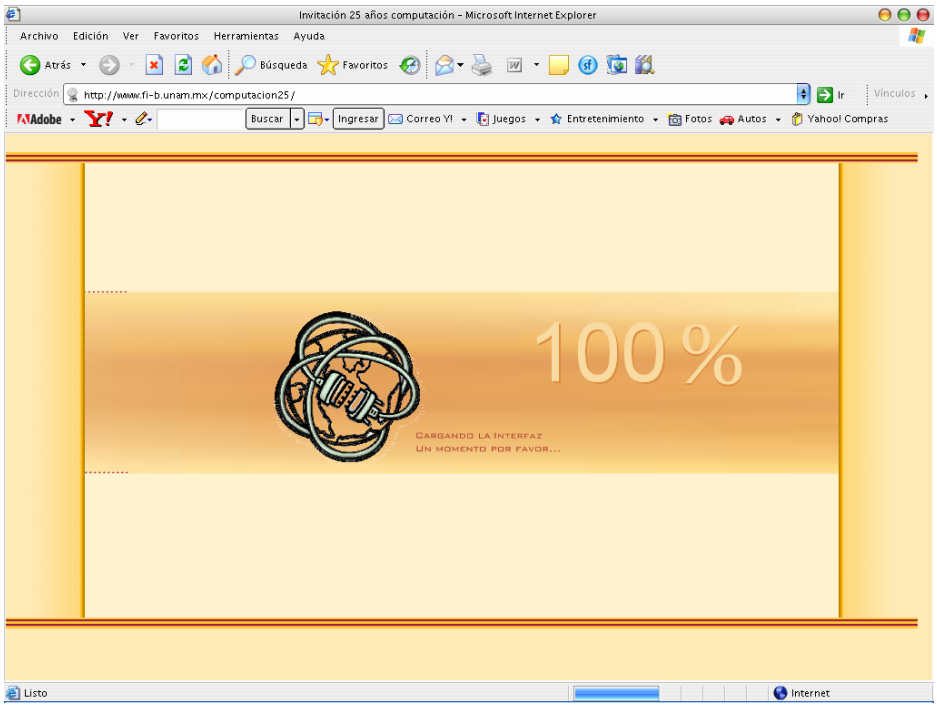


Figura 3.35 Página de estado

En la página principal se encontraba un menú para poder acceder a diferentes partes (véase Figura 3.36) en las cuales se mostraba entre otras cosas, la función del laboratorio (Figura 3.37) los responsables, y un proyecto de Cisco.

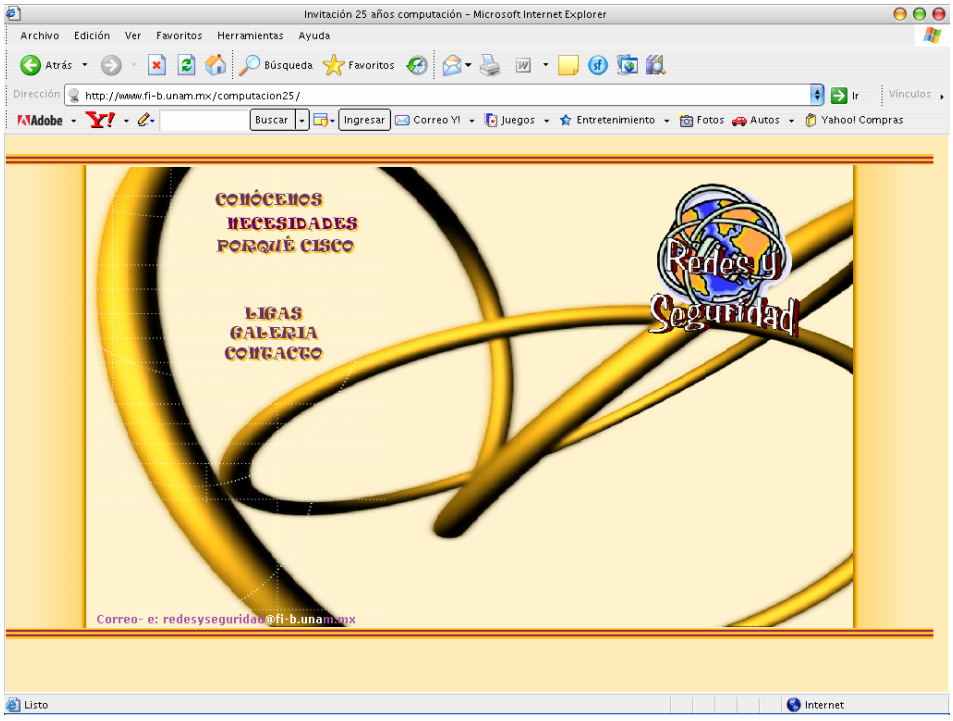


Figura 3.36 Página principal

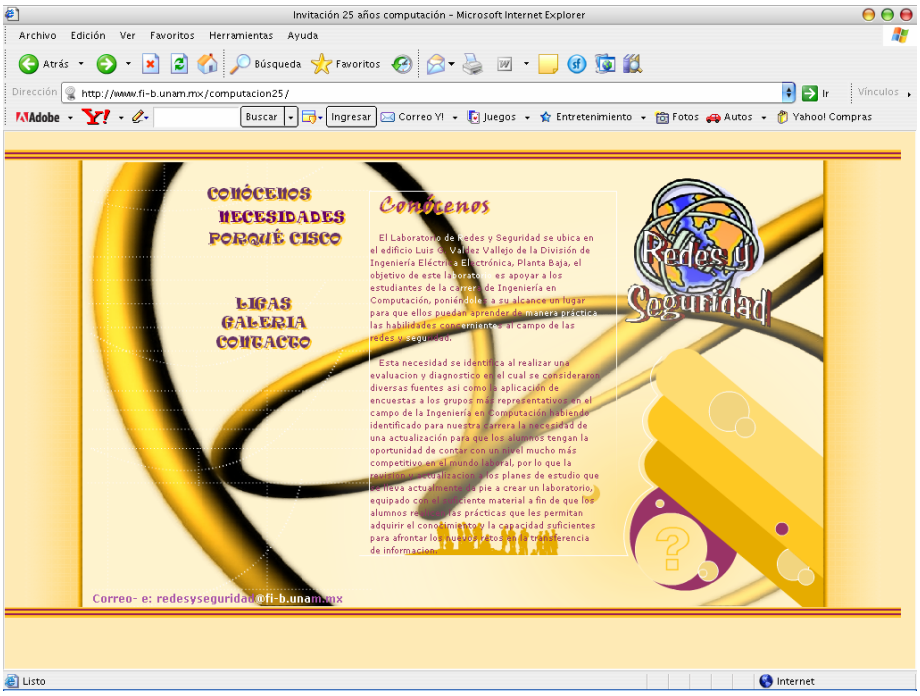


Figura 3.37 Función del laboratorio

La desventaja de esta página es que el tiempo que ocupaba para cargarse era considerablemente largo, por lo que se pensó en la mayoría del código de la página a HTML en lugar de flash.

Para darle una mejor presentación, sólo se hizo una página de bienvenida en flash (véase Figura 3.38), la cual nos conduce a la página principal (Figura 3.39).



Figura 3.38 Página de bienvenida.

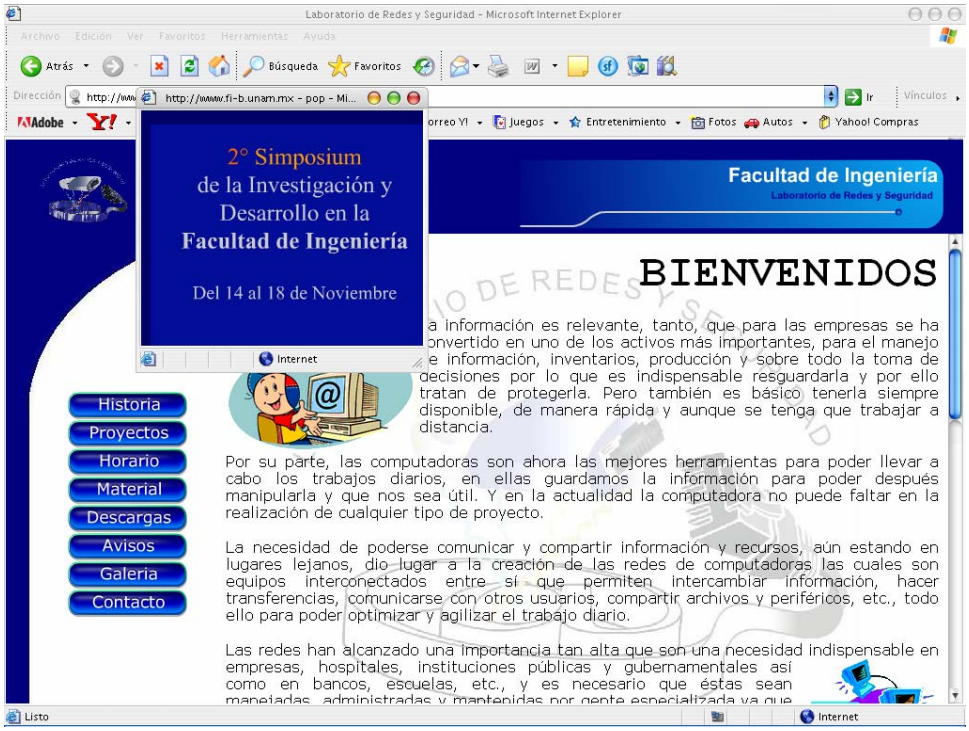


Figura 3.39 Página principal.

En la página principal se tiene un menú para acceder a diferentes apartados, los cuales muestran la historia del laboratorio, los proyectos que se realizan, el horario de atención, el equipo con el que se cuenta (Figura 3.40) y el material que se puede descargar como prácticas, previos y otros documentos de interés.



Figura 3.40 Página del equipo del laboratorio

Como el laboratorio está en renovación constante, todo el tiempo desde sus inicios ha estado sometido a pruebas y a un arduo trabajo de mantenimiento.

El objetivo de realizar un periodo de pruebas es porque era necesario comprobar que todos los equipo funcionaban correctamente y que todos se encontraban en red, que el cableado no fallara, que no hubiera dispositivos sin funcionar, que se contara con el material básico en un Laboratorio de Redes y Seguridad como son las pinzas de impacto, de presión, de corte, cable UTP, conectores RJ45, Jacks, etc.

4.1 EQUIPO

El equipo fue cambiando con el paso del tiempo dentro del laboratorio y fue preciso darle el correspondiente mantenimiento y hacer la instalación de software y las pruebas necesarias para saber si funcionaba de forma adecuada, y en este proceso se presentaron dificultades que hubo que resolver.

4.1.1 Dificultades

- Como ya se explicó en el Capitulo 1 **Antecedentes** el equipo inicial contaba con pocos recursos por lo que se tuvo que trabajar con versiones de Windows y Linux de acuerdo a las características de cada máquina, evitando así una homogeneidad en el laboratorio y limitando los alcances del mismo. Por lo que al inicio de este proyecto la idea principal era una propuesta para el laboratorio.

- El cableado era deficiente y no se encontraba en óptimas condiciones, es decir, los cables tenían conectores “flojos” o con falsos además de que no seguían el estándar T568B que deberían.

Conforme el laboratorio fue creciendo también lo hacían los contratiempos:

- La División de Ingeniería Eléctrica Electrónica, al proporcionarnos tres equipos nuevos y con mayores recursos que los equipos con los que contábamos en un principio nos hizo enfrentarnos a un inconveniente muy importante, hasta ese momento se contaba solamente con un switch de 8 puertos por lo que las máquinas no podían estar conectadas todas a la vez en red.

- Conforme se tenían más máquinas se incrementaban los problemas con el cableado, ya que la capacidad de las canaletas con las que se contaba en ese momento ya era insuficiente.

- Poco después se contó con un hub de 12 puertos que solucionaba el problema de las máquinas al conectarse todas en red, solo que la desventaja era que ahora se tenía un hub en lugar de un switch.

- Al llegar una donación por parte de ISETI de unas máquinas de la marca Compaq, la principal dificultad que se tuvo fue que al tener hardware de la última tecnología en su tipo, se tuvo problemas para instalar Linux en ellas, ya que la mayor parte de los componentes no eran reconocidos por el Sistema y la distribución Fedora por lo que hubo problemas de instalación desde un principio.

- Más tarde, con la donación del cableado estructurado por parte de Hubbell se llegó a solucionar la parte del cableado estableciendo un orden y una

estandarización, pero se tuvieron contratiempos como el que el diseño fue pensado para tener 10 máquinas por las dimensiones del laboratorio, pero actualmente se cuenta con 11 equipos, por lo que la capacidad de las canaletas es insuficiente ahora. Además, por la distribución de las rosetas y los tipos de muebles con los que se cuenta, el acomodo de las máquinas tuvo que adaptarse a las condiciones anteriores y al espacio, dejándolas tal vez no en el mejor lugar. (véase figura 4.1).

- Un problema, que aunque no estaba en nuestras manos resolver, causó graves daños al equipo fueron las fallas constantes de energía eléctrica en el área en la que se encuentra ubicado el laboratorio. Debido a que no se cuenta con reguladores o nobreaks para las máquinas y el resto de los dispositivos, el hecho de que las fallas de energía se presentaran a veces hasta más de cuatro veces al día dañó algunos equipos dejando inservibles los discos duros.

- Por otra parte, el tiempo fue una limitante en cuanto al cableado se refiere, ya que la instalación del cableado fue realizada por una compañía a la que por tener tantos proyectos en puerta no le fue posible finalizarla. Así que nosotras finalizamos la instalación habiendo pasado un tiempo de espera y retrasando así algunos proyectos.

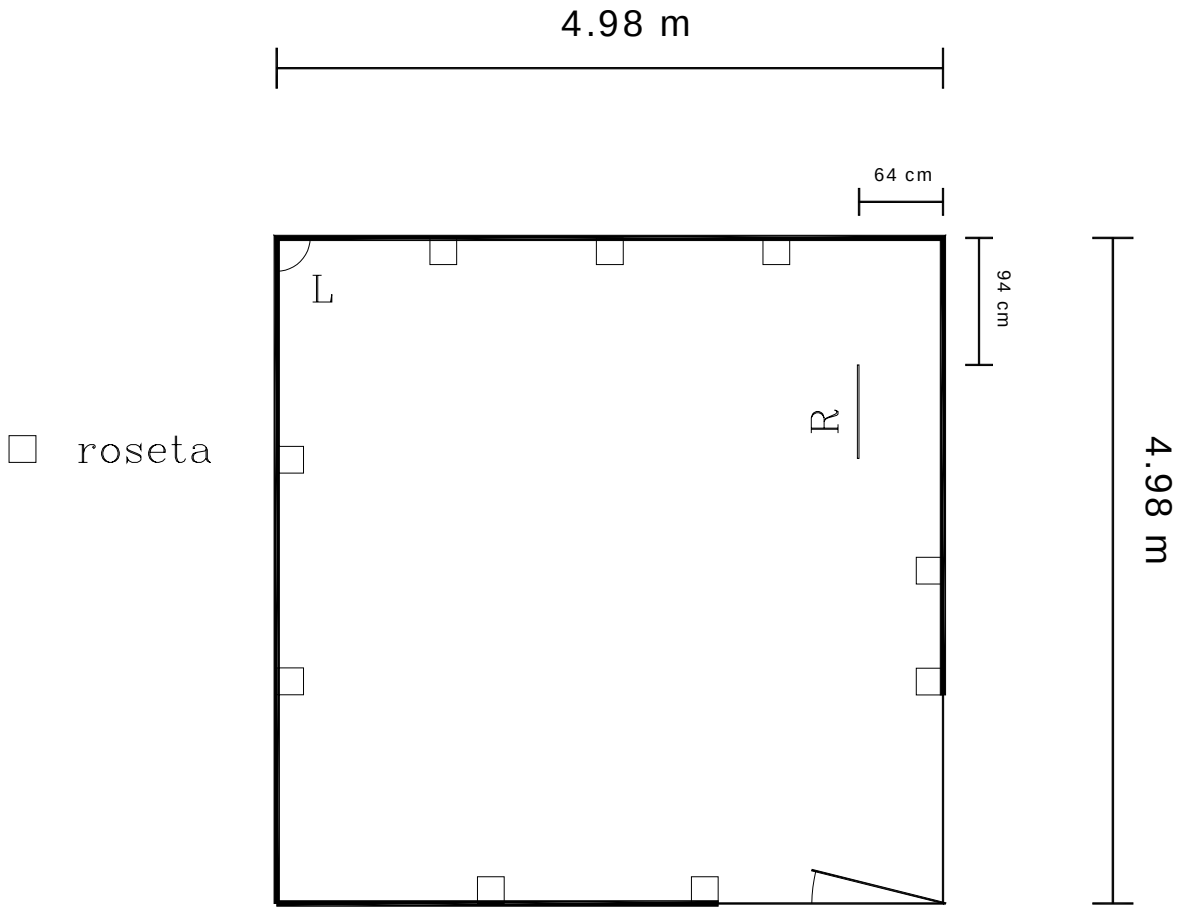


Figura 4.1 Distribución del cableado en el Laboratorio

4.1.2 PRUEBAS

ETAPA INICIAL: Con el equipo que se contaba ¿qué pruebas se realizaron?

Al tener equipos con pocos recursos (un ejemplo es que los equipos con los que se inició contaban con una memoria de 64 MB en RAM y con una capacidad en disco duro que iba desde 200 MB a 4GB, a excepción de una máquina que ya contaba con 40 GB en el disco duro) se instaló una versión antigua de Linux Red Hat, y configurarlas para que estuvieran en red, por las condiciones que nos brindaban estas máquinas constantemente se presentaron errores de kernel, por lo que en repetidas ocasiones fue necesario formatear las máquinas y volver a instalar el sistema operativo. Las primeras pruebas con este equipo fueron las siguientes:

Revisar que estuvieran en red. Siendo un laboratorio de redes esto es importante, ya que las prácticas exigen esta característica en todas las computadoras. Esto fue haciendo un ping hacia el servidor, si nos daba respuesta la prueba había finalizado (Ver Figura 4.2) de lo contrario (Ver Figura 4.3) podrían ser varias cosas: el cable no funcionara por un error al construirlo o una mala configuración de la tarjeta de red, para resolverlo, se probaban otros cables o el mismo en una computadora que funcionara bien en este caso. Y también se revisaba cada archivo perteneciente a la configuración de la tarjeta si es que el error seguía.

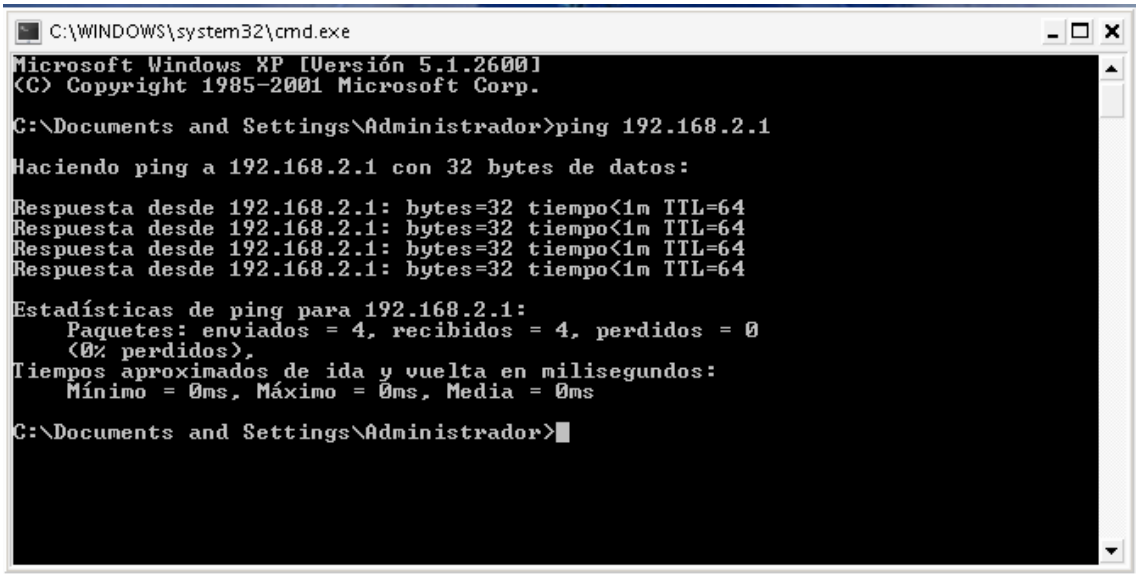


Figura 4.2 Ping con respuesta en Windows

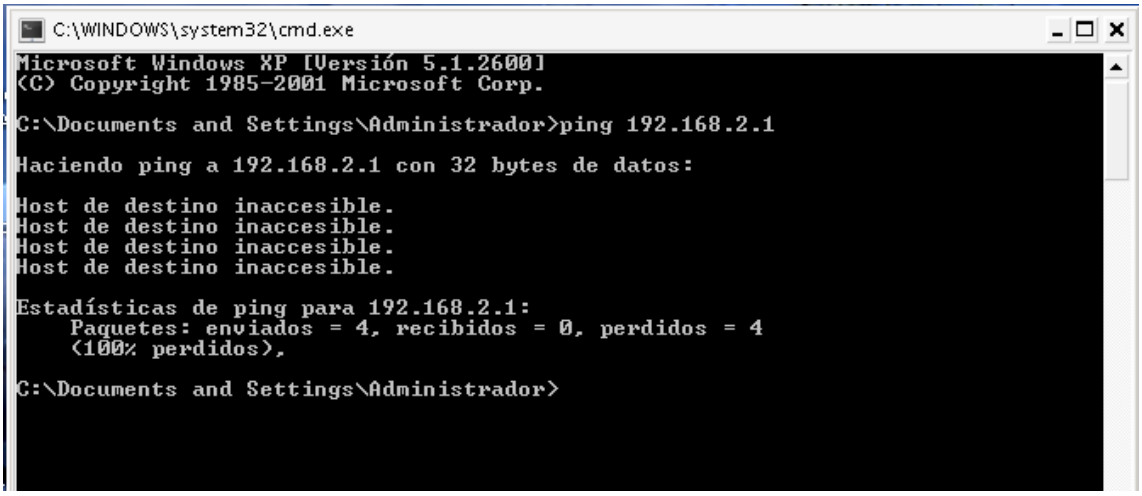


Figura 4.3 Ping sin respuesta en Windows

Al pasar este punto, lo siguiente fue que cada una de las computadoras tuviera salida a Internet, como tenían un ambiente de texto, las páginas de Internet no podían verse en modo gráfico ya que solo se lograban ver algunas letras, para esto se hacía un ping a una máquina fuera de nuestra red, por ejemplo de DGSCA.

Otro equipo con el que se contaba y que fue necesario probar fue el hub, revisando cada uno de los puertos para saber si funcionaban. Se conectaron los equipos y encontramos fallas de red por lo que se procedió a revisar la configuración, los cables y cambiar los cables de puerto, esto último resolvió la situación y se llegó a la conclusión de que 3 de los 12 puertos tenían un falso, pues al mover un poco un cable ya conectado al hub se tenían instantes de servicio y después de unos momentos o con cualquier movimiento, por leve que éste fuera, el equipo se encontraba nuevamente sin servicio.

Finalmente, se hizo una revisión de todo el material con el que se contaba en el laboratorio, como son tarjetas de red, discos duros, memoria RAM, mouses, teclado, cable, conectores, etc. Se probó todo el material tomando en cuenta sus características, funcionamiento y si nos sería útil o no. Muchos discos, memorias Ram y tarjetas de red ya eran obsoletos, por lo que todo este equipo fue dado de baja.

ETAPA FINAL: ¿Cuáles fueron las problemáticas detectadas y cómo fueron resueltas? en lo concerniente a la instalación de cableado estructurado: ¿qué pruebas se llevaron a cabo durante su instalación y al finalizarla?, ¿cuáles fueron los problemas que se encontraron durante dichas pruebas y cómo se solucionaron?

La llegada de equipo (por medio de donaciones y la aportación de la División de Ingeniería Eléctrico Electrónica) con mejor velocidad, mayor capacidad en el disco duro y una gran memoria RAM nos permitió mejorar los servicios que podía ofrecer el Laboratorio, instalar varios sistemas operativos en cada máquina, etc. Para poder hacer lo anterior tuvimos que analizar si era posible instalar algunos programas en las máquinas y corroborar que no trajeran algún problema de fábrica (es decir, que ya hubieran llegado con fallas en su funcionamiento).

A los equipos nuevos simplemente se les realizó una partición del disco duro y se instaló el sistema operativo Linux Fedora Core 3, cuando se configuró la tarjeta de red en ambos sistemas lo siguiente fue probar que la máquina estuviera en red

en ambos sistemas, nuevamente se realizó un ping al servidor, en caso de Linux, el resultado es el que se muestra en la Figura 4.4 y Figura 4.5:

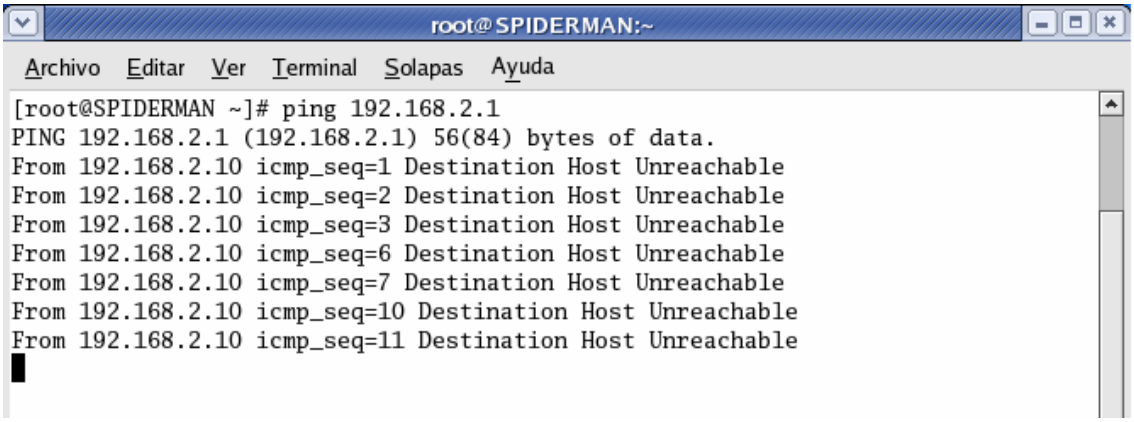


Figura 4.4 Ping sin respuesta en Linux Fedora 3

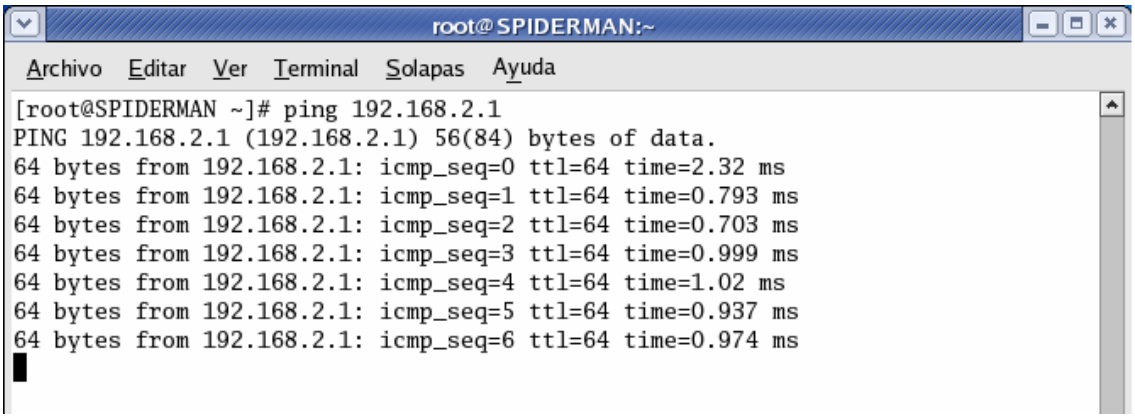


Figura 4.5 Ping con respuesta en Linux Fedora 3

Para el caso de Windows, otro aspecto importante fue la comunicación entre las máquinas, por lo que la siguiente prueba fue hacer un ping a alguna otra máquina que no fuera el servidor y lo siguiente fue revisar la sección de “equipos del grupo de trabajo”(Ver Figura 4.6) la carpeta de “Documentos Compartidos” (Ver Figura 4.7)

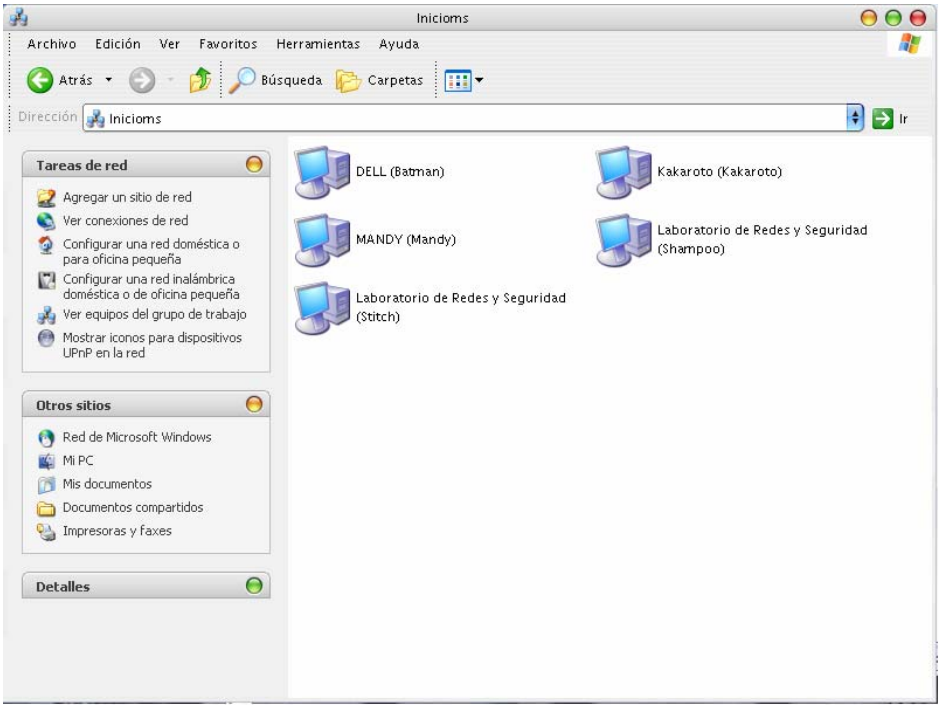


Figura 4.6 Equipos del grupo de trabajo

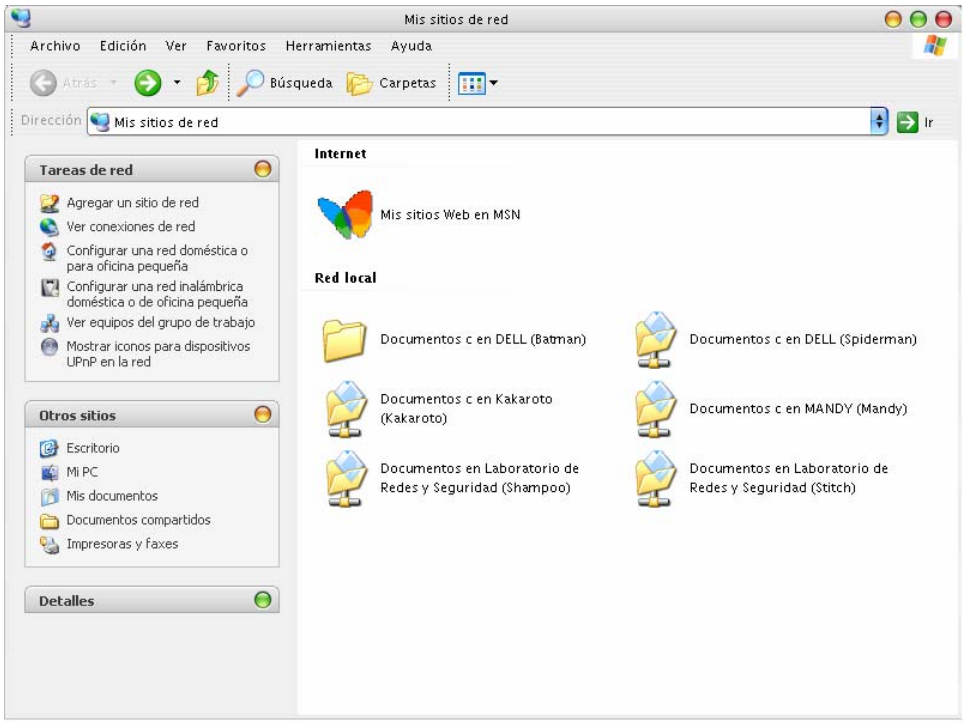


Figura 4.7 Documentos Compartidos

Para el caso de Fedora, se hicieron las pruebas en el apartado de “Servidores de Red” (Ver Figura 4.8) así mismo el acceso a los documentos compartidos por medio de SAMBA (Ver Figura 4.9 y Figura 4.10)

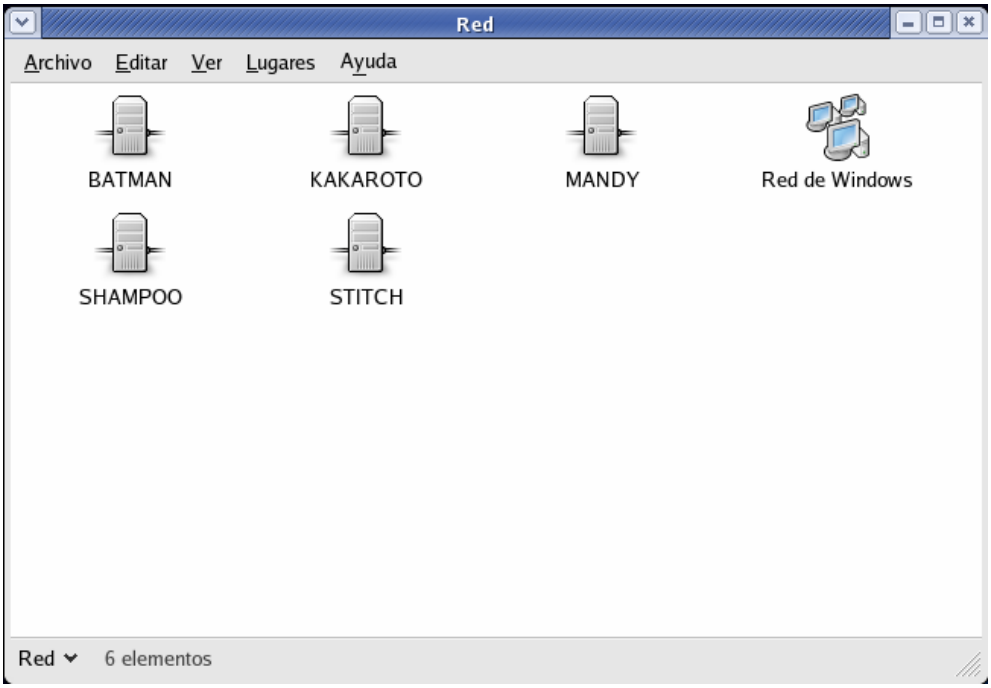


Figura 4.8 Equipos en la Red



Figura 4.9 Autenticación para acceder a documentos compartidos por medio de SAMBA



Figura 4.10 Documentos compartidos por medio de SAMBA

Los inconvenientes vinieron con los equipos donados por ISETI, ya que contenían hardware muy actualizado, se presentaron problemas en la instalación de Fedora, por lo que se decidió cambiar a Red Hat 9, pero muchos de los dispositivos fallaban por lo que la solución inmediata fue dejarlas con el sistema operativo original y en un segundo disco duro instalar Linux Red Hat 9

Durante la instalación del cableado no se dejó de dar servicio a tesistas pues no se realizó la migración hasta que el cableado estructurado fue terminado en su totalidad.

Para probar el cableado, éste tuvo que estar instalado completamente ya que tenía que probarse la vía completa, desde el panel de parcheo hasta la máquina por lo hubo una incertidumbre total hasta el final. Cuando se finalizó la instalación, se probó máquina por máquina, es decir, se hacía un ping hacia el servidor, si había respuesta, esa vía estaba perfectamente, de lo contrario podían ser los siguientes casos:

- mala construcción del cable que va desde la tarjeta de red del equipo hasta la roseta
- algún error en el armado de la roseta (mala configuración de jack o mal ponchado del mismo)
- fracturas en el cable
- mal ponchado de los cables en el panel de parcheo
- error en la construcción del cable que va del panel de parcheo al switch
- falla de los puertos del switch.

Para comprobar todo lo anterior fue de mucha utilidad el que cada dispositivo, equipo y puertos se tuvieran perfectamente identificados por las etiquetas adecuadas, encontrando así una rápida correspondencia y por lo tanto localización de fallas.

Una vez que el laboratorio comenzó a dar servicio a usuarios, se sometió a varias pruebas y se encontraron diferentes problemas que debían resolverse. A continuación se comentarán las pruebas realizadas, se plantearán las dificultades a

las que nos enfrentamos y posteriormente se tratará de las medidas tomadas para la solución de las mismas.

4.2 PRUEBAS DE USUARIOS

En primera instancia, se identifican dos tipos de usuarios:

- Tesistas
- Alumnos (de las Asignaturas de Redes de Computadoras y Seguridad Informática)

4.2.1 Tesistas

Hay estudiantes interesados en los temas de Seguridad y Redes de Datos así como en el desarrollo del laboratorio mismo, de manera que se llevan a cabo diferentes proyectos, los cuales son creados y probados en el laboratorio. Para ello, en muchas ocasiones se necesita tener ciertos privilegios sobre las máquinas, es decir, poder manipular la configuración de las mismas, modificar, crear y borrar archivos, así como instalar nuevos paquetes, entre otras cosas. Por lo que se tuvo la necesidad de crear una cuenta de usuario en las máquinas con privilegios de administrador, llamada administración, y la contraseña fue proporcionada a los tesistas que después de analizar su proyecto y los requerimientos de este, solicitaran dicha cuenta.

4.2.1.1 Dificultades

- Al tener pleno control sobre las máquinas se corren ciertos riesgos, por ejemplo, configurar erróneamente algún dispositivo, dando como resultado un mal funcionamiento; instalar paquetes que ponen en riesgo la seguridad de las máquinas, infectarlas accidentalmente de virus, troyanos o algún tipo de software perjudicial para las mismas.

- Al realizar diferentes pruebas como por ejemplo la instalación y configuración de las tarjetas de red alámbricas e inalámbricas, el instalar programas para el monitoreo de la red, etc., que en algunas ocasiones era necesario desconfigurar algún hardware o la desinstalación de ciertos componentes daba como resultado que hubiera máquinas fuera de servicio para el resto de los tesistas en el tiempo de prueba.

- Un contratiempo importante fue que los tesistas hacían uso del laboratorio en horarios muy diferentes, por lo que hubo la necesidad de tener un horario de servicio que abarcara la mayor parte del día y siempre se contara con la presencia de un encargado para la solución de posibles problemas o dudas generadas con el equipo o la red.

- En un principio el acceso al laboratorio era libre, ya que podían pedir llaves e incluso algunos de ellos contaban con juegos de llaves y podían entrar sin supervisión alguna y esto ocasionó por una parte mal funcionamiento del equipo (por no saber que proyectos se llevaban a cabo en cada equipo) y por otra la pérdida de material y/o dispositivos del laboratorio (switches, mouse, tarjetas de red, memoria RAM, discos duros, etc.).

4.2.2 Alumnos

Para que el laboratorio empiece a ser aprovechado y se identifiquen los problemas que se pueden tener cuando el mismo ya esté abierto y se impartan clases, se dan pequeños talleres, algunas clases y se realiza revisión de proyectos.

En este caso, se necesita una preparación previa del laboratorio:

- Instalación del software específico para el tipo de actividad a desarrollar.
- Creación de cuentas.
- Preparación de herramienta y material.
- Revisión del buen funcionamiento de cada una de las máquinas, antes y después de las actividades desarrolladas.

4.2.2.1 Dificultades

Cuando se tiene un grupo de personas es difícil mantener el control de cada una ellas cuando trabajan en las máquinas, por lo que se presentan diferentes contratiempos antes, durante y después del trabajo grupal:

- **Antes:**

- Mal planteamiento de las prácticas o talleres que como se encuentran en la fase de diseño y pruebas se tienen problemas como en el Sistema Operativo Linux, ya que en diferentes distribuciones e incluso versiones del sistema hay un cambio en la sintaxis de los comandos que realizan una misma función.

- **Durante:**

- La atención se pierde con facilidad, ya que el acomodo de las máquinas no permite a los alumnos tener una misma visión desde cada una de ellas.
- Se necesita la presencia del encargado del laboratorio por posibles fallos en las máquinas o dudas con respecto a ellas, todo esto porque los requerimientos proporcionados para la clase o taller no fueron comunicados al encargado en su totalidad, o por causas ajenas, por ejemplo un mal inicio de sesión en los equipos.

- **Después:**

- En algunas ocasiones se les proporciona a los alumnos una cuenta de administrador para poder realizar la práctica o el taller, ya que el laboratorio también funciona para la asignatura de Administración de Redes y se debe contar con permisos que admitan la ejecución de ciertos programas, por lo que se presentan los problemas mencionados anteriormente en el apartado 4.2.1.1.

Ante las dificultades presentadas, se tomaron algunas medidas para la solución de las mismas.

4.3 SOLUCIONES

4.3.1 Equipo

Las soluciones a estos contratiempos fueron relativamente fáciles de encontrar, la solución a las diferentes versiones de sistemas operativos en Windows vino de la mano con la adquisición de nuevo equipo, en donde la capacidad de memoria y de disco duro permitió homogenizar en Windows XP y Fedora 3.0. Para tomar la decisión de lo anterior se hizo un análisis de las ventajas y desventajas de cada componente, programa o utilidad que viene con el sistema para determinar cual sería la mejor opción para nuestros fines.

Con respecto al cableado también hubo cambios. Hicimos nuevos cables que funcionaran adecuadamente. La instalación de las canaletas, las rosetas y el rack facilitó que el laboratorio estuviera ordenado y fuera de acuerdo con los estándares. Además se logró sin problema tener todas las máquinas en red al mismo tiempo puesto que las canaletas tenían mayor capacidad y las nuevas rosetas ya contaban con dos jacks cada una (dado que se pensó en un futuro crecimiento del laboratorio).

Por ser el espacio con el que se cuenta en el laboratorio algo reducido el hecho de ordenar los equipos y buscar el lugar adecuado para maximizar el espacio contribuyó a tener un mejor ambiente de trabajo.

4.3.2 Usuarios

Con base en la situaciones vividas, como por ejemplo el hecho de que un tesista hacia pruebas en alguna máquina, como la configuración de una tarjeta de red inalámbrica, deshabilitaba completamente la configuración lógica y física de la tarjeta anterior y no concluía la configuración de la nueva, al día siguiente o incluso ese mismo día más tarde se tenía la queja de otro tesista que hacía uso de la misma máquina pero ahora su objetivo era instalar algún programa para monitorear la red y este no podía ver ninguna otra máquina, y se tenía que reconfigurar todo de nuevo, otro ejemplo es que algún tesista instalaba programas para la administración de red que emitía un sonido fuerte cada cierto tiempo y no éramos informadas, así es que cuando el sonido empezó no sabíamos de donde venía y tampoco como quitarlo, eso nos descontroló a nosotros y a otros usuarios que se encontraban en el laboratorio. Otro ejemplo, es que algunos usuarios llegaban al laboratorio en compañía de personas que no eran parte de su proyecto de tesis y hacían uso de las máquinas; y como dicho uso no estaba explícitamente prohibido para personas ajenas se decidió crear un reglamento para el control de acceso al laboratorio, el uso del equipo y las responsabilidades de los encargados. Dicho reglamento lo podemos encontrar en el Anexo 2.

Se diseñó una hoja de registro donde cada usuario debe anotar su nombre, la hora de llegada, la máquina que ocupará ese día, el tipo de cuenta (administrador o usuario sin privilegios) y el tipo de usuario (tesista o alumno). Un ejemplo de la hoja de registro se muestra en el Anexo 3.

Se pidió que con anticipación trajeran por escrito todos los requerimientos para realización de prácticas o talleres, incluyendo software y material, teniendo en cuenta en este último punto los recursos con los que cuenta el laboratorio, además del horario y el número de alumnos.

Se cambió la chapa del laboratorio restringiendo así el acceso, y dando como resultado que siempre estuviera presente un encargado para supervisar las actividades que en ese momento se realizaran.

Para facilitar el desarrollo de la práctica o taller y que los alumnos no pierdan la atención hacia la persona que la está llevando a cabo, se limitó el número de alumnos por clase, teniendo como máximo 10.

4.4 Programa de Mantenimiento

Una vez superados todos los incidentes y dándole solución a los problemas que se fueron suscitando durante el desarrollo del laboratorio, también se tiene pensado un programa de mantenimiento posterior a la apertura oficial para el semestre 2006 – II, que de acuerdo a los planes de estudio dará servicio a estudiantes de las asignaturas de Redes de Datos y Administración de Redes, además de los proyectos de tesistas y usuarios ocasionales interesados en el área de redes, es por esto que se plantea el siguiente programa.

El objetivo principal de la administración de red es mantener operativa la red satisfaciendo las necesidades de los usuarios. La utilización de herramientas adecuadas permite realizar este trabajo de forma fácil y práctica. Hoy en día estas herramientas corren sobre diferentes sistemas operativos y suelen tener la característica de disponer de una interfaz gráfica.

- Bimestralmente se deberá hacer monitoreo del ancho de banda para poder mantener la velocidad de conexión al máximo, utilizando en este caso 3com Network Supervisor, que es un software.

- Se actualizará el antivirus de cada máquina para estar al día de los nuevos virus, troyanos, gusanos, etc. La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en las diferentes máquinas. La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador, comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y archivos de los propios servidores, etc. Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

- Se formatearán las máquinas cada inicio de semestre con el fin de no saturar la capacidad de disco y memoria, dejando únicamente el software necesario para la realización de las prácticas y el desarrollo de algún proyecto de tesis en el cual se este trabajando, permitiendo determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red.

- Se actualizará el inventario de software semestralmente instalado y la autorización a los usuarios para la utilización de los paquetes de software.

- Se actualizará el inventario de hardware semestralmente, asegurando que los usuarios disponen del equipamiento suficiente y necesario para cubrir sus necesidades. Se considerará el Bios del sistema, los archivos de configuración del sistema operativo, características de los discos duros, controladores cargados en memoria durante el funcionamiento de la computadora, además se deberá incluir información como la localización

física, condiciones en las que se encuentra, seguimiento de averías de los componentes de las máquinas, etc.

- Continuamente se realizará un monitoreo de la red, para identificar posibles ataques al laboratorio y con esto no dar pie a explotar vulnerabilidades que puedan ocasionar daños a la integridad del laboratorio. Son transparentes a los usuarios. Se ejecutan en cada máquina sin afectar al rendimiento de las mismas.

- Creación y/o mantenimiento de cuentas de usuarios, así como la asignación de recursos y mantenimiento de la seguridad en los accesos a la red, entendiendo por esto las altas, bajas y modificaciones de los usuarios, monitorización de la actividad de los usuarios.

- Semestralmente se realizará una limpieza en cuando a hardware se refiere de todas las máquinas (teclado, monitor, mouse, cpu, bocinas) con el material adecuado.

- Creación de políticas de seguridad, ya que la seguridad es un aspecto que afecta a todas las áreas de administración, por cada recurso en la red se dispondrán de mecanismos para establecer permisos de utilización, así como monitoreo de la utilización de dichos recursos.

- Actualización del reglamento del laboratorio de redes.

4.5 Errores Frecuentes y Soluciones

Durante la realización de este proyecto de tesis se encontraron errores comunes, los cuales pueden llegar a ocurrir, para se esto se presentan los siguientes puntos y las soluciones a los mismos.

- Al encender la computadora el teclado no funciona.

Esto ocurre con frecuencia cuando el usuario enciende la computadora y al saber que puede arrancar en dos sistemas operativos diferentes comienzan a teclear repetidamente sin que la pantalla de opciones aparezca (Figura 5.1), esto ocasiona que se desborde la memoria y por tanto no funcione algún dispositivo en este caso el teclado, se soluciona únicamente reiniciando la máquina y esperando la pantalla de opciones para seleccionar el sistema operativo que se desee utilizar.



Figura 5.1 Pantalla de opciones

- Conexión de área local, cable desconectado.

Esto ocurre cuando el usuario enciende la máquina y quiere ingresar a alguna página web y aparece un mensaje como el mostrado en la Figura 5.2, se puede deber a varios factores:

1. El cable de red que se encuentra de computadora a roseta se encuentra desconectado.
2. El cable de roseta a patch panel se encuentra desconectado
3. El cable de patch panel a switch se encuentra desconectado
4. La conexión es inalámbrica y el access point se encuentra desconectado.

La solución es revisar únicamente las conexiones.

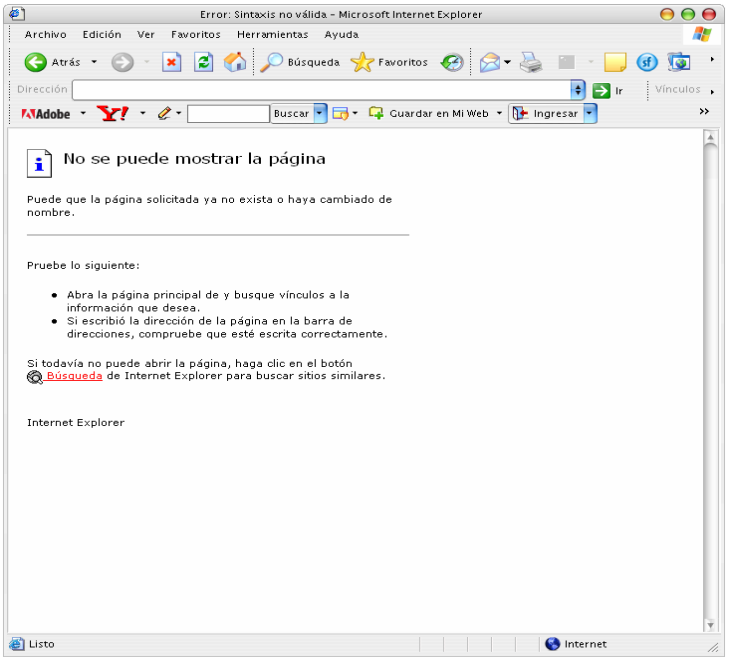


Figura 5.2 Conexión de área local, cable desconectado

- No se puede acceder a los archivos compartidos

Puede deberse a dos causas:

1. El servicio SAMBA se encuentra deshabilitado y únicamente se necesita levantar dicho servicio.
2. Después de formatear un equipo, el usuario puede ver la carpeta de archivos compartidos de otra máquina pero no puede acceder, y se debe a que cuando se formatea una computadora no se habilita por default la opción “Permitir que los usuarios de la red cambien mis archivos” (Figura 5.3)

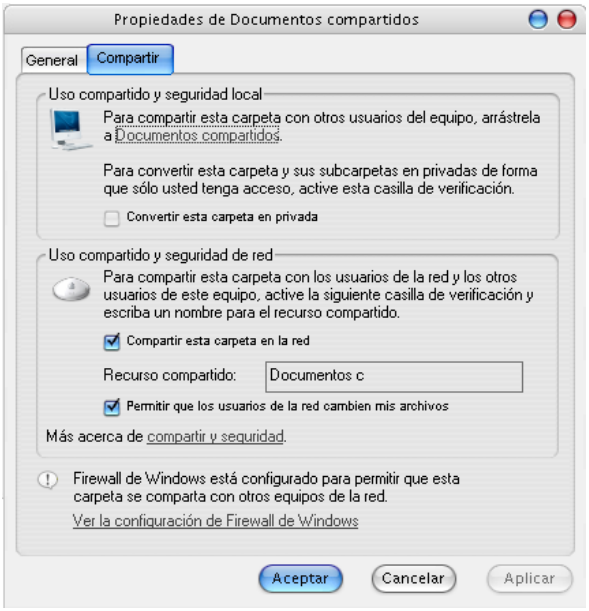


Figura 5.3 Archivos compartidos

- No se tiene acceso a Internet

Esto ocurre después de un apagón general o cuando el regulador eléctrico esta en mantenimiento, se soluciona levantando nuevamente el Firewall instalado en "Jimmy". Se necesita ingresar con una cuenta de superusuario y teclear el siguiente comando:

Sudo /etc/init.d/firewall restart

Este trabajo se basó en los siguientes objetivos:

El primer objetivo considerado para la realización de esta tesis es el de:

Proveer una plataforma de trabajo en hardware y software a los estudiantes y profesores del área de redes de computadoras de la Facultad de Ingeniería.

Este objetivo se trata prácticamente en todo este trabajo de tesis, a lo largo del cual se puede apreciar que se comenzó teniendo que obtener un espacio para el desarrollo de un laboratorio de Redes y Seguridad, seguido de la búsqueda del material que pudiera recaudarse para empezar a construir un espacio en donde alumnos y profesores pudieran desarrollar su trabajo de una manera más eficiente y práctica.

Se logró crear un espacio con equipo actual, con gran capacidad de almacenamiento y excelente velocidad, con los dispositivos adecuados (como el switch y el panel de parcheo) y que sigue las normas indicadas para un área de redes de computadoras. Se cuenta con cableado estructurado y con material para la realización de cables, rosetas, y más.

Al día de hoy se tiene un laboratorio en condiciones óptimas para poder abrir sus puertas a los alumnos de las asignaturas de redes de computadoras, redes de datos y administración de redes que así lo deseen, gracias a la contribución y el trabajo de un gran número de colaboradores (profesores, alumnos, tesistas, ex alumnos) quienes aportando conocimientos, equipo, dispositivos, cableado e incluso su cooperación en el laboratorio (trabajo social) fueron piezas clave en la creación del mismo.

Los estudiantes interesados en el área de redes pueden ahora contar con un espacio que les permita ampliar sus conocimientos y poner en práctica los ya adquiridos.

Los profesores tienen un sitio que servirá de apoyo para sus cátedras fomentando así el interés en sus alumnos.

El segundo objetivo fue:

Apoyar al alumno en el desarrollo de habilidades analíticas y funcionales para la creación, implantación, mantenimiento y administración de redes de computadoras mediante el seguimiento de las prácticas de las distintas materias del área.

Una vez que el laboratorio ya contaba con el material necesario era importante hacer pruebas, dar a conocer el nuevo laboratorio y despertar el interés de los alumnos por la materia y por poner en práctica los conocimientos que están adquiriendo.

Para este objetivo, nos podemos basar en el desarrollo de los capítulos 3 y 4, en donde por medio de talleres los alumnos pudieron ver el armado de cables y de rosetas dentro de una red en funcionamiento, es importante mencionar que se tuvo presente el objetivo de cada materia, de este modo, se pudo dar un apoyo mayor a dichas materias, y los alumnos pudieron tener un panorama en el sentido práctico mucho más amplio, tuvo una respuesta muy favorable, ya que dichos talleres tuvieron

un cupo limitado dado la gran demanda que presentaron.

A futuro se tiene considerado continuar dando talleres de actualización para alumnos que tengan inquietudes sobre redes inalámbricas o también para los alumnos que no decidieron cambiar de plan de estudios, y para los que el laboratorio no es obligatorio, pero además pretendan ampliar sus conocimientos en redes de datos y administración de redes de manera práctica.

El laboratorio cuenta con el equipo adecuado para la realización exitosa de las prácticas, así como para el desarrollo de proyectos que ayuden a crecer y mejorar el mismo.

Las expectativas de este proyecto han sido cubiertas en su totalidad e incluso un poco más, ofreciendo la oportunidad de un lugar hecho para los futuros ingenieros tan cercano al mundo laboral como sea posible.

Comentarios finales

Este trabajo estuvo en constante cambio. Al principio, este proyecto se pensaba en una propuesta de cómo sería el Laboratorio de Redes y Seguridad. Sin embargo, gracias a la División de Ingeniería Eléctrica y a las donaciones realizadas, esta propuesta se convirtió en una realidad, permitiendo así la preparación del laboratorio para que este semestre 2006-II entre en funcionamiento oficialmente.

El interés de los alumnos por contar con un laboratorio de este tipo tuvo una respuesta inmediata y favorable. Hubo una gran concurrencia en los grupos piloto, que con 10 horas a la semana por taller y aproximadamente de 10 alumnos por grupo, para las pruebas de diferentes prácticas. Este interés fue una gran satisfacción y los resultados recabados ayudaron en gran medida a mejorar y optimizar el laboratorio.

Aunque el laboratorio ya está listo para dar servicio formalmente en el semestre que está a punto de empezar, no hay que dejar de lado el hecho de que aún faltan muchas cosas por hacer, puesto que es necesario adquirir más material: pinzas de presión (ya que solamente se cuenta con una), pinzas de impacto (solamente existen 2 en el laboratorio), pinzas de un solo impacto, tester, bases para construcción de jacks, pinzas de presión para fibra óptica, adhesivo especial para fibra, microscopio 400X para fibra, desforradoras, tarjetas de red. Además de otros dispositivos: un switch de fibra óptica, reguladores (como protección para las máquinas en fallas de voltaje), routers.

El laboratorio también estará abierto a la posibilidad de que futuras generaciones hagan contribuciones, cambios y mejoras para que siempre esté actualizado y cumpla correctamente con el objetivo de ayudar a la formación de ingenieros de calidad en el medio laboral.

A

ANCHO DE BANDA: Cantidad de información que puede pasar por una línea de comunicación al mismo tiempo. Se mide en Hertz ("ciclos por segundo") o en bits por segundo (bps).

AUTOMATIZAR: Hacer que un aparato o sistema funcione por sí solo, eliminando los procesos manuales.

B

BACKBONE: Parte de la red que soporta la mayor parte del tráfico de datos. También conocida como troncal, conecta redes más pequeñas o nodos, para crear redes de mayor tamaño. Normalmente transmite los datos a una velocidad más elevada que el resto de la red. En redes muy grandes, como Internet, puede haber varios troncales, cada uno de los cuales cubre grandes zonas de la red. En redes pequeñas, el troncal se puede llamar bus. Literalmente, backbone significa columna vertebral.

BGP: Border Gateway Protocol es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un router que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca. Se trata del protocolo más utilizado para redes con intención de configurar un EGP (external gateway protocol)

BIT: Unidad binaria de información que puede tener dos valores, 0 y 1. La palabra proviene de la contracción de las voces inglesas “binary” y “digit”.

BROADCAST: Paquete de datos que se envía a todos los nodos de una red. Los broadcasts se identifican a través de una dirección de broadcast.

BUG: Error de un programa de computadora. Término aplicado a los errores descubiertos al ejecutar un programa. Fue usado por primera vez en 1945 cuando uno de los pioneros de la programación moderna descubrió que un insecto (bug) había dañado un circuito de una computadora.

BYTE: Es un grupo de ocho bits que se combinan para representar un carácter o una medida de capacidad de memoria.

C

CANALETA: La canaleta es un ducto diseñado para alojar cables de telecomunicaciones que generalmente se instala en las áreas de trabajo.

CODIFICACIÓN: representación de los componentes de un sistema por medio de otros que pertenecen a un conjunto ya predefinido.

CODIGO FUENTE: El código fuente es la descripción del funcionamiento de un programa, en un lenguaje que los humanos somos capaces de entender, pero que a su vez es lo suficientemente formal como para que una herramienta lo transforme automáticamente en algo interpretable por una computadora.

CODIGO FUENTE ABIERTO: Código Fuente que está disponible libremente, y se puede modificar para mejorar el programa o arreglar los fallos.

COLISIÓN: Es el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico.

CONMUTACIÓN: Es el proceso mediante el cual un portador separa los datos en paquetes. Cada paquete contiene la dirección de origen, la dirección de su destino, e información acerca de cómo volver a unirse con otros paquetes emparentados. Este proceso permite que paquetes de distintas localizaciones se entremezclen en las mismas líneas y que sean clasificados y dirigidos a distintas rutas.

CUT-THROUGH MÉTODO: Es un método de diseñado para sistemas de conmutación de paquetes. Cuándo un paquete llega a un switch, éste empieza a reenviar el paquete casi inmediatamente, leyendo sólo los primeros bytes en el paquete para determinar la dirección de destino.

D

DATAGRAMA: Datos agrupados en paquetes que viajan por una red.

DGSCA: La Dirección General de Servicios de Cómputo Académico de la UNAM es la entidad universitaria encargada de la operación de los sistemas centrales de cómputo académico y de las telecomunicaciones de la institución.

DIRECCIONAR: En comunicación de datos, el código exclusivo asignado a cada dispositivo o estación de trabajo conectado a una red.

DNS: (Domain Name System, Sistema de Nombres de Dominio). Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1.

E

ENCAMINAMIENTO/ENRUTAMIENTO: Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

ENCAMINAMIENTO/ENRUTAMIENTO ESTÁTICO: Ruta que se ha configurado e introducido explícitamente en la tabla de enrutamiento Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico.

ENCAMINAMIENTO/ENRUTAMIENTO DINÁMICO: Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico. También denominado enrutamiento adaptable.

ENCRIPTAR: Una manera de codificar la información de un fichero o de un correo electrónico de manera que no pueda ser leído en caso de ser interceptado por una tercera persona mientras viaja por la red. Sólo la persona o personas que tienen el tipo de de software de descodificación adecuado pueden descifrar el mensaje.

ESTACIÓN: Es uno de los equipos de cómputo conectados a una red local que utiliza los servicios y los recursos existentes en dicha red.

ETHERNET: Tecnología de comunicación para redes locales desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation que utiliza el protocolo de contención CSMA/CD y que tiene una velocidad de transferencia de 10 Mbps.

F

FAST ETHERNET: Tecnología de comunicación que fue puesta a disposición en el año de 1992 por Grand Junction Networks y que tiene una velocidad de transferencia de 100 Mbps. Cualquiera de las especificaciones de Ethernet de 100 Mbps. Fast Ethernet ofrece 10 veces más velocidad que el de la especificación Ethernet 10BaseT, preservando características como el formato de trama y los mecanismos MAC y MTU.

FEDORA CORE: El Proyecto Fedora es un proyecto de código abierto patrocinado por Red Hat y soportado por la comunidad. No se trata de un producto soportado por Red Hat, Inc. ¿Su objetivo? Trabajar con la comunidad Linux para construir un sistema operativo completo de propósito general, exclusivamente a partir de software libre. Un foro público. Procesos abiertos. Un terreno de pruebas para nuevas tecnologías que quizás eventualmente formen parte de los productos Red Hat.

FIREWALL: Mecanismo utilizado para proteger una red o computadora conectada a Internet de accesos no autorizados. Una firewall puede construirse con software, con hardware o con una combinación de ambos.

FLASH: Tecnología que permite la creación de animaciones, entre otras cosas, utilizando menos ancho de banda que otros formatos.

FULL DUPLEX: En una comunicación full-duplex existen dos canales, uno para cada sentido: ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono.

G

GUSANO: Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos están especialmente escritos para redes.

H

HACKER: Nombre que se da a un usuario con avanzados conocimientos que dedica mucho tiempo a trabajar con los ordenadores. La palabra hacker se utiliza mucho para designar a las personas que rompen los sistemas de seguridad informáticos para causar daños, robar secretos o, simplemente para demostrar que pueden hacerlo.

HALF DUPLEX: En una comunicación half-duplex existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente: las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados.

HANDHELDS: Pequeña computadora portátil cuya principal característica es que posee una pantalla sensible al tacto, que permite ingresar información directamente a través de ella.

HARDWARE: Conjunto de elementos físicos de una computadora o de una red, a diferencia de los programas o elementos lógicos que los hacen funcionar. Es la parte tangible de la computadora.

HDLC: (Control de Enlace de Datos de Alto Nivel) Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación.

HOST: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

HTML: Lenguaje de etiquetas por hipertexto. Lenguaje de formateo de documentos por hipertexto simple que usa etiquetas para indicar cómo debe interpretar una parte determinada de un documento una aplicación de visualización como, por ejemplo, un navegador de Internet. El HTML le indica al navegador cómo mostrar la información que recibe por medio de una serie de instrucciones estándar (tags o marcas) que indican el formato de cada pieza de información que se incluye en el documento. Los vínculos permiten a los usuarios saltar de un documento a otro relacionado pulsando un icono o un hipertexto.

HUBBELL: Hubbell Incorporated es una compañía diversificada y global con múltiples fábricas y mercados en Estados Unidos, México, Canadá y el resto del mundo. A principios de los noventa, Hubbell decide invertir agresivamente en México, creando Hubbell de México, empresa que coordina la comercialización de todos los productos de la compañía en nuestro país. Su misión es contribuir al desarrollo comercial e industrial del país, con productos y servicios de calidad internacional y vanguardia tecnológica

I

ICONO: Signo o imagen en que hay una relación de semejanza con lo representado.

INTERFAZ: Se denomina así a todo aquel medio físico que conecta un dispositivo periférico con la computadora; también se le conoce así a todo el software que comunica al usuario con la misma.

INTERNET: Conjunto de redes de computadoras que conecta y comunica a millones de personas en todo el mundo. Es una red no comercial que nació en Estados Unidos en 1969 y está integrada por millones de computadoras, llamadas servidores, que comparten un lenguaje común. Las computadoras personales que se conectan y consultan datos de los servidores se denominan clientes.

INTERNETWORKING: Término general que se usa para referirse a la industria que ha surgido alrededor del problema de conectar redes entre sí. El término puede referirse a productos, procedimientos y tecnologías.

IP (Internet Protocol; Protocolo Internet): Protocolo que provee las funciones básicas de direccionamiento en Internet y en cualquier red TCP/IP. Opera en la capa tres del modelo OSI.

ISP: Proveedor de Servicios de Internet (PSI). Es una compañía cuyo negocio es ofrecer acceso a Internet, actuando como pasarela entre el usuario final y la red.

K

KERNEL: Parte fundamental de un sistema operativo. Permite la interacción entre el hardware y el resto del sistema.

L

LATENCIA: Lapso necesario para que un paquete de información viaje desde la fuente hasta su destino. La latencia y el ancho de banda, juntos, definen la capacidad y la velocidad de una red.

LINUX: Es el núcleo de un sistema operativo libre, desarrollado y lanzado al mundo por Linus Benedict Torvalds en 1991.

M

MULTIPLEXAR: Es la acción de combinar varias señales (análogas o digitales) para su transmisión sobre una línea o medio. Un tipo común de multiplexado combina varias señales de baja velocidad para transmitir por una conexión de alta velocidad. Hay varios métodos de multiplexado:
Frequency Division Multiplexing (FDM): a cada señal se le asigna una frecuencia diferente.
Time Division Multiplexing (TDM) : a cada señal se le asigna un intervalos fijo de tiempo en transmisiones alternadas.
Statistical Time Division Multiplexing (STDM): los intervalos de tiempo se asignan a las señales dinámicamente para hacer un mejor uso del ancho de banda.
Wavelength Division Multiplexing (WDM): a cada señal se le asigna una longitud de onda particular. Se usa en fibra óptica.

N

NETBIOS: (Network Basic Input/Output System, BIOS de una red). Se trata del corazón de una tarjeta de red, de forma similar a como el BIOS es el corazón de la placa base de una computadora.

NODO: Cualquier computador conectado a la red. También es otra forma de denominar a un dispositivo que tiene acceso a Internet.

NOTEBOOK: Microcomputadora portátil de gran potencia de cálculo y con batería que le proporciona la capacidad de trabajo sin estar enchufada a la red eléctrica.

O

OPENSOURCE: ver código fuente abierto

OSI: (Open Systems Interconnection, Interconexion de Sistemas Abiertos). Modelo de referencia de interconexión de sistemas abiertos propuesto por la organización de normalización ISO. Divide las tareas de la red en siete niveles.

OSPF: Open Shortest Path First es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Internet Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado identica en todos los encaminadores de la zona.

P

PAQUETE: Se llama así a la unidad de datos que se envía a través de una red

PBX: Private Branch Exchange (Central Telefónica Privada)

PING: (Packet INternet Groper, Rastreador de Paquetes Internet). Programa utilizado para comprobar si un servidor está disponible. Envía paquetes de control para comprobar si el servidor esta activo y los devuelve.

PONCHAR: Es la acción de insertar el conector en la pinza de presión y apretar con firmeza hasta escuchar un “click” para asegurar el cable.

PROTOCOLO: Conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso de comunicación (emisor y receptor). Estos protocolos gobiernan formatos, modos de acceso, secuencias temporales, etc.

R

RACK: Estructura metálica utilizada para montar equipo electrónico y paneles de parcheo. Contiene estructuras de soporte horizontal y vertical, puede estar afianzada a la pared o el piso.

RECURSO: Componente físico o lógico de la computadora. También se denomina así a la actividad de un programa que puede ser utilizada por varias aplicaciones de modo concurrente o simultáneo.

RED HAT, INC.: Es una de las primeras empresas de desarrollo de código libre del mundo y ofrece casi todos sus esfuerzos de desarrollo a la comunidad de desarrollo de Linux.

RIP: Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o IGP (Internet Gateway Protocol) utilizado por los encaminadores (routers).

S

SECUENCIAL: Procesamiento en el que cada operación precede a otra y sigue a otra, sin que nunca dos de entre ellas sean simultáneas.

SEGMENTO: Parte que se corta, se divide o se separa de un todo

SEMÁNTICA: Se ocupa de la relación entre los signos y los objetos denotados por ellos.

SERVIDOR CENTRAL: En el contexto de redes, una computadora que proporciona directamente servicio a un usuario. En contraste con un servidor de la red que da servicios a través de otro que sirve como intermediario.

SHELL: Término en inglés traducido por intérprete de órdenes. Éste es capaz de recoger las órdenes que el usuario realiza, pasándolas al núcleo del Sistema Operativo para su ejecución.

SIMPLEX: En una comunicación simplex existe un solo canal unidireccional: el origen puede transmitir al destino pero el destino no puede comunicarse con el origen. Por ejemplo, la radio y la televisión.

SINTAXIS: Estudia las relaciones de los signos entre sí.

SISTEMA OPERATIVO: Programa de control que dirige el hardware de una computadora. Por lo general es, en realidad, una colección de programas que interactúan juntos.

SITIO WEB: Punto de la red con una dirección única y al que pueden acceder los usuarios para obtener información. Normalmente un sitio web dispone de un conjunto de páginas organizadas a partir de una “home page” o página principal, e integra ficheros de varios tipos, tales como sonidos, fotografías, o aplicaciones interactivas de consulta.

SLOT: Ranura del ordenador en la que se pueden insertar nuevas tarjetas para ofrecer más utilidades.

SNIFFER: (Husmeador) Programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente se usa con fines ilegales.

SOFTWARE: Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras. Parte intangible de la computadora.

SOFTWARE LIBRE: Programas desarrollados y distribuidos según la filosofía de dar al usuario la libertad de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar dichos programa (Linux es un ejemplo de esta filosofía). El software libre no es siempre software gratuito (equivocación bastante habitual que tiene su origen en que la palabra inglesa “free” significa tanto "libre" como "gratuito").

T

TEMPORIZACIÓN: Acción de planificar en el tiempo, los contenidos y las actividades asociadas de una determinada acción.

TERMINAL: Dispositivo en un sistema o red de comunicación en el cual los datos pueden ingresarse o salir, pero no procesarse.

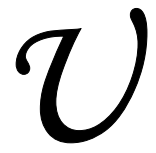
TOKEN PASSING (Paso de ficha): Protocolo que se utiliza en redes Arcnet y Token Ring y se basa en un esquema libre de colisiones.

TOKEN RING: Tecnología de comunicación para redes locales desarrollada por IBM que utiliza el protocolo de acceso Token Passing y que utiliza velocidades de transferencia de 4 y 16 Mbps.

TRÁFICO: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúe a través de una red de telecomunicaciones.

TRAMA: Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

TROYANO: (Caballos de Troya) Programas que, enmascarados de alguna forma como un juego o similar, buscan hacer creer al usuario que son inofensivos, para realizar acciones maliciosas en su equipo. A diferencia de los virus y gusanos los troyanos no se pueden reproducir por si mismos. Un troyano de puerta trasera es un programa que permite el acceso remoto no autorizado al equipo infectado.



UTP: Cable de par trenzado sin apantallar (Unshielded Twisted Pair). Utilizado para conexiones de red de algún tipo.



VELOCIDAD DE TRANSMISIÓN: Se refiere al número de bits por segundo que se pueden enviar a través de un medio de comunicación.

VIRUS: Los virus son programas que se pueden introducir en las computadoras y sistemas de información de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

A1.1 Archivo lmhosts

```
127.0.0.1 localhost
192.168.2.9     batman
192.168.2.8     shampoo
192.168.2.7     stitch
192.168.2.6     kakaroto
192.168.2.5     eva
192.168.2.4     mandy
192.168.2.3     snoopy
192.168.2.2     mickey
192.168.2.10    spiderman
192.168.2.11    pinky
```

A1.2 Archivo smb.conf

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#
#======================= Global Settings
=====================================
[global]

# workgroup = NT-Domain-Name or Workgroup-Name
      workgroup = INICIOMS

# server string is the equivalent of the NT Description field
# Server String es solo una descripciÃ³n del servidor
      server string = Samba Server

# Aquí pondremos el netbios

      netbios name = BATMAN

# Aquí pondremos las "interfaces" que es para seguridad y que no recibirá
# Peticiones provenientes de esa interfaz. esto es útil cuando Samba se ejecuta en
un servidor
# o también de puerta de enlace para la red local, impidiendo se establezcan
conexiones desde
# otra red local.
      interfaces = 192.168.2.254/24

# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
```

```
# the smb.conf man page
# Lo siguiente estaba comentado y lo que hare serÃ¡ descomentarlo para que
puedantener acceso los demas
        hosts allow = 192.168.2. 127.
;    hosts allow = 192.168.1. 192.168.2. 127.

# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
        printcap name = /etc/printcap
        load printers = yes

# It should not be necessary to spell out the print system type unless
# yours is non-standard. Currently supported print systems include:
# bsd, sysv, plp, lprng, aix, hpux, qnx
;    printing = cups

# This option tells cups that the data has already been rasterized
        cups options = raw

# Uncomment this if you want a guest account, you must add this to /etc/passwd
# otherwise the user "nobody" is used
;  guest account = pcguest

# this tells Samba to use a separate log file for each machine
# that connects
        log file = /var/log/samba/%m.log
# all log information in one file
#    log file = /var/log/samba/smbd.log

# Put a capping on the size of the log files (in Kb).
        max log size = 50

# Security mode. Most people will want user level security. See
# security_level.txt for details.
# Use password server option only with security = server
;    password server = <NT-Server-Name>

# Password Level allows matching of _n_ characters of the password for
# all combinations of upper and lower case.
;  password level = 8
;  username level = 8

# You may wish to use password encryption. Please read
# ENCRYPTION.txt, Win95.txt and WinNT.txt in the Samba documentation.
# Do not enable this option unless you have read those documents

        encrypt passwords = yes
        smb passwd file = /etc/samba/smbpasswd

# The following are needed to allow password changing from Windows to
# update the Linux system password also.
# NOTE: Use these with 'encrypt passwords' and 'smb passwd file' above.
# NOTE2: You do NOT need these to allow workstations to change only
#        the encrypted SMB passwords. They allow the Unix password
#        to be kept in sync with the SMB password.
;  unix password sync = Yes
;  passwd program = /usr/bin/passwd %u
;  passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password*
%n\n *passwd:*all*authentication*tokens*updated*successfully*

# Unix users can map to different SMB User names
```

```
;  username map = /etc/samba/smbusers

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /etc/samba/smb.conf.%m

# Most people will find that this option gives better performance.
# See speed.txt and the manual pages for details
      socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

# Configure Samba to use multiple interfaces
# If you have multiple network interfaces then you must list them
# here. See the man page for details.
;   interfaces = 192.168.12.2/24 192.168.13.2/24

# Configure remote browse list synchronisation here
#  request announcement to, or browse list sync from:
#       a specific host or from / to a whole subnet (see below)
;   remote browse sync = 192.168.3.25 192.168.5.255
# Cause this host to announce itself to local subnets here
;   remote announce = 192.168.1.255 192.168.2.44

# Aquí podemos hacer transmisión (Broadcast) hacia la red local, y hacer un
anuncio remoto
      remote announce = 192.168.2.255

# Browser Control Options:
# set local master to no if you don't want Samba to become a master
# browser on your network. Otherwise the normal election rules apply
;   local master = no

# OS Level determines the precedence of this server in master browser
# elections. The default value should be reasonable
;   os level = 33

# Domain Master specifies Samba to be the Domain Master Browser. This
# allows Samba to collate browse lists between subnets. Don't use this
# if you already have a Windows NT domain controller doing this job
;   domain master = yes

# Aquí podemos especificar que el servidor sea el "maestro del dominio" e incluso
sobre cualquier otro en la red
      domain master = yes
      preferred master = yes

# Preferred Master causes Samba to force a local browser election on startup
# and gives it a slightly higher chance of winning the election
;   preferred master = yes

# Enable this if you want Samba to be a domain logon server for
# Windows95 workstations.
;   domain logons = yes

# if you enable domain logons then you may want a per-machine or
# per user logon script
# run a specific logon batch file per workstation (machine)
;   logon script = %m.bat
# run a specific logon batch file per username
;   logon script = %U.bat
```

```
# Where to store roving profiles (only for Win95 and WinNT)
#       %L substitutes for this servers netbios name, %U is username
#       You must uncomment the [Profiles] share below
;   logon path = \\%L\Profiles\%U

# All NetBIOS names must be resolved to IP Addresses
# 'Name Resolve Order' allows the named resolution mechanism to be specified
# the default order is "host lmhosts wins bcast". "host" means use the unix
# system gethostbyname() function call that will use either /etc/hosts OR
# DNS or NIS depending on the settings of /etc/host.config, /etc/nsswitch.conf
# and the /etc/resolv.conf file. "host" therefore is system configuration
# dependant. This parameter is most often of use to prevent DNS lookups
# in order to resolve NetBIOS names to IP Addresses. Use with care!
# The example below excludes use of name resolution for machines that are NOT
# on the local network segment
# - OR - are not deliberately to be known via lmhosts or via WINS.
; name resolve order = wins lmhosts bcast

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable it's WINS Server
;   wins support = yes

# Como lo que se eligio es un servidor WINS debo habilitar lo siguiente
      wins support = yes

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
#       Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# WINS Proxy - Tells Samba to answer name resolution queries on
# behalf of a non WINS capable client, for this to work there must be
# at least one  WINS Server on the network. The default is NO.
;   wins proxy = yes

# DNS Proxy - tells Samba whether or not to try to resolve NetBIOS names
# via DNS nslookups. The built-in default for versions 1.9.17 is yes,
# this has been changed in version 1.9.18 to no.
      dns proxy = no

# Case Preservation can be handy - system default is _no_
# NOTE: These can be set on a per share basis
;  preserve case = no
;  short preserve case = no
# Default case is normally upper case for all DOS files
;  default case = lower
# Be very careful with case sensitivity - it can break things!
;  case sensitive = no

#============================ Share Definitions
==============================
      idmap uid = 16777216-33554431
      idmap gid = 16777216-33554431
      template shell = /bin/false
      username map = /etc/samba/smbusers
      password server = None
      winbind use default domain = no

      security = share
[homes]
      comment = Home Directories
      browseable = no
```

```
        writeable = yes

# Un-comment the following and create the netlogon directory for Domain Logons
; [netlogon]
;   comment = Network Logon Service
;   path = /home/netlogon
;   guest ok = yes
;   writable = no
;   share modes = no


# Un-comment the following to provide a specific roving profile share
# the default is to use the user's home directory
;[Profiles]
;    path = /home/profiles
;    browseable = no
;    guest ok = yes


# NOTE: If you have a BSD-style print system there is no need to
# specifically define each individual printer
[printers]
        comment = All Printers Estoy poniendo compartidas las impresoras
        path = /var/spool/samba
        browseable = no
# Set public = yes to allow user 'guest account' to print
        printable = yes
# Hacemos público
        public = yes

# This one is useful for people to share files
[tmp]
  comment = Temporary file space
  path = /tmp
  read only = no
  public = yes

# A publicly accessible directory, but read only, except for people in
# the "staff" group
;[public]
;   comment = Public Stuff
;   path = /home/samba
;   public = yes
;   read only = yes
;   write list = @staff

# Other examples.
#
# A private printer, usable only by fred. Spool data will be placed in fred's
# home directory. Note that fred must have write access to the spool directory,
# wherever it is.
;[fredsprn]
;   comment = Fred's Printer
;   valid users = fred
;   path = /homes/fred
;   printer = freds_printer
;   public = no
;   writable = no
;   printable = yes

# A private directory, usable only by fred. Note that fred requires write
```

```
# access to the directory.
;[fredsdir]
;   comment = Fred's Service
;   path = /usr/somewhere/private
;   valid users = fred
;   public = no
;   writable = yes
;   printable = no

# a service which has a different directory for each machine that connects
# this allows you to tailor configurations to incoming machines. You could
# also use the %u option to tailor it by user name.
# The %m gets replaced with the machine name that is connecting.
;[pchome]
;  comment = PC Directories
;  path = /usr/pc/%m
;  public = no
;  writable = yes

# A publicly accessible directory, read/write to all users. Note that all files
# created in the directory by users will be owned by the default user, so
# any user with access can delete any other user's files. Obviously this
# directory must be writable by the default user. Another user could of course
# be specified, in which case all files would be owned by that user instead.
;[public]
;   path = /usr/somewhere/else/public
;   public = yes
;   only guest = yes
;   writable = yes
;   printable = no

# The following two entries demonstrate how to share a directory so that two
# users can place files there that will be owned by the specific users. In this
# setup, the directory should be writable by both users and should have the
# sticky bit set on it to prevent abuse. Obviously this could be extended to
# as many users as required.
;[myshare]
;   comment = Mary's and Fred's stuff
;   path = /usr/somewhere/shared
;   valid users = mary fred
;   public = no
;   writable = yes
;   printable = no
;   create mask = 0765


[estudiante]
        comment = Esta es una carpeta compartida configurada desde samba
        path = /home/estudiante
        writeable = yes
        guest ok = yes
```

A1.3 Archivo smbusers

```
# Unix_name = SMB_name1 SMB_name2 ...
root = administrator admin
nobody = guest pcguest smbguest
estudiante = administrador
```



Reglamento interno del Laboratorio de Redes y Seguridad

... Respecto al acceso al laboratorio

1. Todos los usuarios que ingresen al laboratorio serán registrados sin excepción en la bitácora.

2. En caso de que algún usuario deba hacer uso del laboratorio en horario no regular, deberá registrarse en la bitácora correspondiente.

3. No se permite la estancia de usuarios en el laboratorio, en ausencia de algún encargado.

... Respecto al Laboratorio

4. Queda terminantemente prohibido ingerir alimentos, fumar, o hacer uso de cualquier sustancia u objeto que puedan dañar los equipos.

5. En horario de clases no se permitirá la entrada a tesistas, ni visitas al laboratorio.

... Respecto al equipo

6. El uso del equipo de laboratorio es para alumnos de las asignaturas del área de Redes y Seguridad y tesistas que desarrollen su proyecto de tesis en el área mencionada.

7. Sólo permanecerán dos usuarios en cada equipo como máximo y ambos serán responsables del mismo.

8. No se permite la apertura y manipulación del equipo de cómputo, excepto la previa autorización y supervisión del encargado.

9. En caso de que el usuario necesite herramientas o dispositivos adicionales, debe solicitarlos al encargado, quien evaluará el caso.

10. El hardware de las computadoras no se prestará, ni se moverá de lugar sin autorización del encargado.

11. El uso de todo el equipo del laboratorio es estrictamente académico, está terminantemente prohibido realizar actividades extraescolares y/o no éticas de cualquier índole.

12. Está estrictamente prohibido manipular de cualquier forma el HUB y el Patch Panel sin la previa autorización y supervisión del encargado.

... Respecto a los usuarios

13. Cada usuario es el único responsable de respaldar su información en algún medio de almacenamiento; para lo cual se sugiere utilice discos flexibles de 3½" y/o Memoria Flash.

14. Los usuarios del laboratorio deben respetar el horario de servicio, consultándolo con los encargados, acudiendo al laboratorio o consultando la página de Internet del mismo.

15. Cada usuario es responsable de cualquier daño, desperfecto o siniestro a la o las máquinas tanto física como lógicamente, que utilice durante su estancia en el laboratorio.

16. Los usuarios del laboratorio serán responsables de las visitas que los acompañen, y sólo podrán usar el equipo, de acuerdo a la disponibilidad del mismo previa autorización del encargado.

17. Cada usuario debe elaborar un breve reporte de las actividades realizadas durante su estancia, en la libreta correspondiente (equipo utilizado, software instalado o desinstalado, actividades generales, etc.)

18. Si el usuario requiere conectar un equipo portátil a la red, debe dirigirse al encargado para hacer una comprobación previa a fin de asegurar que el equipo no se encuentre infectado con algún software que ponga en riesgo la seguridad de la red y del laboratorio.

19. A todo equipo portátil se le asignará una configuración temporal para tener acceso a la red.

20. Está prohibido para cualquier usuario tener cuenta y/o hacer uso del servidor.

... Respecto a las cuentas

21. Queda estrictamente prohibida la instalación de paquetería y cambios de configuración en el equipo del laboratorio.

22. En caso de requerir la instalación de algún programa, deberá dirigirse al encargado para su autorización.

23. Queda terminantemente prohibido crear otro tipo de cuenta de las ya existentes.

24. Queda estrictamente prohibido cambiar la contraseña o el login de cualquier cuenta.

25. Las cuentas serán asignadas de acuerdo a las necesidades de cada usuario.

... Con respecto a los encargados

26. Los encargados del laboratorio son responsables del buen funcionamiento y mantenimiento del equipo.

27. Son responsables del cumplimiento del horario establecido.

28. Son responsables de dar asesoría con respecto a la configuración original de cada equipo.

29. Son responsables de mantener en funcionamiento la red.

30. No son responsables de fallas en el equipo causadas por la mala instalación de algún software realizada por algún usuario sin previa autorización, en este caso, se formateará el equipo.

31. Los encargados no son responsables de la información almacenada en los equipos.

32. No son responsables de cualquier objeto olvidado en el laboratorio.

... Con respecto a las clases

33. Cuando un profesor requiera dar una clase y ocupe un software en específico deberá entregarlo mínimo una semana antes de la fecha de la clase al encargado. El profesor deberá tomar en cuenta las restricciones del equipo y red.

34. En ausencia del encargado, el profesor en turno será el responsable de lo que suceda dentro del laboratorio.

35. Esta estrictamente prohibido abandonar el laboratorio sin que alguien permanezca a cargo del mismo. Cuando en éste no se encuentre ninguna persona deberá permanecer cerrado bajo llave.

36. Cualquier error a nivel software o hardware en los equipos y/o en la red que ocurra durante las clases, deberá informarse inmediatamente al encargado para dar solución inmediata o posterior.

37. Cualquier aspecto no contemplado en este reglamento será tratado por el encargado.

Facultad de Ingeniería

Laboratorio de Redes y Seguridad

Cuaderno de Visitas

	Fecha	Nombre del Tesista	Nombre de la Tesis	Hora		Observaciones
				Entrada	Salida	
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

Formato 2

Fecha	Nombre	Asunto	Equipo	Cuenta	Entrada	Salida	Observaciones
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			
		C T V		A R			

Capítulo 1

http://www.ciberhabitat.gob.mx/museo/cerquita/redes/fundamentos/01.htm
http://www.itlp.edu.mx/publica/tutoriales/telepro/t4_4.htm#Estrella
http://www.mastermas.com/reportajes/linux/P1.asp
http://www.cida.ve/~hernanr/sl/Software_Libre.html
http://www.pergaminovirtual.com.ar/revista/cgi-bin/hoy/archivos/00000210.shtml
http://www.red.com.mx/scripts/redArticulo.php3?articuloID=6540
http://www.monografias.com/trabajos15/sist-operativos/sist-operativos.shtml

Sánchez Prieto, Sebastián
UNIX Guía del usuario
Alfaomega Grupo Editor
México 1997

Capítulo 2

www.ansi.org
http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/direcciones_mac.htm
http://eia.udg.es/~atm/tcp-ip/index.html
http://www.euskalnet.net/shizuka/rs232.htm(RS232)
http://www.htmlweb.net/redes/subredes/subredes_1.html
http://eia.udg.es/~atm/tcp-ip/tema_4_5_6.htm
http://ditec.um.es/laso/docs/tut-tcpip/3376c22.html
http://www.gobernacion.gob.mx/dof/2005/marzo/dof_01-03-2005.pdf
http://www.imnc.org.mx

Andrew S. Tanenbaum
Redes de computadoras
Pearson Educación
Mexico 2003
4° Edición

Alberto León-García Indra Widjaja
Redes de comunicación

Francisco J. Molina
Redes de área local
AlfaOmega Ra-Ma
México 2004

Magaña Lizarrondo E., Izkue Mendi E., Prieto Miguez M., Villadangos Alonso J.
Comunicaciones y Redes de Computadores
Pearson Education S.A.
Madrid 2003

Capítulo 3

http://www.arqhys.com/arquitectura/cableado-elementos.html
http://medusa.unimet.edu.ve/electrica/fpie43/index12.htm

Bill Ball, Hoyt Duff
Ret Hat Linux Fedora 3
ANAYA
2005

Richard Petersen, Ibrahim Haddad
Red Hat Linux Manual del Administrador
McGraw Hill
España 2004

José Andrés Martinez S.
Linux La Referencia Visual
McGraw Hill
Colombia Julio 2001