UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ESTABLECIMIENTO DE UNA GUÍA PARA LA ADMINISTRACIÓN DE LA RED DE LA FACULTAD DE INGENIERÍA

T E S I S

QUE PRESENTAN PARA
OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

IGNACIO MORALES GARCÍA
ITZEL SÁNCHEZ DEHESA
ABIGAIL SERRALDE RUIZ

DIRECTOR DE TESIS: ING. ELSA ELENA BARÓN MAYO

MEXICO, D.F. 1998

A mis padres por su apoyo y cariño.

A mis hermanos.

A mis sobrinos Grabiel, Jazmín, Miguel, Emmanuel y Sergio.

A mis compañeras de tesis, Abigail e Itzel, por las adversidades que tuvimos juntos, y a pesar de ello logramos salir avante.

A Elsa y Noe, por su apoyo y el tiempo que nos dedicaron para la realización de esta tesis, gracias.

A Eduardo.

A Edgar, por su constante presión.

A Claudia por los días que no pude verla.

Ignacio

Agradecimientos

Agradezco muy especialmente a mis padres que siempre me han apoyado, ayudado y a quienes debo mi amor y respeto. Sin ustedes no hubiera logrado llegar a esta meta.

A mis hermanos Lourdes y Adolfo por la motivación que inspiraron en mí, para nunca darme por vencida y siempre seguir adelante hasta alcanzar todo lo que deseo.

A Daniel por su amor, comprensión y motivación para terminar esta tesis.

A todos mis familiares y amigos quienes han estado cerca de mí.

A mis compañeros de tesis y de la facultad, y a mis profesores, que de alguna manera contribuyeron para que mi aprendizaje y formación profesional culminaran exitosamente.

Itzel

Agradezco y dedico este trabajo a Dios por permitirme alcanzar una meta más en mi vida y por rodearme de personas que me aman.

En primera instancia agradezco y dedico esta tesis a mis padres y hermanas por su apoyo incondicional en el transcurso de mis estudios.

También, por este medio deseo agradecer por todos los momentos de apoyo y comprensión al M. C. Jesús Javier Serralde González.

Agradezco a todas las personas que me asesoraron y apoyaron para culminar este trabajo:

Ing. Elsa Elena Barón Mayo
Lic. Miguel Figueroa Bustos
Ing. Noé Cruz Marín
Ing. Rodolfo Soís Ubaldo

Finalmente quiero dedicar esta tesis a Jorge por ser un buen amigo y gran compañero que siempre me ha acompañado en los momentos más importantes de mi vida.

Abigail

Indice Pág.

CAPÍTULO 2

2. INTRODUCCIÓN A LAS REDES DE DATOS

CAPÍTULO 3

3. ANÁLISIS DE LA RED DE LA FACULTAD DE INGENIERÍA

CAPÍTULO 4

4. GUÍA PARA MEJORAR LA ADMINISTRACIÓN DE LA RED DE LA FACULTAD DE INGENIERÍA

PRÓLOGO

El avance tecnológico en el área de cómputo ha ido creciendo notoriamente y debido a la eficacia de su uso se ha convertido en una necesidad prioritaria tanto para las empresas como para las Instituciones educativas.

El propósito de este trabajo es proporcionar una guía a los administradores de la red de la FI, para mejorar el rendimiento de la misma.

En los dos primeros capítulos se presentan conceptos relacionados con las redes de datos, los cuales sirvieron como base para la propuesta final.

El tercer capítulo consta del análisis de la manera en que está conformada la red (topología y distribución) de la FI; así como el equipo y software que se utiliza, tanto por los administradores de red de cada División como del personal administrativo, académico, alumnos y usuarios en general. Si el lector (ya sea administrador o usuario en general) desea conocer las condiciones en las que se encuentra la red, lo encontrará en este capítulo, esto se enfoca principalmente a aquellos administradores de red que sean nuevos y desconozcan el funcionamiento general con el que cuenta la red.

El último capítulo es una propuesta que servirá de guía a los administradores de la red para aumentar la seguridad, aprovechar al máximo los recursos que se tienen, así como el uso factible de la nueva tecnología con base en lo que cuenta la red de la FI.

Aunque este trabajo está dirigido a administradores de redes, no es necesario que el lector sea un experto para comprender lo que aquí se menciona, por el contrario es conveniente que todo usuario tenga conocimiento de los recursos en los que trabaje, ya que incluso en la guía que se propone al final de este trabajo, se involucra al usuario dándole a conocer sus derechos y responsabilidades en el uso de la red.

INTRODUCCIÓN

Como sabemos, en el mundo de las telecomunicaciones las redes de datos han cobrado especial relevancia últimamente, debido al uso extendido de computadoras para la transmisión de datos.

El siguiente trabajo surge de la necesidad imperante en la Facultad y especialmente de la Unidad de Servicios de Cómputo Académico, para realizar una administración eficiente y funcional de sus redes, con el fin de que todos los procesos de transmisión y recepción de datos en nuestra red se realicen con eficiencia y con un mínimo de error y por lo tanto hacer un mejor uso de todos los recursos de nuestra red.

Asimismo, se proponer realizar un análisis del estado que guarda actualmente la red de la Facultad, su desempeño y eficiencia actual, para obtener como producto final una guía para la administración de los recursos de la red de la Facultad de Ingeniería, que sirva como marco de referencia para aplicarlo al trabajo diario de los laboratorios y centros de trabajo apoyados en la red de la Facultad. No obstante se darán los conceptos fundamentales de redes de computadoras, para que de forma segura se tenga el conocimiento en los aspectos que en algún momento parecieran triviales.

El plan de trabajo propone dar pautas para planear, diseñar, organizar, operar y mantener los sistemas electrónicos de procesamiento de datos de nuestra Institución, además de resolver los problemas que se presenten, y plantear sugerencias para mantener una operación óptima de la red a futuro.

Nosotros, por medio de la investigación, tenemos la tarea de evaluar el desempeño actual de la red, plantear la solución a los problemas que se presenten que proporcione un desempeño óptimo, de acuerdo con el criterio de la red.

Es indudable que en el presente trabajo se pretenden establecer pautas que se seguirán (en caso de ser factible), en la Facultad, en lo referente a lineamientos o estrategias operativas para la administración de la red, que satisfacerá las necesidades de la Red de la Facultad de Ingeniería, además se aplicará al control en la seguridad, direcciones electrónicas, uso eficiente de la red, e interconectividad óptima entre sistemas operativos diversos, es decir, eficientar la red. Para ello se propondrá una estructura de administración, y para demostrar su validez se aplicarán inicialmente en los Laboratorios de la Unidad de Servicios de Cómputo de la Secretaría General, estableciendo un carácter práctico-utilitario en la presente propuesta.

Se tiene la seguridad que esta investigación dará frutos positivos conforme se avance en su desarrollo.

CAPÍTULO 1

1. Conceptos Generales de Redes

1.1. Definición de red y sus tipos

Una red es un conjunto de computadoras enlazadas entre sí y/o con otros equipos, cuya configuración permite que esto sea un medio para transmitir, recibir, compartir y manejar información; y dependiendo que tan grande sea el número de dispositivos conectados a esa red, existen tres tipos de redes:

Redes de área local LAN[1]
Redes de área metropolitana MAN[2]
Redes de área amplia WAN[3]

Redes de área local (LAN)

Una red de área local LAN es un sistema de comunicaciones de datos que permite un número de dispositivos de datos independientes para comunicarse con otros. Una LAN se distingue de otros tipos de redes de datos en que las comunicaciones son normalmente permitidas en una área geográfica de tamaño moderado, como lo es un edificio.

La red LAN es distinguida también por su uso de comunicaciones en modo de paquetes y por una interfaz de nivel de enlace de datos. El canal de comunicaciones de una LAN tiene un rango de datos moderado a alto y un rango consistente de errores bajo. Una red LAN integrada con voz y datos (VD LAN) permite un número de dispositivos de voz y datos integrados independientes para comunicarse con otra igual y con dispositivos de voz y datos integrados en una red WAN o MAN.

El objetivo de las LAN consiste en conectar entre sí las máquinas existentes, por ejemplo, las computadoras departamentales de una universidad, para permitirles comunicarse entre sí. En otros casos, la meta la fija la necesidad de crecimiento, o bien, el obtener una mejor relación costo-rendimiento de una red.

El medio de transmisión común para redes LAN es el par trenzado. La red funciona a una velocidad de 4 Mbps en banda base. Se pueden conectar también, a esta red, todo tipo de microordenadores IBM-PC y PS/2.

[1] Local Area Network
[2] Metropolitan Area Network
[3] Wide Area Network

Un sofisticado sistema de conexiones permiten conectar y desconectar cualquier puesto sin perturbar el funcionamiento de la red. Estas tomas funcionan de forma tal que no existe ninguna apertura de circuito eléctrico en las operaciones de conexión y desconexión.

Redes de área metropolitana (MAN).

Entre las redes LAN y WAN se encuentran las MAN. La red de área metropolitana MAN es un sistema de comunicaciones el cual permite un número independiente de dispositivos de datos para comunicarse con otros; esta red opera internamente con redes de conmutación pública. Se distingue de otras en cuanto a que la comunicación es limitada a una área geográfica, como una ciudad. Utiliza la tecnología desarrollada por la red LAN y por lo tanto gran parte del estudio de los protocolos de estas redes también es válida para el caso de las redes MAN.

Redes de área amplia (WAN)

Las WAN a diferencia de las LAN cubren regiones más grandes con distancias entre nodos de miles de kilómetros además de pertenecer a múltiples organizaciones; pueden fácilmente interconectarse en diferentes partes de un país o del mundo. La operación interna con redes de conmutación múltiple es una capacidad opcional; incluyen redes telefónicas de conmutación pública y redes de datos con conmutación de paquetes.

Las WAN son generalmente redes de medios de comunicación mixtos que emplean una combinación de líneas terrestres y satelitales.

Para alcanzar todo su potencial, las LAN y las WAN deben ser capaces de comunicarse con otras LAN y WAN.

Existen topologías típicas de redes de varias clases, interconectadas, cuyos componentes son varias LAN y WAN. Todas las clases de computadoras y otros dispositivos de procesamiento de información están unidos directamente a ellas.

Con el paso del tiempo las características y necesidades que se analizan en el momento de la implementación de una red pueden variar notablemente. Para que la red no se vuelva obsoleta y pueda crecer tanto como nuestras necesidades, se pueden hacer algunas interconexiones entre los diferentes tipos de redes por ejemplo:

1. LAN-LAN.
2. LAN-WAN.
3. WAN-WAN.
4. LAN-WAN-LAN.

	LAN	MAN	WAN
Diámetro	< 5 Km.	10-150 KM.	< 100,000 Km.
Velocidad	4-155 Mbps	50-622 Mbps	< 2 Mbps
Información	Datos, gráficos, voz, audio, video	Datos, gráficos, voz, audio, video	Datos, gráficos, voz, audio, video
Pertenencia	El usuario (a una sola organización)	Servicio público	Servicio público
Ejemplos	Ethernet, Token Ring, FDDI, Fast Ethernet, ATM	ATM	ISDN, X.25, Frame Relay

Tabla 1 Características de los 3 tipos de redes LAN, MAN y WAN.

1.2 Medios de comunicación

Transmisión por microondas

La transmisión de datos por rayos infrarrojos, láser, microondas o radio, ocupan como medio de transmisión el aire. El uso de sistemas de comunicaciones basados en la radiotransmisión tiene varias ventajas, la principal es que no requiere un medio físico para enlazar el equipo, como el cable. El costo de instalación de un enlace es el de la instalación del transmisor, el receptor y la antena. Otra ventaja es que los nodos de la red pueden ser móviles. El uso de la atmósfera como medio tiene algunos inconvenientes, ya que dependen en gran medida de las condiciones climatológicas del momento. La consecuencia de esto es que el equipo de transmisión puede ser complejo y, por lo tanto, costosos.

La conectividad remota permite la comunicación entre dos o más redes, permitiendo que sus nodos puedan comunicarse entre sí. Surge entonces la necesidad de comunicar las diferentes redes que existen, las cuales nacieron y crecieron en forma independiente.

Comunicación por satélites

Un satélite esta formado por uno o más dispositivos llamados transpondedores (receptores-transmisores), cada uno de los cuales recibe y retransmite a una frecuencia. Este medio de comunicación ocupa ondas electromagnéticas como medio de transferencia. Los satélites tienen la capacidad de transmitir, cubriendo una parte significativa de la superficie de la tierra, o bien, pueden ser estrechos y cubrir una área de cientos de kilómetros de diámetro.

Fibras ópticas

Un sistema de transmisión óptica tiene tres componentes: el medio de transmisión, la fuente de luz y el detector. El medio de transmisión es una fibra delgada de vidrio o silicio fundido. La fuente de luz puede ser un LED [4] (Diodo emisor de luz), o un diodo láser, cualquiera de los dos emite pulsos de luz cuando se le aplica una corriente eléctrica. El detector es un fotodiodo que genera un pulso eléctrico en el momento en que recibe un rayo de luz. Al colocar un LED o un diodo láser en el extremo de una fibra óptica, y un fotodiodo en el otro, se tiene una transmisión de datos unidireccional que acepta una señal eléctrica.

Cuando el rayo de luz pasa de un medio a otro, en este caso del silicio al aire, el rayo se refracta [5] en la frontera del silicio/aire, como se muestra en la **Figura** 1a. En la cual se observa la incidencia del rayo de luz sobre dicha frontera, a un ángulo β, emergiendo a un ángulo α En donde la cantidad de refracción dependerá de las propiedades de los dos medios [6] . El ángulo que permita al rayo de luz refractarse y regresar al silicio, se llama ángulo crítico. Esto permitirá que el rayo de luz se propague a través de la fibra óptica.

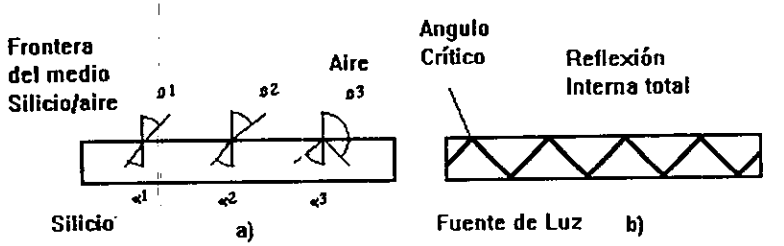


Figura 1. *a) Tres ejemplos de un rayo de luz procedentes del interior de una fibra de silicio y que choca, a diferentes ángulos, contra la frontera del medio aire/silicio. b) Luz atrapada por reflexión interna total.*

En el la figura 1b sólo se muestra un único rayo, pero dado que cualquier rayo de luz se refleja internamente, existirá una gran cantidad de rayos refractándose a distintos ángulos. A ésta situación se le conoce como **fibra multimodo**. Sin embargo, si el diámetro de la fibra se reduce al valor de la longitud de onda de la luz, la fibra actúa como guía de ondas, y la luz se propagará en la línea recta, sin rebotar, produciendo así una fibra de un sólo modo o **fibra monomodo**. Las fibras de un sólo modo necesitan diodos láser para su excitación y no un LED.

Generalmente se clasifica a las fibras ópticas por su indice de refracción, dimensiones del núcleo y su apertura numérica. De acuerdo a estos criterios existen tres tipos principales de fibras:

[4] Light emission diode.
[5] Se desvia
[6] En particular, de sus índices de refracción

Multimodo

1. Con índice escalonado: Utiliza varios modos de propagación, para trasmitir información y por lo mismo limita su capacidad de transmitir información.
2. Con índice gradual: Existe menor dispersión y por lo tanto aumenta la capacidad de transmitir información.

Monomodo

3. Con índice escalonado: Solo utiliza un modo de propagación lo que disminuye la dispersión y pérdidas de información. Es ideal para las comunicaciones.

En la actualidad los sistemas de fibras ópticas son capaces de hacer transmisiones de datos de 100 Mbps en 1 kilómetro. En algunas pruebas realizadas se han podido alcanzar velocidades mayores, pero con distancias más cortas. Experimentalmente se ha demostrado que los láser potentes pueden llegar a excitar fibras de 100 Km de longitud sin necesidad de utilizar repetidores, aunque la velocidad sea más lenta.

Para una red en anillo[7], la interfaz que existe en cada uno de las computadoras, permite el paso del flujo de los pulsos de luz al siguiente enlace, y también sirve como una unión T por medio de la cual la computadora envía y acepta mensajes. Existen dos tipos de interfaces:

Interfaz tipo pasivo

Esta interfaz consiste de dos conectores fusionados con una fibra principal; uno de los conectores tiene un LED o diodo láser en uno de sus extremos (para transmisión) y en el otro tiene un fotodiodo. Se le llama tipo pasivo porque la señal no se regenera cada vez que pasa por una de estas interfaces, por lo que la red tendrá un número limitado de computadoras. Este tipo de conexión es muy fiable, porque si uno de los LED's o fotodiodos se salen de servicio, únicamente se inhabilita la transmisión de la computadora.

Interfaz tipo activo.

Esta interfaz consiste de un receptor óptico, en donde la luz incidente se convierte en una señal eléctrica, que posteriormente pasa al regenerador de señal, este dispositivo regenera la señal a su máximo valor si éste ha disminuido y por último al transmisor óptico, en donde la señal eléctrica se convierte en luz, como se muestra en la **Figura 1**. Por lo que la red tendrá un número ilimitado de computadoras.

[7] Se describirá en la sección 1.3.

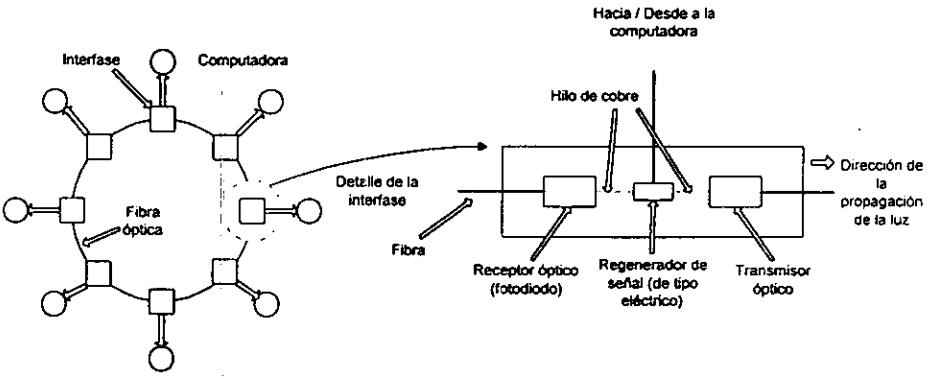


Figura 2. Anillo de fibra óptica

Las fibras ópticas proporcionan un ancho de banda extremadamente grande y tienen una pérdida de potencia muy pequeña, razón por la que se emplean para distancias muy largas entre repetidores. Las fibras, no se ven afectadas por alteraciones de voltaje o corrientes en las líneas de potencia, por interferencia electromagnética o por químicos corrosivos dispersos en el aire, de tal forma que pueden emplearse en ambientes industriales expuestos a condiciones muy severas en las que, los cables serían sumamente inadecuados. Las fibras son también muy delgadas, lo que representan un factor positivo muy importante para las compañías que tienen una gran cantidad de cables y conductos abultados.

Las fibras ópticas acarrean señales en una sola dirección, y una conexión completa utiliza dos tramas de fibras, cada una para las señales que viajan en distintas direcciones.

Ventajas de las fibras ópticas:

- Alto ancho de banda.
- La tecnología tiene una vida potencial larga.
- Es más pequeño y delgado.

Desventajas de las fibras ópticas:

- Expansión inicial alta.
- Más dificultad y consumo de tiempo para instalarlo.

Cableado	Componentes del sistema	Uso típico	Norma
Fibra óptica	Cables de 62.25/125 micras Cable unimodo Conectores tipo SC/ST	10BASE F Token Ring FDDI ATM Video	EIA/TIA - 568 FDDI Canal de Fibra

Tabla 2. Tipos y usos de la fibra óptica.

Par trenzado

El par trenzado consiste en un par de alambres entrelazados en forma helicoidal. La forma helicoidal del cable se utiliza para reducir los efectos de la interferencia eléctrica y electromagnética. La energía radiada por el flujo de corriente en uno de los cables, es cancelado por la energía radiada por el flujo de corriente contraria del otro cable, esto permite reducir el efecto de *crosstalk* [8]. La proximidad de las señales y la referencia a tierra de ambos cables, reducen también el efecto de la diferencia de señal.

Como los pares trenzados están formados por alambres de cobre, sus características se dan por el diámetro del cable. Esta medida en E.U. es llamada como AWG [9] (Calibre Americano).

Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre; en muchos casos se pueden obtener transmisiones de varios megabits por segundo, en distancias de pocos kilómetros. Existen dos tipos de pares trenzados que son los siguientes:

Los pares trenzados blindados (STP) [10].

Estos están protegidos por una cubierta metálica, por lo que son más inmunes al ruido y al efecto de crosstalk.

Los pares trenzados no blindados (UTP) [11].

Estos no tienen una cubierta metálica que los proteja, por esta razón son más susceptibles a los efectos de croostalk y las interferencias de fuentes de poder. Estos son ocupados frecuentemente para las redes telefónicas y en muchos medios de comunicación de datos, con este cable se obtendrán buenos resultados en distancias cortas

[8] Conversaciones cruzadas.
[9] Traducido de American wire gauge.
[10] Shielded Twisted Pair
[11] Unshielded Twisted Pair

Cable coaxial

El cable coaxial consta de un alambre de cobre duro en su parte central [12], el cual se encuentra rodeado por un material aislante. Este material está rodeado por un conductor cilíndrico que se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de **plástico protector**. En la **Figura 3**, se muestran las partes de un cable coaxial.

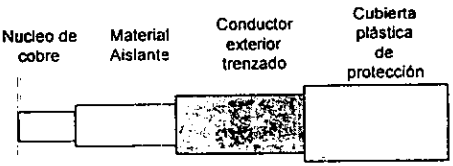


Figura 3. Cable coaxial común

El cable coaxial es empleado frecuentemente en el sistema telefónico y redes de área local. Generalmente el cable coaxial lleva la señal en una dirección, por lo que ocupan un segundo cable, para tener una comunicación bidireccional. Los sistemas de cable coaxial, incluye hasta 8, 12, 20 y 22 cables coaxiales, con dos cables de más, por si existieran problemas en la comunicación.

El cable coaxial proporciona un buen ancho de banda, que se puede obtener dependiendo de la longitud del cable; para cables de 1 km, por ejemplo, es factible obtener velocidades de datos de hasta 10 Mbps, y en cables de longitudes menores, es posible velocidades superiores.

Los sistemas de cable coaxial requieren de amplificadores que refuercen la señal, estos amplificadores solo permiten la comunicación en una sola dirección.

Existen dos formas de conectar dispositivos (por ejemplo computadoras) por medio de un cable coaxial, la primera consiste en cortar el cable en dos partes e insertar una unión en T, que es un conector que se reconecta el cable pero al mismo tiempo provee una tercera conexión hacia el ordenador, este tipo de conector se utiliza generalmente en cable coaxial de banda base. La segunda forma de conexión se obtiene utilizando un conector tipo "vampiro", que es un orificio con un diámetro y profundidad muy precisas, que se perforan en el cable y terminan en el núcleo del mismo. En este orificio se atornilla un conector especial que lleva acabo la misma función de la unión T, pero sin la necesidad de cortar el cable en dos, este conector es generalmente ocupado por el cable coaxial de banda ancha. Existen dos tipos de cables coaxiales, que se muestran a continuación:

Coaxial en Banda	Uso de canales	Resistencia (impedancia)	Transmisión	Velocidad
Base	Un solo canal	50 ohms	Digital (datos)	100 Mbps
Ancha	Varios canales	70 ohms	Analógica (datos, voz y video)	150 Mbps

Tabla 3. Características de los tipos de cable coaxial: banda base y banda ancha

[12] Núcleo de cobre

Los sistemas de cable coaxial requieren de amplificadores que refuercen la señal. Estos amplificadores sólo pueden transmitir las señales a una dirección de tal manera que una computadora que dé salida a un paquete de información no podrá comunicarse con otra computadora que se encuentre en "corrientes arriba" de él, si existe un amplificador entre ellos. Para solucionar este problema, se han desarrollado dos tipos de sistema de banda ancha; el cable dual y el cable sencillo.

Comparación de Medios de Comunicación

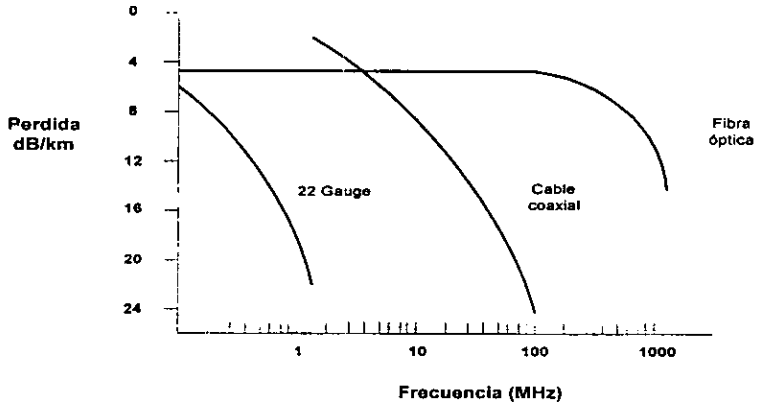


Figura 4. Comparación de Fibra óptica, Cable coaxial y Par trenzado

En la **Figura 4**, se muestra la comparación del par trenzado, cable y la fibra óptica y se observa que la fibra óptica tiene un mejor rango de ancho de banda que el cable coaxial y el par trenzado, y tiene una caída de pérdida de hasta 24 dB/km, para 500 Mhz. La caída del cable coaxial no es tan pronunciada como el de la fibra óptica, la perdida se va acentuado de en un rango 5 a 10 Mhz. El par trenzado tiene una pérdida de 20 dB por kilómetro en un rango de 0 a 1 Mhz.

En la comunicación por satélite y microondas, la pérdida de dB por kilómetro dependerá en cierta medida de las distancias de las antenas y los satélites, de la tasa de error y las condiciones climatológicas de la atmósfera.

1.3. Tipos de transmisión

Transmisión analógica

La transmisión analógica se refiere a sistemas en los cuales las formas de onda que conducen la información se reproducen en el destino, sin el empleo de técnicas digitales. Es importante mencionar las partes fundamentales que requieren el proceso de transmisión, como son el sistema telefónico, módem e interfaces.

RS-232-C

El RS-232-C está localizado entre una computadora y el módem. El RS-232-C es un circuito de 25 pines, el cual considera como -3 Volts un 0 binario y 4 Volts como 1 binario. Se pueden tener velocidades de hasta 20 Kbps.

En la **Figura 5** se muestran 9 de las 25 pines del RS-232-C, principales para el proceso de comunicación, así como una computadora conocida en las normas como DTE [13] (Equipo Terminal de Datos, ETD) y el módem es llamado DCE [14] (Equipo Terminal de Comunicación, ETC). Cuando la computadora se enciende, se está activa la señal "Data Terminal Ready " [15] (pin 20). Cuando el módem se enciende, se activa la señal correspondiente al "Data Set Ready " (pin 6). Cuando el módem detecta una portadora sobre la línea telefónica, se activa la señal de "Carrier Detect" (pin 8). El "Request to Send" (pin 4), indica que la computadora quiere enviar datos. El "Clear to Send" (pin 5), significa que el módem está preparado para aceptar datos. Los datos se transmiten con el "Transmit circuit" (pin 2) y se reciben con el "Receive circuit" (pin 3).

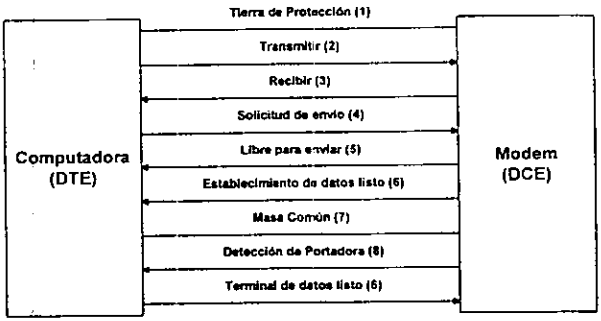


Figura 5. Algunos de los circuitos principales de la interfaz RS-232-C.

Se tienen a disposición otros pines con los cuales se pueden seleccionar la velocidad de los datos, probar el módem, temporizar los datos, detectar señales de llamada y enviar datos en la dirección opuesta, sobre un canal secundario.

El proceso de comunicación está basado en la definición de pares acción-reacción[16], por ejemplo, cuando la computadora desea mandar información, activa la señal "request to send", el módem contesta con un "clear to send", entendiendo que se tiene la capacidad para aceptar la información.

Es común que dos computadoras quieran conectarse por medio de una interfaz RS-232-C, como ninguno de los dos es un módem, surge el problema de interfaz, este problema se

[13] Data terminal equipment
[14] Data comunication equipment
[15] Es decir pone un 1 lógico
[16] Característica principal de un protocolo

resuelve al conectarlos con un dispositivo denominado módem nulo, que conecta la línea transmisora de una máquina con la línea receptora de la otra máquina.

Transmisión digital

La transmisión digital tiene varias ventajas sobre la transmisión analógica. La transmisión analógica requiere de amplificadores, atenuadores y otros tipos de regeneradores de señal, para obtener una señal sin distorsión al final. La transmisión digital, por su propia naturaleza, no necesita de complicados regeneradores de señal, ya que únicamente detectaran niveles de voltaje (unos y ceros). La transmisión digital puede multiplexarse conjuntamente, para hacer un uso más eficiente del equipo.

Conmutación

Para llevar a cabo las comunicaciones de datos se deben tomar en cuenta las diferentes características de los dispositivos existentes, así como los canales de comunicación ya que estos se clasifican por su velocidad o capacidad. Una línea puede ser conmutada o no conmutada (también llamada dedicada), analógica o digital. Los canales de comunicación pueden arreglarse para operar bajo una comunicación simplex, half duplex o full duplex.

Conmutar es la manera de comunicar, transportar e intercambiar información entre dos puntos. Para ello existen diversas formas:

Conmutación de circuitos

Este tipo de conmutación es utilizado por la red telefónica y se caracteriza porque establece una línea física entre dos usuarios antes de cualquier intercambio de información.

Al hacerse el pedido de conexión, es enviado un mensaje especial del nodo origen al nodo destino. Este mensaje produce en el camino recorrido, la asignación de las líneas de los nodos intermediarios hasta el nodo destino, estableciendo una conexión para la comunicación entre dos usuarios. Cuando se completa esta operación, se envía un mensaje de vuelta al nodo origen, informando que la transferencia de informaciones puede empezar. Toda esta operación tarda alrededor de algunos segundos en completarse, pero una vez que la conexión está establecida, el único atraso que sufre la transmisión es el de la propagación. Además, el flujo no estará sujeto a congestionamiento; salvo que todas las líneas estén ocupadas al intentar establecer la conexión, la entrega de las informaciones estará garantizada.

Este tipo de conmutación es adecuado cuando la comunicación se hace entre equipos de naturaleza muy similar, sin realizar ninguna conversión de códigos o velocidades y cuando el flujo de información obedece a una tasa más o menos constante.

Podemos resumir las principales características de la conmutación de circuitos para red telefónica como sigue:

- Una vez establecida una llamada, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red. Este camino equivale a un par de hilos que unan a ambos usuarios.
- Los conmutadores no poseen medios de almacenamiento intermedio para la transmisión, como podrían ser discos duros.
- Debido a la ausencia de medios de almacenamiento señalada, un conmutador puede quedar bloqueado.
- El conmutador de circuito no cuenta con algún tipo de protocolo de línea, sería necesario software o microcódigo adicional.

Conmutación de mensajes

Aquí la información que va a ser enviada se organiza en unidades llamadas mensajes. En este caso, no hay ninguna asignación previa de un circuito antes de la propia transferencia. Un nodo, al recibir un mensaje, procura una línea de salida disponible; si ésta no existe en el momento, el mensaje es almacenado en una memoria secundaria para su posterior transmisión. Este proceso se repite en cada nodo de origen al destino. Si la comunicación involucra más de un mensaje, éstos pueden seguir caminos diferentes en la red, según las condiciones de tráfico. Además, dependiendo de la red, los mensajes pueden ser entregados o no en el orden de transmisión. De cualquier forma, la red es responsable de la entrega de mensajes.

Los mensajes pueden almacenarse temporalmente y encaminarse después hacia los nodos cuando queden libres para aceptarlos. Los conmutadores de mensajes también pueden utilizar cintas para hacer copia de los archivos del disco, con fines de definir tarifas o registros de las transacciones cursadas por el conmutador.

La tecnología de conmutación de mensajes puede operar siguiendo una relación maestro-esclavo. Normalmente, el conmutador efectúa los sondeos y selecciones necesarios para gestionar el tráfico que sale y entra de él.

Se puede observar que este tipo de conmutación permite que haya conversión de códigos o de velocidades entre los equipos de origen y de destino.

Para garantizar la entrega de mensajes de nodos, cada nodo confirma la recepción del mensaje al nodo que lo envió. El nodo transmisor, a su vez, guarda una copia del mensaje hasta la recepción de la confirmación. Si pasa un cierto período de tiempo sin que haya recibido la confirmación, este nodo asume que el mensaje (o su confirmación) se perdió y retransmite nuevamente el mensaje. Este período de tiempo es llamado período de temporización.

Aunque la conmutación de mensajes ha presentado grandes servicios a la industria, adolece de tres defectos. En primer lugar, al tratarse de una tecnología maestro-esclavo, si el conmutador falla, toda la red dejará de funcionar, ya que todo el tráfico debe entrar y salir por él. Para prevenir esta contingencia, muchas empresas duplican el conmutador. Si

falla el primero entra en servicio el segundo. El otro defecto es que la mayoría de los conmutadores de mensajes son el epicentro del sistema. Todo el tráfico debe pasar por ellos, por lo que pueden ser fuente de embotellamientos. Una estructura así puede empeorar el tiempo de respuesta y disminuir el caudal de tráfico cursado. En tercer lugar, la conmutación de mensajes no aprovecha la línea tanto como otras técnicas.

Conmutación de Paquetes

Es una extensión lógica de la conmutación de mensajes. Aquí, el mensaje es dividido en unidades a su mayor capacidad. Los paquetes son enviados independientemente unos de otros, en forma *store-and-forward*[17], y su recepción es confirmada separadamente. Así, cuando un nodo recibe un paquete, inmediatamente procura una línea de salida para retransmitirlo; si no hay alguna línea disponible, el paquete podrá ser almacenado en el nodo por un corto período de tiempo. Los paquetes de un mismo mensaje pueden estar simultáneamente en tránsito en la red siguiendo rutas diferentes.

Este tipo de conmutación permite, a costa de una saturación *(overhead)* mayor en el procesamiento de los paquetes, una mayor utilización de los canales de comunicación.

La red puede (o no) organizarse para que los mensajes transmitidos se entreguen en orden; también es posible la conversión de códigos o de velocidades.

Supeditada a las restricciones sobre la necesidad de establecer o no una conexión entre los usuarios de origen y destino, sobre el orden o no de los paquetes que fluyen entre ambos, y sobre la confirmación del recibimiento de paquetes, la conmutación de paquetes puede hacerse en el modo datagrama o en el modo circuito virtual.

Así tenemos que los objetivos de las redes de conmutación de paquetes son:

- Multiplexar los canales y los puertos.
- Equilibrar mediante muchos usuarios la asimetría del tráfico.
- Proporcionar a todos los usuarios del sistema unos tiempos de acceso rápidos.
- Conseguir una alta disponibilidad de la red para todos los usuarios.
- Distribuir los riesgos y compartir los recursos.

Para saber si nos conviene utilizar conmutación de paquetes debemos considerar las cuatro alternativas de conexión de equipos transmisores de datos:

- A través del sistema telefónico normal, con marcado de números.
- A través de canales telefónicos privados no conmutados.
- A través de redes de paquetes públicas, o de redes privadas de circuitos conmutados.
- A través de redes de paquetes privadas.

Realizando una comparación general de estas tres formas de conmutación , se muestran las siguientes figuras, donde se observan los atrasos sufridos por las informaciones en su flujo por la red del origen al destino.

[17] Almacena-y-sigue

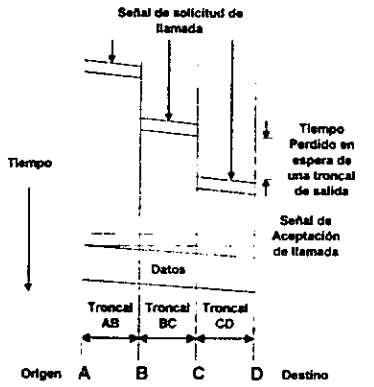


Figura 6. Temporización de eventos en conmutación de circuitos.

En la Figura 6, observamos que el mayor atraso se introduce en el establecimiento de la conexión, que se propaga de nodo a nodo. Al llegar al destino, es procesado el periodo de conexión y enviada de vuelta la señal de OK. A partir de este punto, los datos fluyen sufriendo únicamente el atraso de propagación.

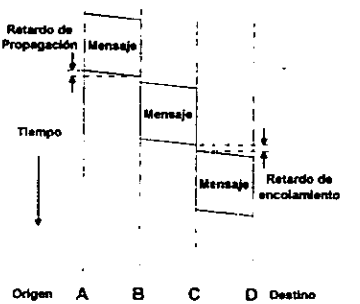


Figura 7. Temporización de eventos en conmutación de mensajes.

En la Figura 7, vemos que hay un atraso muy pequeño para el establecimiento de la conexión. A partir de este punto, cada nodo intermediario recibe el mensaje completamente y lo libera cuando se libera una línea.

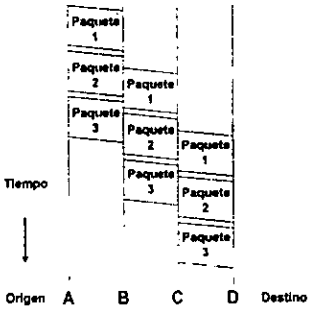


Figura 8. Temporización de eventos en conmutación de paquetes.

En la Figura 8, vemos que un el mensaje fue dividido en paquetes, la retransmisión del paquete 1 por el nodo 1 se da antes de que el paquete 2 haya sido totalmente recibido.

Encaminamiento de paquetes

En los párrafos anteriores observamos que cada nodo de conmutación es responsable del encaminamiento de los paquetes en tránsito por el mismo. Uno de los aspectos más importantes en el diseño de una red es cómo se genera y actualiza la información utilizada para el encaminamiento.

El encaminamiento de paquetes obliga a disponer de una cierta lógica (programas, dispositivos o microcódigo) en los centros de conmutación, para llevar a su destino los paquetes de datos a través de la red. El encaminamiento ha de perseguir tres objetivos fundamentales:

1. Conseguir el menor tiempo de retardo posible y el máximo caudal efectivo.
2. Encaminar los paquetes por la red de la forma más económica.
3. Ofrecer a cada paquete la máxima seguridad y fiabilidad.

Podemos distinguir entre encaminamiento centralizado y distribuido. En el primer caso, existe un centro de control de la red NCC [18] que determina la ruta que seguirán los paquetes. Los conmutadores de paquetes están dotados de menos inteligencia que el nodo central, lo cual se traduce en un menor costo de los centros periféricos de conmutación. Sin embargo, este sistema es vulnerable a un posible fallo del nodo central. Por eso los centros de conmutación suelen estar duplicados. El encaminamiento distribuido exige un mayor grado de inteligencia en los nodos de la red. En contrapartida, la red es menos propensa a fallos, ya que cada nodo toma su propia decisión de encaminamiento sin depender de un nodo central.

[18] Net Control Center

El efecto de multiplicación del tráfico TME [19] se presenta cuando un determinado paquete genera otros paquetes adicionales idénticos. El "puenteado" de un nodo se refiere a cuando se conecta a un canal o nodo ocupado o averiado. La mayoría de las redes de paquetes llevan a cabo el encaminamiento mediante rutinas o tablas al efecto.

Las principales técnicas de encaminamiento de paquetes son las que se mencionan a continuación:

- **Inundación de Paquetes**
  En este método se utilizan todos los caminos posibles entre el nodo emisor y el receptor; se colocan copias del paquete en todos los canales de la red.

  Una ventaja de este procedimiento es que, al utilizarse todos los caminos posibles, el retardo del paquete que llegue primero será el mínimo posible (uno de los objetivos de la conmutación de paquetes). Sin embargo, el efecto de multiplicación del tráfico es muy grande, y el grado de saturación de la red es proporcional a la conectividad de la misma, es decir, que cuantos más canales y rutas existan, más tráfico aparecerá. En contrapartida, la técnica de inundación de paquetes confiere una gran solidez al sistema, ya que siempre habrá una copia del paquete que alcance el nodo final, con tal de que exista algún camino entre ambos extremos. Algunas redes militares utilizan este sistema debido a su gran robustez.

  El efecto de multiplicación de tráfico puede reducirse añadiendo una cierta lógica de mantenimiento a cada conmutador. Este puede ser el esquema a seguir: si un nodo receptor detecta un paquete duplicado, lo descarta y no envía ninguna copia más del mismo. En otras palabras, sólo una copia del paquete sigue su curso. Este proceso se conoce como eliminación o borrado de paquetes, y disminuye de forma considerable el TME. A medida que un paquete va acercándose a su destino, las copias accesorias van desapareciendo.

- **Encaminamiento aleatorio**
  Esta técnica exige un programa en cada conmutador para seleccionar de manera aleatoria un canal de salida. Si el esquema seguido es puramente aleatorio, el canal de salida puede ser el mismo por el que entró el paquete. Los conmutadores necesitan menos lógica para realizar el trabajo de conmutación aleatoria, y además el tráfico, en promedio, se distribuye entre todos los nodos.

  Sin embargo, el encaminamiento aleatorio presenta ciertos inconvenientes:

  1. La ruta total a través de la red es, en promedio, bastante mas larga que con otras técnicas.
  2. El retardo aumenta de manera considerable.
  3. Como el paquete vaga errante por la red, existe una probabilidad no nula de que nunca llegue a su destino.
  4. Debido a este carácter errático, el encaminamiento aleatorio sufre el efecto de multiplicación del tráfico.

[19] Traffic Multiplied Effect

Por todas estas razones esta técnica no se usa demasiado.

- **Encaminamiento por directorio**

  La técnica de encaminamiento más extendida es la que utiliza una tabla o un directorio. Un directorio contiene las direcciones a partir de las cuales los conmutadores transmitirán el paquete por uno o varios canales posibles de salida del conmutador.

  Los directorios de las redes de paquetes se organizan de tres formas:

  1. **Directorios fijos (estáticos)**. Sólo se modifican durante la generación del sistema. Permanecen inalterados durante todas las sesiones de usuario, por ejemplo La red SNA.
  2. **Directorios orientados a sesión**. Se modifican para cada sesión de usuario. Durante el transcurso de una sesión permanecen inalterados, por ejemplo la red pública Tymnet.
  3. **Directorios adaptativos o dinámicos**. Sufren modificaciones durante el transcurso de las sesiones de usuario, por ejemplo la red ARPANET, del Departamento de Defensa Norteamericano.

  Otra clasificación de los sistemas de directorio tiene en cuenta si el directorio es:

  De ruta parcial: sólo se incluyen los nodos adyacentes a un conmutador particular, es decir, los que están conectados directamente al conmutador concreto.

  De ruta completa: contienen toda la serie de nodos intermedios que deberá atravesar el paquete para llegar a su destino.

  Por lo antes expuesto se puede decir que el algoritmo de encaminamiento es responsable de mantener cada nodo informado de la topología de la red, además de permitir que optimice la carga de tráfico que sale del mismo. Un algoritmo de encaminamiento debe satisfacer los siguientes requisitos:

  1. Simplicidad
  2. Fiabilidad
  3. Estabilidad
  4. Adaptabilidad
  5. Optimación global y
  6. Equitatividad

1.4. Topología de redes

Una topología es la forma en que las diversas estaciones de trabajo están interconectadas. En la **Figura 9** se muestran tres tipos de topologías más comunes.

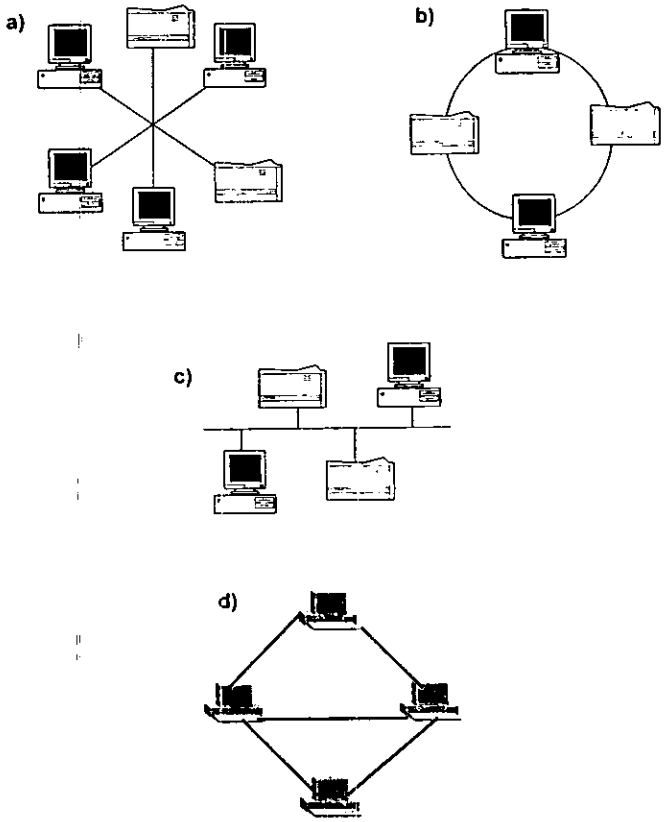


Figura 9. Topologías a) Estrella, b) Anillo, c) Bus, d) Malla

Estrella

Todos los nodos o estaciones están conectados a un nodo central, a través del cual pasan todos los datos. Esta configuración puede ser considerada como un caso particular de una red de área amplia, en la cual, la subred de comunicación está formada por un solo nodo de conmutación. Normalmente, cada nodo puede comunicarse solamente una vez con otro nodo, si bien varios pares distintos pueden estar comunicándose en forma simultánea.

En las redes en estrella, es común que el nodo central posea mayor capacidad de proceso, además de concentrar los periféricos que son compartidos entre los demás nodos. En otros casos, sin embargo, el nodo central tiene únicamente la función de conmutación y diagnóstico. En el caso de redes que utilizan fibras ópticas como medio de transmisión, el nodo central tiene sólo una función pasiva de difusión.

En contraste con la simplificación de las interfaces de los nodos con la red antes mencionada, la red en estrella presenta su mayor deficiencia en la fiabilidad de la red. Cualquier falla en el nodo central causa paro total en la red.

Se puede aumentar la fiabilidad del nodo central a través de redundancia, pero esto acabaría con el beneficio conseguido en el abaratamiento de las interfaces en los nodos.

La presencia del nodo central determina los límites de expansión de la red. El funcionamiento de la red también queda determinado por la capacidad de proceso en este nodo.

Anillo

Una red organizada en anillo está formada por un conjunto de estaciones conectadas punto a punto, formando un lazo cerrado. Normalmente, cada estación está conectada a la red a través de una interfaz especial, que es responsable de transmitir los datos que no están destinados a aquel nodo, leer los datos destinados al mismo e insertar los datos enviados por él.

La comunicación puede circular en el anillo en ambas direcciones (conexiones *full-duplex*[20]) sin embargo, en la mayoría de los casos, las redes de anillo son unidireccionales (*half-duplex*[21]) ya que esto simplifica la interfaz. De este modo, para transmitir el mensaje, el nodo simplemente lo libera en el anillo.

En la red de anillo, los mensajes de difusión se tratan con facilidad, bastando para ello que cada interfaz lea el mensaje cuando pasa por ella. Así, se pueden obtener confirmaciones por medio de un bit extra que se incluye en el mensaje cuando es enviado; el receptor que lo recibe, envía el bit de confirmación, que es verificado a su vez por el transmisor en el momento en que el mensaje vuelve a él por el anillo.

Debido al hecho de que las redes en anillo requieren para su funcionamiento una interfaz activa repetidora, la fiabilidad de la red acaba reduciéndose a la de las interfaces; el fallo de cualquier interfaz acaba seccionando la red e impidiendo su funcionamiento.

Además de este problema, la red en anillo puede presentar a otros relacionados con fallos o errores en el proceso de los mensajes. Por ejemplo, un mensaje puede quedar circulando indefinidamente en la red; también puede suceder que un error en el control de acceso al anillo imposibilite saber quien debe o puede transmitir.

Precisamente, por el hecho de que las interfaces repetidoras son activas, la red en anillo puede, en principio, crecer ilimitadamente. Sin embargo, la inserción de una nueva interfaz crea siempre un atraso adicional en la red, y por lo tanto, su cometido total puede verse perjudicado en caso de estar presentes muchas interfaces.

Podemos notar que entonces existen diversas topologías de anillos, una de ellas sería el anillo rígido, en el cual cada nodo toma, regenera y envía la señal, si no encuentra

[20] También llamado sistema de cable dual

[21] También llamado sistema de cable sencillo

destino, es decir, si un nodo principal se consume la señal o dicho en otras palabras, se la come, da como consecuencia que toda la red falla, un ejemplo de esta técnica es la de *Token Ring* [22].

En el caso del anillo flexible, la situación es más favorable, ya que puede fallar un nodo, pero los demás no se ven afectados por éste, es decir, su servidor es único para todos y no dependen los nodos entre sí.

Es posible conectar hasta 260 puertos sobre el mismo anillo y además se pueden enlazar varios anillos entre sí, lo que permite llegar a un número considerable de puertos.

Bus

En este tipo de organización, los nodos comparten el medio de transmisión a través de interfaces pasivas. Dicha organización es similar a la interna de la computadora que utilizan un bus para conectar el CPU, memoria, periféricos, etc.

Debido a que el bus es compartido por todos los nodos, el acceso al mismo puede ser controlado en dos formas:

Centralizada: El mensaje es enviado a un nodo determinado, que a su vez lo retransmiten hacia el nodo destino. Generalmente, el nodo de control es un nodo especializado y no una estación de propósito general; esta configuración es similar a aquéllas en las que una unidad de control de una computadora controla varias terminales en una línea multipunto, a través de llamadas de interrupción.

Descentralizada o distribuida: Cada nodo es responsable de realizar parte del control, ya sea por acceso a través de multiplexión en frecuencia en el tiempo, o bien a través de acceso con contención.

En términos de fiabilidad, la organización en bus ofrece la mejor potencia, dado que la interfaz, al ser pasiva, no afecta al funcionamiento global de la red en caso de fallo. Un posible error en el modo de transmisión puede ser prevenido a través de relojes especiales, impidiendo que una estación se apodere del medio de transmisión permanentemente. Desde el punto de vista del control de acceso, el control centralizado presenta los mismos problemas que la red en estrella, excepto por el hecho de que, generalmente, cualquier nodo puede asumir el papel de controlador en caso de fallo.

Los únicos límites para la inserción de un nuevo nodo en la red en bus son las características físicas del medio de transmisión; a partir de cierta cantidad de interfaces, se hacen necesarios repetidores[23] para mantener el nivel adecuado de señal. Además el control de acceso puede introducir limitaciones lógicas. Y debido a la naturaleza pasiva de las interfaces, la introducción de nuevas interfaces no crea nuevos atrasos en la red.

[22] De esta técnica se hablará en la sección 1.6.

[23] Se define en la sección 2.1

Grafos o Malla:

Las topologías analizadas hasta ahora pueden considerarse como un caso particular de una topología de malla. Sin embargo, este término suele reservarse para redes que permiten interconexiones más aleatorias que las descritas en las anteriores. Las redes de malla permiten redundancia, ya que puede haber más de un camino para los paquetes entre dos nodos de la red. Por esta única razón, las redes de área extendida normalmente se basan en una malla. Para poder aplicar mallas en las redes locales, los nodos de conmutación no deben operar según el principio de almacenamiento y reenvío, ya que aumentaría el retardo de la red.

Cuadro comparativo de diversas topologías

	Estrella	Anillo	Bus Común	Grafos (Redes Geográficamente distribuidas)
Simplicidad funcional	La mejor de todas	Razonable	Razonable-Un poco mejor que el anillo.	Extremadamente compleja
Encaminamiento	Inexistente	Inexistente en el anillo unidireccional. Simple sin otros tipos.	Inexistente	Bastante complejo
Costo de conexión	Alto	Bajo hacia medio	Bajo	Muy alto
Crecimiento incremental	Limitado a la capacidad del nodo central.	Teóricamente infinito	Alto	Alto
Aplicaciones adecuadas	Aquellas que involucran proceso central de todos los mensajes	Sin limitación	Sin limitación	Sin limitación
Rendimiento	Bajo. Todos los mensajes deben pasar por el nodo central.	Alto. Posibilidad de que más de un mensaje de transmita al mismo tiempo.	Medio	Alto. Se puede adaptar al volumen de tráfico existente.
Fiabilidad	Poca	Buena, si se toman cuidados adicionales	La mejor de todas. Interfaz pasiva con el medio.	Buena debido a la existencia de caminos alternativos.
Retraso de Transmisión	Medio	Bajo, pudiendo llegar a no más de 1 bit por nodo.	El más bajo de todos.	Alto
Limitación en cuanto al medio de Transmisión	Ninguna. Conexión punto a punto	Ninguna. Conexión punto a punto	En la conexión multipunto, su conexión al medio de transmisión puede ser costosa, como en el caso de la fibra de vidrio.	Ninguna. Conexión punto a punto.

Tabla 4. *Comparación de Topologías Estrella, Anillo, Bus y Grafos*

1.5. Estándares de redes de datos

Familia IEEE 802

El proyecto IEEE 802 es un documento en el que se definen estándares y se especifican los requerimientos y guías para redes de área local LAN y metropolitana MAN. La IEEE[24] (Instituto de Ingenieros Eléctricos y Electrónicos) creó un comité para el desarrollo de normas o estándares de redes de área local, debido a las diferentes necesidades de las compañías involucradas en el desarrollo de las comunicaciones en redes de cómputo.

Características de las redes LAN, MAN y WAN según el proyecto IEEE 802.

El fin de las LAN y MAN es para que exista una compatibilidad e interoperatibilidad entre el equipo elaborado por diferentes manufactureras y que una comunicación se pueda llevar a cabo entre el equipo. Para que esto se realice los estándares brindan especificaciones que establecen interfaces y protocolos de las redes mencionadas.

La comunicación de datos de modo paquete en las LAN y MAN está descrita y diseñada conforme a los servicios de niveles y protocolos definidos en el estándar OSI[25] (Interconexión de sistemas abiertos) del modelo de referencia básico.

Los estándares del proyecto IEEE 802 abarcan los niveles físico y enlace de datos del modelo OSI. (Ver Figura 10)

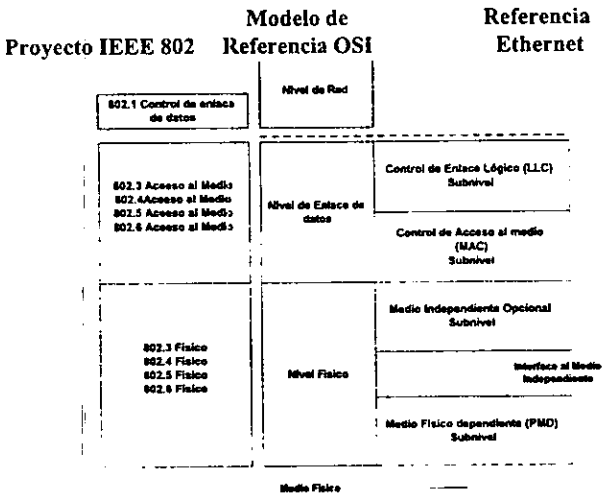


Figura 10. Los estándares del proyecto IEEE 802 en relación con el modelo OSI

[24] Institue of Electrical and Electronics Engineers
[25] Open System Interconnection

El nivel de enlace de datos se divide en dos subniveles:

LLC[26] o Control de enlace lógico, maneja el enlace de datos en la comunicación y define un punto de interfaz lógico para que otras computadoras puedan referenciar y usar la información de este subnivel hacia niveles superiores del modelo OSI.

MAC[27] o control de acceso al medio, comunica directamente la tarjeta de red y es responsable de librar de errores los datos entre dos o más computadoras de la red.

Norma	Descripción
802.1	Introducción a los estándares 802 y la relación que existe entre los estándares de la 802.
802.2	Control de enlace de datos (LLC).
802.3	Redes bajo la técnica de CSMA/CD (la utiliza Ethernet)
802.4	Acceso por paso de token (testigo) en bus.
802.5	Acceso por token (testigo) en anillo (lo utiliza Token Ring)
802.6	Expansión de una red LAN a una WAN.
802.7	Tecnología de banda ancha.
802.8	Tecnología de fibra óptica.
802.9	Integración de voz y datos.
802.10	Seguridad de LAN.

Tabla 5. Descripción general de las normas del proyecto IEEE 802.

Los niveles habrán sido definidos de tal manera que los dispositivos y aplicaciones sean independientes. La intención del modelo de red de área local y metropolitana es permitir un protocolo individual y niveles de servicio para ser reemplazados conforme se necesite sin que se requieran cambios en otros protocolos o niveles de servicio utilizados para realizar el servicio deseado de una LAN.

Las LAN y MAN están hechas para soportar diversas aplicaciones; para tal efecto, estas redes, en conjunto con otros niveles de protocolos más altos deben soportar aplicaciones, procesos y servicios tales como: protocolos de acceso, transferencia de archivos, aplicaciones gráficas, procesamiento de palabras, mensajes electrónicos, automatización industrial, acceso remoto basándose en datos, aplicaciones de voz digital; y también soportan la conexión de varios dispositivos de datos tales como: computadoras, servidores, computadoras personales, estaciones de trabajo, minicomputadoras, mainframes, dispositivos de almacenamiento masivo, impresoras y plotters, equipo de monitoreo y control, puentes, ruteadores y otras redes.

[26] Logical Link Control
[27] Medium Access Control

Token Ring

Este estándar surgió en 1985 aproximadamente, su creador fue IBM, se apega al estándar 802.5 de IEEE y utiliza token passing como método de acceso a la red. Emplea una topología lógica de anillo y una topología física de estrella. Cada estación se conecta a un concentrador central, solo una estación de trabajo puede transmitir a la vez, a dicho concentrador se le designa como MAU [28] (Unidad de acceso a multiestaciones) o un MSAU, el cual consiste en interruptores electrónicos que conectan o desconectan a la estación desde la red de anillo. Dos pares de alambres conectan cada estación con el MAU: uno para recibir datos y otro para transmitirlos. Los paquetes se pasan de estación a estación sobre el anillo; cada estación recibe el paquete, lo reamplifica, y después transmite el paquete a la siguiente estación. Cuando se haga referencia a un producto específico de IBM, el término capitalizado es: Token Ring.

Las características generales son:

Topología	Configuración en anillo
Medio físico	Cable de par trenzado (UTP o STP)
Modo de transmisión	Banda base
Método de acceso	Token passing
Número máximo de nodos	260
Velocidad máxima de transmisión	4 Mbps o 16 Mbps.

Tabla 6. Características generales del estándar Token Ring

La red original Token Ring operaba a 4 Mb/s con un máximo de 100 metros del concentrador de conexiones a una computadora y 72 estaciones que usaban cable UTP especial de IBM. Más tarde en 1989, se extendió hasta 16 Mb/s. Cuando se usa par trenzado blindado (STP) se pueden construir LAN mayores de hasta 260 estaciones.

El mecanismo que sigue el anillo de estaciones para llevar a cabo y controlar la comunicación es el que sigue:

El token circula continuamente de una estación a otra, esto sucede mientras no hay ninguna estación que desee emitir datos. En el momento en que una estación desea realizar el envío de datos, espera a que el token la visite y en ese momento lo toma y en su lugar emite una trama de datos.

La trama de datos circulará por el anillo, siendo retransmitida por cada estación hasta llegar a la estación destino. Dicha estación reconocerá su dirección, recogerá la trama completa, la almacenará internamente y la retransmitirá. La trama continuará circulando hasta alcanzar de nuevo el emisor, el cual retirará y emitirá otra vez el token. Si durante el viaje de la trama de datos, ésta pasa por alguna estación que tenga datos que transmitir, la estación puede indicarlo.

Cuando la trama de datos vuelve otra vez al emisor se analizan aquellos datos con mayor prioridad para poder ser transmitidos antes que los de menor prioridad.

[28] Multiple Access Unit

Debido a que en el medio de comunicaciones pueden producirse errores y a que ciertas condiciones de funcionamiento anómalo de estaciones puede derivar en el funcionamiento inadecuado, existe un nodo especial denominado monitor, capaz de supervisar y en todo caso restablecer el funcionamiento correcto.

Hay dos casos básicos de mal funcionamiento:

1. La desaparición del testigo o token
   El nodo monitor es el encargado de restablecer de nuevo el token. Para ello dispone de un temporizador que inicializa cada vez que le atraviesa el token. Si el token desaparece, el temporizador vencerá y como consecuencia el monitor reinsertará de nuevo el token, con lo que el funcionamiento quedará restablecido.

2. La circulación de una trama de datos.
   El nodo monitor también toma medidas, en este caso usa el bit M del campo AC y cada vez que una trama de datos lo atraviesa activa el citado bit a uno. Cuando la trama de datos da una segunda vuelta sin ser retirada, el nodo monitor lo detecta y la sustituye por el token, restableciendo la normalidad en el anillo.

También existe un mecanismo que permite la detección de rupturas del anillo y su localización, basándose en el conocimiento por parte de cada estación de la dirección de su predecesora.

En los procesos de inicialización e incorporación de estaciones, se asegura de la unidad de la dirección de todas las estaciones del anillo, mediante la emisión, por parte de éstas, de una trama identificadora.

La configuración más sencilla de todas es aquella en la que existe un sólo anillo y se pueden conectar en cascada varios MAUs con lo que resulta un anillo de mayor número de estaciones.

La solución se basa en conectar dos o más MAUs, usando una toma de cada uno para conectarse al otro. Debido a que el número de estaciones está limitado en el anillo y a que el rendimiento puede ser pequeño cuando el número de estaciones es grande, existe una segunda opción: usar puentes [29], los cuales se usan para interconectar dos o más redes de anillo. Cada red posee su propio token circulando, por lo que por el puente pasarán los dos.

Ethernet

Es un estándar de red desarrollado por el centro de investigaciones Xerox Palo alto en 1976, y fue publicada en 1981 por Digital, Intel y Xerox; de la cual se deriva el estándar de la IEEE 802.3. Ethernet utiliza una arquitectura de bus y el protocolo CSMA/CD [30] como medio de control de acceso para sensar el momento en que el canal está libre para

[29] Se describirá en la sección 1.10.

[30] Carrier Sense Multiple Access/Collision Detection

transmitir, detectar y manejar colisiones cuando se presenten; se sustenta en los estratos físico (uno) y de enlace de datos (dos) del modelo OSI.

La parte del estándar que entra en el estrato de enlace de datos consta del substrato de control de acceso a medios y del control del enlace lógico, en lugar de acoplar un protocolo de transmisión de datos completo.

Las características generales son:

Topología	Configuración en bus o árbol
Medio físico	Cable coaxial de 50 ohms
Modo de transmisión	Banda base
Método de acceso	CSMA/CD
Número máximo de nodos	1024
Velocidad máxima de transmisión	10 Mbps.
Separación máxima entre nodos	2.5 km.

***Tabla** 7. Características generales del estándar Ethernet*

Esta red constituye la especificación de los dos primeros niveles de una arquitectura telemática jerarquizada. Por lo tanto, lo único que resuelve la red Ethernet es la problemática de mantenimiento del enlace de datos activo entre dos nodos y libre de errores.

En el aspecto hardware, diversas marcas han provisto al mercado de varios dispositivos y tarjetas capaces de actuar como controladores de enlace Ethernet.

En cuanto al software, puede recurrirse a la adquisición de paquetes especialmente desarrollados, o bien optar por las ofertas que se adaptan a los niveles superiores.

La red local Ethernet típica consta básicamente de tres componentes: los nodos, los controladores y los sistemas de transmisión. El sistema de transmisión incluye todos los componentes necesarios para establecer una comunicación entre controladores o, más propiamente, entre nodos. Esto incluye el medio de transmisión, recepción y opcionalmente, repetidores para extender la capacidad del medio.

El medio de transmisión acaba por ambos extremos en unos dispositivos denominados terminadores, cuya función es la de evitar la pérdida de la señal por reflexiones debido a desacoplos.

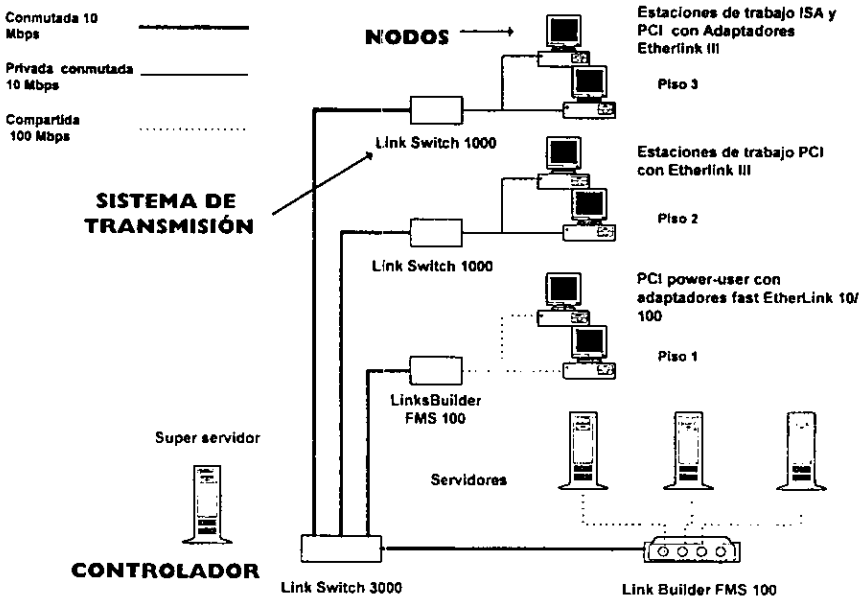


Figura 11. Ejemplo de la conexión de una red Ethernet

FDDI [31]

El FDDI es un estándar desarrollado por el Instituto Nacional Americano para la estandarización (ANSI), el cual especifica una red de fibra óptica que opera en un rango de datos de 100 Mbps. El diseño de la red se deriva de la tecnología Token-ring pero FDDI puede cablearse como un anillo físico o en estrella.

El formato que se utiliza con el FDDI es el mismo que el token-ring de la IEEE 802.5. Sin embargo muchos estándares nuevos fueron establecidos por la FDDI.

Una área en la que la FDDI ha tenido uso es la fundación de un soporte corporativo. Dicho soporte puede extenderse en varios edificios dentro de una red de área metropolitana, es utilizada frecuentemente para ligar a altas velocidades departamentos locales LAN, basados en los estándares Ethernet y token ring. La ventaja de este tipo de esquemas es que concentra la información del tráfico local en donde se encuentra una subred y no permite que fluya en la red principal. También permite a los usuarios con soporte de fibra óptica, accesar aplicaciones e información localizada en servidores conectados a redes de área local.

[31] Fiber Distributed Data Interface

Existe una nueva especificación, CDDI [32], que habilita la ejecución de fibras ópticas sobre un cable de par trenzado. Dicha especificación es una importante tecnología porque sustituye una de las barreras para FDDI, - la instalación y mantenimiento de un sistema de cableado nuevo.

El FDDI es principalmente una tecnología para redes de área amplia, pero se utiliza para redes LAN que requieren niveles de muy alta ejecución. FDDI fue diseñado originalmente para medios ópticos, pero los estándares se han ido desarrollando y pueden habilitarlos para correr sobre algunos tipos de cable de par trenzado. Incluso la Corporación de Equipos Digitales (DEC) ofrece FDDI sobre cable coaxial delgado.

Cada uno de los estándares tiene su protocolo ya dado. Una topología de red define tanto niveles físicos de datos como las trayectorias que las señales eléctricas siguen entre los dispositivos de red.

La red FDDI fue diseñada para cable de fibra óptica. La fibra puede ser utilizada con otro tipo de redes como Ethernet, Token Ring, para extender el rango de una red.

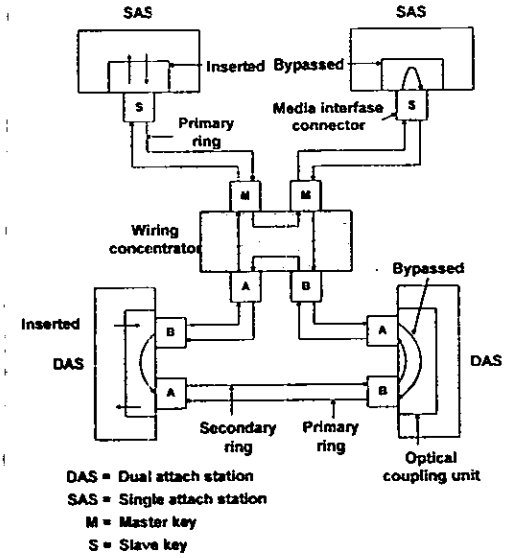


Figura 12. Configuración típica de una red FDDI.

Las redes FDDI consisten de dos anillos, cada uno para una dirección de transmisión, en uno se transmite en un sentido y el otro en sentido contrario, llamados anillo secundario y primario respectivamente. Bajo condiciones normales la información sólo fluye en un anillo (el primario) dejando el anillo secundario como respaldo, es decir, este último se

[32] Interfaz de datos distribuida

activará si se presenta una falla en el anillo primario, para que la red no se quede sin operar.

ATM [33]

El modo de transferencia asíncrono ATM surgió como una evolución de la tecnología ISDN [34] Red digital de servicios integrados. De hecho, el modelo de ATM tuvo su origen en otro modelo conocido como B-ISDN [35]. ATM permite la consolidación de múltiples señales en un solo canal (multiplexión) de diversos servicios, tales como voz, video y datos a muy alta velocidad.

Hasta el momento, ATM ha encontrado mucho uso entre operadores públicos, para transportar datos a alta velocidad, a nivel de *backbone* [36]. Al nivel de acceso existen proveedores de equipos que le permiten al usuario la interconexión directa de sus equipos actuales (PBXs, LANs, Video Codecs, Multiplexores, Computadoras, etc.), a una red ATM, de un modo totalmente transparente.

Por ejemplo en países como México ya existen proveedores públicos, con la capacidad de ofrecer servicios de interconexión de ATM a todos los niveles (acceso, concentración y transporte).

El principio básico de esta tecnología es segmentar los datos en celdas y transmitirlas por medio de conmutación de celdas, debido a que el tamaño de las celdas es fijo y uniforme, se simplifica la conmutación. ATM crea un canal mixto o ruta entre dos puntos en el momento en que se inicia la transferencia de datos.

Servicio	ATM
Velocidad de acceso	25 a 622 Mbps
Enlaces	Digitales y Fibra óptica
Aplicaciones	Transmisión de voz , video y datos a alta velocidad
Ejemplos	Videoconferencias , telemedicina , tele educación consolidación de voz y datos

Tabla 8. Características generales del estándar ATM

Fast Ethernet

En los tipos más simples de redes Ethernet, todas las estaciones de trabajo están en constante competencia por el ancho de banda de 10 Mbps. La mayoría de las redes Ethernet son complicadas, sin embargo cuentan con un conjunto de segmentos que pueden ser concentradores, ruteadores y repetidores. En una red de Segmento Ethernet una estación de trabajo no tiene acceso completo al ancho de banda.

[33] Asyncronous Transfer Mode
[34] Integrated Services Digital Network
[35] Broadband ISDN; en banda ancha
[36] Espina Dorsal de Red

Dos mejoras del concepto original de Ethernet que se han realizado, ofreciendo el incremento del ancho de banda han sido: *Switched Ethernet* y *Fast Ethernet*.

Una red de switcheo Ethernet provee 10 Mbps al ancho de banda de un *hub* o concentrador a una estación de trabajo. Switched Ethernet es un paso intermedio importante para la implementación eventual de Fast Ethernet porque los concentradores que soportan Switched Ethernet usualmente tienen un puerto de Fast Ethernet, el cual permite una conexión fácil de un concentrador Switched Ethernet para un *backbone* de Fast Ethernet.

Una red de Fast Ethernet incrementa el ancho de banda de una red a 100 Mbps. Utilizar este tipo de red incrementa la combinación efectiva del ancho de banda para todos los usuarios de la red. La red de switcheo de Fast Ethernet dedica los 100 Mbps de ancho de banda para cada usuario conectado a un puerto de switcheo de 100 Mbps y es una característica muy útil para usuarios que necesitan que el ancho de banda soporte sus aplicaciones.

En la **Figura 13**, se muestra un "Árbol de decisión de Ethernet" pensado para ayudar a que los administradores de redes escojan entre Segmentado, Switcheo o Fast Ethernet.

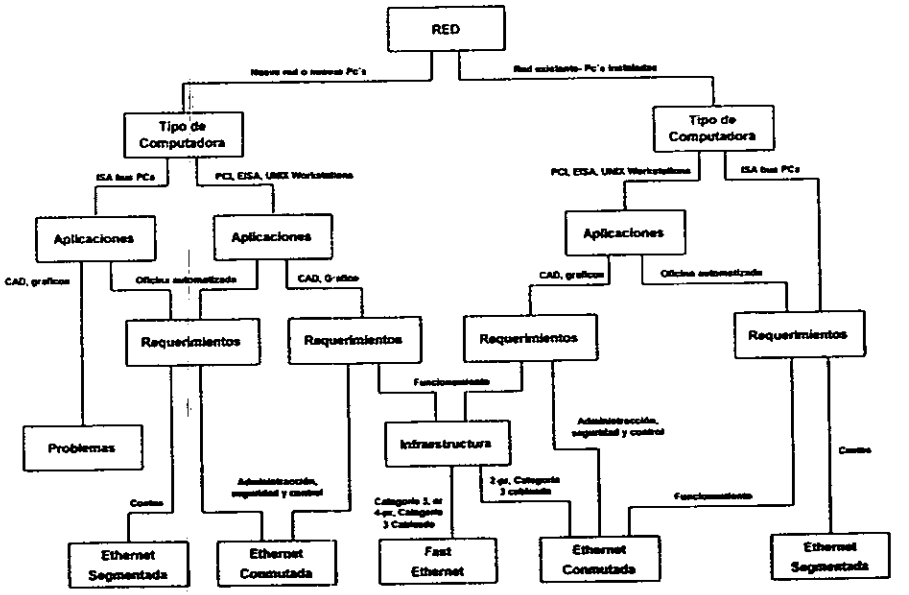


Figura 13. Árbol de decisión de Ethernet.

Fast Ethernet es la tecnología más importante de las diferentes redes Ethernet. En 1993 la Alianza de Fast Ethernet, abarcada por más de 75 compañías de comunicaciones (incluyendo 3Com, un socio estratégico de Dell), formadas para acelerar la adopción de la

tecnología Fast Ehernet y que fuera adoptada por la mayoría de las compañías de comunicaciones.

Tecnología	FDDI	100BASE X	ATM
Estatus	Disponible	Disponible	Emergente
Estándares	ANSI	IEEE802.3 U	Foro ATM IETF, ITU-TSS
Complejidad	Moderada	Baja	Alta
Ancho de Banda	100 Mbps	100 Mbps	25 Mbps/2.5 Gbps
Distancia	200 Km	205 mts. (UTP) 405 mts. (Fibra óptica)	Global
Tipo de Acceso	Token passing	CSMA/CD	Cell Switching
Unidad	Frame variable	Frame variable	Celda fija
Medio Físico	Fibra óptica UTP, STP	Fibra óptica UTP, STP	Fibra óptica UTP, STP
Servicios	Síncronos/ Asíncronos	Asíncronos	Síncronos/ Asíncronos/ Isócronos
Tráfico	Datos, poco multimedia	Datos, poco multimedia	Voz, video, datos y multimedia
Aplicaciones	LAN/Campus Backbone, escritorio	LAN Backbone, servidores, escritorio	Campus, MAN, WAN, escritorio
Costo	Medio	Bajo	Medio - Alto

Tabla 9. Características de diferentes tecnologías

1.6. Interconexión de redes y configuraciones

Cableado estructurado[37]

Es la integración de diferentes tipos de medios, perfectamente adaptados, capaces de soportar todo tipo de tráfico de información de voz, datos, video y sistemas de administración de edificios tales como el control ambiental y seguridad, que obedece a una estructura normalizada por el estándar de la industria ANSI[38]/EIA[39]/TIA[40] 568A.

Existe un límite máximo en la longitud del par trenzado dependiendo del rango de bits que se utilice. Generalmente el limite es de 100m. a 1 Mbps. o con la ayuda de circuitos para eliminar conversaciones cruzadas, con un limite de 100 m. a 10 Mbps. Un arreglo típico es utilizar par trenzado entre cada DTE y el cable más cercano al piso, y después cable coaxial para ligar el cable del piso al concentrador principal del edificio. Para una instalación que involucre múltiples edificios, la fibra óptica es la que se utiliza para unir

[37] Ver apéndice B
[38] American National Standards Institute
[39] Electronic Industries Association
[40] Telecommunications Industry Association

el concentrador de cada edificio al concentrador central. Este último normalmente trabaja en rangos de bits altos y su configuración lógica es como una red de anillo.

EIA 568 y 569

Los estándares comunes para el cableado de Ethernet los proveen asociaciones, constructoras de estándares comerciales de cables de telecomunicaciones conocidas como EIA/TIA[41] 568, la cual especifica el calibre de los cables que se requieren y otros detalles técnicos para asegurar la instalación propia de un cableado y soportar una red Ethernet.

Variantes de Ethernet	Identificación	Tipo de cable	Impedancia	Distancia	Utilización
Thin Ethernet	10Base2	RG-58 (coaxial)	50 ohms	185m.	Redes pequeñas, Dispositivos próximos entre sí.
Thick Ethernet	10Base5	RG-8 (coaxial)	50 ohms	500m.	
Twisted pair Ethernet	10BaseT	RJ-45 (par trenzado no blindado)	100 ohms	100m.	Redes muy pequeñas, dispositivos muy cercanos

Tabla 10. Características para el cableado de Ethernet según la EIA/TIA.

Los estándares de interfaces y de cables EIA/TIA están asociados con Ethernet y Fast Ethernet. Debido a que la interfaz define la forma en que trabaja la señal a través del cable físico conectando la red, los tipos de interfaz y cables deben estar coordinados. Las instalaciones de Switched, Fast Ethernet y las actuales requieren combinaciones cable/interfaz capaces de soportar rangos de transferencia de datos de 100 Mbps como el 10BaseTX, 100BaseT4 y 100BaseFX.

De las cinco categorías de cable EIA/TIA, las categorías 1 y 2 no son adecuadas para aplicaciones Ethernet.

Categoría	Tipo de cable	AWG	Ancho de banda	Impedancia	Velocidad de transmisión	Instalaciones en las que se utiliza
1	No trenzado	22 o 24	-	-	1 Mbps	No recomendable para transmisión de datos
2	Par trenzado	22 o 24	-	-		Conexiones terminales de Apple Localtalk, IBM3270 y AS/4000.
3	Par trenzado	24	10 Mhz.	100 ohms.	10 Mbps	10 Mbps. En Ethernet y 4 Mbps. en Token Ring Voz analógica y digital 100 BASE T (100 mts)
4	Par trenzado	22 o 24	20 Mhz.	100 ohms.	16 Mbps.	16 Mbps. En Token Ring 10BaseT en Ethernet Aplicaciones de la categoría 3
5	Par trenzado	22 o 24	100 Mhz.	-	100 Mbps.	FDDI sobre par trenzado. Aplicaciones de categoría 3 y 4

Tabla 11. Categorías de cables de la EIA/TIA.

[41] Electronic Industries Association (Asociación de industrias electrónicas
Telecommunications Idustry Association (Asociación de la industria de telecomunicaciones)

TIA/EIA 606

El estándar TIA/EIA 606 se refiere a la administración uniforme para la infraestructura de telecomunicaciones que es independiente de aplicaciones. Su propósito es reducir el amplio número de aproximaciones administrativas incompatibles e incompletas que existen.

Las áreas de administración en telecomunicaciones son:

- terminadores
- medio
- trayectorias
- espacios
- enlaces/aterrizados

  Nota: El equipo de usuario final en la estación o dispositivos específicos de aplicación almacenados no están direccionados.
- Identificadores

  Designaciones asignadas para elementos de infraestructura en telecomunicaciones.

  Los identificadores utilizados para accesar registros de un mismo tipo deben ser únicos.

  Los identificadores codificados designan el elemento y proporcionan información acerca de ese elemento.
- Los registros son la colección de información relacionada a elementos específicos.
- Un sistema de administración típica incluye:

  Especificaciones adicionales:

  Cables idénticos empalmados juntos deben ser administrados como un cable simple.

  Cada cable horizontal debe ser etiquetado por ambos extremos.

  Los dispositivos terminales que contengan una o más posiciones terminales, deben ser administrados como una posición terminal.

  Un identificador único asignado a cada dispositivo de unidad terminal.

  Un identificador debe ser marcado a cada unidad de dispositivo terminal o en su etiqueta.

  Las estaciones terminales deben ser etiquetadas sobre la placa de recubrimiento, en un alojamiento o en su mismo conector.

  Las etiquetas pueden pegarse, insertarse o bien utilizar otro tipo de etiquetas; deben ser legibles.

  Código de colores:

  Naranja: Punto de demarcación.
  Verde: Conexiones de red en el lado del cliente.
  Morado: Equipo común.
  Blanco: Primer nivel de backbone (columna dorsal).
  Gris: Segundo nivel de backbone.
  Azul: Cableado horizontal (sólo terminales cerradas)
  Café: Backbone interno.
  Amarillo: Circuitos auxiliares.
  Rojo: Sistemas de claves telefónicas.

1.7 Modelos de Redes

Modelo de referencia OSI

El modelo OSI[42] es la referencia para la interconexión de sistemas abiertos, propuesto por la Organización Internacional de Normas. Este modelo define la estructura de una red como una jerarquía de siete niveles [43].

El modelo OSI define las funciones de cada nivel, más no les define un diseño, tecnología, o la implementación de los mismos.

El propósito de una referencia internacional de interconexión de sistemas abiertos (OSI) es proveer a los sistemas una estandarización en su estructura, de tal forma que estos puedan interconectarse entre sí. Es importante tener en cuenta que el estándar OSI sólo es un modelo. Las redes de computadora no necesariamente se deben de ajustar a una estructura de siete niveles. En algunos casos de red, un nivel puede absorber varios niveles o las funciones de un nivel podrían estar repartidas en los demás niveles.

Los siete niveles (o capas) del modelo de referencia OSI son los siguientes:

1. Físico
2. Enlace
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

A continuación se definen cada uno de los niveles antes mencionados:

Nivel físico

El nivel físico es donde se lleva a cabo el intercambio de señales eléctricas. En este nivel se determinan las características mecánicas y eléctricas de la conexión física. Además de definir los procedimientos para establecer, mantener y liberar las conexiones entre los circuitos eléctricos, que están enlazados en la comunicación. En este nivel también se define el tipo de señal a transmitir, así como el intervalo de tiempo de un bit.

Ejemplos de estándares de esta capa son los protocolos RS-232-C y elementos de X.21 [44].

Nivel de enlace

La tarea primordial del nivel de enlace consiste en que, a partir de un medio de transmisión común y corriente, los datos se transforman en una línea, sin errores de transmisión para la capa de red. Esta tarea la realiza al hacer que el emisor seccione la

[42] Open System Interconnection
[43] Propuesto por Day y Zimermann
[44] Se vieron en la sección 1.2.2

entrada de datos en bloques de información y las transmita en forma secuencial. La capa de enlace reconocerá los bloques, mediante la inclusión de un bit especial al inicio y al termino del bloque.

El bloque al ser transmitido, puede alterarse o destruirse por causas externas (por ejemplo ruido en la línea), en cuyo caso la capa de enlace deberá retransmitir el bloque. Sin embargo, múltiples transmisiones del mismo bloque introducen la posibilidad de duplicar información. Para evitar este problema, el duplicado del bloque podría enviarse, si el acuse del recibo que regresa al receptor se hubiera destruido. Corresponde a esta capa resolver los problemas causados por daño, pérdida o duplicidad de bloques.

Otro de los problemas que aparecen en la capa de enlace [45] es el referente a cómo evitar que un transmisor muy rápido sature con datos a un receptor lento. Se deberá emplear un mecanismo de regulación de tráfico que permita que el transmisor conozca el espacio de memoria que en ese momento tiene el receptor. Frecuentemente, y por conveniencia, los procedimientos de regulación de flujo y control de errores se tratan en forma conjunta.

Ejemplos de estándares de esta capa son los protocolos HDLC [46], LAPB [47], LAPD [48] y LLC [49].

Nivel de red

El nivel de red toma bloques de datos del tamaño del paquete del nivel de transporte y les añade información de dirección y encaminamiento que completan el paquete. La elección del algoritmo de encaminamiento es arbitraria, de modo que puede ser fija o adaptable, en cuyo caso los paquetes se encaminan de acuerdo con las cargas actuales de tráfico en la red. El encaminamiento se puede limitar a una sola red o extenderse a la transferencia de paquetes entre redes interconectadas.

Si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se bloquearan mutuamente y darán lugar a un cuello de botella. El control de tal congestión dependerá también del nivel de red.

Cuando un paquete tenga que desplazarse de una red a otra, el direccionamiento utilizado en la segunda red puede ser diferente al empleado en la primera. La segunda red podría no aceptar el paquete en su totalidad, por ser demasiado grande o bien porque los protocolos pudieran ser diferentes. La responsabilidad, para resolver problemas de interconexión de redes recaerá en el nivel de red.

En la **Figura 14** se muestra un modelo de dos estaciones, las cuales están comunicadas a través de nodos. Los niveles 1 y 2 son protocolos de estación-nodo (locales). Los niveles

[45] También en la mayoría de los niveles superiores.
[46] High Level Data Link Control, se describirá en la sección 1.7.2
[47] Link Access Procedure Balanced. (Procedimientos Balanceados de Acceso a Vínculos)
[48] Link Access Procedure D (Procedimientos de Acceso en el canal D)
[49] Logical Link Control

4 hasta el 7 son protocolos entre las (N) entidades en las dos estaciones. El nivel de red es en donde se efectúa la comunicación directa en ambas redes, por medio de paquetes de información.

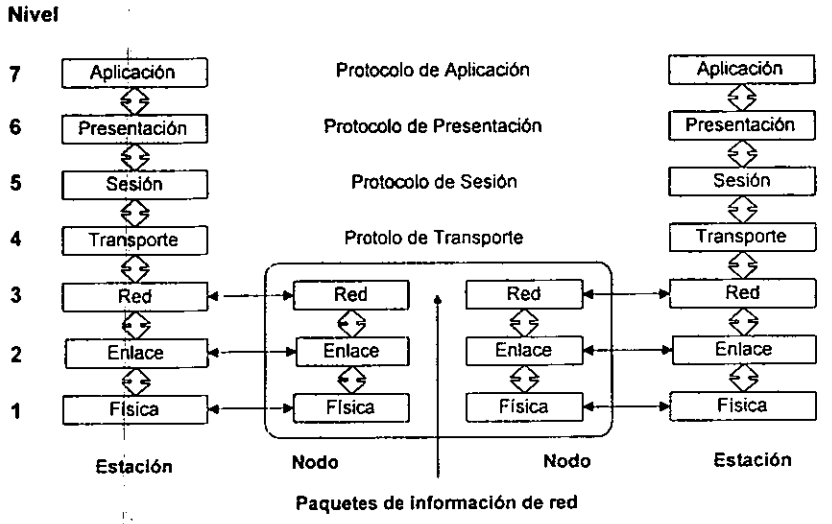


Figura 14. Comunicación en una Red

Nivel de transporte

La función principal del nivel de transporte consiste en aceptar los datos del nivel de sesión, dividirlos, siempre que sea necesario en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen libres de errores al otro extremo. Además, todo este trabajo se debe hacer de manera eficiente, de tal forma que se aísle el nivel de sesión de los cambios inevitables a los que está sujeta la tecnología del hardware.

Este nivel es del tipo origen-destino o extremo a extremo. Es decir, un programa en la máquina origen lleva una conversación con un programa igual al que se encuentra en la máquina destino. Los protocolos, de los niveles inferiores, son entre cada máquina y su vecino inmediato, y no entre las máquinas origen y destino. El tamaño y la complejidad de los protocolos de transporte dependen del tipo de servicio, que pueda requerir el nivel de red.

Nivel de sesión

El nivel de sesión establece, mantiene y termina una conexión con un proceso en una computadora remota. Este nivel debe dar un servicio fiable al nivel de presentación y tener la capacidad de restablecer una conexión en caso de que falle uno de los niveles más bajos de la jerarquía. Mientras establece una conexión, el nivel de sesión debe de poder

negociar con la máquina más próxima ciertos parámetros de la conexión. Estos pueden incluir el tipo de comunicación que se empleará (dúplex o semidúplex).

Permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.

Otro de los servicios de la capa de sesión es la sincronización. Por ejemplo, los problemas que podrían ocurrir cuando se tratara de realizar una transferencia de archivos de dos horas entre dos máquinas en una red con un tiempo medio de una hora entre caída. Después de abortar cada archivo, la trasferencia completa tendría que iniciarse de nuevo y, probablemente, se encontraría de nuevo con la siguiente caída de la red. Para eliminar este problema, la capa de sesión proporciona una forma de insertar puntos de verificación en el flujo de datos, con objeto de que, después de cada caída, solamente tengan que repetirse los datos que se encuentren después del último punto de verificación.

Nivel de presentación

El nivel de presentación proporciona un conjunto de servicios que se pueden usar en el proceso de intercambio de datos a través de la conexión de la sesión. Los servicios pueden incluir, por ejemplo, compresión, traducción y cifrado de los datos. Las computadoras pueden ocupar diferentes tipos de código (ASCII [50] y EBCDIC [51]) para la representación de sus datos (nombres, direcciones, etcétera), entonces el nivel de presentación debe de ser capaz de traducir el código fuente al código correspondiente del destino.

Nivel de aplicación

El nivel de aplicación es donde el usuario trabaja, para él todos los procesos que se realizan en la red son transparentes.

Este nivel es el más alto en la jerarquía de la red, los protocolos interactúan directamente con el software de aplicación que quiere transferir datos a través de la red. Los demás niveles de la jerarquía existen con el único propósito de satisfacer las necesidades de este nivel y ocultar las características físicas de la red subyacente.

El nivel de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay centenares de tipos de terminales incompatibles en el mundo. Considérese la situación de un editor de texto que desea trabajar en una red con diferentes tipos de terminales, cada uno de ellos con distintas formas de distribución de

[50] American Standard Code Interchange Information (Información de intercambio de código estándar americano)

[51] Extended Binary Code Decimal Interchange Code (Código de intercambio decimal a código binario extendido)

pantalla, de secuencias de escape para insertar y borrar texto, de movimientos de cursor, etc.

Una forma de resolver este problema consiste en definir una terminal virtual de red abstracto, con el que los editores y otros programas pueden ser escritos para tratar con él. Con objeto de transferir funciones de la terminal virtual de una red a una terminal real, se debe de escribir un software que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho software deberá emitir la secuencia de comandos apropiados para que la terminal real ubique también su cursor en el sitio indicado. El software completo de la terminal virtual se encuentra en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos. Distintos sistemas de archivos tienen diferentes convicciones para denominar un archivo, así como diferentes formas para representar las líneas de texto, por lo que la transferencia de archivos entre dos sistemas diferentes requiere de la resolución de éstas y de otras incompatibilidades. Este trabajo, así como el correo electrónico, la entrada de trabajo a distancia, el servicio de directorios y otros servicios de propósito general y específico, también corresponden al nivel de aplicación.

Transmisión de datos en el modelo de referencia OSI

El proceso de comunicación comienza en el nivel de aplicación emisor, el cual toma los datos, les añade una cabecera [52] de aplicación. y entrega los mismos a los niveles inferiores, los cuales, a su vez le irán añadiendo sus propias cabeceras a los datos. Cuando los datos llegan al nivel más bajo (nivel físico), contienen las cabeceras agregadas por cada nivel, entonces este último nivel manda los datos a través de la red y estos al llegar a su destino, se inicia un proceso de reconocimiento de cabeceras, es decir, cuando los datos llegan al nivel de enlace receptor, este reconocerá la cabecera de enlace emisora y se la quitara, posteriormente los manda a las capas superiores. Conforme los datos van ascendiendo, se les van eliminando las cabeceras de cada capa, de tal manera que al llegar los datos a la capa de aplicación, el usuario puede hacer uso de ellos.

La idea fundamental a lo largo de este proceso es que si bien la transmisión efectiva de datos es vertical (como se muestra en la **Figura 15**) cada una de las capas está programada como si fuera una transmisión horizontal.

[52] Las cabeceras son códigos propios de cada capa y sólo serán reconocidos por otra capa que tenga la misma función.

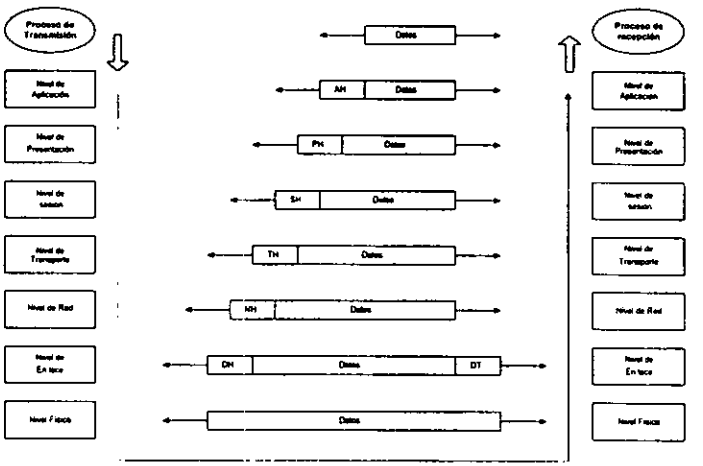


Figura 15. Utilización del modelo OSI

A continuación se muestran los protocolos y dispositivos más comunes, así como los niveles en los que se sitúan con relación al modelo de referencia OSI.

Niveles OSI	TIPOS DE APLICACIONES PARA REDES
5, 6 y 7	Bases de Datos
	Sistemas Operativos
	Software de Automatización de Oficinas (PP, HC, P)
	Multimedia
	Correo Electrónico
	Flujo de Trabajo
	Gateway
	Aplicaciones a la Medida (desarrolladas)
	TCP (Telnet, FTP, SMTP, SNMP, NFS, etc)
	Protocolos OSI
	SNA
	NetBIOS

Tabla 12. Protocolos relacionados con las capas OSI.

Niveles OSI	TIPOS DE APLICACIONES PARA REDES
3 y 4	TCP IP (IP, TCP, ICMP, UDP, ARP, RARP, etc.) IPX/SPX (IPX, SPX, PEP, SAP, ECHO, RIP, ERROR, etc.) Protocolos OSI XNS DECNET Fase 4 SNA X25
2	Drivers de tarjetas de red (NDIS, ODI, etc.)

Tabla 13. Protocolos relacionados con las capas OSI.

1.8 Protocolos

1.8.1 TCP/IP

El protocolo de control de transmisión/protocolo de intered (TCP/IP) es el nombre comúnmente dado a la familia de protocolos de comunicación de datos utilizado para conectar computadoras y equipo de comunicaciones de datos dentro de una red de cómputo. Es utilizado en una gran red internacional llamada internet[53], la cual está compuesta de universidades, actividades gubernamentales, instituciones de investigación y compañías privadas.

TCP/IP es un software de protocolo de comunicaciones que se empezó a utilizar a mediados de los 80's cuando la DARPA [54] requirió que todas las computadoras conectadas a Arpanet utilizaran este protocolo de comunicaciones. También se encuentra en redes de área local (LANs) compuestas de diferentes tipos de computadoras y de estaciones de trabajo.

Desde 1960 la Agencia de Proyectos de Investigación Avanzada (ARPA, ahora DARPA), ha infundido la investigación de redes muy confiables que ligan sistemas computacionales heterogéneos. Los resultados de esta investigación originaron la aparición de ARPANET, una red de switcheo de paquetes, TCP [55] Protocolo de Control de Transmisión, IP [56] Protocolo Internet, FTP [57] Protocolo de transferencia de archivos, entre otros. ARPANET se convirtió posteriormente en Internet.

[53] El sistema internet se puede describir como una conjunto de computadoras principales (*hosts*) y redes interconectadas por ruteadores IP.
[54] Agencia de investigación de proyectos avanzados.
[55] Transmission Control Protocol.
[56] Internet Protocol.
[57] File Transfer Protocol.

Los protocolos de Internet son diseñados para facilitar los procesos múltiples en computadoras que se comunican una y otra por medio de una red. El único requerimiento es que las computadoras son conectadas utilizando una red de switcheo de paquetes. En este modelo, las computadoras están conectadas formando una red, generalmente dentro de una área delimitada, como son edificios o conjunto de ellos. Las redes están conectadas principalmente por dispositivos llamados Gateways [58], los cuales son computadoras que han sido dedicadas para las tareas de switcheo y ruteo de paquetes entre redes.

La importancia de los protocolos de Internet es la eficiencia y confiabilidad entre redes de sistemas de cómputo diferentes que residen en ambientes de red heterogéneos. La conexión fuerte de estos sistemas es el protocolo de intered (IP[59]). Este protocolo está organizado por 4 niveles que toman términos del Modelo de Referencia OSI, son descritos como nivel de aplicación, nivel de transporte (o host a host), nivel de red (o intered), y el nivel físico y de datos ligados (agrupados en un solo nivel para los propósitos del protocolo).

Niveles del protocolo TCP/IP

TCP/IP es un conjunto de protocolos divido en cuatro niveles:

1. Aplicación
2. Transporte
3. Red
4. Interfaz de red

y se describen a continuación.

Nivel de Aplicación

Algunos ejemplos de aplicaciones de redes Internet con programas de comunicaciones interpersonales, como correo electrónico y anuncios, emulación de terminal virtual (TELNET[60]) y transferencia de archivos (FTP[61]). Este nivel contiene grupos de elementos de servicio que pueden ser combinados con elementos específicos de aplicación, para formar una aplicación contextual (nivel de red).

Nivel de transporte

El primer nivel responsable de las verdaderas conexiones finales (*end to end*). Este nivel programa y procesa en computadoras diferentes, conexiones finales y se comunican directamente una y otra. Los dos protocolos definidos en este nivel son el protocolo de

[58] Se describirán en la sección 1.10.
[59] Internet Protocol.
[60] (TELecomunications NETwork,) Es un programa que permite realizar una conexión remota a otra computadora que se encuentre localizada en Internet.
[61] File Transfer Protocol (se describirá más adelante en esta sección).

control de transmisión (TCP[62]) y el protocolo de datos de usuario (UDP [63]). TCP consta de una conexión orientada a un modelo de circuito virtual para la comunicación de la red; UDP consta de un modelo de conexión que es esencialmente el servicio de datagrama dado por el protocolo Internet debajo de él.

Nivel de red

Habilita redes múltiples para conectarlas dentro de internet. Al protocolo definido en este nivel se le llama protocolo de internet (IP), el cual realiza la conexión y servicio de datos a los protocolos de niveles más altos, pero es un servicio no confiable. Estando en el nivel de red, IP realiza un ruteo a las computadoras y es la cola la que liga las redes y la computadora en internet. A los ruteadores de internet se les llama también gateways.

Este nivel proporciona el servicio básico de bloques de datos (datagramas) a su destino a través de múltiples redes. Cada datagrama IP lleva la dirección internet del último destino; la dirección de dicho destino es utilizado por ruteadores en internet para realizar decisiones de ruteo conforme dirigen el datagrama a su destino. Cada datagrama también lleva la dirección internet a su fuente original, la dirección de ésta la utiliza el ruteador para informar a la estación fuente si el datagrama encuentra errores conforme es ruteada a través de la red. El protocolo de resolución de dirección (ARP[64]) mapea las direcciones de internet dentro de direcciones de ethernet y el protocolo de control de mensaje (ICMP) proporciona mensajes de ayuda y error de las condiciones de la red.

Nivel de interfaz de red

Realiza acceso al medio de comunicación con un control opcional del fluido de información así como de detección y corrección de errores. La serie de Internet puede utilizar el protocolo X.25 para redes de área amplia y las especificaciones de la IEEE 802 (como Ethernet 802.3 y token ring 802.5) para la red de área local.

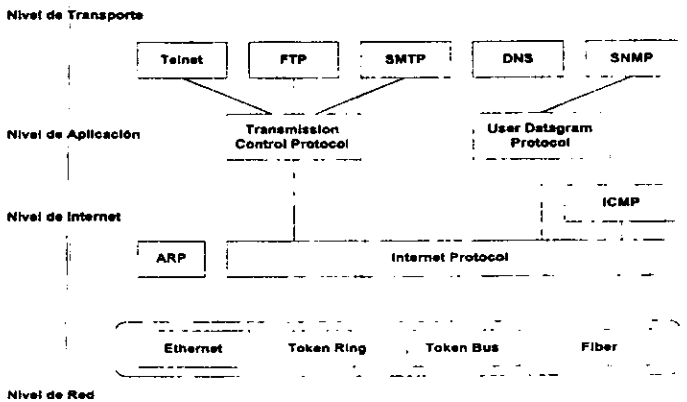


Figura 16. Arquitectura del protocolo TCP/IP

[62] Transmission Control Protocol (se describirá más adelante en esta sección).
[63] User data protocol (se describirá más adelante en esta sección).
[64] Address Resolution Protocol

A continuación se describen los protocolos utilizados en cada nivel del modelo TCP/IP:

Descripción para el nivel de aplicación:

TELNET [65] (Red de telecomunicaciones)
Esta aplicación permite habilitar a un usuario de una terminal para interactuar con un programa que está corriendo en otra computadora. El programa local de TELNET ejecuta una emulación de terminal, y de esta forma el usuario de TELNET sentiría que se encuentra en una terminal normal.

El conjunto de protocolos y aplicaciones que constituyen un sistema TCP/IP son medios estándares y flexibles para comunicarse entre dos sistemas UNIX. Muchos otros sistemas, incluyendo MS-DOS y Windows, tienen protocolos TCP/IP para habilitarlos y también conectarlos a sistemas UNIX.

TELNET permite establecer una conexión a través de INTERNET desde una computadora a otra, con TELNET, los comandos que se invocan son enviados desde esa terminal, a una máquina local con el servicio de INTERNET y de ésta a la computadora remota que se desea accesar.

También es posible verificar el correo electrónico desde otras ciudades, así como bases de datos para investigación o bibliotecas de todo el mundo (para verificar si se encuentra cierto libro que se esté buscando). También ofrece una facilidad para entrar al WWW [66] para quienes no tienen otro modo de accesar las herramientas mencionadas anteriormente.

FTP (Protocolo de transferencia de archivos)
El protocolo FTP [67] utiliza los servicios de TCP/IP para transferir archivos, permite al usuario inicializar la entrada al sistema remoto de UNIX y escribir comandos para recibir o enviar archivos entre dos sistemas. Aunque el FTP se puede utilizar con un programa directamente, sin intervención del usuario, FTP está diseñado principalmente para realizar transferencia de archivos manualmente. FTP realiza servicios de acceso remoto, pero es utilizado específicamente para transferir archivos entre computadoras. Para recibir o enviar archivos desde una computadora a una remota con FTP, se inicia una sesión de FTP en la computadora local escribiendo el nombre del programa " ftp ", posteriormente se introducen las instrucciones para abrir la conexión hacia el sistema remoto. El conjunto de comandos de FTP realiza las siguientes tareas:

- Directorios de búsqueda
- Directorios de cambio
- Recibir archivos desde el sistema remoto
- Enviar archivos al sistema remoto

[65] Telecomunication Network
[66] World Wide Web
[67] File Transfer Protocol

SMTP [68](Protocolo de transferencia de correo simple)
Este protocolo es utilizado para transferir correo confiable y eficiente entre un conjunto interconectado de sistemas de correo electrónico.

Una característica importante de este protocolo es su capacidad para retransmitir correo a través de ambientes de comunicación interproceso (IPCE[69]), los cuales pueden cubrir una o varias redes, o un subconjunto de una red. Los sistemas de transporte o IPCE's no trabajan uno-a-uno con las redes, un proceso puede comunicarse directamente con otro proceso por medio de cualquier IPCE mutuamente conocido. El correo es una aplicación o uso de comunicación interproceso, y puede ser comunicado entre procesos en diferentes IPCE's retransmitiendo a través de un proceso conectado a dos o más IPCE's. Más específicamente, el correo puede ser retransmitido entre computadoras en diferentes sistemas de transporte por una computadora en ambos sistemas de transporte.

DNS[70] (Sistema de nombre de dominio)
El sistema (servidor) de nombre de dominio (DNS) habilita un dispositivo con un nombre común para que sea convertido a una dirección especial de red. Por ejemplo, no se puede tener acceso a un sistema llamado jose_estacion desde una red distante, a menos que esté disponible algún método de verificación de los nombres de las máquinas locales. DNS proporciona la conversión del nombre común local a la dirección física única de la conexión de red del dispositivo.

SNMP[71] (Protocolo de administración de redes simples)
Este protocolo habilita varios sistemas UNIX para que sean administrados desde un sistema de manejo de red común. Se utiliza para enviar y recibir información de manejos-relacionados por medio de una red TCP/IP.

SNMP consiste de un conjunto compuesto simplemente de especificaciones de comunicación de red que cubre todas las necesidades básicas para administrar una red.

Este protocolo intercambia información de la red a través de mensajes (técnicamente conocido como unidades de datos). Existen cinco tipos de unidades de datos que el SNMP emplea para monitorear una red: dos tipos para la terminal de datos de lectura, dos para la terminal de datos de la configuración y otro para los eventos del monitoreo de la red, como puede ser el encendido y apagado de una terminal. Por lo tanto si un usuario desea ver si una terminal está conectada a la red, debe utilizar el SNMP para enviar unidades de datos de lectura a dicha terminal. Si la terminal está o no conectada a la red, el usuario recibirá un mensaje.

[68] Simple Mail Transfer Protocol.
[69] Interprocess Communication Environment.
[70] Domain Name System
[71] Single Network Management Protocol.

El diseño del protocolo SNMP es simple y fácil de implementar en una red grande, no toma tanto tiempo para configurarse, ni deja que la red se sature. Debido a su diseño hace que un usuario programe fácilmente variables que el desee monitorear, cada variable puede consistir de la siguiente información:

- El título de la variable
- Tipo de dato de la variable (por ejemplo entero, cadena)
- Si la variable es sólo de lectura o escritura y lectura
- El valor de la variable

Es importante mencionar que debido a la simplicidad de este protocolo la mayoría de los fabricantes de los dispositivos de la red, como puentes y ruteadores se diseñan para soportar SNMP haciéndolos más fáciles de implementar. Debido a esa simplicidad, es fácil para el protocolo ser actualizado y por lo tanto se puede expandir a las necesidades de los usuarios en el futuro.

Descripción para el nivel de transporte:

TCP (Protocolo de control de transmisión)
El protocolo TCP [72] permite el servicio de un circuito virtual de conexión orientada para procesos de aplicación que son utilizados en las comunicaciones de *host* a *host*. Permite que la información fluya entre procesos y haya una corrección de errores, pero el contenido de flujo de datos no se restringe de ninguna forma. TCP es el estándar del Departamento de defensa (DOD) para las comunicaciones inter-proceso.

TCP realiza pocas adopciones acerca del refuerzo real de los servicios de comunicaciones en los niveles o el medio en el que se encuentra. TCP utiliza los servicios del Protocolo Internet (IP) para enviar diferentes longitudes de datos sobre redes de switcheo de paquetes e interedes. TCP está hecha para asegurar una comunicación confiable de *computadora* a *computadora*, de una conexión de flujo orientada, y se apoya del protocolo IP para tener cuidado en la fragmentación principal y volver a reunir lo que puede requerir para obtener un segmento en una intered heterogénea.

Las aplicaciones que requieren ser confiables, como la conexión de flujo orientada para una aplicación sobre otra computadora, hace uso de los servicios de TCP. Estas aplicaciones de red hacen una interfaz directamente con TCP a través de una interfaz de programa de aplicación API [73] que la provee el protocolo de implementación. Dependiendo del sistema operativo de la *computadora*, el API puede elaborar un componente integral del sistema operativo. La aplicación hace familiar a las llamadas de E/S[74] como son las de lectura, escritura y llamadas para obtener el estado de la conexión.

[72] Transfer Control Protocol.
[73] Aplication Program Intreface
[74] Entrada/Salida

TCP siendo un protocolo de conexión orientada, requiere que una conexión sea establecida entre los dos procesos de comunicación. Este requerimiento necesita que en un periodo de tiempo y esfuerzo necesite ser expandido al principio y al final de una sesión para afectar la conexión establecida y derribarla. Durante el establecimiento de esta conexión, parámetros fundamentales que se utilizarán a través de la conexión son establecidos, incluyendo los *sockets* [75] utilizados, la secuencia de números para datos y el tamaño de la ventana para el control del fluido de información.

TCP utiliza una guía de tres-caminos para el establecimiento de la conexión, la cual utiliza tres mensajes para realizar la misma. Los paquetes enviados tienen banderas de control para indicar el estado del progreso. En particular, las banderas de control de sincronización (SYN) y reconocimiento (ACK) se utilizan de la siguiente manera:

1. La computadora 1 envía un SYN y un número de secuencia a la computadora 2.
2. La computadora 2 envía un ACK y un SYN (ambos enviados en un mensaje simple) a la computadora 1 con el número de secuencia.
3. La computadora 1 envía un ACK del número de secuencia a la computadora 2.
4. Se termina la conexión intercambiando los segmentos con la bandera de control FIN.

La transferencia de datos involucra moviendo un flujo de datos entre procesos que están corriendo en dos computadoras. Los programas de aplicación llaman a la función de envío para mover el dato de una aplicación dentro del buffer de transporte. Utilizando este llamado, el proceso de aplicación no tiene control cuando el dato ya fue transmitido al proceso remoto. En general, TCP espera a su buffer de envío que será llenado para un uso más eficiente de la red.

En algunos casos, una aplicación puede necesitar la señal TCP para enviar el dato inmediatamente. TCP indica esto por medio del uso de la bandera opcional PUSH, la cual coloca el dato a través de la conexión, y para el proceso de recepción de datos, coloca señales que el dato debería presentar a la aplicación sin retardo.

Uno de los servicios más importantes que tiene TCP es tomar un servicio de datos no confiable de IP y crear un flujo-orientado confiable o mecanismo de transferencia de datos. Para proteger alteraciones o daños de segmentos, TCP realiza una verificación de archivo para habilitar la recepción final y asegurar la integridad del dato. Si un paquete llega y es determinado como alterado [76](por medio de la comparación de nuevos verificaciones computacionales con el único en el segmento), TCP deshecha el paquete, forzando posteriormente una retransmisión del dato a la *computadora* de envío.

TCP también requiere que los segmentos sean reconocidos por la *computadora* receptora. Un número de secuencia se utiliza para implementar el mecanismo de reconocimiento.

[75] Al último punto de una conexión TCP se le llama *socket*. Un *socket* es una combinación de la dirección de red, la dirección de computadora y el número de puerto en la *computadora* local. El puerto es un concepto lógico que habilita procesos de aplicación múltiple para utilizar los servicios de transporte de TCP en la misma máquina. Los *sockets* identifican los puntos finales de conexión en la computadora que envía y recibe. Sin embargo, un *socket* únicamente identifica la conexión.

[76] Por medio de la comparación de nuevas verificaciones computacionales, contra el único que se encuentra en el segmento.

Después de que un dato se envía, el envío inicializa el reloj. Si un reconocimiento no se recibe por el segmento antes de que el tiempo termine, el que envía retransmite nuevamente.

UDP (Protocolo de datos de usuario)
El protocolo UDP [77] utiliza el protocolo de intered (IP) para proveer procesos de aplicación con un protocolo de datos confiable en el nivel de transporte, habilitando aplicaciones para comunicar sin sobrepasar las conexiones establecidas y derribarlas. UDP no garantiza la liberación de paquetes, ni la secuencia de paquetes o la supresión de duplicación de paquetes. El Protocolo de datos del usuario es una conexión diseñada para permitir el transporte para mensajes simples y cortos.

El UDP se utiliza para aplicaciones[78] que pueden tener razones especiales para implementar su propia secuencia de liberación de paquetes y su confiabilidad. En estos casos, los servicios realizados por TCP pueden no ser utilizados al agregar un encabezado.

Descripción para el nivel de Internet:

ARP (Protocolo de Resolución de Direcciones)
El protocolo ARP[79] convierte las direcciones IP a direcciones físicas (de red y local); eliminando la necesidad de que las aplicaciones sepan direcciones físicas. Esencialmente, el ARP es una tabla con una lista de direcciones IP y sus direcciones físicas correspondientes. A dicha tabla se le conoce también como caché ARP

IP (Protocolo de Internet)
El protocolo IP [80] realiza una conexión no confiable de servicio de datos para conmutar datos sobre redes de conmutación de paquetes. También ofrece facilidades para fragmentación larga de paquetes para la transmisión y reunión de los mismos en la estación receptora. IP no ofrece ningún control de fluido de datos, ni secuencia o duplicación.

IP se utiliza tanto por TCP como por UDP para rutear y deliberar paquetes a través de la intered. El segmento TCP (encabezado y datos) está ubicado en la sección de datos del diagrama IP. El protocolo IP debe ser implementado en cada computadora que esté conectada a la red y ser capaz de rutear paquetes en la red local. Los gateways de Internet conectan redes, rutean y deliberan paquetes entre ellos.

---

[77] User Datagram Protocol
[78] El sistema de red de la SUN Microsystem (NFS), un sistema de archivo distribuido que está disponible en
muchas computadoras UNIX y no-UNIX, utilizan el UDP para transferir datos.
[79] Addres Resolution Protocol
[80] Internet Protocol.

IP utiliza una estructura jerárquica de la dirección internet y rutea cada dato independientemente de los otros.

El protocolo de intered proporciona diferentes bases para otros protocolos. IP puede correr sobre líneas dedicadas o líneas telefónicas y ser conducida a través de NetBIOS [81] en una PC, como medio de transporte puede utilizar la conexión X.25.

ICMP(Protocolo de intered de control de mensaje)
El protocolo [82] ICMP se utiliza para reportar errores que ocurren durante la deliberación de datos a través de internet. Generalmente, la computadora de destino o un gateway intermediario es el originador del mensaje. Este dispositivo puede reportar que el destino es inalcanzable o que el gateway no tiene suficientes buffers para almacenar y mantener el dato. El mensaje también puede contener información, para el que envía, de la ruta más corta para llegar al destino.

El ICMP lo requiere cada dispositivo que utiliza IP y es una parte esencial de IP. Utiliza a IP para ejecutar la liberación de sus mensajes de control. La confiabilidad en IP hace que ICMP sea no confiable – deliberar el mensaje de control no es una garantía. Por esta razón, los mensajes de control no generan un control en cuanto a errores con los datagramas de ICMP.

Los mensajes de ICMP se distinguen de otros por el valor del primer octeto en la porción de dato del paquete de IP, y ellos habilitan el módulo ICMP para interpretar el significado del mensaje.

Cuando el encabezado del IP se construye, el gateway (o computadora) que está reportando el error, es utilizado como la dirección fuente. El destino es la dirección donde el mensaje será dirigido.

Descripción para el nivel de Red:
Cada uno de estos estándares se describieron anteriormente.

1.8.2 Estándares de Protocolos

RFC
Las peticiones por comentar RFC's [83] son una serie de documentos publicados por la Agrupación de ingeniería de internet IETF [84] y cubre un amplio rango de temas. Los temas principales son los protocolos de Internet y TCP/IP.

[81] Network Basic Input/Output System, Interfaz que permite aplicaciones de red para establecer sesiones de comunicación entre aplicaciones, enviar y recibir datos y nombrar objetos en la red.
[82] Internet Control Message Protocol
[83] Request for comments.

Los documentos de RFC's son notas de trabajo de la investigación de Internet y el desarrollo comunitario. Un documento en esta serie puede ser en esencia cualquier tema relacionado con la comunicación de computadoras y algún reporte de juntas para la especificación de un estándar.

La mayoría de los RFC's son descripciones de protocolos de red o servicios de red, muchas veces brinda procedimientos detallados y formatos para su implementación. Otros reportes de RFC's son los resultados de estudios políticos o resúmenes del trabajo de comités técnicos o tiendas. Todos los RFC's son considerados dominios públicos a menos que explícitamente se marque lo contrario.

Los RFC's que no se refieren a publicaciones, reciben revisiones técnicas tanto de agrupaciones como de experiencia técnica individual, o bien del editor de RFC a medida que se asignen. La mayoría de los estándares se publican conforme a los RFC's, pero no todos especifican estándares.

Cualquiera puede someter un documento para publicarse como un RFC. Los acatamientos deben ser vía correo electrónico para el Editor de RFC.

Una vez que a la documentación se le asigna un número de RFC y se publica, dicho RFC nunca se vuelve a revisar o es reutilizado con el mismo número. No existe una pregunta de tener la versión más reciente de un RFC en particular. Sin embargo, un protocolo (como el FTP protocolo de transferencia de archivos) puede mejorar y documentarse varias veces en diferentes RFC's. Es muy importante tener el RFC más reciente en un protocolo en particular. El memorándum del "Protocolo de estándares oficial de internet" es la referencia para determinar el RFC correcto como referencia para la especificación actual de cada protocolo.

RPC (Llamada de procedimiento remoto)

El RPC [85] es la habilidad de distribuir partes de un programa a otras computadoras en una red. Tiene la facilidad de intercambiar datos entre computadoras para realizar una ejecución remota transparente para el usuario. Las aplicaciones distribuidas basadas en RPC pueden usar recursos de una red distribuida e incrementar significativamente el poder de computación relacionado con problemas complejos. El RPC es un elemento fundamental de un ambiente distribuido de cómputo. Las llamadas crean un ambiente remoto de cómputo distribuido que es establecido y controlado en el nivel de procedimiento dentro de una aplicación.

La tecnología de RPC simplifica el diseño de sistemas de software distribuido, proporcionando un medio para separar un programa dentro de dos procesos utilizando una interfaz *procedural*. Esto es confiable ya que muchos programas dentro de procesos cooperativos se pueden romper en dos secciones a lo largo de una línea *procedural*, separando un conjunto principal de funciones y algunas adicionales para una aplicación

[84] Internet Engineering Task Force.
[85] Remote Procedure Call

en particular. La **Figura 17** muestra como los RPC's pueden ser utilizados para dividir un programa de usuario y una interfaz de programación aplicada (API) en un programa de cliente y un servidor remoto. El fragmento de RPC cliente y servidor, forma la interfaz de comunicación entre el programa de aplicación y el servidor. El fragmento del cliente codifica sus argumentos y los envía por la red para aparear fragmentos en el servidor. Los fragmentos del servidor extraen fragmentos de la red y computan resultados basados en los argumentos. El fragmento del servidor regresa al cliente los resultados de la computación.

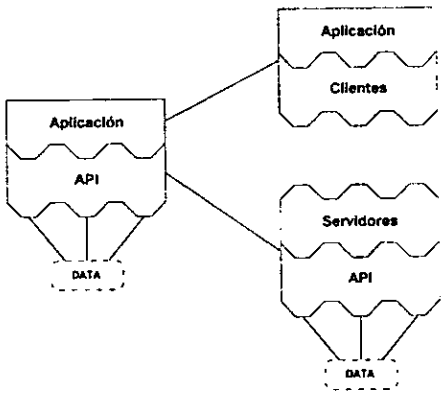


Figura 17. Esquema de un RPC

Los fragmentos de RPC cliente pueden reemplazar a las funciones API invocadas por un programa de aplicación. Una vez que los argumentos han pasado al fragmento del servidor, éste puede comprobar los resultados mediante llamadas a la función API por el cual, el fragmento del cliente es un reemplazo. El fragmento del servidor regresa, como resultado, el valor enviado de la llamada de API. Desde el punto ventajoso del programa de usuario, no existe diferencia entre este tipo de acceso y el accesar un archivo local utilizando la librería estándar de API. Esto se debe a que el fragmento de RPC cliente conserva exactamente la semántica del estándar de API, ya que existe un mapeo de uno-a-uno entre la función de llamada en el fragmento de RPC cliente (es decir, de la librería del cliente); el RPC servidor fragmenta (el protocolo de transmisión) y la implementación estándar de API. Mientras se construye un servidor por este método, se garantiza que no hay cambios semánticos del API, el modo operacional del API cambia radicalmente. Anteriormente el API leía el dato de un archivo, ahora lo lee desde un servidor de datos el cual puede estar localizado en cualquier lugar de una red de computadoras dada. (por ejemplo, el Internet).

Uno de los mayores problemas con la tecnología RPC es que se basa en un paradigma estricto de petición-réplica. Mientras un conjunto de datos trabajan bien en cierto contexto, otros no lo hacen.

Además de la complicación del uso de RPC's, el código de comunicaciones de interprocesos de la red está nominalmente contenida en el servidor RPC. El servidor es responsable de todos los accesos y la seguridad.

XDR (Estándar de representación de datos externos)
El estándar XDR [86] se utiliza para la descripción y codificación de datos así como para transferir datos entre diferentes arquitecturas de computadoras, ha sido utilizada para comunicar datos entre diversas máquinas como la estación de trabajo SUN, VAX, la PC IBM y la CRAY.

XDR se encuentra en el nivel de presentación del modelo de referencia OSI, utiliza una mecanografía implícita y un lenguaje, que no es de programación, solo es para describir formatos de datos confusos de una manera concisa.

Los protocolos como RPC y el NFS [87] (Sistema de archivo de red) utilizan XDR para describir el formato de sus datos (para el caso del NFS, sus servidores son multilínea por lo que múltiples peticiones pueden ser procesadas al mismo tiempo).

El estándar XDR realiza la siguiente actividad: dado un determinado dispositivo, éste deberá codificar los bytes en varias secciones, de tal modo que otros dispositivos de hardware puedan decodificar los bytes sin perder el significado y la información. Por ejemplo, el estándar de Ethernet sugiere que los bytes sean codificados en el estilo " little-indian" o por el primer bit menos significativo.

NCP[88] (Protocolo de núcleo de red)
Este protocolo es un conjunto de núcleos de servicios genéricos que ofrece el sistema operativo de la estación de trabajo por medio de servicios de redes. Está implementado como un *shell* [89] que se sitúa en la parte alta del sistema operativo, redirecciona las peticiones de red al servidor y pasa otras llamadas completas al sistema operativo residente.

Utiliza los servicios que le proporciona IPX [90] (intercambio de paquetes del trabajo internet) y se encuentra en el área de datos del mismo, pero especifica su propio control de sesión, detección de error y retransmisión. Requiere de un reconocedor para cada paquete IPX.

Contiene información tanto para relacionar la petición desde una estación de trabajo o de un servidor como para identificar la conexión de red y los derechos de seguridad asociados a él.

---

[86] External Data Representation Standard
[87] Network File System
[88] Nucleus Control Protocol.
[89] También llamado redirector, es un programa residente siempre en la memoria de la computadora e interpreta órdenes.
[90] Internetwork Packet Exchange.

La estructura del paquete NCP es de la siguiente forma:

- Tipo de petición
- Número de secuencia
- Número de conexión
- Número de tarea
- Reservado
- Código de servicio
- Dato

Únicamente una petición NCP puede ser colocada en cualquier momento dado. El número de secuencia identifica la petición, se incrementa cada que existe una, y permite a la estación de trabajo asociar la respuesta a cada petición. El servicio de código en el paquete NCP identifica el servicio de respuesta por medio de la estación de trabajo desde el servidor.

NFS [91] (Sistemas de archivos de red)
El NFS permite la copia de archivos entre máquinas, registrarse y correr comandos en máquinas remotas, mientras estos comandos de unix remotos hacen procesos sobre más de una máquina fácilmente. El problema es que cada máquina tiene su propio almacenamiento de archivos y por lo tanto, si alguna persona se registra en diferentes máquinas, se tendrán distintos directorios y archivos. Es posible mantener múltiples conjuntos de archivos y programas ocupando RCP, pero esto puede incrementar pérdida de recursos, especialmente en el alcance del problema y el número de máquinas.

Para muchas de las partes interactuando con redes locales, compartir archivos, registrarse en servidores o comunicarse con otras áreas es muy simple. El software de la red es invocado automáticamente y éste es escondido sobre el nivel físico de la red, dando la ilusión de que es un solo sistema. Se puede accesar a un archivo no importando el lugar donde fue solicitado, o mandar mensajes sin importar el origen de la solicitud.

UUCP [92]
Las siglas se basan en el término de Unix-to-Unix CoPy (el comando de copia en Unix es *cp*). Con UUCP es posible conectarse únicamente para enviar o recibir información y con frecuencia es el más eficiente para correo básico y noticias, debido a su proceso no interactivo. El software de UUCP procesa los archivos para desplegarlos, dicho proceso se lleva a cabo cuando una máquina principal envía mensajes a una Mac en forma de archivos.

La tercera implementación de UUCP que salió al mercado se le llamó UUCP/Conexión y su implementación va más allá de solo el código necesario para hablar a un programa remoto UUCP, desagrupa los archivos que entran, los despliega y organiza en varias cajas de correo y en nuevos grupos.

[91] Network File Sytem
[92] Unix-to-Unix Copy

Como su nombre lo indica, básicamente copia archivos de una computadora a otra, así como también realiza determinadas acciones que sean ejecutadas en una computadora remota, realiza copias de trabajos y archivos permitiendo una cooperación entre las máquinas. En el ambiente UUCP el correo es comúnmente transportado con la ejecución del comando **rmail** en una computadora, depositando la dirección y el mensaje a otra computadora y así sucesivamente hasta llegar a la computadora de destino.

UUCP es también un medio de selección para localidades de archivos telefónicos los cuales ofrecen acceso público permitiendo copiar archivos desde un área de archivos públicos. Es ideal para cualquier localidad la cual está corriendo un sistema local de deliberación de correo electrónico.

Para habilitar un nodo UUCP todo lo que se requiere es un módem y una línea telefónica conmutada o dedicada (se puede compartir la línea telefónica que normalmente se utiliza para hablar o para enviar fax), una implementación de trabajo para UUCP y otro nodo UUCP que esté habilitado para distribuir el correo electrónico o mensajes (noticias) y servicio ftp a través de correo electrónico.

IMAP [93] (Protocolo de acceso a mensajes internos)
Es un método de acceso de correo electrónico o una tabla de mensajes que son guardadas sobre un servidor de correo, en otras palabras; éste permite que un programa de e-mail "cliente" pueda accesar mensajes remotos almacenados como si ellos fueran locales, por ejemplo: un e-mail guardado sobre un servidor IMAP que puede ser manipulado de una computadora de casa, una workstation de oficina, etc, sin la necesidad de transferir o recibir mensajes o archivos entre estas computadoras.

Los objetivos principales de IMAP son:

- Compatibilidad con los mensajes de Internet.
- Permite acceso a los mensajes y administración de más de una computadora
- Proporciona soporte de modos de acceso como "online", "offline" y "disconnected"
- Permite el compartimiento de varios correos simultáneamente
- El software del cliente no requiere conocer acerca del formato de almacenamiento de los archivos del servidor.

El protocolo incluye operaciones para creación, borrado, y renombrado de cuadros de correo verificando nuevos mensajes, mensajes que sean removidos, colocar y limpiar banderas de estado, así como buscar y seleccionar atributos de mensajes inesperados.

Existe un protocolo de acceso de configuración aplicada (ACAP) que apoya al IMAP permitiendo la misma localidad de acceso independiente para configurar archivos, direcciones y listas de librerías, que es lo que ofrece IMAP para las cajas de correos.

Como se mencionó anteriormente, existen tres modos diferentes de acceso remoto de mensajes almacenados o (cajas de correo), éstos son: fuera de línea, en línea, y desconectado.

[93] Internal Message Acces Protocol (Está definido por el RFC 1730)

En el modo fuera de línea el programa de correo del cliente, trae mensajes del servidor de correo a la máquina en donde el programa de correo está corriendo, y después borra los mensajes del servidor.

En el modo en línea, los mensajes se quedan en el servidor de correo y son manipulados remotamente por los programas de correo del cliente, posiblemente más de uno al mismo tiempo o en diferentes momentos. En el modo desconectado, el correo del cliente se conecta al correo del servidor, hace una copia de los mensajes seleccionados y después los desconecta del servidor para más tarde volver a conectarlos y resincronizar con el servidor.

En los modos de acceso en línea y desconectado, el correo se queda en el servidor, lo cual es importante cuando la gente utiliza diferentes computadoras en diferentes tiempos para accesar sus mensajes. Estos modos se complementan uno y otro; sin embargo ninguno es compatible con el modo de operación fuera de línea, ya que borra los mensajes del servidor, una vez que fueron copiados al disco de la máquina del cliente.

Existen unas funciones importantes en los modos de acceso "en línea" y "desconectado" para:

manipulación remota de directorios:

- Habilidad para añadir mensajes a los directorios remotos.
- Habilidad para colocar el estado de las banderas de los mensajes estándar y definidos por el usuario
- Apoyo para la actualización simultánea y descubrimiento de directorios compartidos.
- Notificaciones de un nuevo correo

Apoyo de múltiples directorios:

- Habilidad para manipular directorios remotos aparte del INBOX
- Manejo de directorios remotos como crear, borrar, listar, y renombrar
- Soporte para jerarquías de directorios
- Habilidad para el acceso de datos que no son correos electrónicos, por ejemplo, noticias de red y documentos.
  Optimización del rendimiento "en línea"
- Disposición para determinar la estructura de un mensaje sin dejar de llamar mensajes enteros
- Búsqueda de un servidor base y selección para minimizar transferencia de datos

Algunas de estas capacidades son particularmente importantes cuando uno está conectado a un servidor de baja velocidad.

1.8.3 Características de los Protocolos

Control de errores
Cuando un dato se introduce a una computadora por medio del teclado y se presiona una tecla, el código de la palabra resultante es normalmente transmitida a la computadora

serialmente bit a bit, utilizando un UART [94] y una transmisión asíncrona. El programa en la computadora controla la entrada del proceso, después lee y almacena el carácter recibido e inicializa su proceso de salida para desplegarlo en pantalla. Por lo tanto si el carácter desplegado es diferente de la entrada o lo que se desea teclear, entonces el usuario simplemente introduce un control de carácter adecuado, por ejemplo un *delete* o *back space*. Cuando se realiza esta acción, el programa de control descarta el caracter introducido anteriormente y lo quita de la pantalla. De esta forma el usuario está ejecutando una forma manual de control de error.

Un procedimiento similar se utiliza cuando una terminal se conecta a una computadora vía remota, por ejemplo, el PSTN [95] y un módem. A pesar de que cada carácter introducido se despliega directamente en una terminal, se transmite primero a la computadora remota, la cual lee y almacena el carácter y lo retransmite a la terminal que lo desplegará. Si el carácter desplegado es diferente de lo que se tecleó o se desea transmitir, entonces el usuario puede inicializar otra vez la transmisión de un carácter de borrado adecuado. Este modo de control de error se le conoce como verificador de eco.

Por el contrario, cuando una computadora está transfiriendo bloques de caracteres (estructuras[96]) a través de una unión de dato serial a otra computadora, el programa en la computadora receptora que controla el proceso de recepción, debe ejecutar el procedimiento de control de error automáticamente sin ninguna intervención del usuario. Normalmente esto hace que la computadora receptora verifique la estructura recibida para una posible transmisión de errores y posteriormente regresar un mensaje de control corto, tanto para reconocer su mensaje correcto o para pedir que otra copia de la estructura sea enviada. Este tipo de control de error se le conoce como repetición de solicitud automática o ARQ[97].

Existen dos tipos básicos de ARQ:

- **RQ desocupado**

Se utiliza con esquemas de transmisión de datos orientados a carácter (o a byte).

El esquema de control de RQ desocupado ha sido definido para habilitar bloques (estructuras) de control de impresión y formateo de caracteres para ser transferidos confiablemente [98] sobre una unión de dato serial entre un DTE de origen y un DTE de destino.

El protocolo RQ desocupado opera en modo half-duplex desde el origen (expeditor), después de enviar una estructura-I, debe esperar hasta recibir una indicación del destino (receptor) para saber si la estructura fue correctamente recibida o no. Si la trama anterior

[94] Transmisor y Receptor Universal Asincrono.
[95] Red de telefonía pública-conmutada (Public-Switched Telephone Network.)
[96] o trama
[97] Automatic Repeat Request.
[98] Esto es, para una alta probabilidad, sin errores o repetición en la misma secuencia como fue proporcionada.

fue correctamente recibida entonces el origen (expeditor) envía la siguiente trama y si no fue correcta retransmite una copia de la estructura anterior.

- **RQ continuo**

Emplea tanto una repetición selectiva o una estrategia de retransmisión *go-back-N*, y utiliza principalmente esquemas de transmisión orientado a bit.

Con el esquema RQ continuo, las tramas corrompidas se descartan y las peticiones de retransmisión son enviadas únicamente después de la siguiente trama libre de errores

Por lo tanto, aunque los RQ desocupados sean reemplazados en muchas aplicaciones por los más eficientes esquemas RQ continuos, existen muchos protocolos de datos ligados en uso basados en los RQ desocupados.

Manejo del enlace de datos

Para un enlace entre una terminal y una computadora con una separación relativa (por ejemplo 20 m.), el manejo de enlace de datos se puede llevar a cabo por intercambio de señales sobre líneas asociadas adicionales con la interfaz física. A esto se le conoce como procedimiento *handshake* [99]. Por ejemplo, si un usuario desea abrir un diálogo, primero al encender la terminal, en una de las líneas de control se indica a la computadora que la terminal está lista para enviar caracteres [100]. La terminal debe entonces esperar hasta que la computadora responda, enviando por línea de control correspondiente, una indicación de que está lista para recibir caracteres, posteriormente el intercambio de caracteres podrá comenzar.

Cuando los dispositivos que se están comunicando son computadoras y están transfiriendo estructuras a través de un enlace de datos, dicho enlace se establece por medio del protocolo de nivel de enlace, dentro de cada computadora intercambiando un conjunto de control y supervisión de estructuras. En este ejemplo, el enlace se estableció en el momento en que el usuario encendió la terminal; sin embargo, en el caso de la unión de computadora-a-computadora, el montaje del enlace es normalmente iniciada por el nivel más alto de software (por ejemplo, un programa de aplicación) en una de las computadoras, señalando el software de comunicación en el que desea abrir un diálogo con una computadora remota.

1.8.4. Unión de datos con los protocolos.

Protocolos de enlaces de datos

Los protocolos de enlace de datos se encargan de transmitir los datos libres de errores. Existen varios tipos de protocolos que permiten la comunicación libre de errores, esta diversidad, es condicionada por las características propias de la red.

[99] asociado.
[100] Terminal de datos lista.

Los protocolos de enlace, trabajan sobre los extremos de la comunicación (origen-destino), independientemente si la información, tuvo que haber pasado por varios dispositivos o haber tenido una línea directa de comunicación. En la **Figura 18**, se muestran dos formas de comunicación entre dos computadoras.

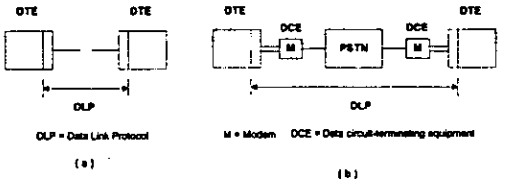


Figura 18. Comunicación Punto a Punto

Existe una gran diversidad de protocolos, pero todos tienen un principio en común, todos están basados sobre protocolos orientados a caracter (RQ Desocupados) o protocolos orientados a bit (RQ ocupados).

El tipo de protocolo de enlace esta en función de la separación física de la comunicación entre dos computadoras, y la velocidad con que trabaja.

Para redes de baja velocidad y de distancias cortas, ocupan protocolos como el Kermit y X-Módem. Estos protocolos están basados sobre RQ desocupados. Básicamente para arquitecturas punto a punto.

Para redes de alta velocidad y de grandes distancias, ocupan protocolos como el HDLC[101], este protocolo esta basado sobre RQ ocupados. Las cuales pueden ocupar como medio de transmisión los satélites.

Algunas arquitecturas de redes requieren que el modo de transmisión sea en una sola dirección como se muestra en la **Figura 19**, esta arquitectura es conocida como multipunto. La computadora central es la que administra y controla el medio de transmisión de la red.

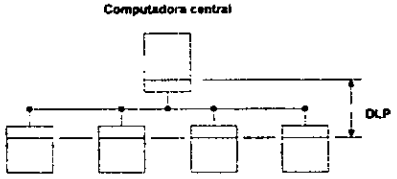


Figura 19. Enlace Multipunto

[101] Control de enlace de datos de alto nivel

Otras redes requieren que el medio de transmisión sea compartido al mismo tiempo, estas arquitecturas están basadas sobre protocolos RQ desocupados, conocidos como BSC [102].

El X.25 es un protocolo de enlace para redes de área amplia, el cual está basado sobre el HDLC y es conocido como LAPB[103], este protocolo es enlace entre el DTE y DCE. El ISDN al igual que el X.25, trabaja sobre redes de área amplia, una vez que la red hace conexión, este trabaja como un protocolo de enlace punto a punto. Este ocupa un protocolo de enlace conocido como LAPD, que es muy parecido al HDLC, como se muestra en la **Figura 20**.

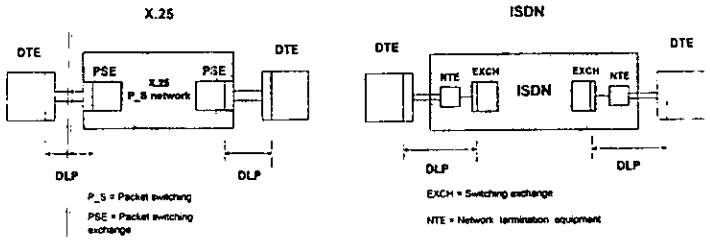


Figura 20. Redes de Area extendida

Para redes LAN's, se ocupan protocolos de enlace conocidos como LLC[104]. Este protocolo es una subclase del HDLC.

Protocolos orientados a carácter

Los protocolos orientados a carácter, se encuentran en arquitecturas punto a punto y multipunto, estos son caracterizados por el control de selección de carácter en varias funciones de control, asociadas con el control de enlace, inicio y fin de paquetes, control de errores y transparencia de datos.

Existen tres tipos de protocolos orientados a caracter, cada uno de ellos es determinado por el tipo de transmisión, que son:

- **Protocolos simplex.**

Este tipo de protocolos trabajan en líneas que permiten la comunicación en una sola dirección. La topología que hace uso de este tipo de protocolo son las de punto a punto, el protocolo mas representativo es el Kermit.

El Kermit contiene un conjunto de comandos que permiten el flujo de información, por lo que es necesario que el programa de Kermit este corriendo en las computadoras que se van a comunicar entre si. Si se esta haciendo uso de módems es necesario que uno de los

[102] Binary Synchronous Control.
[103] Link Access Procedure, balanced
[104] Logical Link Control.

módems este en modo fuente y el otro en modo destino. Ambos módems deben estar corriendo a la misma velocidad de baudios. Para el proceso de transmisión es necesario que los usuarios sigan ciertos pasos para el éxito de transmisión, que son los siguientes:

1. Ambos usuarios deben correr el comando CONNECT.
2. El usuario que recibe el archivo debe correr el comando RECEIVE y
3. El usuario que manda el archivo debe correr el comando SEND seguido con el nombre del archivo.
4. Después del proceso de transmisión es necesario que ambos usuarios corran el comando EXIT.

- **Protocolos half duplex.**
  - Los protocolos half duplex operan en líneas que funcionan en modo bilateral alternado, sobre redes tanto multipunto como punto a punto. Estos protocolos soportan tres conjuntos de códigos de caracteres: ASCII, EBCDIC y el transcódigo de 6 bits de IBM. Normalmente este tipo de protocolos trabajan sobre transmisión síncrona.

- **Protocolos dúplex.**

Los protocolos dúplex trabajan en líneas que permiten la comunicación en forma bilateral[105]. El protocolo más representativo es el que se ocupa en la red ARPANET, este opera en redes punto a punto. El flujo de paquetes de información a través de la línea de enlace interna de la red es mediante IMPs[106] (nodos de conmutación de la red ARPAnet). Este protocolo de enlace hace uso del concepto de protocolos de RQ continuos. En enlaces terrestres multiplexa sobre ocho canales, independientes de manera lógica sobre cada línea física, y para el caso de enlaces por satélite multiplexa 16 canales. Cada uno de estos canales lógicos funcionan mediante el concepto de parada y espera.

Protocolos orientados a bit

Todos los protocolos definen un bit, para indicar el inicio y el fin de un bloque. Existen tres métodos que realizan la señalización de inicio y fin de una estructura, conocidos como **bloques delimitadores**, que son:

- Bits exclusivos de inicio y fin de una estructura, conocidos como banderas (01111110), junto con un bit cero de inserción.
- Un bit exclusivo de inicio de estructura, conocido como inicio delimitador (10101011), y la longitud del bloque (bytes) en la cabeza de la estructura.
- Bits exclusivos de inicio y fin de una estructura, incluyendo un bit de violación de codificación.

[105] Simultánea.

[106] Internet Messages Processor – Procesadores de Mensajes de Internet

Todos los protocolos orientados a bit son derivados del HDLC.

HDLC

HDLC soporta enlaces punto a punto y multipunto, opera en líneas que permiten la comunicación en forma bilateral simultáneamente.

HDLC puede ser ocupado en diferentes configuraciones de red. Estas son mostradas en la **Figura 21**. Los bloques enviados de la estación primaria a la secundaria (origen y destino respectivamente) son conocidos como comandos y de la secundaria a la primaria respuestas. Las configuraciones (a) y (b) tienen una sola estación primaria y son conocidas como configuraciones desbalanceadas, (c) tienen dos estaciones primarias y es conocida como configuración balanceada. Las estaciones de la tercera configuración contienen los conceptos de la primaria y la secundaria y son conocidas como estaciones combinadas.

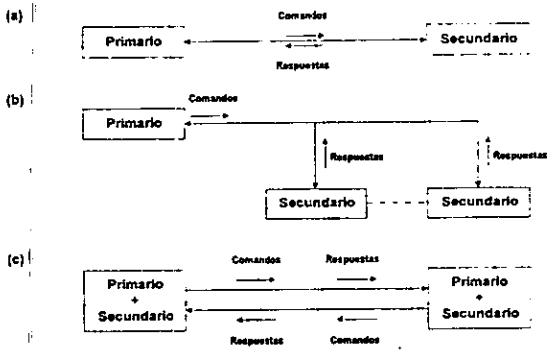


Figura 21. Diferentes tipos de configuraciones de red

HDLC tiene tres modos de operación:

1. NRM [107]: es ocupado en configuraciones desbalanceadas. En este modo de operación, las estaciones secundarias solo pueden transmitir cuando es especificado por la estación primaria. El enlace puede ser punto a punto o multipunto.
2. ARM [108]: es ocupado también en configuraciones desbalanceadas. Permite a las estaciones secundarias iniciar transmisión sin el permiso de la estación primaria. Este es normalmente ocupado en configuraciones punto a punto y en enlaces dúplex, y permite enviar estructuras asíncronamente con respecto a la estación primaria.
3. ABM [109]: este es ocupado en configuraciones balanceadas. Soporta enlaces dúplex punto a punto. Cada estación tiene el mismo nivel, además de manejar los conceptos de primario y secundario.

[107] Normal Response Mode.
[108] Asynchronous Response Mode.
[109] Asynchronous Balanced Mode.

HDLC opera con tres clases de estructuras, que son:

1. Estructuras inumeradas: Estas son ocupadas como funciones de levantamiento y desconexión.
2. Estructuras de información: Estos llevan los datos y normalmente se les llama estructuras-I, las cuales pueden ser ocupados como reconocimiento de dirección cuando el enlace esta operando en los modos ABM y ARM.
3. Estructuras supervisoras: estas son ocupadas para control de errores y de flujo, y contendrán el número de envío y de acuse.

1.9. Sistemas Operativos

UNIX

UNIX es un sistema interactivo de tiempo compartido; es decir, un sistema que ofrece grandes facilidades para permitir que muchos usuarios trabajen juntos y compartan información de una manera controlada. Como en la mayoría de los objetos interesantes, UNIX no es tan fácil de definir.

En el nivel más bajo se encuentra el kernel o núcleo de un sistema operativo; un conjunto de rutinas de supervisión diseñado por Ken Thompson y sus colaboradores de los laboratorios Bell a fines de la década de los 60, para controlar y coordinar las muchas actividades de un sistema multiusuario. UNIX tiene un sistema de archivos que organiza sus dispositivos, directorios y archivos de datos; en su siguiente nivel incluye un shell[110], que es un programa especial para interceder entre el usuario y la computadora, que interpreta comandos y lo protege del kernel.

Las llamadas al sistema UNIX, con las cuales los programas solicitan los servicios al kernel, se definen como funciones en C. Aunque estas llamadas al sistema conciernen principalmente a los programadores. En ocasiones, la única forma de comprender cómo funciona un programa al nivel de usuario es conociendo lo que hacen las llamadas subyacentes al sistema.

La mayor parte del sistema UNIX está escrito en C. Las organizaciones con licencias de los programas fuentes de UNIX pueden modificar el comportamiento del sistema operativo, alterando y recompilando los programas fuente.

El sistema representativo actual es una estación de trabajo con pantalla de alta definición que opera un sistema de ventanas y participa activamente en una extensa red de computadoras.

UNIX es un sistema operativo 100% multitarea. Esto significa que el usuario no tiene que esperar a terminar de correr un proceso para iniciar otro como en el caso de una

[110] [110] También llamado redirector, es un programa residente siempre en la memoria de la computadora e interpreta órdenes.

computadora personal, sino que es factible abrir más procesos y que al mismo tiempo se ejecuten otras tareas.

El administrador de un sistema UNIX puede ajustar las características operativas del sistema mediante la configuración del kernel. Esta configuración comprende principalmente el ajuste de ciertos parámetros internos y la preparación de manejadores que controlan los dispositivos conectados a la computadora. La estructura del kernel es inalterable, el hacerlo equivale a reescribir el sistema UNIX.

Características especiales

El soporte para las redes de trabajo que usa UNIX, siempre ha sido una de las fortalezas del sistema. Desde sus capacidades básicas de los protocolos UUCP hasta el TCP/IP, el NFS[111] y RFS[112], UNIX no cuenta con una variedad de formas para compartir información y recursos entre los sistemas. Además de las redes locales el sistema UNIX excede amplias áreas de las redes. Como ejemplo de ello tenemos la red Internet que está basada en computadora con sistema UNIX. El UUCP es una colección de programas diseñados para permitir a los sistemas UNIX intercambiar información, principalmente usando líneas telefónicas y empleando módems. Un número de archivos y programas componen el paquete UUCP, los cuales incluyen tres capacidades principales: transferencia de archivos remotos, ejecución de archivos remotos, transferencia de correo entre sistema. La habilidad para la ejecución de programas en un sistema remoto está estrictamente controlado por razones de seguridad.

LINUX

Linux es un sistema operativo, clon de Unix en 32 bits, para plataformas Intel x86, DEC Alpha, SUN Sparc, Motorola 68k, etc. Es completamente gratuito y se distribuye con su código fuente.

Además de tener todas las ventajas propias de Unix, Linux es muy rápido y no necesita demasiada memoria. Linux no tiene nada que envidiarle a la mayoría de los UNIX comerciales que hay en el mercado.

Linux es desarrollado por un grupo de programadores a través de Internet, tiene mucho software, pero en su gran mayoría está orientado a redes.

Estrictamente hablando, Linux es un kernel, un archivo de más o menos medio Mb. Sin embargo cuando uno habla de Linux se refiere generalmente a todas las utilidades que son necesarias para usar una computadora con este kernel.

[111] Explicados en el capitulo 1.7.1
[112] Remote File System (otra manera de compartir archivos en UNIX)

El kernel de Linux consiste en diferentes partes: manejo de procesos, de memoria, dispositivos manejadores de hardware, manejadores de sistemas de archivo, de red y de otros bits y piezas.

Probablemente la parte más importante del kernel (nada trabaja sin él) es el manejo de memoria y de proceso. El manejo de memoria cuida de las asignaciones de área de memoria y el espacio de área de swap para los procesos, las partes del kernel y para el "buffer cache". El proceso de manejadores crea procesos e implementa la multitareas mediante el switcheo de procesos activos en el procesador.

Tanto UNIX como Linux no incorporan las interfaces de usuario en el kernel; más bien, dejan que sea implementado por el programa de nivel de usuario. Esto se aplica tanto para modo texto como para el ambiente gráfico.

El ambiente gráfico principalmente utilizado por Linux se le llama *"X Window System"* (X como nombre reducido). X tampoco implementa una interfaz de usuario; únicamente implementa un sistema de ventana, es decir, herramientas con las cuales una interfaz de usuario puede ser implementada.

Algunas de las características más importantes que hacen de Linux una muy aceptable elección son:

- ✓ Multitarea
- ✓ Multiusuario
- ✓ Multiplataforma (x86, Alpha, Sparc, Amiga)
- ✓ Estable
- ✓ 32 bits, protección de memoria, modelo plano de memoria.
- ✓ Soporte de hardware bastante amplio.
- ✓ Soporte de múltiples procesadores.
- ✓ Compatibilidad con la gran mayoría de redes en el mercado.
- ✓ Compatible con TCP/IP (cliente y servidor NFS)

Entre otras características, también existe la opción de un Proxy[113] transparente, el cual permite que una máquina con Linux funcione como un ruteador para intervenir en las conexiones siguiendo un determinado patrón y hacer que otras computadoras se conecten con un proceso local a éste y puedan, a su vez, accesar el WWW de manera totalmente transparente para el usuario.

Sistema operativo MS-DOS

Antecedentes históricos

MS-DOS[114] significa MicroSoft sistema operativo de disco, y fue realizado por Microsoft para computadoras personales, y como consecuencia un sistema monousuario y monotarea, basado en un procesador Intel. El DOS básico o primitivo no contenía

[113] Se describirá en el capitulo 2.
[114] Disk Operating System

gráficos, no podía conectarse a una red de trabajo, y por supuesto no tenía la opción de aplicaciones virtuales.

Es introducido por IBM en 1981, en 1983 surge la segunda versión con un sistema de gestión de archivos (aparición de subdirectorios), disco de 10Mb, instalación de dispositivos de dirección, en 1984 surge la versión 3.0 con un disco de 20Mb, un disco flexible 5.25" de 1.4Mb, la versión 3.1 ya permitía la conexión de computadoras personales en redes de área local y su utilización como servidores en entornos multiusuario. A finales de 1984 es el primer paso para soportar una red de trabajo, en 1986 surge la versión con soporte de token ring. En 1988 se presentan considerables particiones en disco, una utilidad para el manejo del sistema operativo que fue el DOS Shell, en 1991 se presentan avances como un nuevo DOS shell, base para memoria extendida y soporte para MS Windows. Posteriormente apareció la versión 6.22, que es presentada con mayor versatilidad para los usuarios.

Estructura del sistema Operativo

En la **Figura 22** se muestra la estructura del sistema operativo:

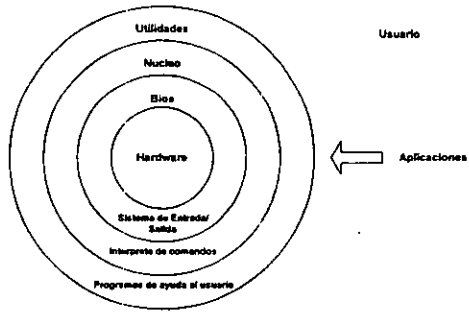


Figura 22. Estructura del sistema operativo DOS

Como puede verse en primer término, rodeando al hardware se encuentra una parte software denominada BIOS (Basic Input Output System) residente en memoria ROM (Read Only Memory), cuyas misiones son las siguientes:

- Realizar un test de todo el equipo en cada proceso de arranque donde se examinan todos los elementos conectados y en qué estado se encuentran.
- Hacer de interfaz entre el software de los niveles superiores y el hardware a través de una serie de rutinas, cada una de ellas con una función específica.

El siguiente nivel corresponde al núcleo del sistema operativo, que permanece constantemente en memoria desde que se enciende el equipo. Está compuesto por el programa intérprete de comandos (COMMAND.COM) que lleva consigo la carga de una serie de comandos residentes permanentes en memoria y dos archivos denominados ocultos, pues no aparecen en el directorio del disco que los contiene pero que se

encuentran presentes. Estos archivos tienen rutinas que permiten ampliar y actualizar (evolución de sus diversas versiones) las rutinas de la ROM BIOS.

Conceptos básicos

Al tratarse de un sistema monousuario y monotarea, el procesador en cada momento está dedicado en exclusivo a la ejecución de un proceso. Por tanto, la planificación del procesador es simple, se dedicará al único proceso activo que puede existir en un momento dado.

El sistema operativo DOS, al igual que la mayoría de los sistemas actuales, cuenta con un conjunto de órdenes para mantener una estructura multinivel de directorios en forma de árbol con la cual se realiza una gestión y organización de archivos muy eficiente.

El intérprete de comandos del DOS es un programa denominado COMMAND.COM que realiza funciones de interfaz entre el usuario y la computadora. Se encarga de mantener el indicador del DOS (promt) y está en espera de recibir una orden para iniciar el proceso que lleve a su resolución, para nuevamente regresar al estado inicial de espera.

Cuando un usuario está bajo el control del intérprete de comandos, puede ejecutar órdenes o programas ejecutables de dos formas:

- Modo interactivo: Con el cual el comando o el programa se ejecuta en ese momento
- Proceso por lotes: Se reúnen un conjunto de comandos y programas que deben ejecutarse uno tras otro en un archivo (extensión BAT) y el procesador cuando recibe la orden así lo hace. Este tipo de procesos es muy flexible ya que admite condicionamientos para algunos de sus elementos, repeticiones y una gran variedad de combinaciones posibles.

Por otra parte, existe un archivo por lotes característico en el DOS cuya misión es la de inicializar el entorno del equipo e incluir todo aquello que se desea ejecutar al arrancar el sistema (AUTOEXEC.BAT).

Además todos estos sistemas operativos DOS ofrecen una serie de herramientas para facilitar al usuario una serie de operaciones básicas: como editor de texto, ordenación de archivos, copias de seguridad, depurador, intérprete del lenguaje BASIC, configuración del teclado, entre otros.

MS-DOS y las redes de computadoras

Por otra parte la capacidad del MS-DOS para apoyar directamente las capacidades de la red como un servidor es limitado. Las estaciones de trabajo que usa este sistema operativo, son usados frecuentemente como estaciones de trabajo LAN, y un gran número de compañías han desarrollado redes que usan estaciones de trabajo con sistema operativo DOS.

Empezando con la versión 3.1, microsoft hizo provisiones internas al MS-DOS para permitir el apoyo de las redes. Al mismo tiempo que se hicieron estas adiciones al sistema operativo DOS, IBM introdujo su adaptador original LAN que es la tarjeta de red para equipo IBM, diseñado por Sytek Inc., contiene 2 Mbps para LAN's basados en el CSMA/CD, ahora equipado con el modelo IEEE802.3 estándar. La tarjeta de la red usa una memoria de sólo lectura que contiene un sistema de entrada salida básica de red, es decir el NETBios.

Aunque las ventajas en el caso del DOS son numerosas, se debe tener cuidado al escogerlo como un sistema operativo en una estación de trabajo. El DOS tiene una serie de errores serios en una red de trabajo: Envío o paso de paquetes, tarea personal por diseño, límites de segmentos de 64K.

Novell netware

Novell está considerado como el líder en la industria de NOS [115] (Sistema operativo de red) con más de una década de experiencia en el ambiente de cómputo cliente-servidor. Novell netware es un medio en el cual los usuarios conectados a la red pueden compartir archivos en un modo consistente y lógico. Netware corre tanto en Macintosh como en PC's permitiendo a los usuarios en un departamento compartir archivos e impresoras entre las diferentes plataformas de cómputo.

La característica más importante es en el NDS[116] (servicios de directorio de red), el cual evita la necesidad de que un usuario entre múltiples ocasiones para ganar acceso a fuentes que pueden ser físicamente localizadas en otras redes. Netware ofrece mayor facilidad en la instalación, manejo centralizado, alta seguridad, licencia adicional, mejora en ruteo y soporte de WAN, comparte un CD_ROM y un mensaje integrado.

Requerimientos mínimos del sistema:

- CPU 80386 DX o mayor.
- 8 MB en RAM
- Disco duro de por lo menos 55 Mb libres para Netware 4.1 y 25 Mb para documentación adicional en línea.
- Una tarjeta de red (preferiblemente de 32 bits)
- Drive para CD-ROM.

Cada individuo que utilice Netware deberá usar un login y un password. Ésta es una información particular del usuario y le permite accesar su drive personal así como al resto de los drives. El usuario deberá teclear dichas claves al iniciar su computadora y cuando desee compartir archivos con otros o bien utilizar otros recursos.

Novell Netware tiene en cuenta el servicio de archivo. Esto permite a todo usuario que haya entrado con su clave, el uso del software que no visualice físicamente en su sistema. Por ejemplo, un usuario que no tiene Word Perfect en su sistema puede utilizar la copia

[115] Netware Operating System.
[116] Netware Directory Services.

que se encuentra en el archivo del servidor de Netware, de cualquier modo el paquete correrá como si se encontrara en su sistema.

Para redes de área amplia

La introducción del protocolo de servicios ligados de Netware (NLSP[117]) se traduce dentro de una mayor comunicación eficiente entre los servidores de Netware sobre una WAN. Los protocolos como IPX[118] , RIP[119] y SAP[120] se distinguían por saturar anchos de banda disponibles haciendo uso de los servidores para manifestar su presencia regularmente. NLSP permite a los usuarios decidir con qué frecuencia los servidores se actualizan uno a otro y se tiene menos tráfico de información.

Soporte de protocolos de UNIX:

Los servicios del sistema de archivo para red de NLM utilizan completamente NDS (servicios de directorio de netware) y no requiere de una emulación. También tiene incluido un DNS [121] (servicio de nombramiento de dominio) para facilidades del NDS en el servidor, el cual permite al usuario tener un solo log-in y un password, a través de los servidores Netware y Unix-básico.

Windows NT

Microsoft Windows NT es un poderoso y avanzado sistema operativo de 32 bits, multitarea que lo soporta Intel (86) y los procesadores RISC, proporciona soporte para procesadores simétricos múltiples. Windows NT para estaciones de trabajo, es el sistema operativo que proporciona el poder de una estación de trabajo con la facilidad de uso, productividad y compatibilidad de una computadora personal, proporciona una red que sea fácil de configurar, manejar y controlar.

Windows NT tiene una interfaz de usuario de gráficos de Windows, red integrada y herramienta para trabajo en grupo, con correo en grupo y aplicaciones de programas, es compatible con Windows, MS-DOS, y OS/2.

Beneficios:

- Proporciona un sistema de integridad, acceso a gran capacidad de memoria y disco, seguridad y protección requerida por usuarios con grandes aplicaciones.
- Ofrece adelantos en el funcionamiento, conectividad y la disponibilidad de otras aplicaciones de servidor de 32 bits que auxilian a usuarios que minimizan sus sistemas al cliente/servidor o viceversa.

[117] Netware Link Services Protocol.
[118] Internet Packet Exchange.
[119] Routing Information Protocol.
[120] Service Access Point – Punto de Acceso de Servicio – Localización en la cual dos aplicaciones pueden intercambiar información
[121] Domain Name Service.

- Soporta plataforma extendida para PowerPC, Servidor Alpha 2100 5/250 y sistemas de estación Alfa 600.
- Proporciona avances en la configuración, en el comando prompt, en controles comunes de Windows 95 y ayuda.

Requerimientos	Para estaciones de trabajo.	Para servidor
PC	386/25 o mayor	386/25 o mayor
Memoria	12 MB (16 MB para RISC)	16 MB
Manejadores de disco	CD-ROM y 3.5	CD-ROM y 3.5
Espacio disco duro	90 MB disponibles (120 para RISC)	90 MB disponibles (120 para RISC)
Adaptador de video	VGA, SPVGA o alta resolución	VGA, SPVGA o alta resolución
Tarjeta	Red	Red
Mouse	Microsoft o compatible	Microsoft o compatible

Tabla 14. Requerimientos mínimos para el sistema Windows NT 3.51.

Comparación de sistemas operativos: Windows NT vs UNIX

Algunas industrias analistas y consultantes de la computación han discutido que el sistema operativo Windows NT no corre bien del todo en sistemas multiproceso, dejando a UNIX como la única opción de sistema operativo para sistemas multiproceso. Esto se ha debido a la confusión en la licencia de Windows NT estándar, la carencia de productos de software de aplicación optimizado para utilizarse con Windows NT y la percepción de la ejecución máxima de Windows NT en sistemas multiproceso.

Microsoft diseñó Windows NT para utilizarse en sistemas con más de 32 procesos y licencias Windows NT para utilizarse en sistemas multiproceso. Las evaluaciones demuestran que la "escalabilidad" de Windows NT en grandes sistemas multiproceso pueden ser probadas cuando se utilizan sistemas y software optimizado para Windows NT.

El funcionamiento ganado de fuentes adicionales para un sistema de cómputo define la escala del sistema.

1.10 Equipos y dispositivos

La conectividad es la capacidad de conectar computadoras o equipos de igual o diferente naturaleza. Existen diversas maneras de conectar equipos entre sí y para aquellas que involucran una o más redes, se tienen las siguientes posibilidades:

La conectividad puede entrelazar dos redes que se encuentran a distancias cortas, por lo que es factible usar cualquier tipo de cable para el logro del transporte de la información. A distancias grandes se debe apoyar la comunicación con *módems*.

Transceivers

Es un dispositivo físico que conecta la interfaz de la computadora principal (host) a Ethernet. Este dispositivo usualmente se encuentra integrada a la tarjeta Ethernet, esta opción es se presenta únicamente en aquellas tarjetas que pueden conmutar entre cable grueso y delgado para Ethernet a través de un software.

Repetidores

Los repetidores son dispositivos diseñados con el fin de extender la longitud de la red más allá de los 500 mts máximos de segmento de cable coaxial, pueden ser tarjetas internas o cajas externas. Haciendo una comparación con el modelo OSI, el repetidor opera en el nivel físico (nivel 1).

Existen dos tipos de repetidores: ***local*** y ***remoto***.

El repetidor ***local*** es usado para conectar dos segmentos de cable separados por una distancia máxima de 100 mts, mientras que el repetidor ***remoto*** (usando fibra óptica) conecta segmentos separados hasta 1000 mts y sólo se puede usar un repetidor remoto en una red.

Puentes

Un puente consiste en enlazar dos o más redes locales. Para tal efecto, se utiliza el servidor o alguna estación de trabajo que actúe como puente entre ambas redes. Los puentes pueden ser internos o externos, entre redes del mismo tipo o de diferentes características, e incluso pueden permitir "platicar" con protocolos de comunicaciones diferentes. Este último sería el caso cuando se conecta una minicomputadora directamente a la red.

Los puentes son dispositivos de interconexión de redes locales para distintos protocolos y arquitecturas, como Ethernet, Token Ring y X.25 entre otras. Normalmente se instalan en una PC de la red, y su tarea es leer y filtrar todos los paquetes y tramas, permitiendo así el paso de aquellas que la dirección destino pertenezca a la red local, de otra forma la envía hacia otra red. Se utilizan para conectar dos o más redes de trabajo. Son dispositivos que se opera al nivel de enlace de datos (nivel 2), por lo que aparte de permitir conectar segmentos de cable de red, también permiten conectar dos o más redes locales o remotas en una red lógica simple y particionar una red de área local simple en múltiples subredes.

Los puentes leen la dirección fuente de cada paquete Ethernet y la utilizan para construir su tabla de direcciones y rutas de las diversas redes interconectadas. Después, leen la dirección destino para determinar a que red enviarla.

Ruteadores

Los ruteadores sirven para la interconexión de redes locales, pero con capacidad para decidir la mejor ruta puesto que son multiprotocolarios, es decir estos acoplan a diferentes

topologías y distribuyen el tráfico entre redes. Para su mejor funcionamiento utilizan métodos de compresión de datos.

El ruteador esta programado para consultar en sus tablas y analizar el estado de la comunicación para determinar como y por donde enviar el paquete IP.

Los puentes y ruteadores funcionan de manera similar a las oficinas de correo. Se guían por información detallada para distinguir el remitente y destinatario geográficamente.

Los puentes y ruteadores son el corazón de la conectividad entre redes. Estos tienen la capacidad para reconocer aquellos paquetes que deben salir de una red hacia otra y de traducir datos de otro protocolo diferente al utilizado en la red, todo esto es transparente al usuario quien sólo se limita a mandar a imprimir al plotter instalado en otra oficina desde Ethernet a Token Ring.

El Router tiene como misión principal permitir a los usuarios hacer uso de las comunicaciones sobre la red telefónica conmutada, usando una amplia gama de productos de comunicaciones.

- El SNA permite conectar la red con sistemas IBM que lo soporten.
- El X.25 es una extensión del Router que incluye además la posibilidad de usar redes de conmutación de paquetes que soporten protocolos X.25 para establecer el intercambio de información con otros procesadores.

Para llevar a cabo la comunicación en las redes es necesario utilizar los puentes y ruteadores.

Gateways

Un *gateway* es un fragmento de software que comprende a dos o más protocolos y puede traducir datos de un protocolo a otro, es decir, comunica a una red local con otro ambiente, a través de una sola línea. Lo anterior hace posible que desde cualquier estación de trabajo de la red, se pueda accesar otro ambiente, que regularmente es un equipo mayor.

Existe también la posibilidad de conectar redes Ethernet a otros tipos de redes, tanto locales como de área extendida, esto se puede conseguir por medio de gateways.

Los principales tipos son:

- Ruteadores
- SNA
- X.25
- Para concentradores 3270

Controladores

El controlador posee el conjunto de funciones y algoritmos necesarios para dirigir el acceso al canal común. Aquí se realizan prácticamente todas las acciones a desarrollar por el nivel físico de esta arquitectura.

El controlador normalmente, suele ser una tarjeta de circuito impreso que trabaja conjuntamente con la estación conectada a la red y que ejerce de interfaz con la conexión de la misma.

La combinación de redes locales con Puentes y Gateways, proporciona la posibilidad de crear conjuntos de redes cuya extensión geográfica es ilimitada, y cuya capacidad permite la coordinación de cientos, quizás miles de equipos de distintas características.

CAPÍTULO 2

2. Introducción a las Redes de Datos

2.1 Internet

Internet nació en DARPA[1] (Agencia de Proyectos de Investigación Avanzada) a mediados de los setentas, utilizando una tecnología de intercambio de paquetes. Con el advenimiento de la Internet, nació también TCP/IP.

La Internet ha demostrado la viabilidad de interconectar una amplia variedad de tecnologías de red. Además de abarcar cientos de redes localizadas a lo largo de E.U., Europa y América Latina.

La tecnología Internet constituye lo que se conoce como un sistema abierto. Este hecho ha contribuido de manera notable aumentar la popularidad de TCP/IP, ya que a diferencia de los sistemas de comunicación comerciales, sus especificaciones son públicas y cualquier persona puede obtenerlas sin costo alguno. De esta forma, es posible construir el software necesario para comunicarse a través de una Internet a costos muy bajos. Algo más que se debe resaltar, es que toda esta tecnología ha sido diseñada para soportar una comunicación entre máquinas de diversas arquitectura de hardware y para adaptarse a diversos sistemas operativos.

La organización que se encarga de manejar los detalles administrativos de la Internet, además de distribuir la documentación sobre el trabajo hecho en ella es el NIC[2] (Centro de Información de Red). Las proposiciones para nuevos protocolos y TCP/IP aparecen en una serie de reportes técnicos denominados RFC[3] (Peticiones de Internet para Comentarios).

2.1.1 Arquitectura de la Internet

La interconexión de las redes físicas que forman una Internet se realiza mediante computadoras denominadas gateways. Estos dispositivos cuentan con conexiones directas a varias redes y se encargan de transferir paquetes de información entre las mismas.

En la Figura 1 se muestra como un gateway G se encarga de conectar dos redes. La función del gateway consiste en capturar los paquetes destinados a nodos que se encuentren en la misma red en le cual se originaron; una vez capturados, los paquetes serán retransmitidos en la red correcta.

[1] Defense Advanced Research Proyect Agency
[2] Network Information Center
[3] Internet Request for Comments

2.1.3 Representación decimal de direcciones IP

Aunque las direcciones IP son enteros de 32 bits, existe una notación especial que se utiliza para especificarlas. En esta representación, llamada *notación decimal puntual*, una dirección se denota con cuatro enteros decimales separados por puntos, en donde cada entero representa el valor de un byte de la dirección IP. Por ejemplo, una dirección como la siguiente:

10000100 11111000 00110110 000000010

se representa como:

132.248.54.2

Existen ciertos valores para las direcciones IP que se utilizan con propósitos especiales. Si uno de los identificadores tiene como valor cero, este se refiere al mismo objeto que emite el mensaje (red o nodo). Por ejemplo, para el nodo 132.248.54.1, la dirección 132.248.0.0 se refiere a él mismo; mientras que la dirección 0.0.54.2 se refiere al nodo 54.2 dentro de la misma red.

Existe otra dirección especial, llamada *dirección broadcast* que se utiliza para hacer referencia a todos los nodos dentro de la red; esta dirección se especifica encendiendo todos los bits del identificador de nodo. Por ejemplo, la dirección 132.248.255.255 ve a todos los nodos de la red 132.248.

Las direcciones cuyo primer byte es 127 son conocidas como direcciones de *loopback*. Cuando se utiliza este tipo de direcciones, el software de protocolo regresa los datos al nodo emisor sin transferirlos a la red, la cual puede ser utilizado para realizar pruebas o intercomunicar procesos dentro de la misma máquina. Las direcciones de loopback más comunes son 127.0.0.0. y 127.0.0.1.

2.2 Asignación de direcciones IP

Para asegurar que las direcciones de una red sean únicas, existe una autoridad central llamada NIC[5] (Centro de Información de Red), la cual se encarga únicamente de asignar las direcciones de red y delega la responsabilidad de establecer las direcciones de los nodos del organismo encargado de la red en cuestión.

Con el fin de ayudar a controlar la asignación de direcciones IP a las organizaciones que no estaban conectadas a Internet, se reservo una serie de direcciones privadas de red. Esto se logro en la RFC 1,597.

[5] Network Information Center

2.2.1 Máscaras

Cada nodo de una red tiene una dirección IP específica para permitir que otros nodos se comuniquen con él. Dependiendo del tipo de red puede haber cualquier número de nodos entre 253 millones en una red. Sin embargo, no sería práctico para una dirección de tipo A o B estar restringido a una red con miles y millones de nodos. En respuesta a este problema se desarrollaron las subredes, para dividir la porción de nodo de la dirección en redes adicionales.

Las subredes funcionan tomando la porción de nodo y dividiéndola mediante una máscara de red. Esencialmente, la máscara de red mueve la línea divisoria entre la red y los nodos, de un lugar a otro dentro de la dirección. Esto tiene el efecto de incrementar el número de redes disponibles, pero reduce el número de nodos que pueden conectarse a cada red.

El uso de subredes tiene ventajas. Muchas organizaciones pequeñas pueden obtener solo una dirección de clase C, pero pueden tener muchas oficinas separadas que deban vincularse. Si solo tienen una dirección IP, el ruteador no conecta dos ubicaciones ya que esta requiere que cada red tenga una dirección particular. Al dividir la red en subredes, puede usar el ruteador para conectar las dos redes, ya que ahora tiene una dirección de red característica.

La subred se interpreta a través de la máscara de red o de la máscara de subred. Si el bit está en la máscara de red, ese bit equivalente en la dirección se interpreta como un bit de red. Si el bit está afuera, es considerado parte de la dirección de nodo. Es importante hacer notar que la subred se conoce solo en forma local; para el resto de Internet, la dirección parece como una dirección IP estándar.

Como se señala en la Tabla 1 cada clase de direcciones IP tiene asociada una máscara de red predeterminada.

Clase de dirección	Máscara de red predeterminada
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

***Tabla 1.** Máscara de red estándar*

Suponiendo que se tiene la dirección de red 198.53.64.0 y se quiere separar en subredes. Para dividir aún más la clase C de subred, es necesario que se usen algunos bits de la porción de nodo, o el último byte, de la dirección como parte de la porción de red. Si bien esto incrementa el número de redes que se puede tener, reduce el número de nodo que puede haber en cada subred.

La solicitud de comentarios (RFC) 950 de Internet también requiere que se reserve la primera y última división de cada subred. Esto significa que el número real de subredes utilizables es dos menos que el número total de divisiones. Por ejemplo, se quiere dividir la red de clase C en dos divisiones, no podrá conectar ningún nodo. Si desea tener 6 subredes, se debe dividir la red en 8.

El siguiente ejemplo ilustra como se establecen los bits del último octeto y como pueden crearse muchas subredes y un nodo para cada una de las subredes. La porción variable que representan los bits usados para la porción de nodo se identifica con la letra V. La porción fija de la dirección se identifica con la letra F.

8	7	6	5	4	3	2	1	Divisiones	Subredes	Nodo/Subredes
F	V	V	V	V	V	V	V	2	0	0
F	F	V	V	V	V	V	V	4	2	62
F	F	F	V	V	V	V	V	8	6	30
F	F	F	F	V	V	V	V	16	14	14
F	F	F	F	F	V	V	V	32	30	6
F	F	F	F	F	F	V	V	64	62	2
F	F	F	F	F	F	F	V	128	126	0

El ejemplo anterior muestra que se puede usar efectivamente solo un mínimo de cuatro divisiones, con dos subredes y 62 nodos por red, a un máximo de 64 divisiones, que producen 62 subredes de dos nodos cada una. El primer ejemplo podría usarse para dos redes ethernets separadas, mientras que el segundo podría usarse por una serie de vínculos de protocolos de punto a punto.

Sin embargo la selección del tipo de subredes que deben elegirse está determinada por el número máximo de usuarios que se requerirá en cualquier subred, así como por el número mínimo de subredes requeridas.

Las posibles porciones de red, regeneradas en el desarrollo de sus divisiones son creadas con la formación de los valores de la porción fija del último byte. Revisando el ejemplo anterior se verá que para dividir una dirección de clase C en ocho divisiones, o seis subredes, necesita fijar los primeros seis bits del último octeto. Las porciones de red se forman mediante la evaluación de la porción no fija del último byte, considere el siguiente ejemplo, que en lista las combinaciones de bits e ilustra como se separa en subredes la dirección de clase C.

8	7	6	5	4	3	2	1	Valores Decimales
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	0	0	0	96
1	0	0	0	0	0	0	0	128
1	0	1	0	0	0	0	0	160
1	1	0	0	0	0	0	0	192

Como se muestra en el ejemplo anterior, los primeros tres bits -8, -7 y 6- están fijos pues se utilizan como parte de la dirección de nodo. Esto significa que las redes disponibles son las siguientes, donde N, O y P representan los primeros tres octetos de la dirección, respectivamente:

Red
N.O.P.32
N.O.P.64
N.O.P.96
N.O.P.128
N.O.P.160
N.O.P.192

La máscara de red estándar para una dirección de clase C es 255.255.255.0. Para nuestra red dividida en subredes, los primeros tres bytes permanecen igual. El cuarto byte se crea estableciendo a 1´s la porción de red y a 0´s la porción de nodo. Si se observa en el ejemplo anterior se verá cuales serían las direcciones de red. Se utiliza el mismo formato para determinar la mascara de red.

Esto significa que las máscaras de red para estas subredes son las siguientes:

Red	Difusión	Mascara de red
N.O.P.32	N.O.P.31	255.255.255.32
N.O.P.64	N.O.P.63	255.255.255.64
N.O.P.96	N.O.P.95	255.255.255.96
N.O.P.128	N.O.P.127	255.255.255.128
N.O.P.160	N.O.P.159	255.255.255.160
N.O.P.192	N.O.P.191	255.255.255.192

El resultado final es que se divide esta dirección de clase C en seis subredes, con lo que aumenta su espacio de dirección disponible sin necesidad de solicitar una dirección de red adicional.

Cuando se observa la mascara de red, es fácil comprender porque muchos administradores se apegan a las máscaras de red orientadas a bytes: son mucho más fáciles de entender, sin embargo, si se utiliza un enfoque orientado a bits en la máscara de red pueden lograrse muchas configuraciones diferentes. Al usar una máscara de red de

255.255.255.192 en una dirección de clase C, por ejemplo, se crean cuatro subredes. Sin embargo la máscara de red en una dirección de red crearía más de mil subredes.

2.2.2 Sistema de dominio de Nombres

El esquema de direccionamiento IP utiliza enteros de 32 bits para identificar a los diferentes nodos de una Internet; sin embargo, para la mayoría de los usuarios de aplicaciones interactivas resulta difícil manejar este tipo de direcciones, por lo que hace necesario un esquema que permita utilizar identificadores de más alto nivel. Estos identificadores, o nombres, son cadenas de caracteres mnemónicos que sirven para referirse de manera única a cada nodo.

Identificadores

Al hacer uso de cadenas de caracteres como identificadores de dirección, estas deben estar ligadas a una dirección IP. El sistema actual se basa en un esquema jerárquico de nombres llamado DNS (Domain Name System). Este sistema contempla dos aspectos: Un aspecto abstracto que especifica la sintaxis y reglas para la asignación de nombres, y un aspecto concreto que especifica la implementación del mapeo de nombres a direcciones IP.

En este sistema, cada nombre se divide en varios campos que son asignados por organismos diferentes. El NIC determina el contenido del primer campo; los campos restantes son asignados por organismos locales que obtienen autorización del NIC para hacerlo así. Por ejemplo, un nombre puede tener la forma:

nombre_local.dominio_primario

En donde *dominio_primario* es el nombre que determina la autoridad central y *nombre_local* es el nombre controlado por el organismo local. El nombre local puede tener a su vez varios campos determinados por diferentes autoridades. Por ejemplo, en

cancun.fi-a.unam.mx

unam.mx se determina centralmente, *fi-a* es asignado por una autoridad a nivel de la universidad, y *cancun* es el nombre dado a nivel local. Note que en el DNS un nombre está formado por etiquetas separadas por puntos. Todas las máquinas que son administradas por el mismo organismo, y por lo tanto comparten el mismo sufijo en sus nombres, forman grupos llamados dominios.

Es importante resaltar que aunque el valor de estas etiquetas puede ser arbitrario, el hecho de utilizar un sistema jerárquico garantiza que cada nombre sea único en todo el dominio de nombres.

Como ya se mencionó el campo de más alta jerarquía es asignado centralmente; los valores oficiales propuestos por el NIC para este campo, son los que se muestran en la Tabla 2.

Nombre	Significado
com	Organizaciones comerciales
edu	Instituciones Educativas
gob	Instituciones Gubernamentales
gov	Instituciones Gubernamentales (siglas en inglés)
mil	Grupos militares
net	Centro de soporte de redes
org	Organizaciones de soporte de redes
arpa	Dominio Temporal de Arpanet
int	Organizaciones Internacionales
pais	Código de país (dos letras)
decom	Digital Equimpement Corporation
pardue	Universidad de Pardue
unam.mx	Universidad Nacional Autónoma de México

***Tabla 2.** Muestra de una pequeña parte de la jerarquía de nombres de la Internet*

Tipos de nombres

El sistema de dominio de Nombres no sólo se puede utilizar para nombrar nodos en la red, sino que es lo suficientemente general para permitir diferentes jerarquías en el sistema. De esta manera, es posible utilizarlo para identificar tanto nombres de nodos como documentos, estándares y otras entidades. Por esta razón se hace necesario especificar un tipo para diferenciar entre varios objetos con el mismo nombre. Por ejemplo, cuando una aplicación de correo electrónico necesita mapear un nombre, debe especificar que ese nombre corresponde a un *mail exchanger* (Intercambiador de correo).

Es importante notar que la sintaxis de un nombre no es suficiente para determinar el tipo del objeto a que se refiere ese nombre, por ejemplo se puede tener un nodo llamado

Kelem.fi-a.unam.mx

mientras que

comunicaciones.fi-a.unam.mx

se puede referir a un dominio, aunque los dos tengan el mismo número de elementos.

2.2.3 Mapeo de nombres a direcciones

El esquema de dominio de nombres incluye un sistema distribuido de traslación de nombres a direcciones. Este sistema está formado por un conjunto de elementos cooperativos, llamados servidores de nombres, que se encargan de mapear nombres de máquinas a direcciones IP (a este mapeo se le conoce como *resolución de nombres*).

Los servidores de nombres se organizan en forma jerárquica, tal como se muestran en la Figura 5. El servidor raíz contiene información de la raíz del sistema y de los dominios del primer nivel (dec, nfs, purdue, unam); mientras que cada organización en este nivel debe tener un servidor que conozca los nombres de todas sus máquinas.

Cuando una máquina necesita mapear un nombre, debe contactar al servidor de su dominio; si éste no puede resolver el nombre por alguna razón puede consultar a un servidor de un nivel más alto, llegando incluso a consultar al servidor raíz

Existen dos tipos de consultas: iterativas y recursivas. En la primera si el servidor no puede responder a la consulta regresa la dirección IP de un servidor que si puede hacerlo. En una consulta recursiva, el servidor se encarga de contactar a otros servidores hasta resolver el nombre.

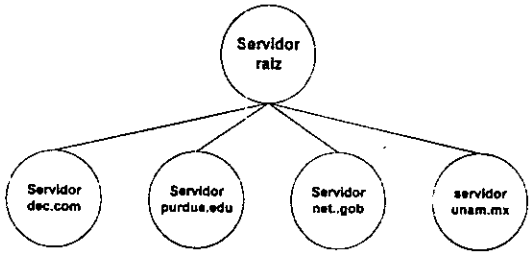


Figura 5. Esquema jerárquico de servidores

Observe que la resolución de nombres comienza de los niveles inferiores hacia los superiores, de tal forma que la mayoría de las consultas pueden resolverse localmente, dado que se refieren a máquinas locales. De esta manera se logra un mapeo eficiente.

Aún con este esquema, el mapeo de direcciones no locales podría tener problemas de eficiencia. Para evitarlo, los servidores utilizan una memoria cache en la que almacenan los resultados de las consultas más frecuentes con el propósito de anticipar las necesidades de los clientes y evitar consultas innecesarias.

Se dice que un servidor es *autoridad* para el dominio al que pertenece. Las respuestas que proporciona un servidor para máquinas que no se encuentran en su dominio son llamadas *no autorizadas*.

Formatos del mensaje de servidor de nombres

Un mensaje puede tener peticiones para varios nombres. Cada consulta consta del nombre del dominio y la especificación del tipo de consulta y el tipo de objeto deseado. El servidor responde con un mensaje similar, con las direcciones para las cuales tiene asociada una entrada. Si el servidor no puede responder a todas las peticiones, la respuesta contendrá información de los nombres de los servidores que pueden proporcionar dichas respuestas (consulta iterativa). La Figura 6 muestra el formato de dicho mensaje.

Cada mensaje inicia con un encabezado fijo que contiene un campo de identificación que usa el cliente para coordinar las respuestas y las consultas. En el encabezado, el campo denominado parámetro especifica la operación requerida y un código de respuesta.

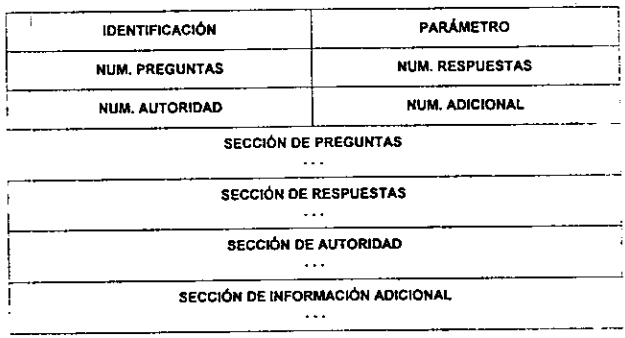


Figura 6. Formato de mensaje de servicio de nombres

Los campos *Número de* dan el número de entrada en la sección correspondiente. A continuación se analiza cada una de esas secciones.

Cada consulta consiste del *Nombre del dominio*, seguido de un tipo de consulta y un campo *Clase de consulta*, tal como se muestra en la Figura 7. El campo *Nombre de dominio* es de longitud variable; más adelante se verá como el receptor puede saber la longitud exacta del mensaje. El *tipo de consulta* especifica si se refiere al nombre de una máquina o de una dirección de correo. El campo *clase de consulta* permite utilizar el dominio de nombres para objetos arbitrarios, además de las direcciones Internet.

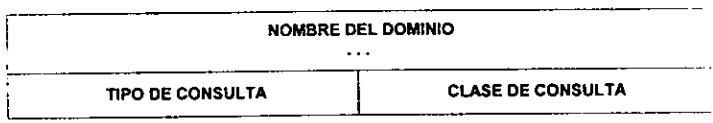


Figura 7. Campo clase de consulta

Las secciones de *respuesta, autoridad* e *información adicional* consisten de un conjunto de registros fuentes que describen el dominio de nombres y su mapeo correspondiente. Cada registro fuente describe un nombre, como lo muestra la Figura 8.

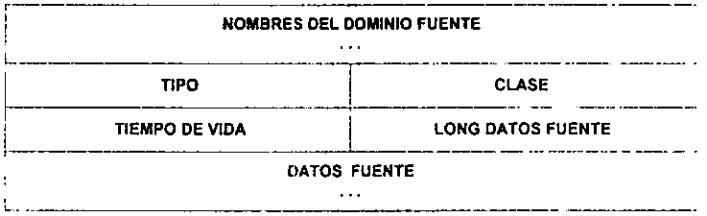


Figura 8. Descripción del dominio de nombres

El campo *Nombre del dominio fuente*, de longitud arbitraria, contiene el nombre de dominio al cual este campo se refiere. El campo *Tipo* especifica el tipo de datos incluidos en el registro fuente y el campo *clase* especifica su clase. El campo *Tiempo de vida* contiene el número de segundos que éste registro puede estar en memoria caché. Los últimos dos campos contienen el resultado de la asociación junto con el campo *Longitud de datos fuente*, el cual especifica el número de octetos en el campo *Datos fuente*.

Los nombres de dominio se representan en el mensaje como una secuencia de etiquetas. Cada Etiqueta inicia con un octeto que especifica su longitud; de esta manera, el receptor crea un dominio de nombres leyendo repetidamente un octeto de longitud y posteriormente una etiqueta de esa longitud. Un octeto que contiene ceros marca el fin del nombre. Los servidores de nombres frecuentemente regresan respuestas múltiples a una consulta.

Abreviaturas de nombres

Cuando se escribe el nombre de alguna máquina sin especificar todo su prefijo, éste se busca en el dominio local. Lo único que se debe hacer es concatenar al nombre una serie de prefijos locales y seguir el procedimiento de consulta normal. No obstante, no es recomendable generar aplicaciones que dependan de este esquema, ya que entonces dichas aplicaciones quedarían restringidas a un sólo dominio. Este mecanismo únicamente se ofrece a los usuarios para hacer más sencilla la iteración con las posibles aplicaciones.

2.3 Utilerías de TCP/IP

2.3.1 Sesiones remotas

TELNET

El comando telnet permite establecer una sesión en cualquier máquina de la red utilizando una terminal conectada a cualquier otra máquina. La manera de utilizar este comando es

% telnet nodo

Comandos Telnet

Telnet cuenta con series de comandos que pueden auxiliar al usuario durante su conexión con algún sistema. Estos comandos deben utilizarse desde el llamado modo de comandos de telnet. Hay dos formas de entrar a este modo; usando a telnet sin especificar ningún nodo, o usando la secuencia de control ^] ², al estar conectado con el sistema remoto. De cualquiera de las dos maneras, telnet indica al usuario que se encuentra en modo de comandos con el prompt telnet>. Dentro de este modo, el usuario puede utilizar diversas órdenes para configurar a telnet, así como para establecer y terminar conexiones. La *Tabla 3* describe los comandos más usuales de telnet

Comando	Función
open nodo	Establece una sesión en el nodo indicado
close	Termina la sesión remota
quit	Termina el comando telnet
z	Suspende temporalmente a telnet
status	Despliega el estado de la sesión de telnet

Tabla 3. Comandos telnet

El comando *z* suspende a telnet, lo cual permite reanudar la sesión en la máquina local temporalmente. Si se usa C Shell o Korn Shell, telnet se puede reanudar con el comando fg.

Servicios con telnet

Dentro de la organización de la Internet existe un organismo que se encarga de muchas de las tareas de administración de la red, así como de distribuir información sobre ella. Este organismo, llamado Network Information Center (NIC), presta como uno de sus servicios el acceso a un tutorial sobre el uso de la Internet. Este tutorial puede usarse a través de telnet con el siguiente comando:

%telnet nic.ddn.mil

2.3.2 FTP

La transferencia de archivos permite obtener o hacer copias de archivos hacia un nodo remoto de la red. A través de este servicio, la Internet permite el acceso gratuito a bases de datos que contienen software de dominio público e información sobre diversos temas.

La utilería de transferencia de archivos que proporciona la mayoría de las implementaciones de TCP/IP es el FTP. Las aplicaciones típicas de ftp incluyen: el acceso a archivos almacenados en computadoras centrales desde computadoras personales, el acceso a bases de datos públicas y la distribución de información a través de una red.

El funcionamiento de ftp se basa en un conjunto de comandos que permiten el acceso a la información de una máquina remota, así como la configuración de la misma utilería.

Manipulación de directorios

Ftp cuenta varios comandos que permiten navegar por el sistema de archivos del nodo remoto; todos estos comandos son muy semejantes a los del shell de Unix y se muestra en la Tabla 4.

Comando	Función
Pwd	Despliega el directorio de trabajo
cd dir	Cambia el directorio de trabajo a dir
Mkdir dir	Crea el directorio especificado
Rmdir dir	Borra el directorio especificado
Ls	Despliega el contenido del directorio actual

Tabla 4. *Comando de manipulación de directorios.*

Manipulación de archivos

De manera similar, ftp proporciona varios comandos para manipular los archivos del nodo remoto, tal como se muestra la Tabla 5.

Comando	Función
Delete *archivo*	Borra el archivo especificado
Rename n1 n2	Cambia el nombre de n1 a n2
Chmod perm archivo	Cambia los pemisos del archivo

Tabla 5. *Comandos de manipulación de archivos*

Transferencia de archivos

Los comandos get/put permiten copiar un archivo desde/hacia cualquier sistema remoto. La sintaxis de dichos comandos es la siguiente:

ftp> get archivo-remoto [archivo-local]
ftp> put archivo-local [archivo-remoto]

Cuando no se especifica el segundo argumento, ftp asume que el nombre de los archivos remoto y local es el mismo.

Transferencias múltiples

Aunque los comandos *get* y *put* proporcionan un gran potencial a ftp, en algunas ocasiones (por ejemplo cuando se necesita transferir un conjunto numeroso de archivos) pueden resultar poco prácticos. Los comandos *mget* y *mput* permiten el uso de las expresiones regulares del shell de Unix para especificar sus argumentos; la Tabla 6 muestra los metacaracteres permitidos y su función.

Metacaracter	Función
*	Sustituye a cualquier cadena de caracteres
?	Sustituye a cualquier caracter
[C1, C2....CN]	Sustituye a cualquier caracter entre C1, C2....CN

Tabla 6. Metacaracteres validos en ftp

Formatos de transferencia

Por default ftp únicamente permite la transferencia de archivos de texto (caracteres ASCII 0-127): cuando se desea transferir archivos binarios (por ejemplo archivos ejecutables o textos en ascii extendido) se debe utilizar antes el comando *binary*. El comando *ascii* regresa a ftp a modo ASCII.

Redireccionamiento de entrada/salida

El nombre de cualquier archivo que se especifique en FTP puede sustituirse por el carácter -;en todo caso, el archivo que se utiliza es la entrada estándar (stdin) o la salida estándar (stout), dependiendo de si el nombre sustituido representaba un archivo de entrada o de salida.

Por otro lado, si el nombre de un archivo inicia con el carácter , se interpreta como un comando de Unix y la salida de la transferencia se redirecciona a la entrada de ese comando, es decir se hace *pipe*.

FTP anónimo

Muchos de los nodos de la Internet distribuyen de manera gratuita información de dominio público basándose en FTP. Para permitir el acceso a su información, cada uno de esos nodos proporciona una cuenta pública llamada *anonymous* que generalmente tienen password *guest* o *ident* (algunos nodos aceptan cualquier password, mientras que otros solicitan la dirección de correo electrónico del usuario). Este método de acceso es llamado *FTP anónimo*.

La información que se distribuye de esta manera incluye temas como compiladores, ambientes gráficos, virus, juegos, música, documentación de la red (RFC's), literatura, imágenes digitalizadas, etc. La Tabla 7 muestra algunos nodos y la información que distribuyen.

Nodo	Descripción
ads.com	Listas de correo
aeneas	Kerberos (autentificación de redes)
aisunl.ai.uga.edu	Utilerías para MS-DOS
allspice.lcs.mit.edu	SNMP (administración de redes)
argus.stanford.edu	Información de la Internet
arisia.xeros.com	Código fuente de TCP/IP
chalmers.se	RFC's (documentación de la Internet)
cs.toronto.edu	Aplicaciones X (aplicaciones gráficas de red)
cs.uwp.edu	Música clásica y popular
ento.tamu.edu	Juegos para VAX/VMS
expo.lcs.mit.edu	Código Fuente de X (aplicaciones gráficas para red)
nnsc.nsf.net	Guía de recursos de la Internet
nmic.ddn.mil	Información sobre el "gusano" de la Internet
sh.cs.net	Mapas de la red

Tabla 7. Ejemplos de nodos e información que distribuyen

Muchos de los archivos que se mantienen en estas máquinas se encuentran en formato comprimido o empacado en formato de cinta (formato *tar*). En el primero de los casos (el archivo tienen extensión *Z*), el comando *uncompress* realiza la descompresión; en el segundo caso (el archivo tiene extensión *tar*) se debe utilizar el comando *tar xvf*

2.3.4 Correo electrónico

El servicio de correo electrónico permite que los usuarios puedan intercambiar mensajes a través de la red sin importar la localización de los nodos que utilizan para ello. Bajo Unix, el correo electrónico es proporcionado por la utilería de correo, la cual se invoca de la siguiente manera.

% mail dirección

en donde *dirección* tiene la forma *usuario* si la persona a la que se desea enviar el mensaje se encuentra en el mismo nodo o *usuario@nodo* si esa persona se encuentra en otro nodo.

Enviando mensajes

Cuando el usuario de mail escribe el texto del mensaje, puede hacer uso de una serie de comandos que auxilian en su tarea; todos esos comandos inician con el carácter '~', por lo que son llamados *comandos tilde*, y deben escribirse en la primera columna de la pantalla. La Tabla 8 describe los más relevantes.

Comando	Función
-c *usuarios*	Envía copias a los *usuarios* especificados
-s *cadena*	Usa *cadena* como asunto (subjet) del mensaje
-r *archivo*	Incluye el *archivo* en el mensaje
-m *mensaje*	Incluye en el texto los *mensajes* especificados
0-q,-Q	Sale de *mail*; salva el texto en *dead.letter*
-x	Sale de mail , no salva el texto
-d	Incluye en el mensaje al archivo *dead.letter*
-v	Edita el mensaje con *vi*
-w *archivo*	Escribe el mensaje en el archivo *especificado*
-! *command*	Ejecuta un comando del shell sin salir de mail
-?	Despliega la lista completa de comando tilde

Tabla 8. Comando Tilde

El archivo *dead.letter* al que se refiere algunos comandos de la Tabla 8 es generado por mail cuando por alguna razón se interrumpe el proceso en el momento en que se está escribiendo una carta. La especificación de los mensajes sobre los que actúa el comando *~m* se hace con el número de identificación de los mismos.

Leyendo el correo

Cuando un usuario recibe un mensaje nuevo por medio de mail, el sistema operativo se encarga de notificárselo la siguiente vez que se hace uso de su cuenta con el mensaje

You have mail

Si el usuario se encuentra en sesión cuando recibe el mensaje, el sistema operativo no dará aviso de ello a menos que haya usado el comando

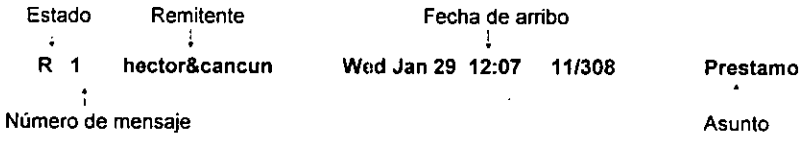
atl>biff y

Si éste es el caso, la notificación se hace en cuanto termina el comando que se esté ejecutando en el momento en que se recibe el mensaje.

Un usuario puede leer el correo que ha recibido utilizando el comando mail sin argumentos. Cuando se usa de esta manera, mail despliega la lista de mensajes recibidos y el prompt '&', indicando que ésta listo para recibir comandos:

```
atl> mail
Mail (version 3.2) ype ? for help                          Leer Correo
"/usr/spool/mail/nam": 3 messages
 N 3 aamador          Wed Jan 29 29 12:08 11/308  C++
>U 3 jramirez         Wed Jan 29 29 12:08 11/209  Re: Curso
 R 3 hector&cancun    Wed Jan 29 29 12:07 11/308  Préstamo
&
```

La lista de mensajes desplegada por mail incluye los siguientes campos:



El estado de un mensaje puede tomar tres valores:

N	El mensaje acaba de ser recibido
U	El mensaje fue recibido anteriormente, pero no ha sido leído
R	El mensaje ya fue leído

El carácter '>' llamado cursor, indica el mensaje actual (el que será leído enseguida). Los comandos más relevantes de mail se muestran en la Tabla 9.

Observe que la lista de mensajes es opcional; cuando no se especifica, sólo se incluye al mensaje actual (el apuntador por el cursor). Una lista de mensajes puede especificarse como un rango o un asterisco. La mayoría de los comandos pueden abreviarse con su primera letra.

Comando	Función
Type [*Lista*]	Despliega los mensajes de la *lista*
<*Return*>	Despliega el mensaje actual
header	Despliega los encabezados de los mensajes
next	Se salta el mensaje actual (avanza el cursor)
vi [*lista*]	Edita los mensajes de *lista*
delete [*lista*]	Borra los mensajes especificados
undelete [*lista*]	Recupera los mensajes borrados
write [*lista*] a	Graba los mensajes en el archivo a
reply [*lista*]	Responde a los mensajes especificados
mail *usuario*	Envía correo al *usuario* especificado
quit	Sale de mail; salva los mensajes no leídos
exit	Sale de mail; salva todos los mensajes
! comando	Ejecuta el comando de shell especificado
?	Despliega la lista de comandos completa

Tabla 9. Comandos de mail

Lista de correo

La Internet proporciona un servicio de distribución de correo electrónico a nivel mundial. Con él es posible mantener foros de discusión sobre diversos temas, hacer consultas relacionadas con esos temas o proporcionar acceso a diferentes boletines electrónicos.

Este servicio de correo electrónico se basa en las llamadas *listas de correo* que consisten en grupos de usuarios que desean intercambiar correo relacionado con un tema de específico. Existen cientos de listas de correo en todo el mundo, que incluyen temas como música, literatura, bases de datos, programación orientada a objetos, deportes, sistemas operativos y muchos otros; cualquier usuario de la Internet puede unirse a ellas de manera gratuita.

En muchas máquinas de la Internet se mantiene un archivo (/pub/interest-gruops) que contienen una relación de las listas de correo, además de una pequeña descripción de cada una de ellas. Esa descripción incluye la manera de suscribirse a cada lista.

Gateways

Cuando se desea enviar correo electrónico a un destino fuera de la Internet, únicamente es necesario especificar la dirección de un gateway que permita la conexión con la red en la que se encuentra el destino. La Tabla 10 muestra algunos gateways más importantes y la forma de especificarlos en la dirección del destinatario:

Red	Formato de la dirección
ACSNET	usuario@nodo.oz.au
BITNET	usuario%nodo.bitnet@cunyvm.cuny.edu
EASYNET	nodo::usuario@decwrl.dec.com
JUNET	usuario%nodo.junet%utokyo-relay@relay.cs.net
NASAMAIL	usuario@nasamail.nasa.gov
SPAN	usuario@span.nasa.gov
UUCP	usuario@nodo.uucp@uunet.uu.net

Tabla 10. Gateways más importantes

El proceso inverso (enviar un mensaje de alguna red hacia la Internet) también es posible, usando los formatos que se muestran en la Tabla 11.

Red	Formato de la dirección
ACSNET	usuario@nodo.dominio.oz.au
BITNET	usuario%nodo.dominio
EASYNET	decwrl::usuario@dominio
JUNET	usuario%nodo.dominio.arpa
NASAMAIL	usuario@nodo
SPAN	ames::usuario@dominio
UUCP	uunet!nodo.dominio!usuario

Tabla 11. Formatos de dirección

Comunicación interactiva entre usuarios

Aunque mail permite que dos usuarios puedan establecer comunicación entre si mediante correo electrónico, en algunas ocasiones es necesaria entablar la comunicación de manera interactiva (en modo conversacional).

El comando *talk* permite realizar este tipo de comunicaciones. Para esto los dos usuarios que desean establecer la conversación deben estar en sesión al mismo tiempo y uno de ellos debe de iniciar la comunicación con el comando

atl> talk jramirez

el cual limpia el contenido de la pantalla, la divide a la mitad con una serie de guiones y despliega el mensaje

Waiting for you party to respond

El destinatario de talk verá desplegarse en su terminal el mensaje

```
Mesage from Talk_DAemon@atl.fi-a.unam.mx at 20:10 ...
talk: connection requested by nam@atl
talk: respond with:talk nam@atl
```

y deberá contestar de la siguiente manera:

atl>talk nam

Una vez que esto se hace, se establece una conexión entre los dos usuarios y cada carácter que se capture se desplegará en las terminales de los dos usuarios. La conexión debe terminarse con la secuencia ^C.

Talk permite que los dos usuarios estén localizados en máquinas diferentes, en cuyo caso deberá emplearse la sintaxis

% talk usuario@nodo

Se debe considerar que para usar talk, los dos usuarios deben estar en sesión. Para revisar que esta condición se cumpla, se pueden usar los comandos *who* (que despliega los usuarios conectados a la máquina local) y *rwho* (que despliega los usuarios conectados a máquinas en la red local).

Ejecución de comandos en nodos remotos

Unix proporciona una utilería muy parecida a telnet llamada rlogin; sin embargo esta utilería sólo puede ser usada para establecer sesiones en sistemas Unix, a diferencia de telnet, que puede ser usada aún ambientes heterogéneos.

Una característica de rlogin que no posee telnet es que una persona puede autorizar a un grupo de usuarios de otras máquinas a utilizar su cuenta sin proporcionar password. Para lograrlo, se debe crear el archivo *.rhosts* en el directorio raíz de la cuenta (*home*); Este archivo contiene los nombres del nodo y del usuario autorizado para usar la cuenta.

Un comando asociado con rlogin es *rsh*[3], que permite ejecutar un sólo comando en un nodo remoto. La sintaxis de ese comando es

% rsh nodo comando

El usuario de rsh debe tener autorización para ejecutar comandos en el sistema remoto (esa autorización se especifica, de igual manera que para rlogin, en el archivo.rhosts). El siguiente ejemplo muestra como obtener un listado del directorio /etc del nodo kelem:

atl> rsh kelem ls/etc

es importante notar que el redireccionamiento de entrada/salida se hace en le nodo local a menos que el metacaracter de redireccionamiento se "escape" del shell:

```
atl>rsh kelem ls/etc > listado          "listado" se crea en la máquina local
atl>rsh kelem ls/etc '>'                 ahora se crea en la máquina remota
listado
```

Un uso muy común de rsh es ejecutar una aplicación de X-Windows (u otro ambiente de ventanas) en un nodo remoto, pero desplegando las ventanas en el nodo local:

atl> rsh kelem /usr/bin/XII/xtem -ls-display atl:0:0

2.3.5 ARCHIE

Es un sistema que permite explorar índices disponibles en los servidores públicos especiales. Hasta 1994 existían aproximadamente 1200 servidores y 2.5 millones de archivos catalogados por Archie, como usuario se le puede pedir que encuentre nombres de archivos que correspondan a ciertos criterios de búsqueda o que muestre archivos que contengan ciertas palabras. Archie devuelve los nombres de archivo que contienen esos archivos.

Archie crea su catálogo preguntando por toda la red quiénes están ejecutando programas servidores de FTP anónimo para anotarlos. Esto se hace cada mes, se conecta a los servidores FTP anónimo y lista su directorio guardando el contenido en su base de datos, así cuando se pregunta por una palabra en específico, Archie explora en los directorios catalogados y envía los nombres de archivos que concuerdan con la cadena proporcionada, junto con los nombres de los servidores, el servicio de Archie lo brindan ciertas máquinas que tienen instalado el software correspondiente, es por ello que para poder utilizarlo se debe tener corriendo un servidor local o bien conocer la dirección de un servidor remoto que tenga una cuenta especial con la cual se puede acceder a Archie. Existen múltiples servidores de Archie en todo el mundo y lo más importante es que existe información entre ellos permitiendo así que no todos los servidores tengan toda la información acerca de los servidores de FTP anónimo, sino que si un servidor no encuentra información referente a la cadena de búsqueda solicitada puede conectarse a otro servidor de Archie y pedirle que revise en su catálogo.

2.3.6 GOPHER

Gopher es un servicio, que permite encontrar información a través de la red en forma catalogada, esto es, existe una base de datos con la información clasificada de tal manera que el usuario cuando accede a este servicio puede conectarse directamente al servidor en el cual está la información que está viendo en el catálogo, la forma en que accede gopher a los servidores donde se encuentra la información es a través de FTP anónimo.

Al igual que Archie, existen múltiples Gopher en toda la red y entre ellos existe comunicación; por lo que si en determinado momento no se encuentra información en el catálogo, se puede conectar a otro y buscar en él, la ventaja de Gopher consiste precisamente en el hecho de que la información está clasificada y dar una mayor idea de hacia dónde dirigirse para realizar una búsqueda adecuada.

Gopher realiza las acciones que hace Archie y FTP, es decir conexiones de FTP anónimo para acceder a la información mostrada en el catálogo y no obstante puede mostrarla de

manera que se pueda valorar si realmente es información que sea de interés, una ventaja más sobre Archie y FTP, que para ver el contenido de algún archivo de interés se tienen que ejecutar comandos del sistema operativo y más aún muchos de los archivos que se encuentran en los servidores de FTP anónimo, se encuentran comprimidos por lo que es necesario descomprimirlos y después listar su contenido, mientras Gopher se pueda ver y también enviar por correo al buzón para poder manipularla, y todo se realiza con la interfaz que nos brida Gopher.

La interfaz que Gopher brinda es tipo texto, cuenta con menús de comandos dependiendo de la parte del catálogo en el cual se encuentra; en terminales gráficas se puede utilizar el ratón para desplazarnos entre las opciones del catálogo o bien existen teclas de control que permiten ejecutar una acción en específico.

Para poder utilizar Gopher se requiere conocer la dirección IP de algún servidor que cuente con este servicio, como en la mayor parte de los servicios en Internet todos pueden utilizarlo si se conoce su dirección IP y alguna clave de acceso.

Para ello hacemos uso del TELNET o Rlogin.

Telnet Direción_IP_del_servidor_gopher.
Telnet nombre_enDominio_del_servidor_Gopher.

La mayoría de los servidores de Gopher en el mundo tienen una clave de acceso llamada "gopher" sin password, esto para garantizar que todos puedan utilizar este servicio sin necesidad de tener una cuenta especial en el servidor, además de que esta clave cuenta con los privilegios necesarios para ejecutar el software de Gopher y claro acceder a todos los servidores de información que aparecen catalogados en él, así como la ejecución del correo electrónico cuando se requiere enviar información al usuario en la máquina local.

El Gopher es un servicio basado en una base datos que a diferencia de Archie sí tienen que actualizarse manualmente, es decir que los creadores de su Gopher tienen que preguntar a aquellos que brindan servicio de información a través de la red si quieren tener una entrada en su catálogo y así crear su vínculo correspondiente.

Por otro lado la información dentro del Gopher se restringe solo aquella que aparezca catalogada, sin que esto represente una limitante mayor ya que cuenta con la conexión hacia otros gophers en los que probablemente se encuentre información referente a lo que se esta buscando. La conexión se hace automática, aunque en ocasiones al tratar de acceder a otros gophers se indica la clave y password que se debe utilizar para poder hacer uso de sus servicios.

Con gopher al igual que con FTP trae hacia la cuenta del usuario la información deseada, esto se realiza a través del correo electrónico, es decir una vez que se localiza la información deseada gopher puede mandar un mail el contenido del archivo que esta desplegando en pantalla.

2.3.7 VERONICA[6]

VERONICA es un servicio que permite realizar búsquedas por temas y palabras especiales sobre el servicio de Gopher, es decir , realiza la búsqueda sobre los catálogos y da como resultados la posición en el catálogo correspondiente, ya sea en el Gopher local el cual se esta ejecutando o bien en algún Gopher remoto.

VERONICA extrae datos exactamente igual que Archie; visita servidores de Gopher alrededor del mundo y consulta sus menús.

Lo más importante de VERONICA es que se utiliza como cualquier índice del menú que nos presenta Gopher y solicita palabras para configurar la búsqueda e integrar los resultados en un menú especial. Los elementos de menú son los elementos provenientes de todos los Gophers alrededor del mundo los cuales contienen en su nombre las palabras que se han especificado.

2.3.8 WAIS

WAIS "Servicio de Información de Gran Cobertura " (Wide Area Information Service) es otro de los servicios de Internet: WAIS permite realizar búsquedas a través de archivos que contengan ciertos grupos de palabras.

WAIS es un software diseñado para trabajar con conjuntos de datos o bases de datos.

WAIS es un sistema distribuido de exploración de texto. Está basado en un estándar llamado Z39.50 que describe la manera en que una computadora solicita a otra que realice una búsqueda en un lugar de ella.

Para hacer que un documento esté disponible a través de un servidor WAIS alguien crea un índice para ese servidor con el fin de que sea utilizado en la búsqueda. Para información textual, cada palabra en el documento por lo regular esta indexada. Cuando se solicita una búsqueda desde cliente WAIS solicita a cada servidor, en su momento, que explore su índice en busca de un conjunto de palabras. Entonces, el servidor envía una lista de documentos que pueden ser los apropiados y una "calificación" que le indica que tan apropiado supone que es cada uno. Las calificaciones se otorgan de manera que el documento que mejor coincida con el criterio de búsqueda obtendrá la mayor puntuación por ejemplo 1000 y los demás van descendiendo proporcionalmente de acuerdo a las coincidencias con respecto a las palabras de búsqueda.

Sin embargo, esta búsqueda no es del todo certera o bien real ya que las calificaciones se otorgan a cada documento de acuerdo a la incidencia de las palabras de búsqueda, por ejemplo; se hace una búsqueda de la frase "matemáticas aplicadas a la computación", en este caso puede ser que nos regrese un documento en el cual encontró la palabra

[6] Very Easy Rodent-Oriented Net-wide Index to Computerized Archives"

"computación" y sin embargo ese documento recibe la mayor puntuación, es por ello que no se puede considerar que es una forma cien por ciento eficaz, pero si de gran ayuda.

2.3.9 Word Wide Web

EL WWW comienza a existir a raíz de un proyecto para distribuir información científica a través de computadoras en una red por medio de un sistema conocido como hipertexto. La idea fue permitir a los investigadores presentar sus investigaciones con texto, gráficas o algunos otros elementos de multimedia.

El WWW es un concepto asociado al servicio más reciente en Internet. El Web está basado en una tecnología flexible y sencilla que permite "navegar" por Internet, sus aplicaciones están basada en sistemas hipermedios distribuidos y continúan desarrollándose.

Los tres elementos principales que componen el Web son:

- El hipertexto.
- Internet misma es decir el conjunto de redes conectadas
- Multimedia (imágenes, audio y vídeo)

Un documento en hipertexto es un documento capaz de proveer ligas visibles hacia otros documentos, un ambiente de computadoras con hipertexto se crea al seleccionar una liga en un documento y moverse directamente hacia otra máquina.

Con respecto a Internet, es importante aclarar que el Web es el concepto surgido de mantener ligas en un sistema de red, pudiendo ser ésta una Internet (es decir una red de área local), mientras que el WWW se refiere a este mismo concepto pero ya bajo en Internet (la red de redes), cabe hacer la aclaración de que el WWW no es Internet, es sólo el foco de interés para todos aquellos usuarios de ésta red.

Al igual que cualquier otro servicio de Internet se debe contar con el programa cliente o con el servidor, en el caso de tener el cliente lo que realmente trabaja es un software que en la terminología del Web es conocido como "examinador " (browser) o bien "navegador" entre los examinadores más conocidos y más utilizados se encuentra Mosaic, Internet explorer y Netscape, éste último realmente vino a sustituir a Mosaic y es el "navegador" utilizado aproximadamente por el 80 % de los usuarios de Internet.

Los examinadores pueden acceder archivos a través de FTP e incluso hasta buscar documentos en una base de datos.

WWW es un intento por organizar toda la información en Internet, a manera de un conjunto de documentos en hipertexto, y la forma de recorrer la red es a través de vínculos.

Los vínculos son palabras que dan paso a la conexión con otros servidores o bien que permiten abrir otros documentos.

El Web proporciona una interfaz uniforme para diferentes tipos de servicio, el modelo de hipertexto del Web le permite seguir un vínculo y realizar una búsqueda no importa qué tipo de recuso se esté utilizando. Además el Web elimina la barrera entre los datos del usuario y los "datos públicos". Si se configura un servidor WWW y un editor de hipertexto adecuado, se pueden integrar notas personales.

Características y Funcionamiento

La forma en la que el Web trabaja se puede explicar a partir del protocolo de transferencia que utiliza HTTP (Hipertext Transfer Protocol), el cual realiza cuatro fases claves:

- Conexión
- Petición
- Respuesta
- Desconexión

En al etapa de conexión la aplicación cliente (por ejemplo Mosaic o Netscape) pretende conectarse con el servidor, esto aparece en la barra de estado de la mayoría de los "navegadores" 'Connnecting to HTTP server' si el cliente no puede ejecutar la conexión se manda un mensaje explicatorio.

Una vez que se estableció la conexión con el servidor HTTP el cliente manda una petición específica sobre cual protocolo será utilizado y que objeto es el que será utilizado, el protocolo puede ser desde luego el mismo HTPP, más FTP y NTP (Network Transfer Protocol), Gopher o WAIS, esto es conocido como método de acceso y se realiza a través de los URL[7] (Uniform Resource Locator) que consiste de una cadena de caracteres que identifica de manera única algún recurso; el formato básico para los URL es el siguiente:

método de acceso ://host:port/ruta de acceso al recurso

método de acceso: Puede ser alguno de los ya mencionados HTTP, FTP, Telnet, NTTP, Gopher.
Host: es la computadora en el cual reside el recurso.
port: Es un número particular que identifica el servicio que se esta pidiendo con respecto al servidor, este provee si el servicio esta instalado en un puerto diferente al puerto estándar para ese servicio, la ruta de acceso al recurso: es la identificación de la localización.

Como se menciono un examinador puede desplegar archivos a través de otros recursos que Internet proporciona por ejemplo FTP, así un archivo disponible a través de un servidor

[7] Localizador uniforme de recursos, que es la forma estándar de dar una dirección de cualquier recurso en Internet que es parte de la WWW.

FTP y encontrado por un examinador tendría un nombre a través del URL llamado:

ftp://cozumel.fi-a.uman.mx/usuarios/unicafi/claus/htdoc.html

donde nuevamente ftp indica tanto el tipo de servidor como el acceso al documento /usuarios/unicafi/claus/htdoc.html que se encuentra en el servidor de ftp anónimo cozumel.fi-a.unam.mx.

2.3.10 Mosaic y Netscape

Mosaic fue diseñado como examinador del WWW, presenta una interfaz multimedia para Internet. Realiza más que la presentación de hipertexto con vínculos hacia otros documentos, en realidad es una herramienta de hipermedia lo cual quiere decir que puede manejar audio, imágenes y vídeo (imágenes en movimiento) y reúne casi todas las herramientas antes mencionadas en un sólo paquete, en ocasiones las herramientas especializadas realizan una mejor tarea, pero si se desea instalar sólo un software de navegación los examinadores de Internet son la mejor solución.

El Netscape es un programa de aplicación para la comunicación entre máquinas de forma gráfica. Aglutina una serie de herramientas para poder utilizar convenientemente la mayoría de los recursos que proporciona la red Internet.

Utiliza para la comunicación las direcciones URL que además de la dirección propiamente dicha, da información del modo de acceso a la misma. Por ejemplo una dirección de este tipo sería http ://www.ulpgc.es/index.html. En esta dirección se especifica por un lado que se necesita acceder a la computadora "www.ulpgc.es" que lo queremos hacer a través del servidor "htmls" http y que queremos acceder a la página "index.html". Otro ejemplo sería ftp ://ftp.ulpgc.es/pub/linux/. Aquí se especifica la dirección "ftp.ulpgc.es" de la computadora, el servidor de la petición que en este caso será un servidor de ftp y que queremos ir al subdirectorio "/pub/linux/". En los accesos a servidores ftp el Netscape asume que se realizan a través del usuario "anonymous".

El Netscape trabaja principalmente con páginas en formato "html". Este formato permite definir un hipertexto en los que se pueden incluir gráficos y enlaces a otras direcciones URL.

2.3.11 EUDORA

Es uno de los correos más completos y premiados en el mercado, basado en el Servidor POPMail. Es una aplicación en ambiente windows de correo electrónico más avanzada y utilizada para comunicarse con cualquier persona vía Internet. Tenemos por ejemplo que Eudora Pro es una aplicación nativa de Internet, esto quiere decir que no es necesario disponer de otro software para conectarse con su proveedor de Internet. Esto hace que su uso sea muy fácil. Eudora está pensada para sacar el máximo provecho al e-mail (correo electrónico) con el mínimo esfuerzo. Algunas de sus características principales son:

Notificación de cuando llegue correo, separación del correo importante del menos importante a través de filtros. Enlazar archivos gráficos, hojas de cálculo, etc. al correo. Agenda personal, creación de carpetas para organizar el correo, da prioridad a los mensajes más importantes, busca mensajes por palabras o direcciones, posibilidad de trabajar sin conexión para ahorrarse los costes telefónicos, soporte de codificación y decodificación, pinchar y arrastrar los mensajes, ayuda en línea, utilización de SMTP y POP3, soporte de MIME y seguridad Kerberos para autenticidad de passwords.

Es decir, Eudora es un software que lleva el poder y la flexibilidad de los sistemas de correo electrónico al entorno accesible y amigable de la computadora personal: PC o Macintosh.

En vez de entrar a una máquina diferente como terminal remota y utilizar un editor de texto desconocido, los mensajes de Eudora se componen en su ordenador, en su entorno de ventanas. MS Windows o Apple Macintosh. Con un editor que funciona como un editor habitual, con lo cual no se tendrá que aprender un nuevo editor de textos. Las funciones de "cortar y pegar" funcionan entre cualquier programa del entorno en uso y Eudora. También se pueden utilizar las funciones "arrastrar y soltar" para enviar archivos a través del correo electrónico.

Con Eudora se puede intercambiar cualquier tipo de información. Permite adjuntar a los mensajes cualquier número de archivos de todo tipo incluyendo documentos de un editor de textos, imágenes, dibujos o vídeo. Eudora ayuda a trabajar en grupo, intercambiando borradores de sus documentos de trabajo o ensamblando piezas creadas por personas diferentes e intercambiadas utilizando Eudora.

Una vez compuesto el mensaje en la computadora, éste se envía a un servidor de correo. El servidor almacena el correo hasta que es distribuido al destinatario. De igual forma el correo recibido se almacena en el servidor hasta que sea recuperado.

Recordar que:

- La edición de mensajes en la computadora personal es en entorno amigable y no en una terminal de un sistema "obscuro" y desconocido.
- La impresión y archivo de los mensajes en la computadora pueden ser almacenados como archivo tipo texto e impresos en papel.
- Una comprobación automática del correo, donde se comprueba con periodicidad si se tienen correos pendientes y advierte la presencia de nuevos mensajes.
- El envío de documentos adjuntos, es decir se adjuntan mensajes de cualquier archivo de la computadora.
- El libro de direcciones permite consultar los números telefónicos o las direcciones electrónicas de las personas con las que se quiere comunicar.
- En las listas de distribución y alias, Eudora permite crear listas de distribución a grupos de usuarios así como definir alas o mnemónicos de los destinatarios más frecuentes del correo.
- La organización del correo por carpetas o directorios jerárquicos, permite organizar la correspondencia de forma eficiente a través del sistema de directorios jerárquicos.

- Con la clasificación automática del correo, se puede clasificar automáticamente el correo en función del remitente o destinatario. Esto ahorra mucho trabajo si la correspondencia es voluminosa.
- La búsqueda y ordenación del correo permite localizar mensajes por contenido y ordenar mensajes por asunto, fecha, remitente, o prioridad.
- Con el acceso remoto, se pude acceder al correo desde fuera a través de una conexión telefónica por módem con el servidor de correo. No es necesario software adicional.

En cuanto a las características de Eudora para el Administrador de la Red se tiene:
- Conectividad TCP/IP. Eudora conecta directamente a las redes TCP/IP utilizando los protocolos SMTP y POP3[8] (protocolo que determina a qué servidor de correo se dirige el cliente) para intercambiar correo con otros sistemas, incluyendo Internet.
- Implementación de SMTP y MIME[9]. Eudora se integra en entornos de correo electrónico diverso y es compatible con la mayoría de las redes de datos. Acceso a Internet. Eudora se basa en los estándares de la Internet y utiliza las convenciones de direccionamiento RFC-822, para alcanzar cualquier nodo de la Internet sin conversión de direcciones.
- Soporte MIME. Permite el intercambio de archivos y datos binarios incluyendo el uso del juego completo de caracteres internacionales en los mensajes.
- Acceso Remoto. Eudora incorpora el software remoto SLIP[10] y PPP[11] que permite acceder al servidor de correo a través de línea telefónica.
- Compatibilidad UNIX. Eudora es compatible con el correo electrónico estándar en UNIX y permite intercambiar mensajes con usuarios de este sistema. Eudora es compatible con los ficheros UNIX.

2.4 SNMP

Recordemos que el SNMP es un protocolo que está diseñado para proporcionar al usuario la capacidad de administrar remotamente una red de cómputo mediante el poleo y configuración de los valores de terminales así como el monitoreo de eventos de la red. Corre bajo TCP/IP (nivel 7 de aplicación)

2.4.1 Elementos de SNMP

MIB

La información que el SNMP puede obtener de la red está definida como un MIB[12] (Base de información de administración). La estructura de un MIB es similar a la de un árbol, en la parte de superior se encuentra la información general acerca de la red, cada rama del árbol proporciona mayor detalle de un área específica de la red. Los dispositivos pueden

[8] Post Office Protocol (Protocolo de Oficina de Correo)
[9] Multipurpose Iternet Mail Extensions
[10] Serial Line Internet Protocol, (Protocolo de Internet a través de Línea Serial)
[11] Point to Point Protocol, (Protocolo de Punto a Punto)
[12] Management Information Base

ser parte del árbol, sus hijos serían los dispositivos seriales y paralelos. La parte superior del árbol MIB de una LAN es usualmente conocida como "Internet[13]".

Existe sólo un árbol MIB definido por ISO, sin embargo parte de éste árbol tiene secciones para extensiones específicas. Usualmente cada extensión específica de red tiene su propio MIB que contiene a su vez nombres variables (por ejemplo IBM tiene su propio MIB, así como SUN, HP, etc.). Aunque los nombres variables sean diferentes, la información contenida en cada extensión específica MIB es generalmente la misma.

ADMINISTRADOR

El administrador está localizado en la computadora principal de la red. Su papel principal es investigar a los agentes para cierta información demandada.

AGENTE

El agente obtiene información de cada nodo de la red, recolecta información de la red y lo especifica en el MIB. Algunos softwares de unix lo incluyen con el software de la terminal. Un trabajo de programación común es extender un agente para llevar a cabo las necesidades específicas de la red y dicha tarea está regularmente dirigida para dar los recursos correctos.

2.4.2 Visión general de SNMP

SNMP es el lenguaje utilizado por los productos de administración de red de 3COM, es un método industria-estándar para administrar interredes.

Existen tres partes para administración de red SNMP-basada y son las siguientes:

- Agentes.- La inteligencia en cada dispositivo que envía y recibe instrucciones de administración de red.
- Estaciones de administración de red.- Una PC host o estación de trabajo que corre el software.
- MIB's.- Las Bases de información de administración son estructuras de información que almacenan la información acerca de dispositivos en la red. Tanto el agente como el administrador almacenan el MIB, y utilizan comandos de SNMP para intercambiar información MIB. Dicha información es almacenada en una estructura de árbol (tree-like), con la información del administrador de red estándar almacenada en la raíz y la información especifica - (vendor-specific) en las ramas. Los objetos (por ejemplo, el estado de los dispositivos y la información de la configuración)del MIB pueden observarse o modificarse utilizando las herramientas del administrador SNMP como el software de administración Transcend.

[13] interconexión de equipos

Las aplicaciones de administración de red del software Transcend trasladan las acciones que se ejecutan en la estación de administración en comandos SNMP, las cuales son enviadas después al agente que se especifica.

El agente SNMP también puede enviar mensajes de alerta a los administradores de la red y se les llama *traps*. Un *trap* es un método de agentes que notifican a la estación de administración que un evento en particular (por ejemplo, un puerto que se inhabilitará o un nuevo dispositivo que aparece en la red) acaba de ocurrir.

2.4.3 Configuración requerida de SNMP

Antes de que se utilice el software Transcend para administrar la red, es necesario configurar algunos o todos los puntos siguientes de información del SNMP para cada agente:

- Cadenas comunitarias.- Son utilizadas como passwords y el SNMP las utiliza para verificar (o autentificar) comandos. Un comando enviado a un agente o estación de administración que no contiene la cadena comunitaria correcta se ignora, y puede causar un mensaje de alerta (*trap*) indicando que una violación de seguridad ha ocurrido. Las cadenas comunitarias establecen lo siguiente:
  - Estaciones SNMP en la red que accesan y/o modifican información del agente.
  - Estaciones SNMP que reciben *traps* del agente.
- Receptores de *traps*.- Utilizado por las estaciones de administración de red en las que se requiera recibir mensajes de alerta (*traps*) desde este agente. La dirección IP de la estación que está corriendo el software de Transcend debe estar en esta lista.

Algunos dispositivos de 3COM también permiten especificar cuales mensajes (*traps*) son enviados y a cuales estaciones de administración de red son enviadas. Esta característica ayuda a reducir el tráfico de llamadas de red y a prevenir a las estaciones de recibir mensajes innecesarios. Los agentes de 3COM utilizan una variedad de implementaciones de cadenas comunitarias.

2.4.4 Monitoreo

El Consejo Consultivo Internet (Internet Advisory Board, IAB) ha desarrollado, o ha adoptado un cierto número de estándares par a la administración de red. La mayoría de ellos se ha diseñado específicamente para que cumplan los requisitos de TCP IP, aunque siempre que es posible, también cumple con la arquitectura OSI. Un grupo de trabajo Internet responsable de los estándares de administración de red adoptó un enfoque en dos pasos para proporcionar necesidades actuales y futuras.

El primer paso incluye el uso del protocolo simple de administración de red (SNMP), que el grupo de trabajo diseñó e implementó. En la actualidad, SNMP se usa en muchas redes Internet y está integrado en muchos productos comercialmente disponibles. Conforme la tecnología ha mejorado, SNMP ha evolucionado y se ha vuelto más completo.

El segundo paso comprende a los estándares de administración de red OSI conocidos como Servicios de Información de Administración común. (CMIS[14]) y el protocolo de información de administración común (CMIP[15]), los cuales se usarán en futuras implementaciones de TCP/IP. El IAB ha publicado el protocolo y servicio de información de administración común (CMOT[16]) sobre TCP/IP como un estándar para la administración de TCP/IP y OSI.

Tanto SNMP como CMOT sostienen el concepto de que administradores de red intercambian información con los procesos dentro de los dispositivos de red como estaciones de trabajo, puentes, ruteadores y multiplexores. La estación de administración primaria se comunica con los distintos procesos de administración, elaborando información relativa al estado de la red. La arquitectura tanto de SNMP como de CMOT es tal, que la información reunida se almacena de una manera que le permite leerla a otros protocolos.

El administrador SNMP maneja el software y las comunicaciones generales entre dispositivos mediante el protocolo de comunicaciones SNMP. El software de soporte proporciona la interfaz de usuario, lo que permite que un administrador de red observe el estado de todo el sistema, de los componentes individuales y que vigile cualquier dispositivo específico de la red.

Todos los dispositivos administrados por SNMP contienen el software de agente SNMP y una base de datos conocida como base de información de administración (MIB). MIB tiene actualmente 126 campos de información relacionada con el estado del dispositivo, rendimiento del dispositivo, sus conexiones a distintos dispositivos y su configuración. El administrados SNMP consulta MIB a través del software agente y puede especificar modificaciones a la configuración. La mayoría de los administradores SNMP consultan los agentes a intervalos regulares, como cada 15 minutos, a menos que el usuario indique otra cosa.

El software de agente SNMP es por lo general muy pequeño (comúnmente menor de 64 KB) porque el protocolo SNMP es sencillo; se diseñó para ser un protocolo de encuesta, lo cual significa que el administrador enviará mensajes a la gente. Para la eficiencia y el tamaño pequeño de programas ejecutables, los mensajes SNMP están encerrados en un datagrama UDP y enrutados vía IP (aunque se podrían utilizar muchos otros protocolos). Sólo hay cinco tipos de mensajes disponibles en SNMP:

- Obtener solicitud: se usa para consultar un MIB
- Obtener siguiente solicitud: se emplea para leer secuencialmente a través de un MIB
- Obtener respuesta: se usa para una respuesta a un mensaje y obtener solicitud
- Establecer solicitud: se emplea para establecer un valor en la MIB
- Trampa: se usa para informar eventos

[14] Common Management Information Services
[15] Common Management Information Protocol
[16] Common Management Information Services and Protocol Over TCPIP

A pesar de su amplio uso, SNMP tiene algunas desventajas. La más importante también puede ser una ventaja, su dependencia de UDP, debido a que UDP es sin conexión, no hay ninguna confiabilidad inherente en el envío de mensajes. Otro problema es que SNMP proporciona solamente un protocolo sencillo de envío de mensajes, por lo que no se puede realizar la filtración de éstos y se aumenta la carga del software receptor. Por último, SNMP usa consultas, lo que consume una gran cantidad de amplitud de banda. Las compensaciones entre SNMP y su sucesor mas reciente, CMIP, hará más difícil la decisión sobre un protocolo de administración en el futuro.

SNMP activa la administración de apoderado, lo cual significa que un dispositivo con un agente SNMP y MIB, se pueda comunicar con otros dispositivos que no tengan el software completo de agente SNMP. Esta administración de apoderado permite controlar otros dispositivos a través de una máquina conectada, colocando el MIB del dispositivo en la memoria del agente. Por ejemplo una impresora se puede controlar mediante administración de apoderado desde una estación de trabajo que actúa como agente SNMP, la cual también ejecuta el agente apoderado y el MIB para la impresora.

La administración de apoderado es útil para descargar algunos dispositivos con carga pesada. Por ejemplo, bajo SNMP es común el uso de apoderado para manejar procesos de certificación que consumen recursos considerables, pasando esta función a una máquina menos cargada. Los sistemas de apoderados también pueden afectar el procesamiento que se debe realizar en un puente, cuando el apoderado hace el cambio de formato de los datagramas que llegan para descargar al puente de esta tarea que consume mucho tiempo.

Se debe tener en cuenta que para utilizar el SNMP y el MIB es necesario realizar previamente una configuración de red, la información siguiente es necesaria para la mayoría de las redes y sus tarjetas de interfaz:

- Dirección física (MAC): Generalmente la proporciona el fabricante de la interfaz
- Dirección IP: Opcional, con interfaz de línea serial
- Máscara de subred: Especifica la dirección de red
- Protocolo: IP, si se usan TCP o UDP
- Protocolos de enrutamiento: Si se emplean ARP y/o RARP
- Dirección de difusión: Formato a usar en difusiones normalmente en unos (1's)

Los dispositivos que manejan dos redes lógicas como los ruteadores, usan las direcciones IP secundarias. Las interfaces seriales no necesitan una dirección IP, aunque se puede suministrar una. Las interfaces seriales también requieren un ajuste para indicar si el dispositivo está configurado para actuar como equipo terminal de datos (DTE) o equipo de comunicación de datos, la tasa y paridad de baudios del puerto serial, así como el tamaño máximo de una transmisión.

Cualquiera que sea el equipo usado en la red, todos tienen una conexión física con el medio de transporte de red. Típicamente se trata de una tarjeta de red en una estación de trabajo, una pc de escritorio o una impresora. El software suministrado con el dispositivo controla la interfaz, eliminando la mayor parte de las preocupaciones de hacer coincidir hardware, software y protocolos. Después de decidir sobre una dirección IP, se puede

programar el ajuste mediante interruptores o software y el dispositivo queda listo para comunicarse con la red.

2.5 Administrador de red Transcend

El Software de administración Transcend para Windows proporciona aplicaciones basadas en SNMP (Administrador Enterprise y Administrador de Trabajo en grupo del Transcend) el cual integra la administración punto apunto de equipo 3COM como son concentradores, adaptadores, puentes, ruteadores y switches.

Productos principales
El software de administración Transcend para Windows se compone de dos productos diferentes:

- Administrador de Trabajo en grupo, el cual está elaborado para las necesidades de redes pequeñas.
- Administrador Enterprise, que está diseñado para grandes redes LAN e interredes globales.

El software de administración Transcend proporciona los siguientes beneficios:

- Análisis y monitoreo de la red.- Permite la administración de la herramienta RMON (solo con el Administrador Enterprise de Transcend) y monitoreo de estadísticas de agentes, combinado con el software SmartAgent, para permitir la autocalibración del origen de las alarmas y acciones principales en eventos destacados.
- Administrador virtual de LAN.- (Solo Transcend Enterprise Manager) Permite administrar redes LAN virtuales para soportar grupos de trabajo de trabajos independientes, y utilizar la emulación de una LAN (LANE) y otras capacidades de la red ATM.
- Integración de la plataforma HP OpenView.- Permite la integración con la plataforma de administración de red HP OpenView.
- Configuración fácil.- Ejecuta las operaciones de configuración simultáneamente en múltiples dispositivos o en puertos de concentrador múltiple. Permite la actualización de software a través de múltiples ruteadores utilizando las herramientas de administrador de red.
- Documentación en línea.- Permite acceso instantáneo para completar librerías de documentación de software y hardware, y tiene la habilidad de buscar en áreas que el usuario selecciones.

2.5.1 Arquitectura del administrador de redes Transcend

El administrador de red de 3COM está basado en una arquitectura de tres niveles llamada Transcend.

Nivel 1: Software smart agent

Cada dispositivo 3COM utiliza un agente que recibe y responde a las instrucciones del administrador de red. El tipo de agente depende del dispositivo en el que el agente está diseñado para administrar:

- Las tarjetas adaptadoras tienen agentes proxys que residen en la PC que contiene la tarjeta.
- Los concentradores tienen agentes que residen en el módulo de administración del concentrador.
- Los ruteadores y switches tienen agentes integrados en el software del dispositivo.

Para tareas simples de administración, la mayoría de los agentes soportan entradas directas utilizando conexiones seriales de panel frontal. Se utilizan este tipo de conexiones para configurar los parámetros que permiten administrar el agente remotamente utilizando el software de administración Transcend.

Nivel 2: Plataforma de administración de red

El software de administración Transcend está diseñado para correr sobre HP OpenView. Con esta plataforma es posible ejecutar tareas de administración de red y de dispositivos y construir mapas de la red. Se utiliza el mapa de red para localizar los dispositivos de red y poderlos administrar con el software.

Nivel 3: Aplicaciones del software de administración Transcend

Las aplicaciones de este software están diseñadas para ejecutar funciones específicas para varios dispositivos. Ejemplos de estas funciones incluyen lo siguiente:

- Administrador de dispositivo.- Permite configurar y administrar los dispositivos, cuando se selecciona un dispositivo para administrarlo desde el mapa de plataforma de administración de red, la plataforma automáticamente lanza la aplicación de administración de dispositivo apropiada.
- Monitoreo y análisis.- Permite monitorear dispositivos, recolectando estadísticas y el estado de los dispositivos.
- Administrador de alarmas.- Permite controlar selectivamente el manejo de las alertas de red recibidas desde los dispositivos.

2.5.2 Aplicaciones del software de administración del Transcend

Las aplicaciones están agrupadas en 6 categorías de acuerdo al tipo de operación de administración en la red y son las siguientes:

- Plataforma
- Configuración y estadísticas
- Monitoreo y análisis
- Configuración de experta

- Administración de ATM y VLAN
- Herramientas de información

El software de administración Transcend está estructurado, con lo que es posible instalar únicamente aquellas aplicaciones que son relevantes para el tipo de red con que se cuente. Conforme la red cambia, se pueden instalar aplicaciones del software de administración Transcend conforme se vayan necesitando. Este software también incluye el software PC Link SmartAgent.

Las aplicaciones del software de administración Transcend se presentan desde la plataforma de despliegue HP OpenView, la cual es una plataforma para programas de administración de redes. Proporciona una interfaz gráfica estándar, con lo que las múltiples aplicaciones de red pueden compartir un sistema de alarma y despliegue común. También cuenta con funciones de administración básica de redes para dispositivos de la red.
HP OpenView para Windows cuenta con las siguientes características:

- Mapas
- Autodescubrimiento
- Alarmas
- Administrador de SNMP

Mapas

Los dispositivos de la red se despliegan en mapas, por lo que es posible organizar dispositivos y subredes en submapas adaptándose a las necesidades de la red. Se pueden crear submapas por separado ya sea de los dispositivos, agrupándolos por las funciones que realiza cada uno, de la organización de redes o de la organización corporativa. Se pueden utilizar los mapas para administrar la red desde un despliegue sencillo aún cuando la red incluya dispositivos de diferentes tipos.

Es posible cambiar el desplegado del estado de la red en el mapa de red, con iconos que representan a dispositivos. El color del icono indicará el estado del dispositivo.

Autodescubrimiento de dispositivos

El autodescubrimiento utiliza información como el rango de direccionamiento de la red, nombres comunitarios, y el tipo de dispositivos de la red para localizar todos los dispositivos presentes. HP OpenView puede dibujar un mapa de red basado en los dispositivos encontrados.

Alarmas

Los cambios en el estado de los dispositivos o "alarmas" brindan notificación al mapa de Open View cuando los eventos ocurren en la red. La base de datos de la alarma permite generar reportes o archivos del rendimiento de la red. Además en los mensajes de

pantalla, las alarmas pueden ser configuradas para disparar un sonido o incluso activar una página remota, basado en el tipo de alarma recibido.

Poleo

La prueba de poleo permite verificar si un dispositivo de red está corriendo o no. Un poleo (poll) es una simple petición enviada a n dispositivo que pide al dispositivo que responda. Si el dispositivo responde, entonces está funcionando.

Traps

Los dispositivos de 3Com envían mensajes cuando ciertas condiciones se presentan. Las condiciones pueden ser: iniciar, apagar, error de dato o cierto nivel de actividad. El mensaje resultante de la condición de un dispositivo se le llama *trap*.

Una vez que los dispositivos están configurados para enviar *traps* a la consola de OpenView, estos serán registrados en la alarma por default. Es posible personalizar la manera en que el OpenView responde a los *traps* utilizando su Diálogo de *Traps* Personalizado.

2.5.3 Estadísticas

Es posible utilizar las siguientes aplicaciones de administración de dispositivos Transcend para configurar el hardware de 3Com y obtener estadísticas observando la operación de la red y el dispositivo.

- Vista del dispositivo (*Device View*)
- Administrador ONcore (ONcore Manager)

Vista del dispositivo

Brinda un administrador gráfico de la familia de 3Com como concentradores, switches y ruteadores. Muestra el número y tipo de unidades formando un dispositivo de soporte (por ejemplo las unidades individuales en un stack), muestra el estado individual de los puertos, y permite colectar detalladamente estadísticas de los puertos y del dispositivo.

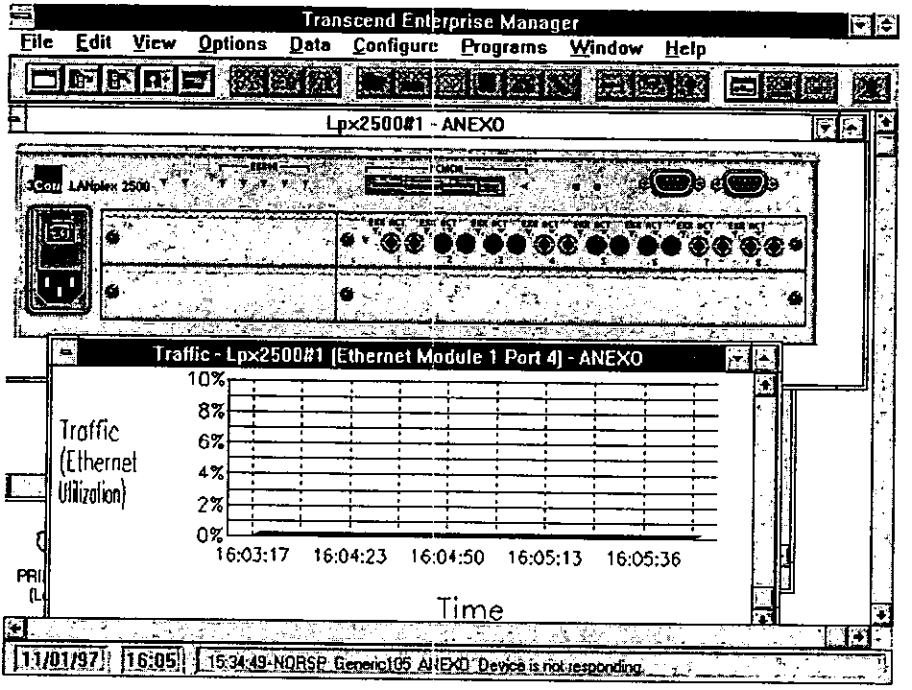


Figura 9. Ejemplo de porcentaje de utilización de un dispositivo

2.5.4 Como trabaja el administrador de red

Así como en la mayoría de los productos de administración y comunicación de red, en una red Transcend se usa el protocolo de comunicación TCP/IP y el lenguaje de administración de red SNMP.
El proceso es como sigue:

1. El software de administración de red traslada la petición del usuario al SNMP.
2. Este mensaje se coloca en un empaquetador de TCP/IP llamado datagrama UDP.
3. El empaquetador es direccionado con el protocolo IP del agente (target agent).
4. Dicho mensaje viaja a través de la red hasta su destino. Un datagrama UDP puede viajar por Ethernet, Token Ring, FDDI o una combinación de protocolos. El único requerimiento es que exista una conexión de red entre la estación de administración y el agente.
5. EL agente en el dispositivo (target device), que también cuenta con el SNMP recibe el mensaje y abre el empaquetador.
6. El agente lee el mensaje y ejecuta la instrucción.

Existen diferentes tipos de datagramas UDP intercambiables por la estación de administración y el agente.

- Configuración.- Ocurre cuando la estación de administración quiere cambiar la configuración de la información del agente.
- Adquirir.- Ocurre cuando la estación de administración pide información del agente.
- Adquirir respuestas.- Ocurre cuando el agente llama a una operación de Adquirir (get) o configurar (set).
- Traps.- Ocurre cuando el agente envía un mensaje a la estación de administración para notificar a la estación que un evento en particular ocurrió (por ejemplo, un cambio de configuración)

2.5.5 Visión general de TCP/IP y la relación con el SNMP

Como ya se mencionó anteriormente TCP/IP es el nombre común que se aplica a la familia de protocolos de comunicaciones de datos utilizado para conectar computadoras y equipo de comunicaciones de datos para formar redes de computadoras. También es el protocolo de comunicaciones requerido por el SNMP.

Las aplicaciones del software de administración Transcend utilizan TCPI/IP para intercambiar información entre la estación de administración de red y los SmartAgents. TCP/IP también permite un método aceptado globalmente de identificación de dispositivos individuales. Los dispositivos en la Internet están asignados con direcciones únicas. Entonces Internet se comporta como una red virtual utilizando estas direcciones asignadas cuando se envían y se reciben paquetes.

2.5.6 Configuración requerida de TCP/IP

Antes de utilizar el software de administración Transcend, se debe configurar algunas o todas de las características siguientes:

- Dirección IP del agente.- Para participar en las comunicaciones TCP/IP, cada agente debe tener una dirección IP única. La dirección IP se utiliza en la red para rutear correctamente información enviada (intended) por el agente.
- Ruteador o Gateway por defatult.- Es la dirección IP del gateway (por ejemplo un ruteador) que recibe y pasa los paquetes cuya dirección es irreconocible por la red local. El agente utiliza el gateway por default cuando envía paquetes de alerta a una estación de trabajo en una red más que en la red local. (other than the local network)
- Máscara de subred.- La máscara de subred es utilizada para esconder (mask off a group) un grupo de números comunes que forman el lado izquierdo de todas las direcciones IP de la misma subred (este grupo de números se llama también Red ID)

Los números principales (remainig) en una dirección IP (a la derecha de la red ID), únicamente identifica cada host. La dirección de la host consiste de 1 a 3 grupos de números. La siguiente tabla muestra las configuraciones de máscaras para varias clases de subredes IP.

Clase	Longitud del id del host	Ejemplo de una máscara de subred
A	3 grupos (máscara.host.host.host)	ff.0.0.0
B	2 grupos (máscara.máscara.host.host)	ff.ff.0.0
C	1 grupo(máscara.máscara.máscara.host)	ff.ff.ff.0

Tabla 12. Clasificación de redes en Internet

2.5.7 Código de colores

En este producto el código de colores se utiliza constantemente. Esto con el fin de ubicar de una manera rápida el estado de cualquier dispositivo o gráfica que se esté utilizando. Por lo tanto se aplica a dispositivos, grupos y redes, así como gráficas. Existen 6 códigos de colores los cuales se presentan en la Tabla 13 desde una importancia alta una baja.

COLOR	DESCRIPCIÓN
ROJO	Error crítico, Reservado para errores para dispositivos o fallas de puertos
NARANJA	Advertencia mayor. Una condición seria que debe ser revisada
AMARILLO	Advertencia menor. Un error que ha ocurrido y probablemente no sea tan serio (por ejemplo, el puerto de un concentrador no particionado)
VERDE	Condición normal. Todo está operando satisfactoriamente
AZUL	Apagado o no reconocido. Ya sea que el estado sea desconocido (ej. No está siendo poleado) o que un puerto fue deshabilitado por administración.
PURPURA	Para información

Tabla 13. Códigos de colores

2.6 LANALYZER

2.6.1 Características generales del software de monitoreo LANalyzer® para Windows™ 2.1

Herramienta basada en sistema microsoft Windows para monitoreo y análisis de tráfico sobre redes Ethernet y token ring. El tráfico puede ser monitoreado diario o periódicamente (por largos periodos de tiempo) para analizar la red en problemas específicos. Operando desde el uso fácil de la interfaz del panel de control, LANalyzer provee una fotografía instantánea activa, cada minuto de la operación de la red y permite al usuario capturar los paquetes de red para el análisis de protocolo.

LANalyzer para Windows es un producto de software único que se instala en una estación Netware. Se puede operar tanto en primer plano como en segundo bajo MS Windows y es útil para monitorear una red día a día y para localizar problemas en la red conforme vayan ocurriendo.

Es posible llevar a cabo un monitoreo de la red y analizar funciones en todos los paquetes de la misma así como filtrar el tráfico y analizar un subconjunto de paquetes de redes.

2.6.2 Requerimientos de hardware

El siguiente hardware es recomendado para utilizar LANalyzer para Windows:

- Procesador 386 (o mayor)
- 2 MB en RAM (recomendado 4 MB)
- Monitor VGA o SVGA(recomendado a color)
- 5 MB de espacio en disco duro
- Mouse que soporte Windows 3.1
- Tarjeta de red Ethernet o token ring

2.6.3 Software requerido

- MS-DOS 3.3 o mayor, DR DOS 6.0 o Novell DOS 7.0 o mayor
- MS Windows 3.1
- Controlador ODI (Open Data Link Interfase™) para Ethernet o token ring.

2.6.4 Monitoreo y estadísticas de red

LANalyzer para Windows monitorea la red desplegando estadísticas de red en tiempo real por medio de medidores, gráficas y tablas. También monitorea a través de un Monitor de estación el cual despliega una tabla con una lista de las estaciones activas en la red y sus estadísticas relacionadas.

LANalyzer para Windows usa alarmas indicadoras y de mensajes que alertan de condiciones no usuales u ocurrencia de eventos en la red. Analiza el rendimiento de la red mediante la capturación y decodificación de paquetes de red, los cuales los muestra a través de una ventana de buffer de captura.

2.6.5 Filtrado del tráfico de red

La función de filtrado del LANalyzer para Windows permite monitorear los paquetes de red y el tráfico hacia y desde estaciones específicas, captura paquetes de ciertos tipos de protocolos, y captura paquetes basados en la presencia o ausencia de errores. Las siguientes opciones de paquetes de captura están disponibles:

- Paquetes de captura de un tipo de protocolo en específico
- Paquetes de captura hacia, desde o entre estaciones seleccionadas
- Captura de paquetes de entrada o una parte de paquetes seleccionada de paquetes
- Captura de todos los paquetes, paquetes buenos únicamente, o paquetes de errores.

2.7 FIREWALL

La misión fundamental de un firewall es proveer seguridad, e impedir que usuarios no autorizados accedan a la información reservada de una organización. Al mismo tiempo, deben permitir transferir archivos y accesar la Internet junto con todas las funciones que se requieren de ella, como enviar y recibir correo electrónico, ver imágenes o escuchar audio, pero en forma segura y controlada.

Las restricciones pueden ser basadas de la siguiente manera:

- Tipo de acceso (email, telnet, ftp, etc.)
- Contenido de datos accesados.
- Supervisión.
- Direcciones de redes IP autorizadas (tanto internas como externas)
- La hora del día.
- Nodos Autorizados.

Hay diferentes técnicas usadas para proteger sistemas. Entre ellas, están los filtros de paquetes, los proxies, aplicación gateway.

Los filtros de paquetes constituyen una tecnología más antigua, incorporada en algunos ruteadores o ruteadores de información. Es un mecanismo que provee un nivel básico de seguridad de red. Mediante tablas complejas se configuran para indicar cuales protocolos de comunicación son permitidos de entrar o salir de una red. Por ejemplo, prohibir accesos externos de aplicaciones peligrosas como telnet, o restringir ciertas direcciones IP. Muchos Firewalls tienen la funcionalidad de filtro de paquetes.

Los proxies son programas que permiten a los firewalls actuar por cuenta de otra computadora al efectuar la comunicación. Por ejemplo, si un usuario de una red interna confiable, trata de contactar a otra red externa, no confiable, será el proxy del firewall quien haga dicha conexión por cuenta de la computadora interna. La seguridad es la habilidad de ser escudo entre máquinas internas y externas. Para la máquina externa, le parecerá que es el firewall con quien está conectado, no la máquina interna. Algunas marcas comerciales de firewalls proveen proxies transparentes, lo que no es necesario configurar cada aplicación en forma especial, sin que el firewall se encarga de ello.

Un "aplication gateway" es un componente clave de un firewall robusto. Todos los sitios Internet reciben y procesan información provenientes de otras partes de la Internet. Por ejemplo, es deseable recibir correo electrónico desde cualquier parte, y permitir que cualquiera lea la información del servidor Web. Pero desde el punto de vista de la seguridad es peligroso permitir el acceso a máquinas internas que manejan esos servicios usando esos protocolos. Las aplicaciones tales como correo electrónico, grupos de noticias, servidores Web, etc., se canalizan a través de gateways o puertas, las que han sido diseñadas pensando en la seguridad.

Hay firewalls que establecen una tercera red, que no es la interna, segura, ni la externa, insegura. Es lo que se denomina un Zona Desmilitarizada o DMZ. Allí se ponen los servicios como el servidor Web o de correo, los que pueden ser accesados tanto desde el

exterior como el interior pero con distintos privilegios. La seguridad radica en que no se compromete el resto de la red interna, en la eventualidad que se encuentren hoyos de seguridad.

Un firewall dinámico solamente permite accesos a través de la red cuando se desea y solamente por el tiempo deseado. El firewall examina cada paquete a través de la interfaz de red. Cuando un paquete satisface los requerimientos de las reglas del firewall, a éste le es permitido el paso a la red. Estas reglas abren, cierran y tiempo todos los aspectos de cada sesión.

Las reglas de un firewall dinámico proporcionan uno de los mejores caminos para controlar entrada y salida de paquetes. Estas reglas operan fuera de los protocolos de la red y son transparentes para el usuario. Generalmente estas reglas son almacenadas en los ruteadores de la red. Estas reglas implementan un sistema de administración de policías para el tráfico de red. Los policías realizan uno da las siguientes premisas:

A. El cual no este expresamente prohibido es permitido
B. El cual no este expresamente permitido es prohibido

Obviamente, la premisa B es menos permisible que A. Esto es mas seguro, si un paquete no coincide con las reglas, no pasa a la red. Alcanzar la premisa A requiere de una constante atención, esta requiere una planeación para añadir reglas, cuando un nuevo servicio es añadido a la red y si es filtrado y coincidente con las reglas este será bloqueado.

2.7.1 Router de selección

Muchos ruteador comerciales proporcionan la capacidad de seleccionar paquetes con base en criterios como el tipo de protocolo, los campos de dirección de origen y dirección de destino para un tipo particular de protocolo y los campos de control que son parte del protocolo. A esos ruteadores se les llama ruteador de selección.

Estos pueden proporcionar un mecanismo poderoso para controlar este tipo de red que puede existir en cualquier segmento de una red. Al controlar este tipo de tráfico, los ruteadores de selección pueden controlar el tipo de servicios en un segmento de red. Por lo tanto, pueden restringir servicios y pueden poner en peligro la seguridad de red.

Los ruteadores de selección pueden discriminar entre el tráfico de red con base en el tipo de protocolo y en los valores de los campos del protocolo en el paquete. A la capacidad del ruteador para discriminar entre paquetes y restringirlos en sus puertos con base en criterios específicos de protocolo se le denomina filtración de paquetes. Por esta razón, los ruteadores de selección también son llamados ruteadores de filtración de paquetes.

Zonas de riesgo

En la Figura 10 se muestra un servicio de filtración de paquetes implantado por un ruteador de selección. En esta figura se observa una red de una empresa conectada a Internet a través de un ruteador que realiza la filtración de paquetes.

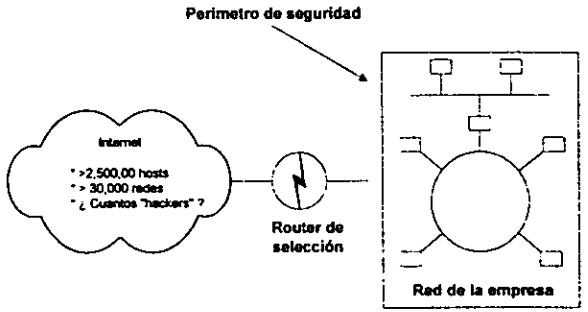


Figura 10. Un ruteador de selección formando un perimetro de seguridad.

En la red de la Figura 10, al límite de la red de la empresa se le llama perimetro d seguridad. Debido a que los hackers maliciosos abundan en Internet, es útil definir una zona de riesgo. Esto incluye a todas las redes con capacidad TCP/IP, a las que se tienen acceso directo a través de Internet. Capacidad TC//IP significa que el host soporte al protocolo TCP/IP y sus protocolos de soporte. Acceso directo significa que no hay fuertes medidas de seguridad (no hay puertas con cerradura) entre Internet y los host de la red de la empresa.

Desde su punto de vista las redes nacionales, y de backbone de Internet representan una zona de riesgo, los host dentro de una zona de riesgo son vulnerables a los ataques. Es muy deseable colocar sus redes y host fuera de la zona de riesgo, sin embargo un dispositivo que pueda bloquear ataques contra su red, la zona de riesgo se extenderá a toda su red. El ruteador de selección es un dispositivo que puede reducir la zona de riesgo para que no se penetre el perímetro de la seguridad de su red.

El modelo de referencia OSI y los ruteadores de selección

Los ruteadores de selección trabajan sobre la capa de red. La función primaria de un ruteador (incluyendo un ruteador de selección) reside en a capa de red. Cuando este ruteador ve un paquete de IP, examina la dirección de IP del destino en el paquete.

Una dirección IP consta de un número de red y un número de host, el ruteador, examina la porción del número de red de la dirección de IP del destino en el paquete y lo compara

con las entradas en su tabla de enrutamiento. Si no coincide y no hay una ruta predeterminada se rechaza el paquete.

Los ruteadores de selección pueden utilizar criterios además de la tabla de enrutamiento para pasar el paquete o rechazarlo. El ruteador de selección puede realizar la filtración en la capa de red con base en la dirección de IP de origen, la dirección de IP de destino y las opciones de IP (enrutamiento de origen o enrutamiento de origen perdido). En la Figura 11 se muestran los campos dentro del paquete de IP en que el ruteador de selección puede realizar la filtración.

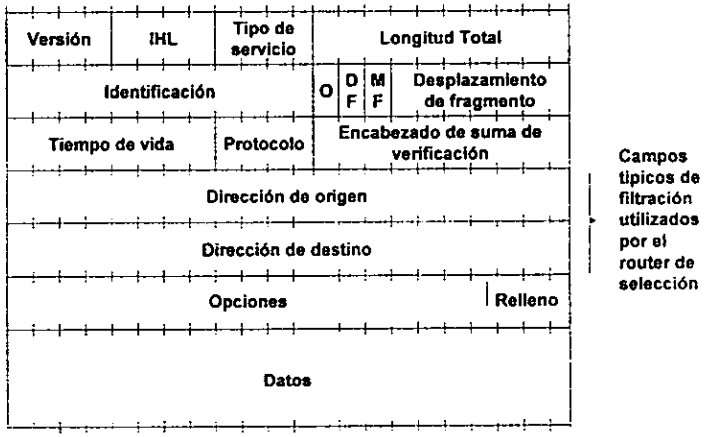


Figura 11. Campos del paquete utilizados por el ruteador de selección

En TCP/IP, el término números de puerto es utilizado para identificar direcciones de transporte. Los ruteadores por lo general no aplican procesamiento en la capa de transporte. Sin embargo los ruteadores de selección pueden examinar campos de número de puerto en el encabezado TCP. Pueden desarrollar decisiones de filtración con base en los valores de número de puerto del encabezado TCP.

Además de los números de puerto los ruteadores de selección son capaces de filtrar paquetes con base en indicadores de TCP. Los indicadores de TCP se utilizan para designar el tipo de paquete de TCP, como sigue:

- Conexión abierta
- Acuse de recibo de conexión abierta
- Paquete de acuse de recibo o paquete de datos

Los ruteadores de selección aplican la filtración de paquetes con base en lo siguiente:

- Número de puerto de origen
- Número de puerto destino
- Indicadores TCP

Routers de selección y firewalls en relación con el modelo OSI

En la Figura 12 se comparan los ruteadores de selección y los firewalls en relación con el modelo OSI. En esta figura ser muestra que las funciones principales del ruteador de selección corresponden a las capas de red (protocolo IP) y transporte (protocolo TCP) del modelo OSI, sin embargo, los ruteadores de selección también pueden incluir los datos de las capas de vinculo de datos y física , porque la mayor parte de los sistemas de filtración se aplican al tipo de interfaz, los medios de red en uso e incluso la dirección MAC misma. Los firewalls a menudo son descritos como gateway. Los gateways pueden desarrollar un procesamiento en las siete capas en el modelo OSI. Por lo general, los gateway realizan el procesamiento en la séptima capa del modelo OSI, esto es verdadero para los gateways de firewall.

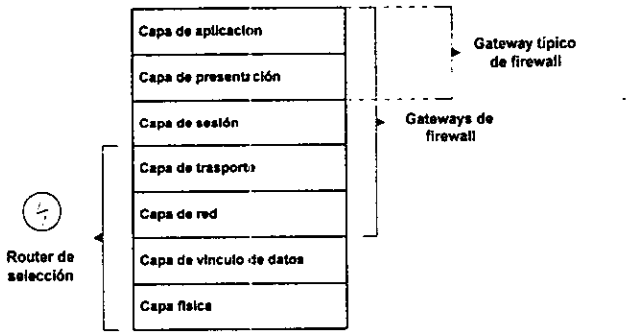


Figura 12. Routers de selección, firewalls y el modelo OSI

En la Figura 12 también se muestra que como los firewall cubren las capas de red y de transporte, pueden desarrollar las funciones de filtración de paquetes. Algunos fabricantes, tal vez por razones de mercadotecnia, hacen confusa la distinción entre un ruteador de selección y entre un firewall, al grado de que llaman a sus productos de ruteador de selección productos de firewall.

2.7.2 Modelo simple para la filtración de paquetes

Por lo general un filtro de paquete se coloca entre uno o más segmentos de red, como se muestra en la Figura 13. Estos segmentos de red están clasificados como segmentos de red externos o internos. Los segmentos de red externa conectan una red con redes externas como Internet. Los segmentos de red internos se utilizan para conectar los host de la empresa y otros recursos de la red.

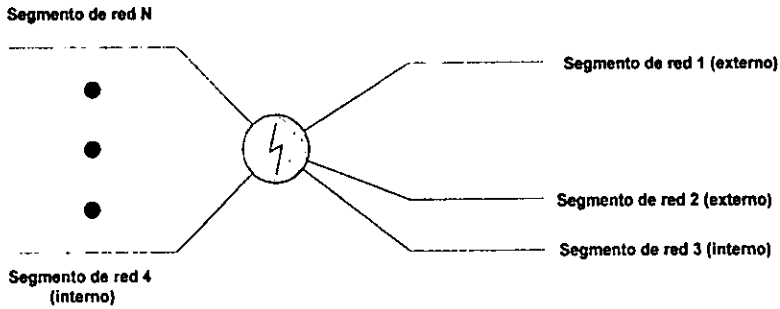


Figura 13. Filtro de paquetes colocado entre segmentos múltiples

Cada uno de los puertos de filtración de paquete puede utilizarse para implementar políticas de red que describan el tipo de servicio de red accesible a través del puerto. Si es grande el número de segmentos de red que se conectan con el dispositivos de filtración de paquetes, puede resultar complejas las políticas que implanta el dispositivo de filtración de paquetes. En general debe evitarse las soluciones complejas a los problemas de seguridad debido alas siguientes razones:

- Son más difíciles de mantener
- Es fácil cometer errores en la configuración de filtración de paquetes.
- Tienen un efecto adverso en el desempeño del dispositivo en que se implementan.

Operaciones de filtración de paquetes

Casi todos los dispositivos de filtración de paquetes actuales (ruteadores de selección o gateway de filtración de paquetes) operan de la siguiente manera:

1. Los criterios de filtración de paquetes deben almacenarse para los puertos del dispositivo de filtración de paquetes. A los criterios de filtración de paquetes se les llaman reglas de filtración de paquetes.
2. Cuando el paquete llega al filtro, se analizan los encabezados del paquete. La mayoría de los dispositivos de filtración de paquetes examinan los campos sólo en encabezados de IP, TCP o UDP.
3. Las reglas de filtración de paquetes se almacenan en un orden específico. Cada regla se aplica al paquete en el orden en el que la regla de filtración de paquetes se almacena.
4. Si una regla bloquea la transmisión o la recepción de un paquete, este no es permitido.
5. Si una regla permite la transmisión o la recepción de un paquete, a dicho paquete se le permite proceder.
6. Si un paquete no satisface alguna regla, se le bloquea.

En la estas reglas se encuentran expresadas como un diagrama de flujo. A partir de las reglas 4 y 5 debe darse cuenta de que es importante colocar las reglas en el orden correcto. Un error común en la configuración de las reglas de filtración de paquetes es colocar las reglas en el orden equivocado. Si las reglas de filtración de paquetes se

colocan en orden incorrecta se podría terminar rechazando servicios válidos, mientras que permitiría los servicios que deseaba rechazar.

Las regla número 6 sigue esta filosofía: aquello que no está permitido expresamente, está prohibido. Se trata de una filosofía a prueba de fallas que debe seguir cundo se diseñe redes seguras. Es opuesta a una filosofía que dice: Aquello que no está prohibido expresamente, esta permitido.

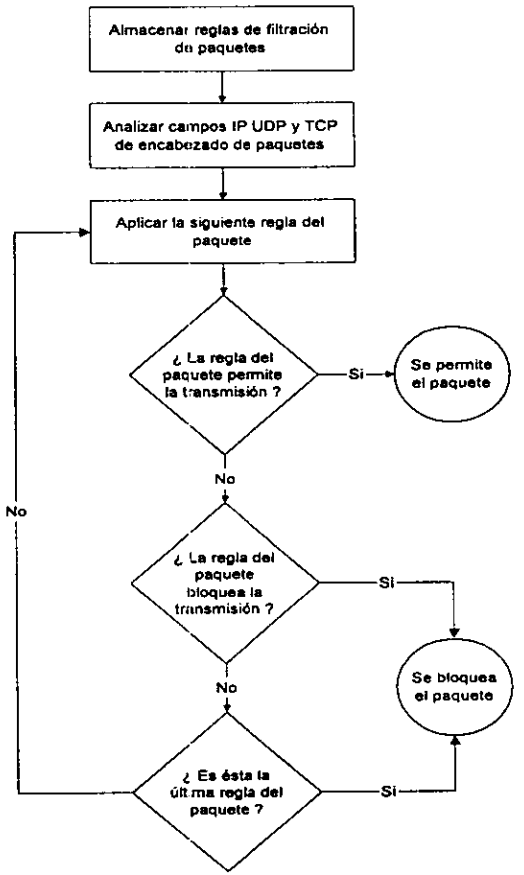


Figura 14. Diagrama de flujo de la operación de filtración de paquetes.

Diseño de la filtración de paquetes

Considerar la red de la Figura 15 en la que el ruteador de selección se utiliza como primera línea de defensa entre la red interna protegida y una red externa no confiable.

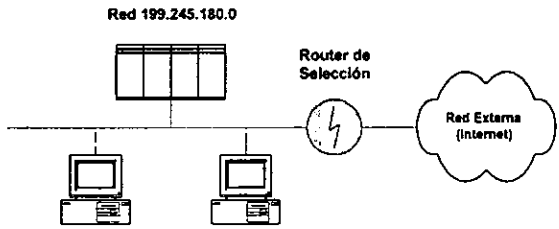


Figura 15. Red de ejemplo para el diseño de la filtración de paquetes.

Suponiendo que la política de seguridad de red necesita que el correo de Internet se reciba de host externos en un gateway específico, y que se desee rechazar el tráfico de la red que se origina en el host llamado CREEPHOST en el que no se confía, en este ejemplo, la política de seguridad de la red en SMTP debe traducirse en reglas de filtración de paquetes. Se puede traducir las reglas de seguridad en la red en lenguaje común:

- Regla de filtración 1.- No confiar en conexiones del host CREEPHOST
- Regla de filtración 2.- Permitir conexiones al gateway de correo.

Estas reglas pueden codificarse en la tabla de reglas que se muestran en la figura 17 el asterisco se utiliza para hacer coincidir cualquier valor de esa columna.

Para la regla de filtración uno (en la Figura 16) hay una entrada para la columna host externo, y todas las demás columnas tienen el asterisco. La acción es bloquear la conexión. Esto se traduce en lo siguiente:

Bloquear cualquier conexión de CREEPHOST surgida de cualquiera (asterisco) de sus puertos a cualquiera (asterisco) de los puertos propios en cualquiera (asterisco) de los hosts.

Para la regla de la filtración 2 hay una entrada para las columnas de los host propios y puerto en host propios. Todas las demás columnas tienen el asterisco. La acción es permitir la conexión. Esto se traduce en lo siguiente: permitir cualquier conexión desde cualquier (asterisco) host externo surgida de cualquiera (asterisco) de sus puertos hacia el puerto 25 del host propio GW-Correo.

El puerto 25 se utiliza porque este puerto de TCP está reservado para SMTP.

Numero de regla de filtración	Acción	Nuestro Host	Puerto en nuestro host	Host externo	Puerto en ruteador externo	Descripción
1	Bloquear	*	*	CREEPHOST	*	Bloquear tráfico de CREEPHOST
2	Permitir	GW-Correo	25	2	*	Permitir conexión a nuestro gateway de correo
3	Permitir	*	*	3	25	Permitir tráfico de SMTP de salida a un gateway de correo remoto

Figura 16. Un intento de codificar las reglas de filtración de paquetes.

La regla se aplica en el orden de su número en la tabla. Si un paquete no coincide con cualquiera de las reglas es rechazado.

La tercera regla ilustra cómo un host interno sería capaz de enviar correo de SMTP al puerto 25 de un host externo. Esto permite que el host interno envíe correo a sitios externos. Si el sitio externo no está utilizando el puerto 25 para SMTP, no se permitirá el proceso de remitir SMTP para enviar correo. Esto es equivalente en el correo a no tener soporte en el host externo.

Reglas de filtración de paquetes y asociaciones totales.

En la Figura 17 se muestra una hoja de trabajo que puede utilizarse para diseñarse reglas de filtración de paquetes. Los ruteadores de selección en general, pueden filtrar con base en cualquiera de los valores de campo que se encuentran en los encabezados del protocolo TCP o IP. Para la mayoría de las políticas de seguridad de redes que pueden implementarse con ruteadores de selección, sólo se requiere especificar los indicadores de TCP, las opciones de IP y los valores de las direcciones de origen y destino.

Numero de regla de filtración	Dirección	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Opciones de indicadores de protocolo	Descripción
1								
2								
3								
4								
5								
6								
7								
8								

Figura 17. Una hoja de calculo para el diseño de reglas de paquetes.

Una asociación completa se ilustra en la Figura 18, en la cual se muestra que una conexión de TCP entre dos hosts puede describirse con la siguiente información:

- Tipo de protocolo
- Dirección de IP local.
- Número de puerto TCP local.
- Dirección de IP remota.
- Número de puerto TCP remoto.

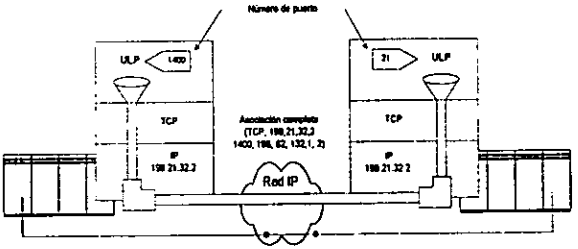


Figura 18. Una asociación completa

En la Figura 18, el tipo de protocolo es TCP, la dirección de IP local es 199, 21, 32, 2, el número de puerto de TCP local es 140, la dirección de IP local es 199,21,32,2, el número de puerto de TCP es remoto es 21. La asociación completa para el circuito está representado como un quinteto, este quinteto es:

(TCP, 199. 21. 32. 2, 1400,196.62..132.1, 21)

2.8 SERVIDORES PROXY

El proxy actúa de agente intermedio entre el cliente (mosaic, netscape, Internet explorer, etc.) y los servidores de la WWW, de forma que cuando se quiere acceder a una página de un servidor de la WWW, el cliente se conecta al servidor proxy que gestiona la obtención de la página desde el servidor solicitado.

Esto hace que el Proxy sea un eficaz sistema para mantener una memoria intermedia (caché muy grande) con los documentos accedidos más recientemente. Lo normal es que algunos servidores sean accedidos por diversos clientes en un mismo período de tiempo, por tanto si almacenamos las páginas e imágenes de estos servidores en una máquina local, el proxy, en la primera conexión obtiene la página requerida desde el servidor, siendo el acceso lento, y en los siguientes accesos a la misma página el acceso será mucho más rápido ya que se obtendrá directamente desde el proxy, si la página no ha cambiado, sin conectarse al servidor original.

Es decir, cuando un usuario pide una información a un servidor de Internet, el servidor Proxy comprueba si tiene la información pedida en su caché, si es así y la información almacenada es muy reciente, se la sirve inmediatamente al usuario, con lo que se ahorra el tiempo de traérsela de un servidor congestionado o lento. Si la información del caché no es reciente, el servidor Proxy comprueba con el servidor original, que la información del caché sigue siendo válida (este proceso es bastante rápido), en caso afirmativo, sirve al usuario la información del caché; en caso negativo, el servidor Proxy actualiza su información y simultáneamente se la envía al usuario. En caso de que un usuario pida información que el servidor Proxy no tenga en caché, este traslada la petición del usuario al servidor de Internet, cuando la recibe la envía de inmediato al usuario y simultáneamente la almacena.

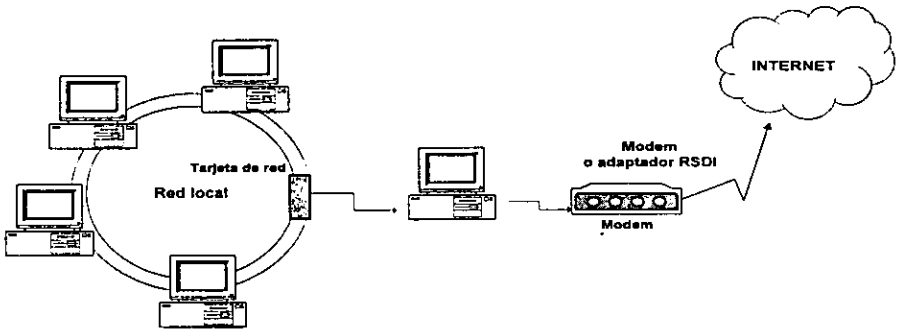


Figura 19. Ubicación del proxy server dentro de una red.

2.9 Intranets

Recordemos que Internet es por definición una red de alcance mundial, cuyos largos brazos se extienden a más de cien países de todos los continentes. Sin embargo, es en ámbitos reducidos e incluso locales donde se ha descubierto una nueva aplicación de gran interés: las Intranets, que no son más que redes locales privadas que trabajan internamente con protocolo TCP/IP. Hasta hace poco cada red local usaba un protocolo diferente, siendo Token Ring y Ethernet los dos estándares más popularizados.

2.9.1 Intranets e Internet

La mayoría de empresas que están implantando Intranets no lo hacen únicamente a nivel interno (es decir, usando TCP/IP dentro de sus redes locales). Más bien lo que se sigue es un esquema global de informatización, que incluye tanto a las Intranets como a los puntos de presencia en Internet de la empresa. Así, dentro de la misma estrategia se suele planificar el uso de redes corporativas internas, pero también el establecimiento de páginas web "externas", que se puedan consultar desde cualquier lugar del mundo. Esta filosofía nos lleva a un esquema bastante estándar, que es el que muestra la Figura 20:

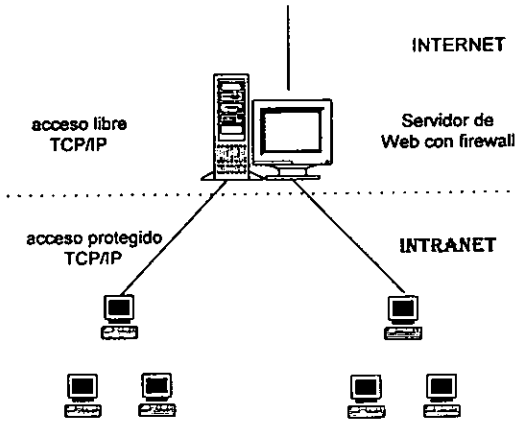


Figura 20. Intranets e Internet

Se trata de la parte que podrá ver cualquier usuario empleando un navegador desde su PC. Por otro lado, existe una segunda área, que es la Intranet propiamente dicha. Se trata de la instalación privada, que utiliza el personal autorizado para agilizar su trabajo.

2.9.2 Seguridad

Es evidente que no se desea que visitantes extraños puedan pasearse por la Intranet, y acceder a información confidencial. Es por ello que el tema de la seguridad en las Intranets es sumamente importante. No es de extrañar, por tanto, que existan un buen número de soluciones para garantizar la privacidad e integridad de datos, todas ellas de probada confianza. La más habitual (que es la que comentaremos aquí), pasa por el uso de firewalls.

2.9.3 Servidores de web

Usar una PC como servidor de web y punto de enlace con una Intranet es una decisión arriesgada, sobre todo si la instalación que ha de abastecer es mínimamente grande.

Evidentemente, una workstation es mucho más interesante que una PC en cuanto a prestaciones se refiere. Sin embargo, su precio aumenta en una relación casi directa. Es decir, una estación de trabajo que sea el cuádruple de rápida que un PC costará más o menos el doble que una que sea dos veces más rápida que la misma PC. Por ello su uso es especialmente interesante para nodos que soporten mucho tráfico, ya sea interno (proveniente de la intranet) o externo, pidiendo páginas web.

Por otro lado, una estación de trabajo es bastante más compleja de administrar que una PC. Se requiere personal calificado para manejarlas, ya que la mayoría de ellas trabajan con sistema UNIX, que es sumamente potente, pero nunca se ha caracterizado por su sencillez de uso.

Finalmente, sólo una workstation es capaz de gestionar el tráfico generado por un web y una Intranet de tamaño mediano o grande.

2.9.4 Groupware

En el contexto de las Intranets es evidente que el software que se emplee juega un papel capital. Es por ello que se ha llegado a crear un tipo de software especialmente diseñado para Intranets, que facilite la comunicación entre empleados o departamentos. Se trata del groupware, que podríamos definir como las aplicaciones de software diseñadas para optimizar el trabajo en grupos.

Algunas personas creen que el groupware lo componen herramientas como el Netscape Navigator o Eudora, y sin embargo la idea es muy diferente: no se trata de dar herramientas diseñadas para Internet y usarlas en entornos empresariales: se trata de reinventar muchos de los programas que actualmente se encuentran en uso, para que se concentren en el trabajo en grupo. Por ejemplo, la eficiencia de la Intranet depende en gran medida del software que se use. Las principales características de este tipo de software suelen ser:

- Arquitectura abierta, de manera que podamos usar el mismo soft en diversas máquinas, sistemas operativos y entornos.
- Soporte para web y forms. La representación de la mayoría de datos de las Intranets usan estos sistemas.
- Soporte para arquitecturas cliente-servidor.
- Soporte para aplicaciones distribuidas, RDBMS, etc.

Así pues, tenemos que una INTRANET es de acceso corporativo sólo interno, por ello, la idea fundamental de la INTRANET es soportar sólo aplicaciones corporativas, siendo uno de los objetivos de la intranet facilitar la distribución de información así como su fácil localización.

Recordemos que existen diferencias entre INTRANET e INTERNET, entre ellas figuran la privacidad (información sólo interna; pudiéndose acceder a la red local desde la red pública sólo por personal autorizado); control y administración; mejor rendimiento; aplicaciones seleccionadas, en caso de requerirse.

Un método para desarrollar una INTRANET es combinar Groupware y las aplicaciones con tecnologías Internet tales como el WEB, TCP/IP, visualizadores para generar nuevas aplicaciones como: publicación, búsqueda, grupos de discusión y manejo de documentos. Pero aunque el WEB es la pieza fundamental del desarrollo de la INTRANET requiere de otros elementos como el correo electrónico (SMTP), transferencia de archivos (FTP) y servicios de directorios (DNS).

No se deben perder de vista los componentes de hardware y software que requiere una intranet como son. Servidor de Intranet, software para dicho servidor, protocolo TCP/IP, visualizadores, firewall, componentes avanzados como Hot Java, Perl, entre otros.

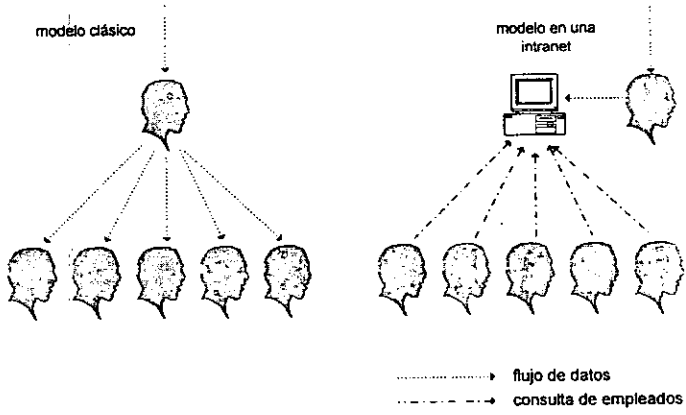
Como las aplicaciones en una intranet son escalables, es importante identificar las áreas de desarrollo, es decir establecer claramente las necesidades de información, para poder construir una estrategia de flujo de información, además de identificar las fuentes de contenidos o autores. Alternativamente, los contenidos deben enviarse a los administradores de información, los cuales determinarán las actividades de gestión de esa información así como los requerimientos de seguridad.

2.9.5 Mejorando el flujo de información

La idea de Intranet es sumamente simple, pero puede reportar grandes ventajas a cualquier empresa que decida a implementarla. Estas mejoras se dejan notar especialmente en dos áreas, que son la de la mejora de la comunicación entre empleados o departamentos, y la de la mejor estructuración de la información interna.

Por un lado, el hecho de contar con un protocolo como TCP/IP nos permite usar el tan popular correo electrónico. Avisos, circulares, notas o informes... todo se puede enviar por correo, con un considerable ahorro en tiempo y dinero. Por otra parte, gracias a su velocidad todo el personal podrá mantenerse en contacto casi continuo, y así mejorar su rendimiento. En este mismo contexto ya son varias las empresas que están empleando el servicio de IRC para mantener reuniones virtuales a través de Internet. Incluso ya existen paquetes de software específicos para realizar videoconferencia en Intranets.

En segundo lugar hablábamos de estructurar la información. Por ejemplo un día típico en una oficina: docenas de empleados transfiriéndose gráficos, expedientes, documentos... en resumen, información, el flujo de datos es unidireccional, y esto es uno de los grandes problemas que las Intranets resuelven. Veámoslo con un ejemplo clásico:



Aplicando el esquema clásico de circulación de datos en Intranets: el responsable de sección o departamento recibe la información que debe hacer llegar a sus empleados, pero no se la envía. En lugar de hacer esto, la sitúa en algún lugar accesible por todos los empleados a su cargo (habitualmente una home page de WWW). De esta manera, como cada empleado va a buscar la información, y nadie tiene que enviar los datos a todo el grupo de empleados, el flujo de datos es mucho más equilibrado. Lo que el empleado hace entonces es visitar la home page, y tomar la información que necesita.

Vemos que esto contribuye de manera colateral a arreglar un problema que casi todos los empleados padecen: el desorden. Cuando un empleado recibe un informe escrito, es posible que lo pierda, y esto es irreparable ya que tendremos que volverle a enviar otra copia. En cambio, si lo dejamos en un servidor de Web nada se puede perder, y todo estará bien organizado.

2.9.6 Mejorando la coordinación interna

La empresa clásica (como puede ser nuestro caso), como ya hemos subrayado, es bastante caótica: los informes se pierden, las tareas se repiten, etc. Por ello, no es extraño que a veces existan situaciones de falta de sincronización. Por ejemplo, imaginemos la siguiente situación: se solicita que se haga un determinado trabajo, y por falta de coordinación, este trabajo es realizado por dos empleados. Es evidente que aquí se ha desperdiciado potencial productivo, ya uno de los dos empleados no debería haber hecho ese trabajo. Esta situación es relativamente frecuente, y no es más que la punta del iceberg de la descoordinación inter e intradepartamental, que acecha tras cualquier esquina de la empresa clásica. Veamos qué pueden hacer las Intranets en este contexto, y cómo son una solución que, si bien no resuelve en sí misma el problema, ayuda bastante.

Para empezar, estos problemas de descoordinación se deben prácticamente siempre a una falta de comunicación. Si los dos empleados hubiesen hablado el uno con el otro, se hubiesen dado cuenta de que estaban trabajando innecesariamente. Esto no nos debe extrañar, ya que en una empresa con un número considerable de empleados es normal que sea difícil decirle a todos "El trabajo X ya lo hago yo", para evitar que otro empleado malgaste su tiempo. Se puede ver que el caso se parece mucho al problema que hemos citado antes sobre el flujo de información: un empleado que ha de pasar datos (en este caso, un aviso a los demás) al resto de la plantilla. Si se fija, la solución que adoptaremos es similar a la de aquel caso: invertir el flujo de datos, de manera que todo fluya de manera más natural y equilibrada. Se puede ver el resultado en la Figura 21:

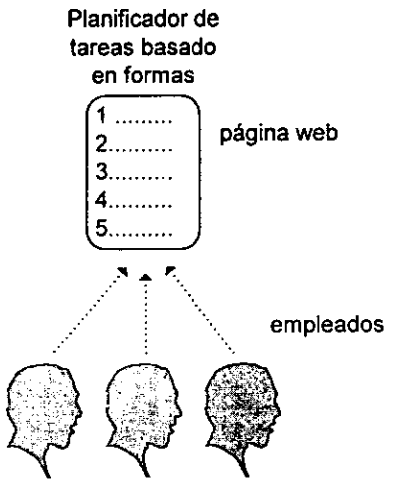


***Figura 21.** Flujo de información através de una página WEB*

Como se puede comprobar, aquí tenemos tres empleados que deben realizar unas tareas (de la uno a la cinco). Lo que podemos hacer es colocar la información en una página web interna, donde se describa cada tarea, quién se encarga de ella y su estado, así como posibles comentarios. Esta página sería el llamado planificador de tareas. Cada empleado puede acceder a él, y consultar quién se encarga de cada cosa, y qué tareas quedan pendientes de realización. Cuando un empleado inicia una tarea, lo hará accediendo al planificador de tareas mediante un formulario de HTML (form). Este formulario puede estar conectado a un programa que borre las tareas ya iniciadas de la lista de pendientes, y así evitar que dos empleados hagan lo mismo. El programa puede ser un CGI, o algo más sofisticado y eficaz como Java. En cualquier caso, con este pequeño sistema, que cualquier programador puede preparar en unos instantes, estamos aumentando sustancialmente la eficiencia de nuestra empresa.

Además para solicitudes externas lo podemos manejar con correo electrónico y de la misma forma responder a la petición

Como se puede notar, cada propuesta es una pieza de un gran rompecabezas, que es la estructura de la empresa del futuro. Una empresa donde el flujo de datos esté altamente automatizado, y que con ello consiga cumplir dos objetivos primordiales:

- Tiempo de respuesta muy bajo a peticiones del exterior y del interior.
- Alto nivel de coordinación y sincronización interna.

Lo que se propone es un mecanismo, que aumente la productividad sin por ello empeorar las condiciones laborales. Se trata de eliminar muchos puntos negros del día a día de las empresas, todo aquello que es ineficiente, y que la hace lenta e inoperante.

Esta nueva empresa podría tener una estructura interna como la que se muestra en la siguiente Figura 22:

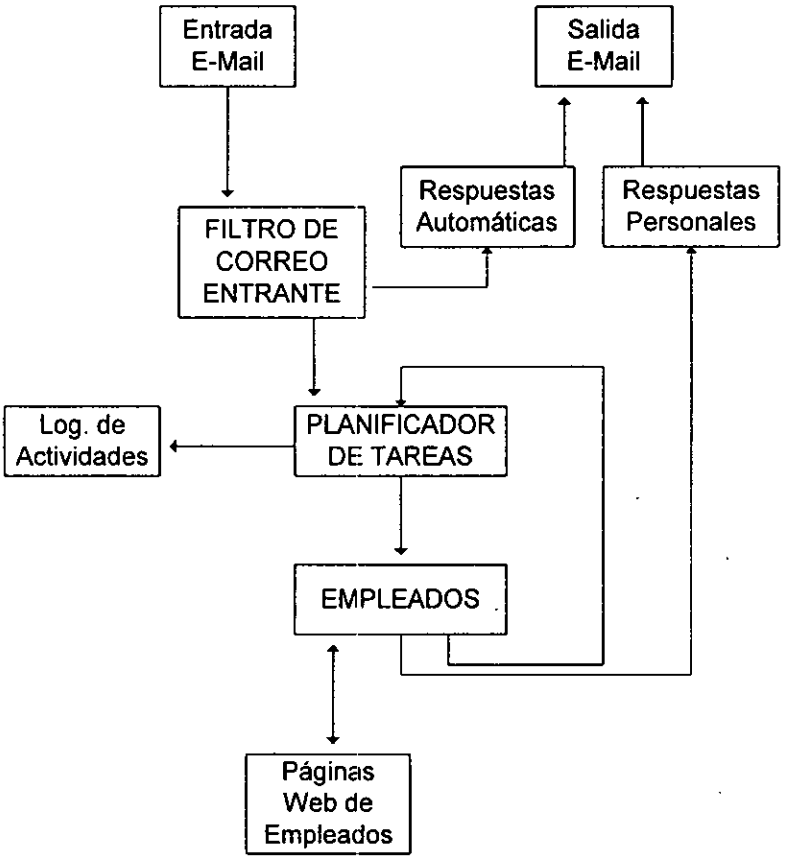


***Figura 22.** Estructura Interna de una empresa con Intranet*

Resulta evidente que, de todo el correo que reciba nuestra empresa, sólo una pequeña proporción realmente requiere un tratamiento personalizado. En muchas ocasiones una respuesta automática puede ser suficiente, aún cuando no conviene abusar de ellas. Por ejemplo, la mayoría de compañías dispone de mecanismos tipo "Si desea información sobre este tema, envíe un mensaje con la palabra "Info" en el campo subject". Todos estos mensajes no llegarán hasta los empleados, sino que serán filtrados por un CGI, y tratados convenientemente. Por otro lado, el correo que realmente necesite atención "humana" será pasado al famoso planificador de tareas, que será el centro neurálgico del sistema de control de la información dentro de la empresa.

El planificador es realmente el núcleo de nuestro sistema de información. Lo que intenta es dar un máximo rendimiento (medido en cantidad de peticiones satisfechas en un cierto tiempo). De hecho el planificador no es más que un gestor de una cola, donde los encargos se van amontonando hasta poderse satisfacer. La gestión eficaz de esta cola hará que nuestra empresa trabaje con más o menos rapidez. Un elemento a considerar cuando se programe este planificador es cómo se van a ordenar las tareas a realizar, es decir, qué es lo que se considera más urgente, y qué lo menos prioritario.

El planificador controlará dos tipos de encargos: por un lado, los provinientes del exterior, es decir, directamente desde algún punto de entrada. Estos deberían ser tratados prioritariamente, de manera que, vista desde fuera, nuestra empresa sea lo más parecido a un coche de carreras. Por otro lado, tenemos los encargos internos, que son realizados por un empleado. Por ejemplo, se puede tratar de un encargo generado por un jefe de departamento. En este caso el método a seguir ha de ser tal que haga que todas las tareas pendientes avancen a un ritmo más o menos parecido, pues no conviene que un cierto encargo se "haga viejo" dentro del planificador, sin nadie que lo atienda.

Finalmente, el planificador se debería encargar, de manera automatizada, de mantener un log, que no es más que un registro de incidencias y actividades, que se usaría para controlar el rendimiento. Por ejemplo, se debería guardar constancia de cuándo se recibe un encargo, cuándo se empieza a servir, y cuándo se completa, de manera que se puedan llevar a cabo estudios posteriores sobre lo bien o mal que funciona cada empleado, departamento o la empresa en general.

2.9.7 Visión de INTRANET según:

MICROSOFT

- Integración de pc's LANs, con aplicaciones cliente/servidor, sistemas basados en tecnologías anteriores y red pública Internet.
- El término INTRANET se usa ampliamente para describir la aplicación de la tecnología Internet en redes corporativas internas.
- Su uso principal es: publicar y compartir la información.

- Integración de la tecnología Internet con los sistemas cliente/servidor apoyados principalmente por el WWW.

Factores claves:
- Incluir los estándares Internet
- Extenderlos a nuevos servicios (transacciones comerciales)
- Innovación en áreas como: servicios de directorios, multimedia, seguridad, comercio electrónico y desarrollo de contenidos.

NETSCAPE

- La visión de Nescape esta en ofrecer un "Servicio Completo INTRANET - SCI"
- La visión deNetscape de SCI define como una compañía puede tomar ventaja de la tecnología Internet para Compartir Información, comunicaciones y aplicaciones sobre tecnologías de redes y plataformas abiertas.
- Las INTRANETs hace a las personas más productivas, mejores esquemas de acceso a la información corporativa y navegación a través de todos los recursos y aplicaciones de una compañía.

VISION NOVELL

- "Muerte al NOS (sistemas de red abiertas) nacimiento a la INTRANET"
- La nueva estrategia de Novell esta basada en IntranetWare, el cual incluye NetWare 4.11, Web Server 2.5, WAN routing, mejor soporte a TCP/IP y compuerta IP-IPX.
- Desarrollo de una Maquina Virtual JAVA como plataforma de desarrollo de aplicaciones INTRANET.
- La estrategia de novell para INTRANET estará acompañada de servicios de mensajería electrónica, administración y desarrollo de aplicaciones Cliente/Servidor.
- Novell posiciona al Visualizador (Browser) como el elemento universal de acceso a la información

VISION LOTUS NOTES

Lotus Notes es el líder en el mercado de productos para el soporte al groupware. Su nueva estrategia en INTRANET esta en sus productos: Lotus InterNotes y su servidor Domino, el cual nos brinda todas las ventajas de la Filosofía Notes en conjunción con la tecnología Internet principalmente basada en el WEB y el Correo Electrónico.

2.10 Gigabit Ethernet

Gigabit Ethernet es una extensión al estándar IEEE 802.3 o Ethernet 10/100 Mbps y conserva el mismo protocolo de control de acceso al medio (MAC: Media Access Control): CSMA/CD y es conocido también como estándar IEEE 802.3z.

En la Figura 23, se puede observar la arquitectura básica de la tecnología Gigabit Ethernet, cuyas implementaciones iniciales son a través de canales de fibra óptica y esquemas de codificación y decodificación de 8B/10B, los cuales son usados para serialización y deserialización de los datos.

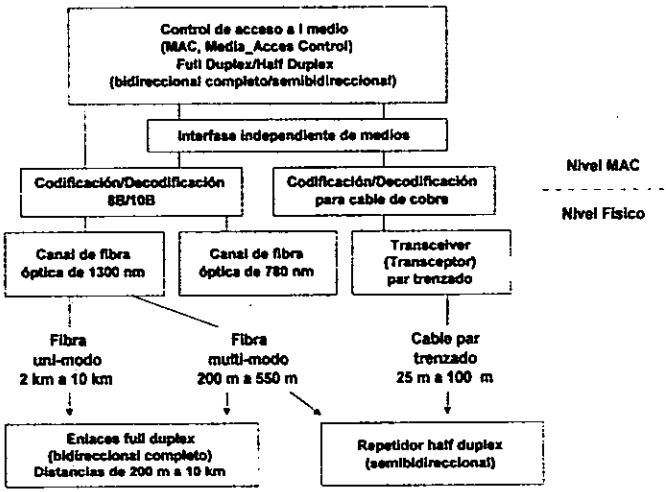


Figura 23. Arquitectura básica de la tecnología Gigabit Ethernet.

La tecnología actual de los circuitos integrados (IC: Integrated Circuits) para codificación y decodificación de señales sobre canales de fibra operan a 1.063 Gbps (Giga bits por segundo), pero ya están siendo mejorados para transmisiones de 1.250 Gbps.

A nivel de MAC se utiliza CSMA/CD con codificación y decodificación 8B/10B a través de canal de fibra. Sin embargo, en un futuro se piensa operar sobre cable par trenzado no blindado (UTP) categoría 5, para lograr distancias de hasta 100 metros. Para conseguir lo anterior es necesario establecer un módulo intermedio entre el nivel MAC y el nivel físico, que permita la utilización de otro tipo de método de codificación con el fin de lograr las interfaces entre el canal de fibra y el cable UTP, y soportar modos de operación (FDX) Full-Duplex (bidireccional completo) y (HDX) Half-Duplex (Semibidireccional).

Al operar en modo full-duplex, el trabajo de Gigabit Ethernet será exactamente igual al de fast Ethernet, sólo que más rápido (de 100 a 1000 Mbps). Pero al operar en modo half-duplex, se afectará el trabajo de Gigabit Ethernet, adicionando al protocolo CSMA/CD dos nuevas características: una es con respecto a la extensión de la portadora (carrier) de la señal y la otra es una modificación al paquete de datos.

2.10.1 Implementación de la tecnología Gigabit Ethernet.

Las empresas que tiene tecnología Ethernet o fast Ethernet (10/100 Base T) pueden emigrar muy fácilmente a Gigabit Ethernet desde los siguientes puntos de vista: conexiones de servidores a un switch; conexión switch a switch; mejorar el backbone (columna vertebral) Fast Ehternet; mejorar un backbone FDDI y mejorar su red local con estaciones conectadas, utilizando la nueva tecnología Gigabit Ethernet.

En cualquiera de los escenarios planteados, los sistemas operativos de Red (NOS; Network Operating Systems), las aplicaciones y los drivers (unidades de disco) de las tarjetas de interfaz de red (NIC: Network Interfase Card) permanecerán sin cambio en las estaciones. A continuación se describe cada uno de los escenarios mencionados.

2.10.2 Enlaces de Switch a switch.

En la Figura 24a, podemos ver dos switches Fast Ehternet que enlazan dos redes 10/100 Base T cada una con sus propios servidores y estaciones. La transmisión entre los switches de enlace de las dos redes es de 100 Mbps. Esta configuración puede ser mejorada si cambiamos los switches Fast Ehternet por switches Gigabit Ehternet 100/1000 Mbps, como se muestra en la Figura 24b. En esta configuración, la transmisión de datos entre los switches Gigabit Ehternet será de 100 Mbps, lo cual permitirá aumentar la eficiencia de respuesta entre las estaciones y los servidores de ambas redes

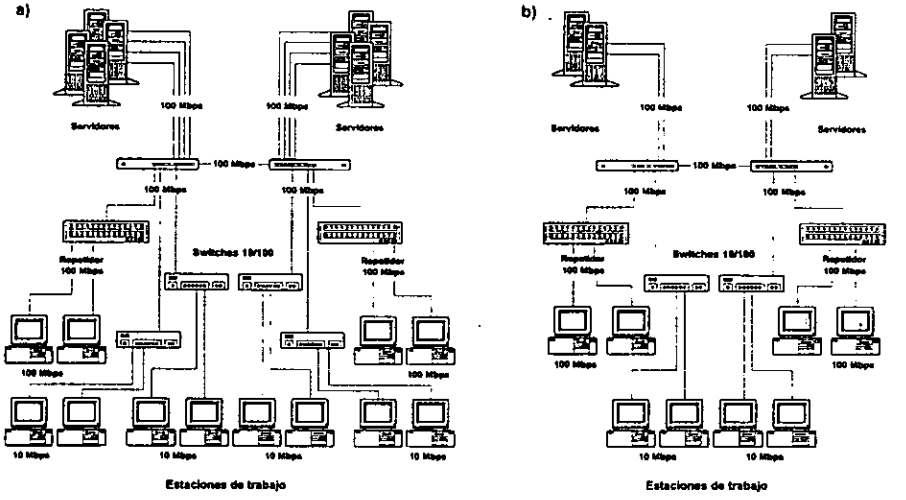


Figura 24. a) Switches Fast Ethernet, b) Switches Gigabit Ethernet

2.10.3 Enlaces de servidores a switch.

En la Figura 25, se puede observar una red local 10/1000 Base T con servidores conectados a un switch Fast Ehternet , al que se conectan concentradores o repetidores de 10 y de 100 Mbps, a los cuales están conectadas estaciones de trabajo a 10y 100 Mbps , respectivamente. Esta configuración puede ser mejorada , si se cambia el switch Fast Ehternet por un switch Gigabit Ehternet por un switch Gigabit Ethernet. A este switch se conectarán los servidores de la red con tarjetas de interfaz de red (NIC) Gigabit Ehternet, lo que hará que el trabajo entre los servidores y el switch se lleve acabo a 100 Mbps. Al switch Gigabit Ethernet se conectarán los otros concentradores o repetidores a 10/100 Mbps. Esta configuración permitirá una mejor respuesta de los servidores a las estaciones de trabajo.

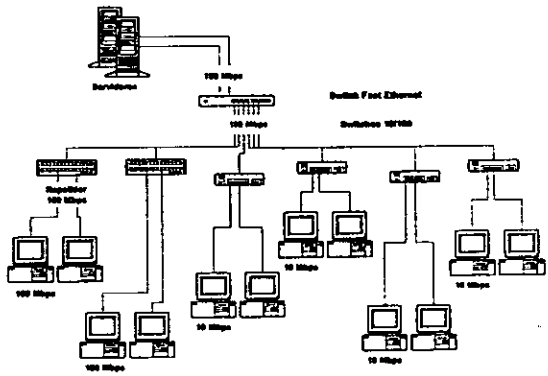


Figura 25. Red local 10/100 Base T

2.10.4 Mejorar el backbone

En la Figura 26a, podemos observar un backbone (columna vertebral) 10 Mbps con un switch Fast Ehternet. Este backbone permite comunicar estaciones de trabajo a través de switches o concentradores (concentradores) a 10/100 Mbps. El backbone puede modificarse y mejorarse si se cambia el switch Fast Ehternet por un switch Gigabit Ethernet, permitiendo la conexión con los switches 10/100 Mbps (véase Figura 26b).

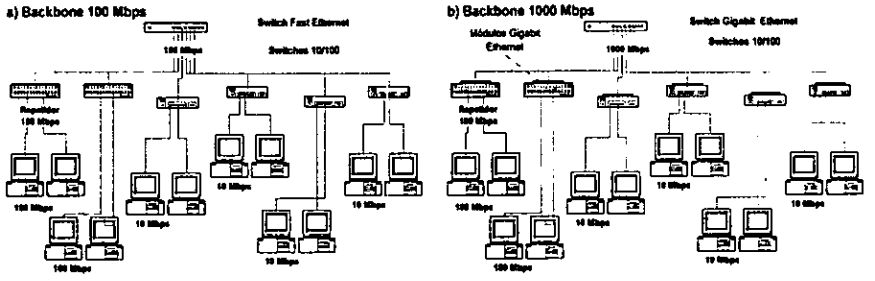


Figura 26. a) Backbone 10 Mbps, b) Backbone 1000 Mbps

Al switch Gigabit Ehternet pueden conectarse servidores con tarjetas de red Gigabit Ehternet.

2.10.5 Mejorar el backbone con tecnología FDDI.

Un backbone con switches FDDI puede ser modificado por un backbone Gigabit Ehternet, reemplazando un concentrador FDDI o un ruteador Ehternet FDDI con un switch Gigabit Ethernet. Además, se instalarán nuevas interfaces Gigabits Ethernet en los ruteadores o switches.

2.10.6 Redes de alto rendimiento con Gigabit Ehternet.

En la Figura 27a, se puede observar una red Fast Ehternet o FDDI con estaciones conectadas a un switch Fast Ehternet o FDDI. Se puede tener una red local utilizando exclusivamente tecnología Gigabit Ehternet (véase Figura 27b). Cada una de las estaciones y los servidores deben tener una tarjeta de interfaz de red (NIC) Gigabit Ehternet, y se conectarán a un switch Gigabit Ehternet. Con está configuración se mejorará el desempeño o rendimiento de la red, pues estará trabajando a 1000 Mbps; a diferencia de la red con configuración Fast Ehternet o FDDI, las cuales trabajan a 100 Mbps.

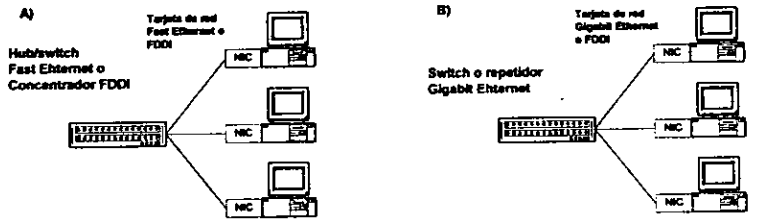


Figura 27. a) Red Ethernet o FDDI, b) Red Gigabit Ethernet

Finalmente, el costo de entrenamiento, mantenimiento y solución de problemas para Gigabit Ethernet será muy bajo en relación con otras tecnologías, si se toma en cuenta que la empresa o institución tiene su base en la tecnología Ethernet, la cual es casi idéntica a Gigabit Ethernet.

Además de los costos otra ventaja es que Gigabit Ethernet es más rápida que otras tecnologías como son Ethernet, Fasth Ethernet, Token Ring, FDDI y ATM.

2.11 Niveles de Seguridad en una Red

De acuerdo con las normas de seguridad establecidas por el Departamento de la Defensa de los Estados Unidos, los criterios estándar de evaluación de computadoras confiables, conocidos como "Libro Naranja[17]", usan varios niveles de seguridad para proteger de ataques el hardware, el software y la información almacenada. Estos niveles se refieren a diferentes tipos de seguridad física, autentificación de usuario, confiabilidad del software de sistema operativo y aplicaciones de usuario. Estos estándares también imponen límites a los sistemas que se puedan conectarse al propio.

NIVEL D1

El nivel D1 es la forma más baja de seguridad. Esta norma establece que el sistema entero no es confiable. No se dispone de protección para el hardware; el sistema operativo se compromete fácilmente y no existe autentificación respecto de los usuarios y sus derechos a tener acceso a la información almacenada en la computadora. Este nivel de seguridad por lo general se refiere a los sistemas operativos como MS-DOS, MS Windows y el Sistema 7.x de Apple Macintosh.

[17] El Libro Naranja ha permanecido sin cambios desde que se adoptó como estándar del Departamento de Defensa en 1985. Durante muchos años ha constituido el método básico para evaluar la seguridad de sistemas operativos multiusuarios en mainframes y mini. Otros subsistemas, como las bases de datos de redes, ha sido evaluados mediante la interpretación del Libro Naranja, como la interpretación de Bases de Datos Confiables y la Interpretación de Redes Confiables.

Estos sistemas operativos no distinguen entre los usuarios y no tienen definido ningún modelo para determinar quién está en el teclado. Asimismo, no tienen ningún control con respecto a la información a la que se pueda tener acceso en las unidades de disco duro de la computadora.

NIVEL C1

El nivel C tiene dos subniveles de seguridad: el C1 y el C2. El nivel C1, Sistema de Protección de Seguridad Discrecional, se refiere a la seguridad disponible en un Sistema Unix típico. Existe cierto nivel de protección para el harware, ya que éste no puede comprometerse fácilmente, aunque es posible. Los usuarios deben identificarse ante el sistema mediante su login y su contraseña. Se emplea esta combinación para determinar los derechos de acceso a programas e información que tiene cada usuario. Estos derechos de acceso son los permisos de archivo y de directorio. Los controles de acceso discrecional permiten al dueño del archivo o directorio, así como al administrador del sistema, evitar que cierta persona o grupos tengan acceso a dichos programas o información. Sin embargo, no se impide que la cuenta del administrador del sistema realice ninguna actividad.

Además, muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por el login de usuario llamado raíz (root).

NIVEL C2

El segundo subnivel, C2 está diseñado para ayudar a resolver los problemas anteriores. Además de las funciones del C1, el nivel C2 cuenta con características adicionales que crean un ambiente de acceso controlado. Este ambiente tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos comandos o tengan acceso a ciertos archivos, con base no sólo en los permisos sino también en los niveles de autorización. Además, este nivel de seguridad requiere que se audite el sistema, lo cual implica registrar una auditoría por cada acción que ocurra en el sistema.

La auditoría se utiliza para llevar registros de todas las acciones relacionadas con la seguridad, como pueden ser las actividades efectuadas por el administrador del sistema. La auditoría requiere de autentificación adicional, pues sin ésta, ¿cómo estar seguro de que la persona que ejecuta el comando realmente es quien dice ser?. La desventaja de la auditoría es que requiere recursos adicionales del procesador y del subsistema de disco.

Con el uso de autorizaciones adicionales, es posible que los usuarios de un sistema C2 tengan la autorización para realizar tareas de administración del sistema sin necesidad de la contraseña raíz. Esto permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

No debe confundirse estas autorizaciones adicionales con los permisos SGID y SUID que pueden aplicarse a un programa. Más bien se trata de autorizaciones específicas que permiten al usuario ejecutar comandos específicos o tener acceso a ciertas tablas de acceso restringido. Por ejemplo, cuando ejecutan el comado ps, los usuarios que no tienen autorización de ver la tabla de procesos sólo verán sus propios procesos.

NIVEL B1

El nivel de seguridad B consta de tres niveles. El nivel B1, llamado Protección de Seguridad Etiquetada, es el primer nivel con soporte para seguridad de multinivel, como el secreto y el ultrasecreto. En este nivel se establece que el dueño del archivo no puede modificar los permisos de un objeto que esté bajo control de acceso obligatorio.

NIVEL B2

El nivel B2, conocido como protección Estructurada, requiere que todos los objetos estén etiquetados. Los dispositivos como discos, cintas y terminales, pueden tener asignado uno o varios niveles de seguridad. Éste es el primer nivel en el que se aborda el problema de la comunicación de un objeto con otro que se encuentra en un nivel de seguridad inferior.

NIVEL B3

El nivel B3, llamado de Dominio de Seguridad, refuerza los dominios con la instalación de hardware. Por ejemplo, se utiliza hardware de manejo de memoria para proteger el dominio de seguridad contra accesos no autorizados y modificaciones de objetos en diferentes dominios de seguridad. Este nivel requiere también que la terminal del usuario esté conectada al sistema a través de una ruta de acceso confiable.

NIVEL A

Es conocido como el Diseño Verificado, constituye actualmente el nivel de seguridad validada más alto en todo el Libro Naranja. Cuenta con un proceso estricto de diseño, control y verificación. Para alcanzar este nivel, deben incluirse todos los componentes de los niveles inferiores: el diseño debe verificarse matemáticamente, y debe realizarse un análisis de los canales cubiertos y de distribución confiable. La *distribución confiable* significa que el hardware y el software hayan estado protegidos durante su traslado para evitar violaciones de los sistemas de seguridad.

2.11.1 Cómo Diseñar una Política de Red

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información. Una política de seguridad en redes

efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

Política de seguridad del sitio

Una organización puede tener muchos sitios, y cada uno contar con sus propias redes. Si la organización es grande, es muy probable que los sitios tengan diferente administración de red, con metas y objetivos diferentes.

Un sitio es cualquier parte de la organización que posee computadoras y recursos relacionados con redes. Algunos, no todos, de estos recursos son los siguientes:

- Estaciones de trabajo.
- Computadoras, hosts y servidores
- Dispositivos de interconexión: gateways, ruteadores, puentes, repetidores
- Servidores de terminal
- Software para conexión de red y de aplicaciones
- Cables de red
- La información de archivos y bases de datos

La política de seguridad del sitio debe tomar en cuenta la protección de esos recursos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

Planteamiento de la política de seguridad.

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra pérdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ¿Que recursos se están tratando de proteger?
- ¿De quien se necesita proteger los recursos?
- ¿Que tan posibles son las amenazas?
- ¿Que tan importante es el recurso?
- ¿Que medidas se pueden implementar para proteger los bienes de forma económica y oportuna?
- Examinar periódicamente la política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

La Figura 28 muestra una hoja de trabajo que ayuda a canalizar ideas conforme estos lineamientos.

- Número de recursos de red: es un numero de red de identificación interna de los recursos que van a ser protegidos (si se aplica).
- Nombre del recurso de red: es la descripción en lenguaje común de los recursos. La importancia del recurso puede estar en una escala del 0 a 10.

- Tipo de usuario del que hay que proteger al recurso: a los usuarios se les puede designar internos, externos, o grupos de nombres.
- Posibilidad de amenaza: Puede estar en una escala numérica del 0 al 10.
- Medidas que se implementaran para proteger el recurso de red:

Recursos de la fuente			Tipo de usuario del que hay que proteger el recurso	Posibilidad de amenaza	Medidas que se implementarán para proteger al recurso de la red
Número	Nombre	Importancia Del recurso			

Figura 28. Hoja de trabajo para establecer lineamientos

2.11.2 Cómo asegurar la responsabilidad hacia la política de seguridad.

Un aspecto importante de la política de seguridad de red es asegurar que todos conozcan su propia responsabilidad para mantener la seguridad. Las políticas pueden asegurar que para cada tipo de problema haya alguien que lo pueda manejar de manera responsable.

Análisis de riesgo

Se debe conocer cuáles recursos vale la pena proteger, y cuáles son más importantes que otros. También se debe identificar la fuente de amenazas que se está protegiendo la red.

El análisis de riesgo implica determinar lo siguiente:
- ¿Qué se necesita proteger?
- ¿De qué se necesita protegerlo?
- ¿Cómo protegerlo?

Los riesgos deben clasificarse por nivel de importancia y gravedad de la pérdida. En el análisis de riesgo hay que determinar los siguientes dos factores:
- Estimación de perder el recurso (Ri)
- Estimación de la importancia del recurso (Wi)

Puede asignarse un valor numérico como paso para cuantificar el riesgo de perder un recurso. Por ejemplo, puede asignarse un valor de 0 a 10 al riesgo (Ri) de perder un recurso, en donde 0 representa que no hay riesgo y 10 representa el más alto riesgo. De igual modo, a la importancia de un recurso (Wi) se le puede asignar un valor del 0 al 10, en donde 0 representa que no tiene importancia y 10 representa la máxima importancia. El riesgo evaluado del recurso será el producto del valor del riesgo y de su importancia. Esto puede escribirse como sigue:

$$WRI = Ri * Wi$$

Donde

Wri = Riesgo evaluado del recurso "i"
Ri = Riesgo del recurso "i"
Wi = Importancia del recurso "i"

La Figura 29 muestra una hoja de trabajo, que ayuda a registrar los datos anteriores.

- Número de recurso de red: es un número de red de identificación interna del recurso.
- Nombre del recurso de red: es una descripción en lenguaje común de los recursos.
- Riesgo de los recursos de red (RI) puede estar en una escala numérica del 0 a 10.
- Importancia del recurso (Wi): puede estar en una escala numérica del 0 al 10.

Recursos de la fuente		Riesgo de los recursos de la red (Ri)	Importancia Del recurso (Wi)	Riesgo evaluado (Ri*Wi)
Número	Nombre			

Figura 29. Hoja de trabajo que ayuda a registrar datos

La evolución de la amenaza y los riesgos no debe ser una actividad de una sola vez; debe realizarse con regularidad, como se defina en la política de seguridad del sitio.

2.11.3 Identificación de recursos

Es importante identificar a todos los recursos de la red que puedan ser afectados por un problema de seguridad. La RFC 1244 enlista los siguientes recursos de red que se deben considerar al calcular las amenazas a la seguridad general.

- Hardware
- Software
- Datos
- Personas
- Documentación

Definición del acceso no autorizado

Se considera que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado.

Riesgo de revelación de información

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Se debe determinar el valor y delicadeza de la información guardada en las computadoras.

Uso y responsabilidad de la red

Existen numerosas cuestiones que deben abordarse al elaborar una política de seguridad:

- ¿Quién está autorizado para usar los recursos?
- ¿Cuál es el uso adecuado de los recursos?
- ¿Quién está autorizado para conceder acceso y aprobar el uso?
- ¿Quién puede tener privilegios de administración del sistema?
- ¿Cuales son los derechos y las responsabilidades del administrador del sistema en comparación con los usuarios?
- ¿Qué hacer con la información delicada?

La política de seguridad de red debe identificar quién está autorizado para conceder acceso a sus servicios. También se debe determinar que tipo de acceso puede conceder dichas personas.

Si la organización es grande y descentralizada, quizá haya muchos puntos centrales. La administración centralizada puede crear problemas cuando los departamentos deseen tener mayor control sobre los recursos de la red.

El objetivo es equilibrar el acceso restringido a los privilegios especiales para hacer más segura la red, con el otorgamiento de acceso a las personas que necesitan esos privilegios para realizar sus tareas. En general, se debe conceder sólo los privilegios suficientes para cumplir con las tareas necesarias.

La Figura 30 se muestra una hoja de trabajo que puede usarse para llevar un registro en papel de los permisos que se otorguen a un usuario. La siguiente es una descripción de las columnas usadas en la hoja de trabajo:

- Número de recurso de red: es un número de red de identificación interna del recurso.
- Nombre del recurso de red: es una descripción en lenguaje común delos recursos.
- Tipo de acceso: Puede usarse para describir el recurso, como acceso de lectura y ejecución del directorio.
- Permisos del sistema operativo: Contiene los indicadores del sistema operativo usados para implementar el acceso de seguridad (Lectura, escritura y ejecución)

Recursos de la fuente		Tipo de	Permiso de sistema operativo
Número	Nombre	Acceso	UNIX:rwx

Figura 30. Hoja de trabajo para registro de permisos

También se debe tener una política para seleccionar la contraseña inicial. El momento de otorgar la contraseña inicial es muy vulnerable para la cuenta de usuario. Las políticas como aquellas donde la contraseña inicial sea igual al nombre del usuario, o que se quede en blanco, pueden dejar al descubierto las cuentas. Asimismo, se recomienda evitar establecer la contraseña inicial como una función del nombre de usuario, o parte de éste, o alguna contraseña generada por un algoritmo que pueda adivinarse con facilidad. La selección de la contraseña inicial no debe ser tan obvia.

Determinación de las responsabilidades de los usuarios y de los administradores de sistemas

La política de seguridad de la red debe definir los derechos y responsabilidades de los usuarios que utilizan recursos y servicios de la red. El derecho de un usuario podría ser su privacidad en su información, y como responsabilidad, el respaldo de su información. Es necesario que el usuario tenga conocimiento de sus derechos y responsabilidades.

La política de seguridad de la red debe especificar el grado al que el administrador del sistema pueda examinar los directorios y archivos de un usuario, solo y solamente en caso de peligro de la seguridad o prevención de la misma.

Además, se debe proponer un plan de acción cuando se viole la política de seguridad establecida, ya sea para proteger y continuar o investigar y sancionar.

Interpretación y Publicación de la Política de Seguridad

Es importante identificar a las personas que interpretarán la política. Generalmente no es aconsejable que sea una sola persona, ya que podría no estar disponible en el momento de la crisis. Se puede designar un comité, pero también se recomienda que no esté constituido por muchos miembros. Con cierta periodicidad, se debe convocar al comité de política de seguridad para interpretar, repasar y revisar el documento.

Una vez redactada la política de seguridad y se haya alcanzado el consenso en sus puntos, el sitio debe asegurarse de que la declaración de política se divulgue y discuta

ampliamente, por ejemplo, a través de listas de correo. Por otra parte, puede reforzarse la nueva política mediante educación interna, como seminarios de capacitación, sesiones informativas, talleres, reuniones personales con el administrador, etc.

CAPÍTULO 3

3. Análisis de la Red de la Facultad de Ingeniería

3.1 Condiciones Actuales de la Red

El presente capítulo hará referencia de las condiciones físicas y lógicas actuales de la red en la Facultad. Se tratarán temas como la estructura que guarda la red, así como su topología, sistemas operativos, los equipos y dispositivos que operan en ella, software de comunicación y control o monitoreo de la red.

Este capítulo también mostrará un análisis en el que se da una visión en términos generales de las condiciones en las que opera la red.

Es importante mencionar que la red de la FI está conectada a Red UNAM por medio de fibra óptica. Red UNAM tiene sus nodos principales en la DGSCA (Dirección General de Servicios de Cómputo Académico), IIMAS (Instituto de Investigaciones Aplicadas y Sistemas), y el Instituto de Astronomía.

La red de la Facultad está dividida en 5 zonas (Tabla 1), las cuales se encuentran distribuidas como se muestra en la *Figura 1*.

Zona	Ubicación
A	Edificio Principal
B	DIMEI y Valdés Vallejo
B	Edificio de Posgrado
C	DICTyG, DCB, Talleres Mec., Lab. Termo., Biblioteca y UNICA (Fundación UNAM).
D	Palacio de Minería

***Tabla 1.** Asignación de zona, para cada división*

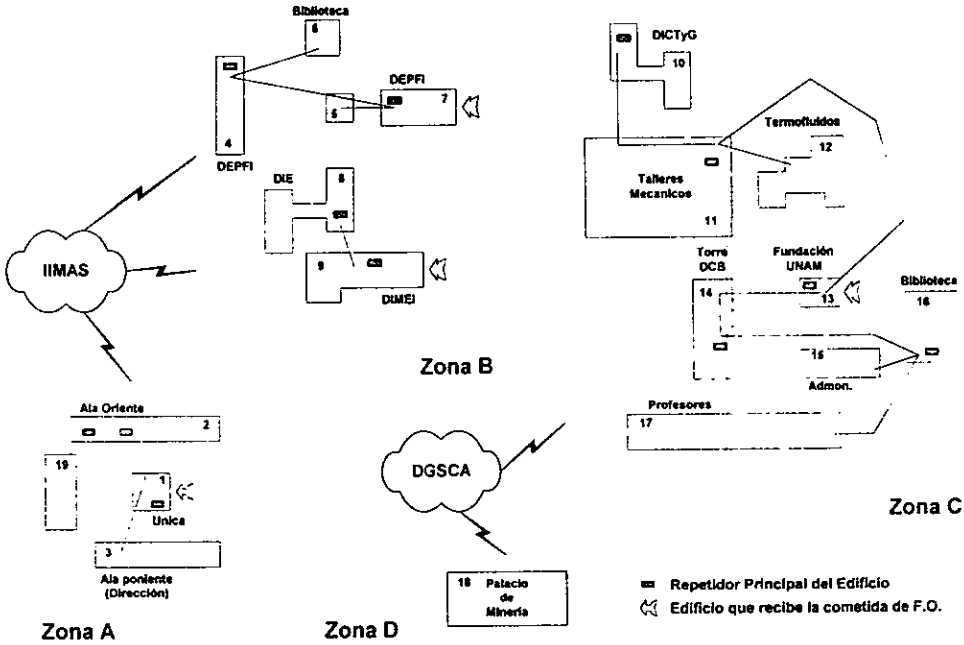


Figura 1. Diagrama oficial de la Red de la Facultad de Ingeniería [1]

3.1.1 Estructura

Tipo de red

La red de cada una de las zonas de la FI está considerada como una red LAN que en su conjunto forman una red WAN.

Sistema operativo

Por los fines académicos que persigue la FI se podrá notar que no existe un sistema operativo de red uniforme, esto se refleja en los laboratorios de computadoras y programación de la DIE, de UNICA y en del laboratorio de Fundación UNAM.
A continuación se presentan los sistemas operativos que normalmente se utilizan en cada división.

[1] Diagrama publicado en "Facultad de Ingeniería: Órgano informativo FI, UNAM", No. 69; 25 de agosto de 1997.

En la Zona A:

Edificio 1: Sistema operativo UNIX, Windows NT, Windows 95 y Netware.

Edificio 2: Sistema operativo Windows 95 y Netware.

Edificio 3: Sistema operativo Windows 95 y Netware.

En la Zona B:

Edificio 4: Sistema operativo Windows 95, UNIX y NT.

Edificio 5: Sistema operativo Windows 95, NT y Netware.

Edificio 6: Sistema operativo Windows 95, UNIX, Windows NT y Netware.

Edificio 7: Sistema operativo Windows 95, UNIX, Windows NT y Netware.

Edificio 8: Sistema operativo Windows 95, UNIX, LINUX y Netware.

Edificio 9: Sistema operativo Windows 95 y Netware.

En la Zona C:

Edificio 10: Sistema operativo Windows 95 y Netware.

Edificio 11: Sistema operativo Windows 95, UNIX y Netware.

Edificio 12: Sistema operativo Windows 95 y Netware.

Edificio 13: Sistema operativo UNIX, Windows NT, Windows 95 y Netware.

Edificio 14: Sistema operativo UNIX, Windows NT y Windows 95.

Edificio 15: Sistema operativo UNIX, Windows NT y Windows 95.

Edificio 16: Sistema operativo UNIX, Windows NT y Windows 95.

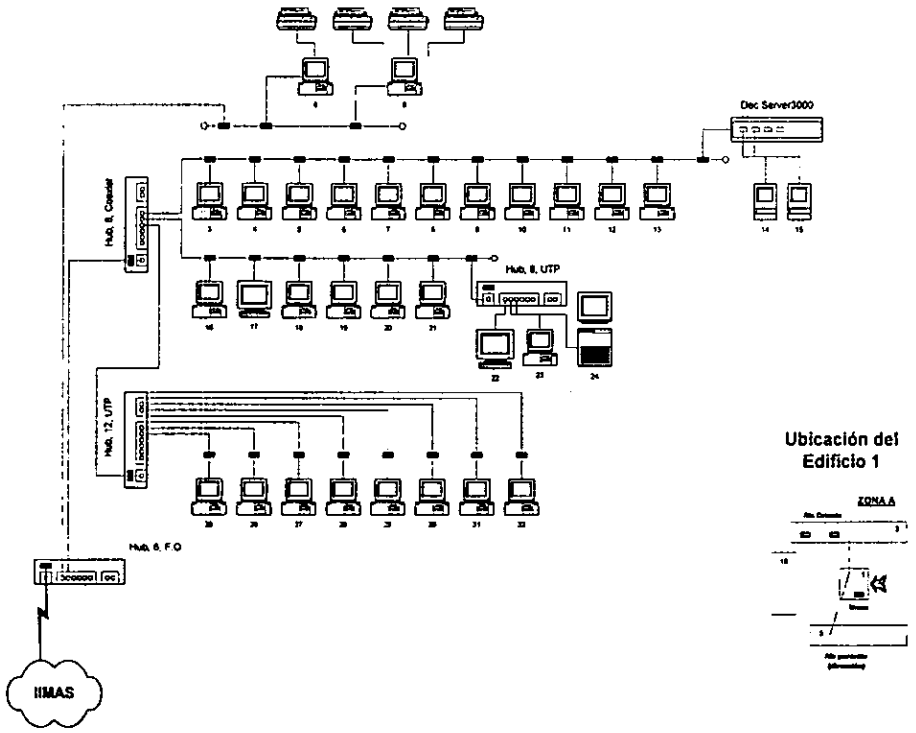
Edificio 17: Sistema operativo UNIX, Windows NT y Windows 95.

Topología

La red de la FI se basa en la tecnología Ethernet, que es una topología de bus ramificada. A continuación se muestra en forma gráfica dicha topología localizada en las diversas zonas para las que se hace referencia[2]:

Zona A

La punta de fibra óptica se recibe del IIMAS y llega al concentrador ubicado en la planta baja del edificio 1, para distribuirse a los edificios restantes de la zona. En esta zona es donde se encuentran los servidores Cozumel, Cancún y Mixquic en UNICA; Cerebro y Cosmeg en USECAD entre otros.

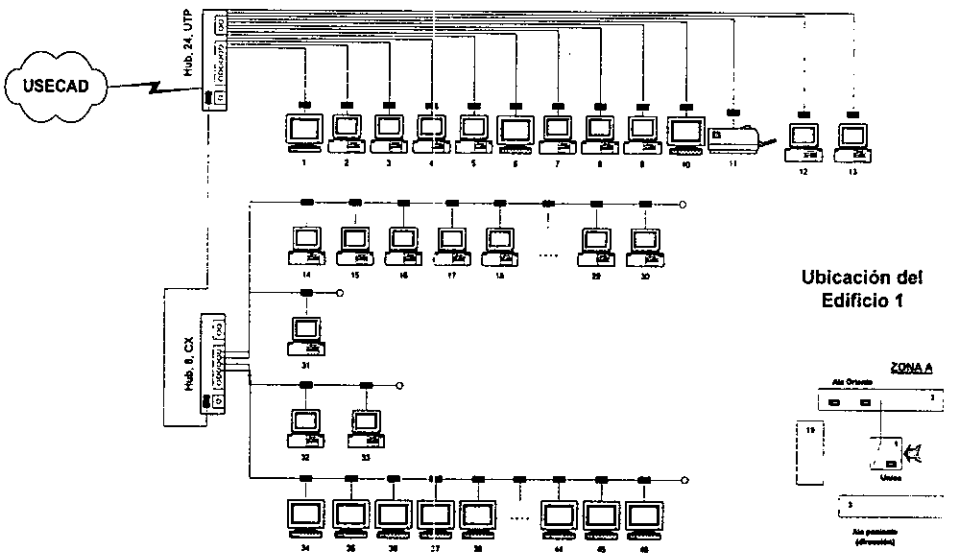


[2] Las direcciones referidas en las tablas, únicamente denotan las últimas tres cifras de la dirección IP

Núm.	Ubicación	Nombre	Dirección	Dispositivo
1	Planta baja			PC
2	Planta baja			PC
3	Planta baja	reins_3	123	PC
4	Planta baja	reins_2	251	PC
5	Planta baja	reins_1	122	PC
6	Planta baja	marco_polo	110	PC
7	Planta baja	becarios_1	114	PC
8	Planta baja	becarios_2	130	PC
9	Planta baja	cosmeg	106	PC
10	Planta baja	zaratustra	109	PC
11	Planta baja	wolverine	121	PC
12	Planta baja	servidor	129	PC
13	Planta baja	spider	125	PC
14	Planta baja			
15	Planta baja			
16	Planta baja	pathworks_hp	113	PC

Núm.	Ubicación	Nombre	Dirección	Dispositivo
17	Planta baja	coordinador	248	WS
18	Planta baja	gustavo_2	247	PC
19	Planta baja	hulk	154	PC
20	Planta baja	flash	104	PC
21	Planta baja	mandrake	115	PC
22	Planta baja	cleopatra	111	ws
23	Planta baja	xxx	105	PC
24	Planta baja	cerebro	101	PC
25	Planta baja			PC
26	Planta baja			PC
27	Planta baja			PC
28	Planta baja			PC
29	Planta baja			PC
30	Planta baja			PC
31	Planta baja			PC
32	Planta baja			PC

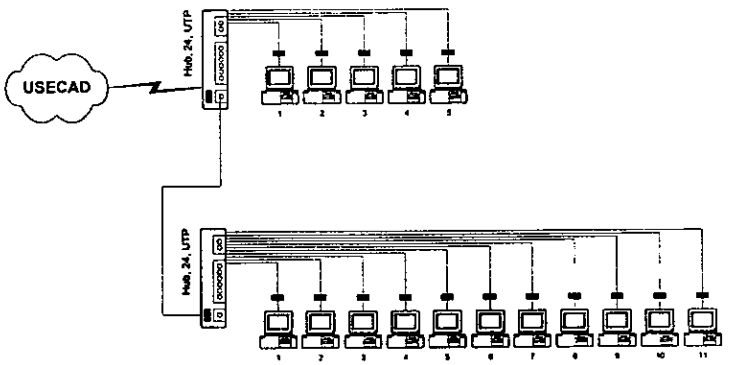
Figura 2. Edificio 1

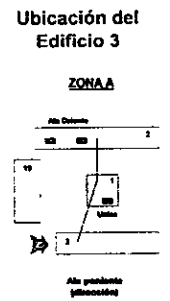


Núm.	Ubicación	Nombre	Dirección	Dispositivo
1	Primer Piso	biani	67	WS
2	Primer Piso	jhon_lennon	244	PC
3	Primer Piso	paul_mcarney	233	PC
4	Primer Piso	aztlan	50	PC
5	Primer Piso	itza	55	PC
6	Primer Piso	mixquic	66	WS
7	Primer Piso	hetzhi	34	PC
8	Primer Piso	becarios_2	64	PC
9	Primer Piso			PC
10	Primer Piso	ixtan	29	WS
11	Primer Piso			impresora
12	Primer Piso	matarl	69	PC
13	Primer Piso	saul_hernadez	46	PC
14	Primer Piso	iztac	52	PC
15	Primer Piso	halo-bopp	48	PC
16	Primer Piso	orion	42	PC
17	Primer Piso	tlatoani	41	PC
18	Primer Piso	control	33	PC
19	Primer Piso	etienne	51	PC
20	Primer Piso	tekila	49	PC
21	Primer Piso	manuel	62	PC
22	Primer Piso	champagne	57	PC
23	Primer Piso	tauro	58	PC
24	Primer Piso		211	PC
25	Primer Piso	libra	56	PC
26	Primer Piso	casper	45	PC
27	Primer Piso	diablo	47	PC
28	Primer Piso	taz	40	PC

Núm.	Ubicación	Nombre	Dirección	Dispositivo
29	Primer Piso	piscis	39	PC
30	Primer Piso	anthrax	54	PC
31	Primer Piso	alex_lora	43	PC
32	Primer Piso		xxx	PC
33	Primer Piso		xxx	PC
34	Primer Piso	alika	14	WS
35	Primer Piso	balam	4	WS
36	Primer Piso	caxumel	13	WS
37	Primer Piso	tork	3	WS
38	Primer Piso	tulum	18	WS
39	Primer Piso	chacmol	23	WS
40	Primer Piso	calmecac	28	WS
41	Primer Piso	xilbaba	26	WS
42	Primer Piso	nepohual	27	WS
43	Primer Piso	ayaic	20	WS
44	Primer Piso	uxmal	16	WS
45	Primer Piso	xelha	21	WS
46	Primer Piso	tikal	19	WS
47	Primer Piso	itza	5	WS
48	Primer Piso	kabah	9	WS
49	Primer Piso	edzna	8	WS
50	Primer Piso	kay	6	WS
51	Primer Piso	ixtapa	11	WS
52	Primer Piso	iztac	17	WS
53	Primer Piso	tonantzi	24	WS
54	Primer Piso	ehecatl	7	WS
55	Primer Piso	ati	2	WS
56	Primer Piso	cancun	10	WS

Figura 3. Edificio 1

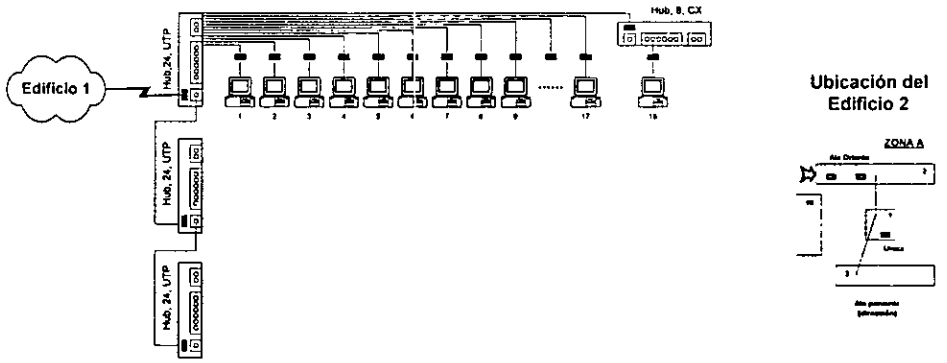




Núm.	Ubicación	Nombre	Dirección	Dispositivo
1	Planta baja	neptuno	182	PC
2	Planta baja	esfinge	185	PC
3	Planta baja	jupiter	184	PC
4	Planta baja	saturno	183	PC
5	Planta baja	urano	181	PC
6	Planta baja		170	PC
7	Planta baja		179	PC
8	Planta baja		165	PC

Núm.	Ubicación	Nombre	Dirección	Dispositivo
9	Planta baja		178	PC
10	Planta baja	espinela	161	PC
11	Planta baja		162	PC
12	Planta baja			PC
13	Planta baja	gema	177	PC
14	Planta baja		160	PC
15	Planta baja			PC
16	Planta baja			PC

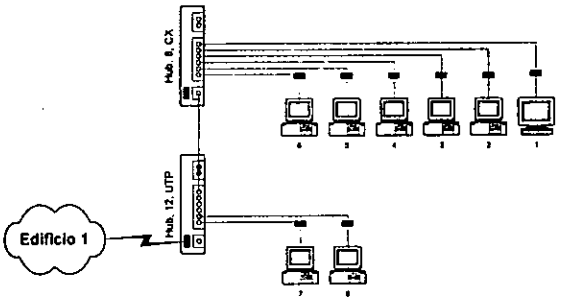
Figura 4. Edificio 3.

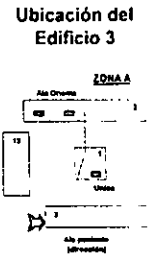


Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1		auxiliar	153	PC
2		topacio	157	PC
3		espinela	151	PC
4		amatista	162	PC
5		esmeralda	171	PC
6		rubi	166	PC
7		jade	172	PC
8		berilo	169	PC
9		peridoto	175	PC

Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
10		diamante	173	PC
11		malquita	168	PC
12		granate	165	PC
13		brillante	167	PC
14		zafiro	164	PC
15		turqueza	160	PC
16		opalo	163	PC
17		turmalina	158	PC
18		zircon	159	PC

Figura 5. Edificio 2



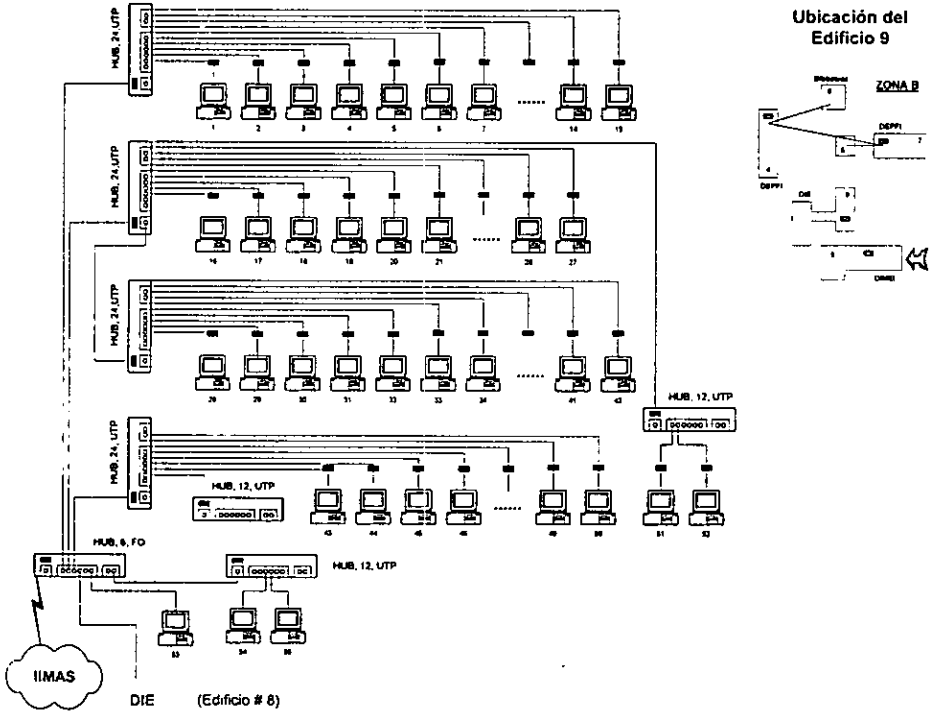


Número	Ubicación	Nombre	Dirección IP	Dispositivo
1	Salon 17	sacbe	151	WS
2	Salon 17	sacbe1	152	PC
3	Salon 17	sacbe2	153	PC
4	Salon 17	sacbe3	154	PC
5	Salon 17	sacbe4	155	PC
6	Salon 17	sacbe5	156	PC
7	Planta baja	cuarzo	174	PC
8	Planta baja	aguamar	176	PC

Figura 6. Edificio 3

Zona B

Otra Punta de fibra óptica que viene del IIMAS llega a un concentrador al edificio 9.



Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1	Tercer piso	detron1	160	PC
2	Tercer piso	detron2	162	PC
3	Tercer piso	detron3	167	PC
4	Tercer piso	detron4	170	PC
5	Tercer piso	detron5	171	PC
6	Tercer piso	detron6	176	PC
7	Tercer piso	detron7	161	PC
8	Tercer piso	detron8	166	PC
9	Tercer piso	detron9	175	PC
10	Tercer piso	detron10	177	PC
11	Tercer piso	detron11	178	PC
12	Tercer piso	detron12	179	PC
13	Tercer piso	detron14	164	PC
14	Tercer piso	detron15	165	PC
15	Tercer piso	detron16	173	PC
16	Segundo piso	aries	1	PC

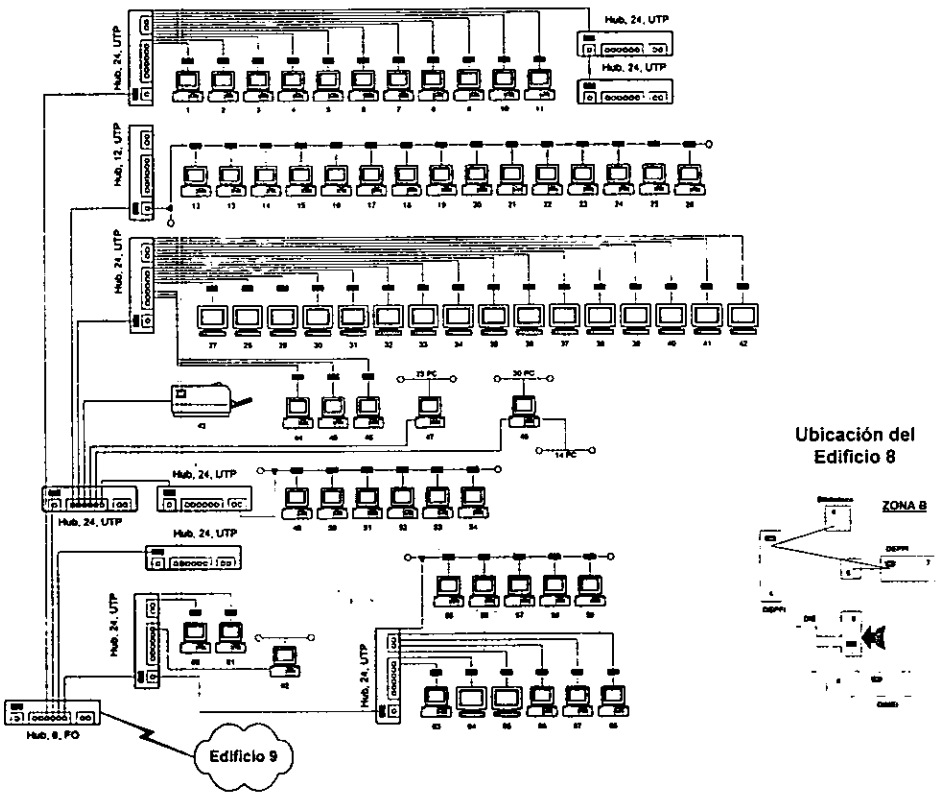
Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
29	Segundo piso	nyquist	102	PC
30	Segundo piso	jury	103	PC
31	Segundo piso	ackermann	104	PC
32	Segundo piso	evans	105	PC
33	Segundo piso	ricatti	106	PC
34	Segundo piso	ziegler	107	PC
35	Segundo piso	bristol	108	PC
36	Segundo piso	maxwell	111	PC
37	Segundo piso	watt	114	PC
38	Segundo piso	kalman	115	PC
39	Segundo piso	bucl	116	PC
40	Segundo piso	taylor	117	PC
41	Segundo piso	maria	118	PC
42	Segundo piso	davinci	128	PC
43	Segundo piso	stand	130	PC
44	Segundo piso	jdle131	131	PC

Figura 7. Edificio 9

Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
17	Segundo piso	cronos	2	PC
18	Segundo piso	eclipse	19	PC
19	Segundo piso	perseo	24	PC
20	Segundo piso	limbo	32	PC
21	Segundo piso	urban	33	PC
22	Segundo piso	frida	34	PC
23	Segundo piso	cellan	35	PC
24	Segundo piso	dlecor1	201	PC
25	Segundo piso	dless	202	PC
26	Segundo piso	dlecor3	203	PC
27	Segundo piso	dlecor4	204	PC
28	Segundo piso	nichols	101	PC

Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
45	Segundo piso	idle132	132	PC
46	Segundo piso	idle133	133	PC
47	Segundo piso	idle134	134	PC
48	Segundo piso	idle135	135	PC
49	Segundo piso	idle136	136	PC
50	Segundo piso	idle137	137	PC
51	Segundo piso	routh	103	PC
52	Segundo piso	bradley	113	PC
53	Planta baja	idimei	205	PC
54	Planta baja	labii	206	PC
55	Planta baja	depii	207	PC

Figura 8. Edificio 9

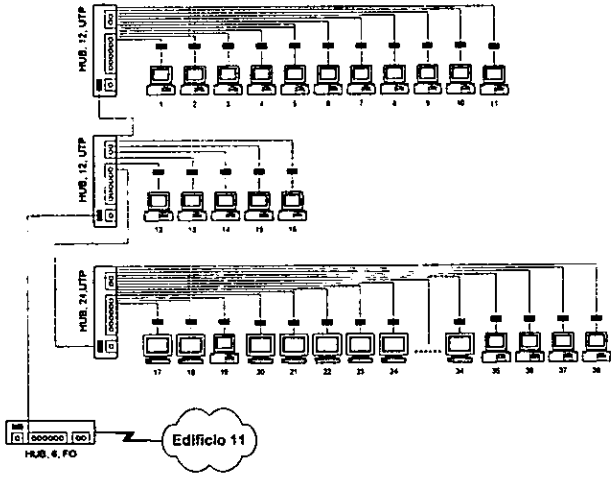


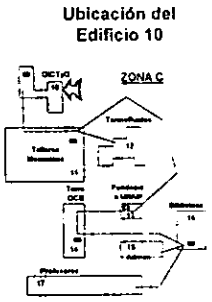
Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1	Tercer Piso	telecom01	180	PC
2	Tercer Piso	telecom02	181	PC
3	Tercer Piso	telecom03	182	PC
4	Tercer Piso	telecom04	183	PC
5	Tercer Piso	telecom05	184	PC
6	Tercer Piso	telecom06	185	PC
7	Tercer Piso	telecom07	186	PC
8	Tercer Piso	telecom08	187	PC
9	Tercer Piso	telecom09	188	PC
10	Tercer Piso	telecom10	189	PC
11	Tercer Piso	telecom11	190	PC
12	Segundo Piso	cubi208	53	PC
13	Segundo Piso	cubi209	54	PC
14	Segundo Piso	cubi210	55	PC
15	Segundo Piso	cubi211	56	PC
16	Segundo Piso	cubi212	57	PC
17	Segundo Piso	cubi213	58	PC
18	Segundo Piso	fanny	52	PC
19	Segundo Piso	cubi201	46	PC
20	Segundo Piso	cubi202	47	PC
21	Segundo Piso	cubi203	48	PC
22	Segundo Piso	cubi204	49	PC
23	Segundo Piso	cubi205	50	PC
24	Segundo Piso	cubi206	51	PC
25	Segundo Piso	cubi207	52	PC
26	Segundo Piso	icomp96	96	PC
27	Segundo Piso	zeus	3	WS
28	Segundo Piso	brahm	4	WS
29	Segundo Piso	rha	5	WS
30	Segundo Piso	odin	6	WS
31	Segundo Piso	garmur	7	WS
32	Segundo Piso	quiron	8	WS
33	Segundo Piso	feuris	9	WS
34	Segundo Piso	gias	10	WS
35	Segundo Piso	hera	11	WS
36	Segundo Piso	vesta	12	WS
37	Segundo Piso	siva	13	WS
38	Segundo Piso	vishu	14	WS
39	Segundo Piso	isis	15	WS
40	Segundo Piso	osiris	16	WS
41	Segundo Piso	thor	17	WS
42	Segundo Piso	loki	18	WS
43	Segundo Piso	mercurio	60	impresora
44	Segundo Piso	prometeo	25	PC
45	Segundo Piso	carellian	62	PC
46	Segundo Piso	arrakis	65	PC
47	Segundo Piso	icomp98	98	PC
48	Segundo Piso	linux1	66	PC
49	Segundo Piso	io	21	PC
50	Segundo Piso	catalli	23	PC
51	Segundo Piso	febo	30	PC
52	Segundo Piso	balder	41	PC
53	Segundo Piso	lestat	42	PC
54	Segundo Piso	draco	44	PC
55	Planta baja	mmedia1	36	PC
56	Planta baja	mmedia2	37	PC
57	Planta baja	mmedia3	38	PC
58	Planta baja	mmedia4	39	PC
59	Planta baja	icomp97	97	PC
60	Planta baja	aztlan	140	PC
61	Planta baja	becan	141	PC
62	Planta baja	icomp99	99	PC
63	Planta baja	mezcal	45	PC
64	Planta baja	tequila	40	WS
65	Planta baja	pulque	43	WS
66	Planta baja	detron13	163	PC
67	Planta baja	detron17	174	PC
68	Planta baja	detron3	3	PC

Figura 9. Edificio 8.

Zona C

La acometida de fibra óptica llega al edificio 13 (Sala de Fundación UNAM), para distribuirse en siete líneas a los edificios 10 (DICTyG), 11 (CDM[3]), 12 (Lab. Termofluidos), 14 (DCB), 15 (Admon.), 16 (Biblioteca) y 17 (Profesores). Del edificio 11 se distribuyen dos lineas a los edifios 10 y 12.



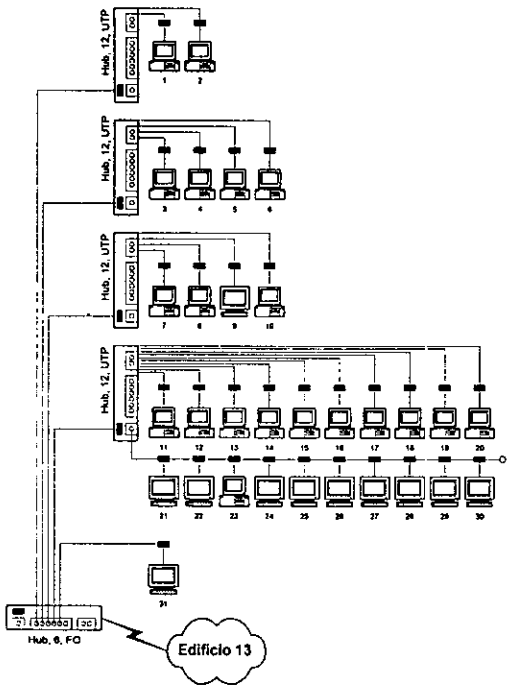


Núm.	Ubicación	Nombre	Dirección	Dispositivo
1	Planta baja	sanitario	120	PC
2	Planta baja	hidraulica	123	PC
3	Planta baja	card_topo	121	PC
4	Planta baja	topografia	117	PC
5	Planta baja	orien	141	PC
6	Planta baja	geodesio	102	PC
7	Planta baja	sistemas	114	PC
8	Planta baja	geotecnia	19	PC
9	Planta baja	Estructura	16	PC
10	Planta baja	Practicas	15	PC
11	Planta baja	Construye	13	PC
12	Planta baja	Dictyg	142	PC
13	Planta baja	Sec_acad	144	PC
14	Planta baja	Propuesto	145	PC
15	Planta baja	Profesrado	146	PC
16	Planta baja	Sec_tec	147	PC
17	Primer piso	Gondor	106	WS
18	Primer piso	Numenor	107	WS
19	Primer piso	Antares	110	PC

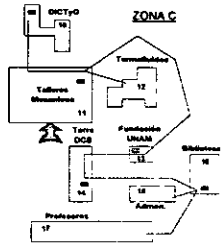
Núm.	Ubicación	Nombre	Dirección	Dispositivo
20	Primer piso	rohan	109	WS
21	Primer piso	gondolin	108	WS
22	Primer piso	bilbo	111	PC
23	Primer piso	frodo	112	WS
24	Primer piso	lunien	113	WS
25	Primer piso	elfo	114	WS
26	Primer piso	bered	115	WS
27	Primer piso	orco	116	WS
28	Primer piso	elrond	117	WS
29	Primer piso	tirith	118	WS
30	Primer piso	valinor	119	WS
31	Primer piso	aragorm	120	WS
32	Primer piso	durin	121	WS
33	Primer piso	barbol	122	WS
34	Primer piso	ringlord	123	WS
35	Primer piso	prueba1	124	PC
36	Primer piso	prueba2	125	PC
37	Primer piso	prueba3	126	PC
38	Primer piso	phonix	127	PC

Figura 10. Edificio 10

[3] Centro de Diseño y Manufactura (Talleres de Ing. Mecánica)



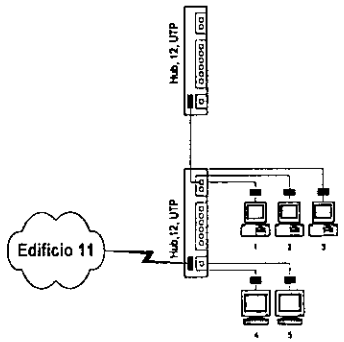
Ubicación del Edificio 11



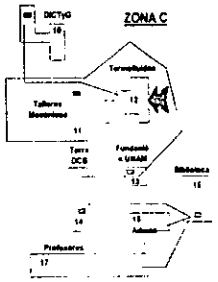
Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1	Ed. B	Depmc	27	PC
2	Ed. B	Udiatem	35	PC
3	Ed. A	Cdm1pc	22	PC
4	Ed. A	Admin	32	PC
5	Ed. A	Depmt	25	PC
6	Ed. A	Ciadt	24	PC
7	Ed. A	Cdm1	21	WS
8	Ed. A	Cdmpc2	23	PC
9	Ed. A	Invap	31	PC
10	Ed. A	Jcdm	26	PC
11	Ed. A	Limacpc2	17	PC
12	Ed. C	Limac2	2	WS
13	Ed. C	Limac	1	PC
14	Ed. C	Limacpc1	19	PC
15	Ed. C	Limac6	6	PC
16	Ed. C	Limac3	3	PC

Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
17	Ed. C	limac7	7	PC
18	Ed. C	limac8	8	WS
19	Ed. C	limac4	4	WS
20	Ed. C	limac5	5	WS
21	Ed. C	limac11	11	WS
22	Ed. C	limac9	9	WS
23	Ed. C	limac10		WS
24	Ed. C	limac17		WS
25	Ed. C	limac14	14	WS
26	Ed. C	limac16	16	WS
27	Ed. C	limac18	18	WS
28	Ed. C	limac13	13	WS
29	Ed. C	limac12	12	WS
30	Ed. C	limac15	15	WS
31	Ed. C	cdm	19	WS

Figura 11. Edificio 11

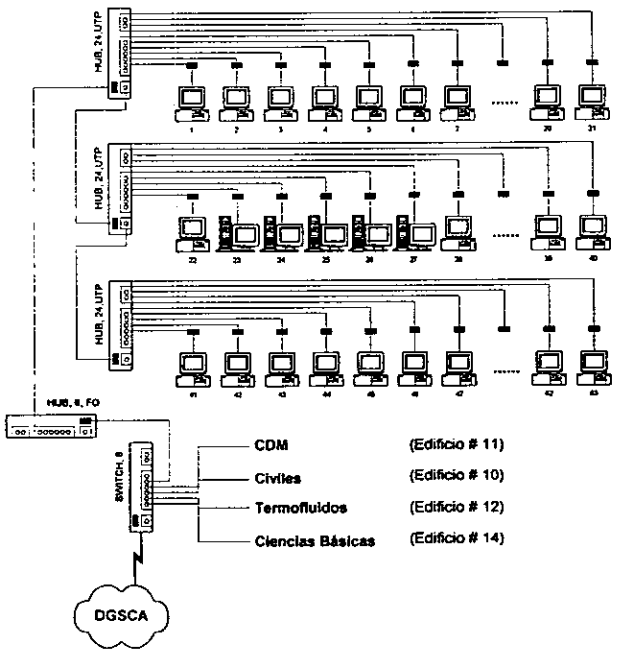


Ubicación del Edificio 12

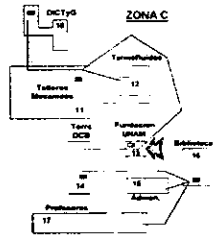


Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1	Planta baja	termoe6	33	PC
2	Planta baja	labtf4	34	PC
3	Planta baja	labtf1	29	PC
4	Planta baja	labtf2	30	WS
5	Planta baja	deptf	28	WS

Figura 12. Edificio 12



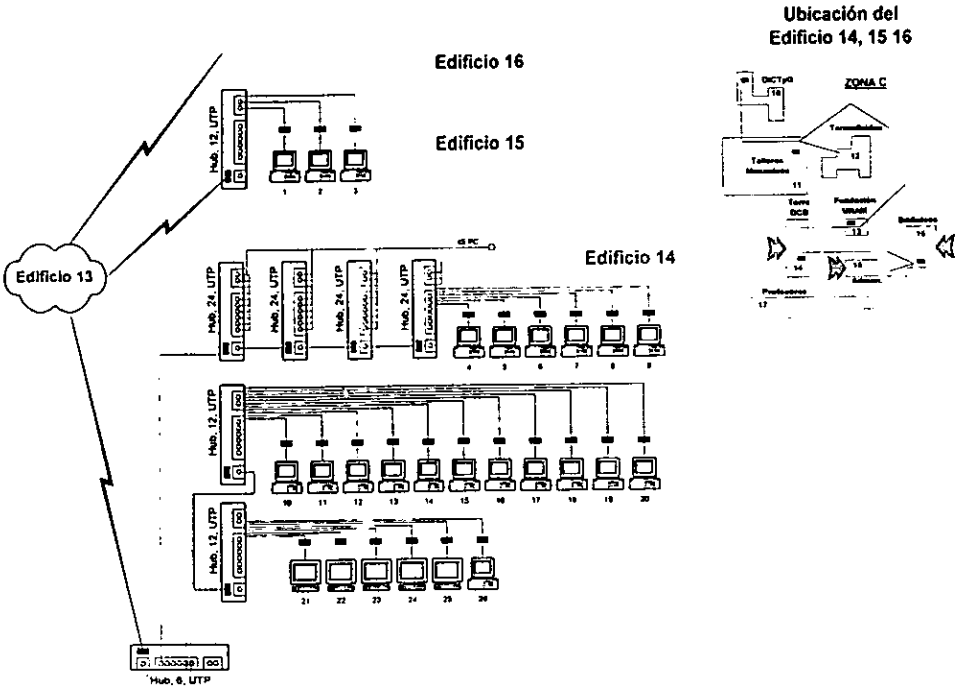
Ubicación del Edificio 13



Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1	Sala D	Maquina_22	131.107.2.1	pc
2	Sala D	Maquina_23	131.107.2.2	pc
3	Sala D	Maquina_24	131.107.2.3	pc
4	Sala D	Maquina_25	131.107.2.4	pc
5	Sala D	Maquina_26	131.107.2.5	pc
6	Sala D	Maquina_27	131.107.2.6	pc
7	Sala D	Maquina_28	131.107.2.7	pc
8	Sala D	Maquina_29	131.107.2.8	pc
9	Sala D	Maquina_30	131.107.2.9	pc
10	Sala D	Maquina_31	131.107.2.10	pc
11	Sala B	Maquina_1	192.1.1.3	pc
12	Sala B	Maquina_2	192.1.1.4	pc
13	Sala B	Maquina_3	192.1.1.5	pc
14	Sala B	Maquina_4	192.1.1.6	pc
15	Sala B	Maquina_5	192.1.1.7	pc
16	Sala B	Maquina_6	192.1.1.8	pc
17	Sala B	Maquina_7	192.1.1.9	pc
18	Sala B	Maquina_8	192.1.1.10	pc
19	Sala B	Maquina_9	192.1.1.11	pc
20	Sala B	Maquina_10	192.1.1.12	pc
21	Sala B	Maquina_11	192.1.1.13	pc
22	Sala B	Maquina_12	192.1.1.14	pc
23	Servidores y Otros	itzcoalt	131.248.162	Servidor
24	Servidores y Otros	quetzalcoalt		Servidor
25	Servidores y Otros	thor		Servidor
26	Servidores y Otros			Servidor
27	Servidores y Otros			Servidor
28	Sala C	USR_1	132.248.139.191	pc
29	Sala C	USR_2	132.248.139.190	pc
30	Sala C	USR_3	132.248.139.189	pc
31	Sala C	USR_4	132.248.139.199	pc

Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
32	Sala C	USR_5	132.248.139.193	pc
33	Sala C	USR_6	132.248.139.194	pc
34	Sala C	USR_7	132.248.139.199	pc
35	Sala C	USR_8	132.248.139.200	pc
36	Sala C	USR_9	132.248.139.201	pc
37	Sala C	USR_10	132.248.139.202	pc
38	Sala C	USR_11	132.248.139.187	pc
39	Sala C	USR_12	132.248.139.186	pc
40	Sala C	USR_13	132.248.139.185	pc
41	Sala C	USR_14	132.248.139.195	pc
42	Sala C	USR_15	132.248.139.196	pc
43	Sala C	USR_16	132.248.139.197	pc
44	Sala C	USR_17	132.248.139.198	pc
45	Sala C	USR_18	132.248.139.202	pc
46	Sala C	USR_19	132.248.139.203	pc
47	Sala C	USR_20	132.248.139.204	pc
48	Sala C	USR_21	132.248.139.205	pc
49	Sala A	cucho	132.248.139.170	pc
50	Sala A	benito	132.248.139.171	pc
51	Sala A	demostenes	132.248.139.172	pc
52	Sala A	panza	132.248.139.173	pc
53	Sala A	don_gato	132.248.139.174	pc
54	Sala A	matute	132.248.139.175	pc
55	Sala A	espanto	132.248.139.176	pc
56	Sala A	batman	132.248.139.177	pc
57	Sala A	spiderman	132.248.139.178	pc
58	Sala A	superman	132.248.139.179	pc
59	Sala A	hulk	132.248.139.180	pc
60	Sala A	robin	132.248.139.181	pc
61	Sala A	doom	132.248.139.182	pc
62	Sala A	acertijo	132.248.139.183	pc
63	Sala A	gatubela	132.248.139.184	pc

Figura 13. Edificio 13

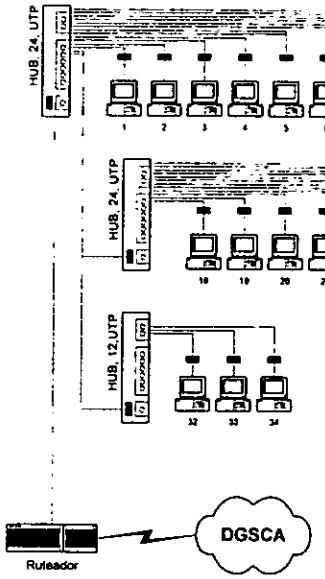


Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
1	Edifico 15	cahualzin	132,248,139,70	PC
2	Edifico 15	dcb	60	PC
3	Edifico 15	yolotzin	69	PC
4	Edifico 14		83	PC
5	Edifico 14		82	PC
6	Edifico 14		81	PC
7	Edifico 14		84	PC
8	Edifico 14		85	PC
9	Edifico 14		86	PC
10	Edifico 14	tpr9	79	PC
11	Edifico 14	tpr8	78	PC
12	Edifico 14	tpr7	77	PC
13	Edifico 14	tpr6	76	PC

Núm.	Ubicación	Nombre	Dirección IP	Dispositivo
14	Edifico 14	tpr5	75	PC
15	Edifico 14	tpr4	74	PC
16	Edifico 14	tpr3	73	PC
17	Edifico 14	tpr2	72	PC
18	Edifico 14	tpr1	71	PC
19	Edifico 14	maxtla	67	PC
20	Edifico 14	centeo	68	PC
21	Edifico 14	citlalli	62	servidor
22	Edifico 14	quetzal	63	servidor
23	Edifico 14	malinche	64	servidor
24	Edifico 14	nayoona	65	servidor
25	Edifico 14	yozune	66	servidor
26	Edifico 14	basicas	61	PC

Figura 14. Edificio 14, 15 y 17

Zona D
(Palacio de Minería)



Ubicación del Edificio 18

Núm	Ubicación	Nombre	Dirección	Dispositivo
1	A	moastil	22	PC
2	Primer piso	jgomez	14	PC
3	Primer piso	bonetts	15	PC
4	Primer piso	bonetl	16	PC
5	Primer piso	recepcion	17	PC
6	Primer piso	caja	18	PC
7	Primer piso	ddusion	27	PC
8	Primer piso	sida	11	PC
9	Primer piso			PC
10	Primer piso	sarias	12	PC
11	Primer piso	mperez	13	PC
12	Primer piso	raxoho	2	PC
13	Primer piso	taurus	3	PC
14	Primer piso	virum	4	PC
15	Primer piso	boari	10	WS
16	Primer piso	totsa	1	PC
17	M	sefi	25	PC

Núm.	Ubicación	Nombre	Dirección	Dispositivo
18	Primer piso			PC
19	Primer piso			PC
20	Primer piso			PC
21	Primer piso			PC
22	Primer piso			PC
23	Primer piso			PC
24	Primer piso			PC
25	Primer piso			PC
26	Primer piso	mpadilla	21	PC
27	Primer piso	jvargas	20	PC
28	Primer piso	tgarcia	24	PC
29	M	feria	26	PC
30	M	almacen	30	PC
31	M			PC
32	M	rmarino	23	PC
33	M			PC
34	M			PC

Figura 15. Edificio 18

3.1.2 Equipos y Dispositivos

La red de la Facultad de Ingeniería, cuenta con diversos dispositivos por zona, es importante hacer notar que dichos datos se obtuvieron de las gráficas anteriores de la red, pero también cabe resaltar que los mismos cambian continuamente debido al dinamismo que representa en sí la red de la Facultad.

Zona	Edif.	Nivel	División	HUBS						Switch	Workstation/ Servidores
				FO 6	UTP 24	UTP 12	UTP 16	CC 40	UT P 8		
A	1	Planta Baja	USECAD	1			1		2		2
	3	Primer Piso	UNICA		1			1			26
		P.B. y 4° piso	DICT		1			2			
	2	Planta Principal	DICT			1		1			
		Planta Baja	Dirección, DCSyH y DICT		4			1			
			TOTALES	1	6	1	1	5	2		28
B	8		DIE		8	1					18
	9		DIMEI	1	4	3					
			TOTALES	1	12	4					18
C	10	P.B.	DICTyG	1	1	2					16
	11		CDM	1		4					
	12		Termofluidos	1		2					2
	13		Fundación UNAM	1	3					1	5
	15		Admon.			1					
	14		Torre DCB		4	2					5
			TOTALES	4	8	11				1	28
D	18		Palacio de Minería		2	1					1
			TOTALES		2	1					1

Tabla 2. *Equipos y dispositivos de la red de la FI.*

3.1.3 Software de comunicación en la red

Uno de los elementos importantes para el funcionamiento de la red es el software de comunicación, en la Facultad existe una variedad de ellos, unos más utilizados que otros, pero todos en su conjunto forman el software que nosotros llamamos software de comunicación.

Internet

Por lo que se refiere al software de internet, Red UNAM utiliza una dirección internet clase B, y en particular la red de la Facultad de Ingeniería es de clase C.

Para asegurar que las direcciones de una red sean únicas, éstas son asignadas por la autoridad central NIC. Dicha autoridad se encarga únicamente de asignar las direcciones de red y delega la responsabilidad de asignar las direcciones de los nodos al organismo encargado de la red en cuestión. Así por ejemplo, el NIC asignó a la Red UNAM la dirección 132.248.0.0. y es la Universidad quien se encarga de asignar las direcciones a cada nodo de su red.

Por ejemplo en:

cancun.fi-a.unam.mx

unam.mx se determina centralmente, *fi-a* es asignado por una autoridad a nivel de la universidad, y *cancun* es el nombre dado a nivel local.

TELNET

El comando telnet permite establecer una sesión en cualquier máquina de la red utilizando una terminal conectada a cualquier otra máquina.

FTP

Nos permite hacer la transferencia de archivos o hacer copias de archivos hacia un nodo remoto de la red. A través de este servicio, la internet permite el acceso gratuito a bases de datos que contienen software de dominio público e información sobre diversos temas.

Correo electrónico

El servicio de correo electrónico permite que los usuarios puedan intercambiar mensajes a través de la red sin importar la localización de los nodos que utilizan para ello. La conexión de la Red_UNAM con la internet permite que la comunidad de la universidad pueda comunicarse mediante correo electrónico a los organismos educativos más importantes de todo el mundo, además de algunas empresas gubernamentales y comerciales de diferentes países.

Bajo Unix, el correo electrónico es proporcionado por la utilería mail.

Comunicación interactiva entre usuarios

El comando *talk* permite realizar este tipo de comunicaciones. Para esto los dos usuarios que desean establecer una conversación deben estar en sesión al mismo tiempo y uno de ellos debe de iniciar la comunicación con dicho comando.

Transferencia de archivos

El comando rcp presta un servicio muy parecido al de ftp, pues permite copiar archivos a través de la red, aunque su interfase es mucha más sencilla.

ARCHIE, GOPHER y VERONICA[4]

Archie es un sistema que permite explorar índices disponibles en los servidores públicos especiales, mientras que Gopher es un servicio (software), que permite encontrar información a través de la red en forma catalogada.

Así como existe un servicio de búsqueda para FTP (Archie) para Gopher existe también este servicio, VERONICA.

VERONICA es un servicio que permite realizar búsquedas por temas y palabras especiales sobre el servicio de Gopher, es decir, realiza la búsqueda sobre los catálogos y da como resultados la posición en el catálogo correspondiente, ya sea en el Gopher local al cual se está ejecutando o bien en algún Gopher remoto.

Este software de comunicación ya no es utilizado como en años anteriores (trabaja bajo el ambiente unix), pues actualmente, se utilizan más las herramientas para el entorno WINDOWS, por su sencillez y su fácil acceso al ambiente.

Worl Wide Web

Es un servicio más reciente en Interne, ya que está basado en una tecnología flexible y sencilla que permite "navegar" por Internet. Además sus elementos como hipertext y multimedia hacen que se autilizado por la mayor par5te de los usurios de la red.

Netscape e Internet Explorer

El Netscape y el Intenet Explorer están en ambiente windows, son programas de aplicación para la comunicación entre máquinas de forma gráfica, pero también cuentan con la opción de enviar o recibir correos electrónicos (muy similar a Eudora). De esta forma, son las herramientas en la facultad más utilizada para navegar.

Eudora y Microsoft Outlook

Son aplicaciones en ambiente windows de correo electrónico, son los más actuales y utilizados para comunicarse con cualquier persona vía Internet. Es decir, es un software que lleva el poder y la flexibilidad de los sistemas de correo electrónico al entorno accesible y amigable de la computadora personal: PC o Macintosh. Por ello cada vez se incrementa el número de usuarios de este software. Ya que permite adjuntar a los mensajes cualquier número de archivos de todo tipo incluyendo documentos de un editor de textos, imágenes, dibujos o video.

3.2 Administración actual de la red

Ante la problemática de dirigir, coordinar, controlar y vigilar el crecimiento de la red de cómputo de la Facultad, surgió la necesidad de crear un comité de cómputo que analizara las condiciones o situaciones que se presentaran en la red. Estableciéndose así el actual Comité Asesor de Cómputo que tiene las siguientes funciones:

[4] Very Easy Rodent-Oriented Net-wide Index to Computerized Archives"

- Constituir un foro de discusión sobre los siguientes aspectos sobre la problemática de computo de la Facultad.
- Participar en el establecimiento de un plan de desarrollo de computación en la Facultad que de manera integral contemple a la computación y sus disciplinas afines; tales como la informática, las telecomunicaciones y la electrónica.
- Asesorar a la dirección de la Facultad de Ingeniería en el establecimiento de políticas de adquisición y mantenimiento de equipo de computo que permitan optimar el aprovechamiento de los recursos disponibles dentro de la Facultad de Ingeniería
- Sugerir y buscar recursos para apoyar el desarrollo de la computación en la Facultad.
- Acatar las políticas por el consejo asesor de cómputo de la Universidad, en los diversos aspectos relacionados con la computación.
- Establecer mecanismos y normas para la integración del acervo en materia de software, así como el establecimiento de políticas en cuanto su adquisición, uso, tendencias, normalización y otros.
- Establecer mecanismos que permitan el acceso y uso eficiente de los sistemas de información en la Facultad, en la UNAM y en su entorno.
- Sugerir políticas que permitan la formación especifica de recursos humanos de apoyo en el área de computo.
- Proponer mecanismos para evaluar el uso y los recursos de computo.
- Promover el intercambio en el área de computo con otras instituciones del país y el extranjero.
- Promover la cultura informática en todos los ámbitos de Ingeniería.
- Generar acciones para lograr que la Facultad este a la vanguardia del conocimiento en el área de computación.
- Establecer los mecanismos y normas para integrar redes de computo locales por división y secretarias, y una red a nivel Facultad.
- Establecer los mecanismos necesarios para la computación sea una herramienta de apoyo a la docencia y a la labor académico-administrativa.

El grupo de administradores está formado por representantes de todas las Divisiones y Secretarías, siendo la Secretaría General la encargada del contacto con la DGSCA.

Se han realizado los objetivos de interconectar los edificios de interés de la Facultad de Ingeniería con fibra óptica. Quedando establecido que cada División o Secretaría será responsable de la administración y mantenimiento de su red.

Actualmente se está realizando una normalización de croquis de la red, planos y una base de datos de la información de la red. Así como la información que abarca los temas que debe dominar un administrador de red.

3.2.1 Administración Lógica

Asignación de direcciones IP

Para asegurar que las direcciones de una red sean únicas, existe la autoridad central NIC[5] (Centro de Información de Red), la cual se encarga únicamente de asignar las direcciones de red y delega la responsabilidad de establecer las direcciones de los nodos del organismo encargado de la red en cuestión.

El NIC determinó para la RedUNAM la dirección 132.248.0.0. y es la universidad (DGSCA[6]) quién se encarga de asignar las direcciones a cada nodo de su red, a dicha dirección se le dio el nombre de *unam.mx* como dominio primario.
Para la Facultad de Ingeniería se asignaron cinco dominios los cuales son:

ZONA	NOMBRE	DIRECCIÓN IP	GATEWAY	UBICACIÓN
A	fi-a.unam.mx	132.248.54.xx	132.248.54.254	Edificio Principal
B	fi-b.unam.mx	132.248.59.xx	132.248.54.254	DIMEI y Edificio Valdés Vallejo
B	fi-p.unam.mx	132.248.52.xx	132.248.54.254	Edificio de Posgrado
C	fi-c.unam.mx	132.248.139.xx	132.248.139.254	DICTyG, DCB, Talleres Mec., Lab. Termo., Bib. Nueva y UNICA Anexo.
D	minería.unam.mx	132.248.138.xx	132.248.138.254	Palacio de Minería

Y la distribución, así como la utilización de las direcciones IP son las siguientes (datos obtenidos hasta marzo de 1998):

ZONA A

Sección o División	Rango de Direcciones	No. de Direcciones	Ocupadas	%
Sec. General	1-90	90	51	56.66%
Dirección	91-100	10	2	20.00%
Sec. Acad.	101-130	30	16	53.33%
Sec. Adm.	131-150	20	4	20.00%
DCT	151-180	30	29	96.66%
DCSyH	181-190	10	5	50.00%
Secretaría General	191-244	54	2	3.70%
Monitoreo	245-253	9	3	33.33%
Concentrador	254	1	1	100.00%
Total		253	113	44.66%

[5] Network Information Center
[6] Dirección General de Servicios de Cómputo Académico

ZONA B

Sección o División	Rango de Direcciones	No. de Direcciones	Ocupadas	%
DIE	1-204	204	120	58.82%
DIMEI	205-244	40	3	7.57%
Reservadas	245-253	10	1	10.00%
Concentrador	254	1	1	100.00%
Total		254	125	49.21%

ZONA C

Sección o División	Rango de Direcciones	No. de Direcciones	Ocupadas	%
DIMEI (CDM)	1-55	55	29	52.72%
DCB	56-105	50	23	46.00%
DICTYG	106-155	50	38	76.00%
SEC. GENERAL	156-205	50	50	100.00%
Secretaría Académica	206-209	4	1	25.00%
Biblioteca	210-244	35	0	0.00%
Monitoreo	252-253	2	2	100.00%
Reservadas	245-251	7	0	0.00%
Concentrador	254	1	1	100.00%
Total		253		

3.2.2 Seguridad en el acceso a la red.

Para la seguridad en el acceso a la red, generalmente existe un administrador en cada edificio y plataforma de la FI. Para el caso de la sala de UNICA

Existen dos tipos de usuarios:

Superusuario (administrador o root)
Usuario

Como se mencionó en capítulos anteriores, la red de la FI está basada en un sistema UNIX por lo que la administración y seguridad dependen en gran parte de esta plataforma. El sistema operativo que se utiliza actualmente es HP_UX 9.05 que soporta aproximadamente 64,000 usuarios, pero se está migrando a la versión HP_UX 10.20 la cual tiene capacidad para soportar 2 millones de usuarios. Es importante mencionar que esta capacidad está excedida en mucho a las necesidades reales de la FI pero es necesaria esta actualización debido a que este nuevo sistema registra el año en cuatro dígitos, lo cual se ocupará a partir del año 2000 y la fecha es importante en los procesos que se ejecutan para seguridad en la red.

Cada archivo tiene asociado tres atributos (lectura, escritura y ejecución, que a su vez son asignados a tres áreas identificadas como dueño del archivo(quien lo crea), grupo (clasificación según tipo de usuario) y generales (cualquier otro usuario). Dependiendo de las necesidades de los usuarios se les puede asignar una mayor capacidad en disco.

La principal parte de la seguridad de un sistema UNIX la constituyen Set User ID (SUIDE, Establecer identificación de usuario) y Set Group ID (SGID, Establecer identificación de grupo).

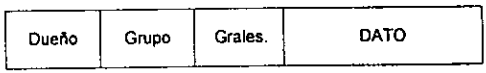


Figura 16. Ejemplo de la división de asignación de asignación de atributos.

El administrador de la red asigna todos los atributos a los usuarios, pero este último tiene el privilegio de modificarlos, es decir, permitir o restringir la lectura, escritura o ejecución de sus archivos en las áreas de grupo y generales.

En la Facultad de Ingeniería existen cinco grupos:
Usuarios (estaciones de trabajo), PC (computadoras personales), unicafi (miembros de UNICA), Facultad (Académicos de la dependencia) y profesores.

En la DICTyG Se realizan los mismos procesos de administración y seguridad de la red, diferenciándose en 3 el número de grupos:

- Académicos y profesores
- Usuarios en general (Alumnos)
- Administradores

En esta división hay dos servidores en los que se tiene instalados el sistema operativo UNIX 10.01 y 9.05 respectivamente.

Otra medida de seguridad es la contemplada en la asignación de cuentas o claves a usuarios. Únicamente se permite acceder a la red de la FI (páginas de WEB o FTP) por medio del servidor llamada Cozumel a través de cuentas anónimas. Porque en la mayoría de los casos es información referente a la difusión de las actividades de la Facultad.

En cuanto a la asignación de cuentas o claves, se solicita al usuario sugerir su nombre y password, y el administrador verifica que no sea un nombre que pueda causar confusiones o conflictos en la red. El tiempo límite para los usuarios del grupo UNICAFI y Facultad es casi indefinido, pero para el grupo usuario y pc es restringido por el tiempo que dura un semestre. Al término de este periodo, se bloquean las claves de los grupos usuario y pc y se activan al inicio del siguiente semestre.

Se ha tomado la política de que a cada usuario se le asigne como máximo 400 archivos o 12 Mb. Si se llega exceder este limite el sistema envía mensajes al usuario, y si este no libera espacio en el disco su cuenta se congela automáticamente.

El disco asignado para los grupos es de 2 Gbytes, para el servidor Cancun, es de 4 Gbytes y para Cozumel es de 1 Gbyte. También se cuenta con un protocolo de encriptación llamado MD5 el cual, encripta los números de cuenta que llegan a las páginas del WEB, para que no pueda ser visto por algún usuario que no tiene el privilegio de hacerlo.

Existen programas para llevar un control de las cuentas o claves de los usuarios, entre los que se utilizan son:

Edquota - Modifica las cuentas en caso de que se haya generado un error en el momento de asignar una cuenta a un usuario.
Edquotacheck - Verificar que la cuenta este en vigencia.
Rquota - Genera un reporte de las cuentas que se han dado de alta.

El total de aplicaciones disponibles en la red de la FI (entorno unix), son los siguientes:

Edición gráfica
- Gift Tool
- Gimp

Correo Electrónico
- FTP
- Telnet
- ELM
- Pine

Navegadores de Internet
- Netscape
- Mosaic

Editores de texto
- Convertidores de post-script a PDF

Programas para accesar a Internet
- BBS
- Gopher

Visualizador de archivos
- Ghost view
- XV

3.2.3 Administración para uso de Páginas WEB

Retomando el capítulo anterior sabemos que el WWW (World Wide Web), es un servicio que se obtiene a través de Internet,. Y está formado por una colección de documentos interconectados que se encuentran almacenados en computadoras ubicadas en todas partes del mundo. Dichos documentos pueden contener texto, gráficos y sonidos, conocidos como páginas.

La Facultad de Ingeniería cuenta con una página principal del Web para publicar información sobre sus actividades académicas y culturales. A partir de ésta, se tienen ligas con páginas propias de las Divisiones, Secretarías, profesores, etc. Por lo tanto, para continuar con la organización que ha caracterizado a la Facultad, se está elaborando un reglamento para la publicación de páginas de web.

En la Facultad ya se encuentra aprobada "La Normatividad y Lineamientos Generales para uso de Páginas Web en la Facultad de Ingeniería" (puede consultarse en http://www.fi-a.unam.mx/comite-asesor/reglamentoWEB.html).

El primer punto que se ha considerado es la creación o asignación de un subcomité de administradores del web. Cada elemento representa una Secretaría o División.

Este subcomité es el encargado de tratar los temas relacionados con la estructuración, presentación, y contenido de las páginas de la Facultad. Y tiene como objetivos, los siguientes:

- Establecer una normalización de la administración del web en la Facultad de Ingeniería.
- Administrar de manera óptima los recursos destinados a la Facultad.
- Control de la Información que se publicará en el web.
- Participar en la normatividad del web.

El subcomité está prescedido por el webmaster de la Secretaría General, quien fungirá como moderador en las juntas de este subcomité y tomará nota de los acuerdos a los que llegue. Estos acuerdos se tomarán como base para la creación de todas las páginas que dependan de la Facultad de ingeniería.

Entre otras funciones asignadas a los webmaster, se encuentran:

- Creación, mantenimiento y control de las páginas del área a la cual pertenecen.
- Notificar al webmaster de Secretaría General de cualquier cambio en la liga de la página principal del área.
- Asistir a las juntas de webmaster, las cuales serán al menos una vez por mes.
- Estar al tanto de las actividades relacionadas con su correspondiente División o Secretaría (Conferencias,. Congresos, fechas escolares, etc.) para tener su información actualizada. Deberá publicar tales actividades en las páginas de su área o notificar al webmaster de la Secretaría General para que agregue la información en la página de información general.

- Dar respuesta a los correos que les sean enviados, relacionados con el área al cual pertenecen. En caso de que no tuviesen la información que se les solicita, indicarán el nombre de alguna persona que pueda resolver la duda, o simplemente contestar que no tiene la información solicitada.
- Dar de alta las páginas de los usuarios y entregarles el reglamento que deben cumplir para poder tener derecho a la publicación de sus páginas.
- Revisar periódicamente las páginas de los usuarios de su área, con la facultad de desactivar las páginas que no cumplan con los lineamientos señalados.
- El webmaster de la Secretaría General podrá reconvenir sobre la estructura y contenidos de las páginas, siempre que éstas no se apeguen a los lineamientos que se indican en el reglamento para la administración del web. Tiene además la facultad de deshabilitar páginas que no cumplan con los lineamientos establecidos.

3.2.4 Software de control o monitoreo actual en la red

Recordemos que el SNMP es un protocolo que está diseñado para proporcionar al usuario la capacidad de administrar remotamente una red de cómputo mediante el poleo y configuración de los valores de terminales así como el monitoreo de eventos de la red. Corre bajo TCP/IP (nivel 7 de aplicación). En la Facultad, este protocolo es la herramienta que nos ayuda para tener control en la red, es decir, es la parte importante para que pueda operar el Software de Monitoreo Transcend; por medio del cual sabemos el estado que guarda la red. Los problemas de comunicación o saturación que pueden presentarse.

La FI no contaba con un sistema de monitoreo interno debido a que no había sido posible instalar el software que para tal efecto estaba destinado. La FI cuenta con los recursos necesarios para llevar a cabo dicho monitoreo, por lo que fue posible realizar la instalación de dos sistemas, además de configurar[7] los dispositivos necesarios para abarcar un mayor porcentaje de la red de la FI.

Los dos sistemas de monitoreo son Transcend Enterprise Manager para Windows versión 3.0 (producto de 3COM) y LANalyzer versión 2.1 (producto de Novell Netware).

Transcend Enterprise Manager

Para poder poner en marcha el sistema de monitoreo en la Facultad utilizando el software de 3Com (Transcend) fue necesario cumplir con las características mínimas para su instalación, para el caso de la red de la FI se utilizó una máquina con las siguientes características:

- Windows para trabajo en grupo 3.11
- MSDOS 6.22
- 500 Mb en disco duro

[7] Ver apéndice B

- 32 MB en memoria RAM
- Mínimo 16 MB de memoria virtual
- Drive de 3.5"
- Monitor VGA
- Mouse
- Tarjeta de red de 3COM EtherLink III Family 3C509

También se requirió la instalación previa de un paquete de TCP/IP que podía ser cualquiera de los siguientes:

- Distinct TCP/IP 3.21 (proporcionada con el software)
- NetManager Chamaleon 4.0
- Novell LAN WorkPlace 4.2

en este caso se instaló el TCP/IP para LAN WorkPlace y se le agregaron las siguientes líneas al archivo Net.cfg:

```
PATH SCRIPT C:\NWCLIENT\SCRIPT
PATH PROFILE C:\NWCLIENT\PROFILE
PATH LWP_CFG C:\NWCLIENT\HSTACC
PATH TCP_CFG C:\NWCLIENT\TCP
ip_router       132.248.54.254
ip_netmask      255.255.255.0
ip_address      132.248.54.70
udp_sockets     20
```

Como se deseaba también administrar dispositivos que se encuentran conectados por medio de una red Novell (con dirección IPX), fue necesario tener instalado dicho sistema y activar el cuadro de detección de dispositivos con comunicación IPX en el momento de realizar la instalación del Transcend.

El paquete de instalación contiene un software llamado SoftHub que se instala en una máquina PC (la cual estará dedicada para dicho software) para observar los dispositivos que están conectadas en una red LAN, por medio del componente Workgroup PC Links que viene incluido en el paquete Transcend, permitiendo observar las siguientes características de una PC:

- Dirección MAC
- Velocidad de la máquina
- Tipo de Procesador
- Capacidad de memoria
- Etc.

En la *Figura 17* se muestran las pantallas que aparecen en el software Workgroup PC Links con el cual a partir de un doble click en el dibujo se accesa a una máquina que contiene el software softhub (el cual se observa en dicha figura, como parte de las máquinas que se reconocen).

En las figuras 16, 17, y 18 se muestran las pantallas del software WorkGroup PC Links que nos permite obtener información de equipos conectados a red local. Esto se logra con el software instalado en una máquina dedicada a reconocer todos estos equipos; el softhub.

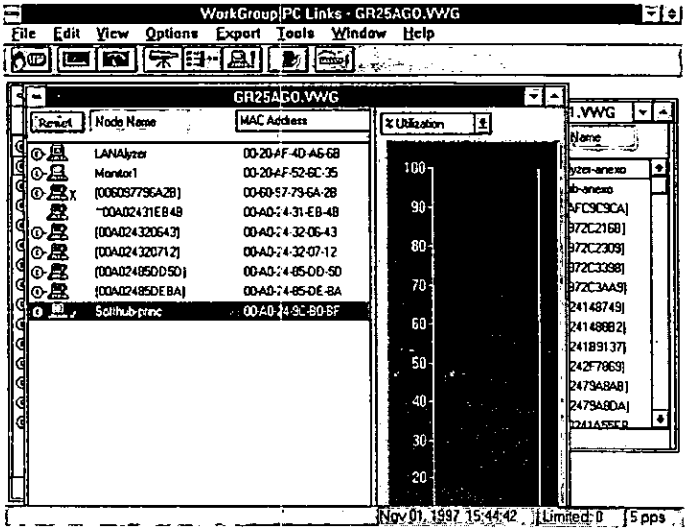


Figura 17. Se muestran las máquinas reconocidas por el softhub y una gráfica que puede mostrar porcentajes de utilización, paquetes de entrada y salida y de error en la red.

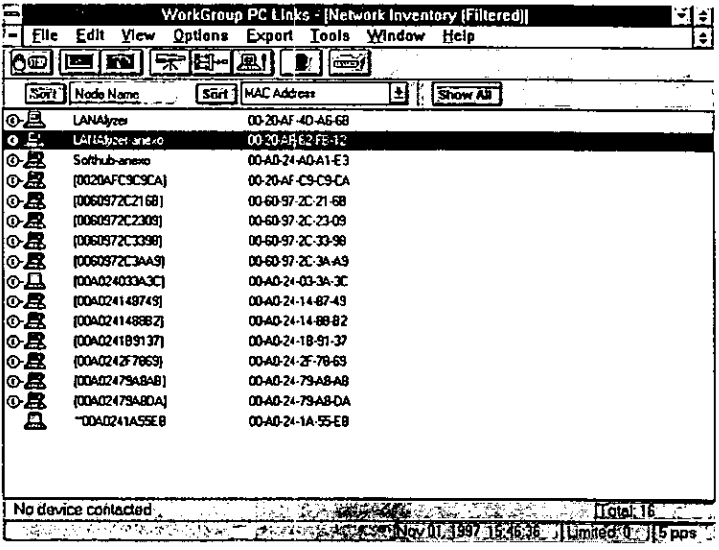


***Figura 18.** Máquinas reconocidas por el softhub, ubicadas en el edificio principal con sus respectivas direcciones MAC.*

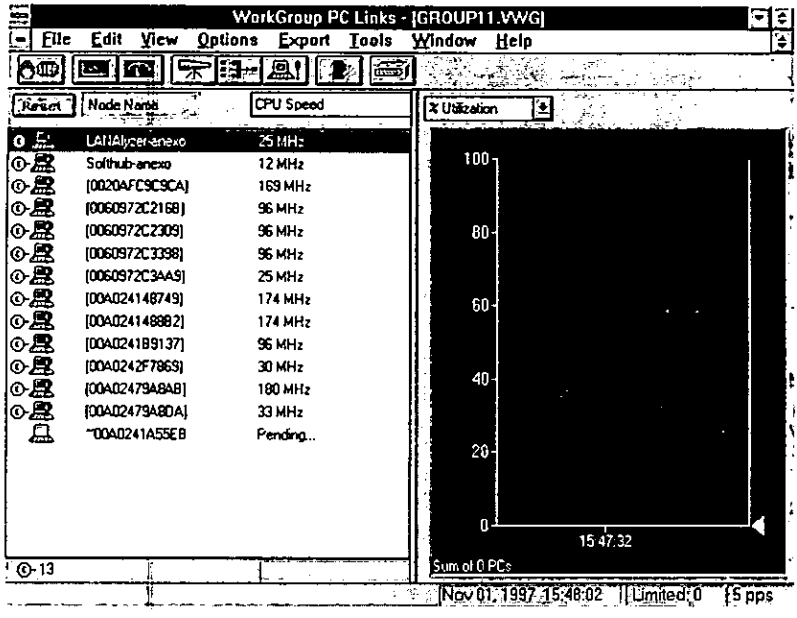


Figura 19. Se muestra la velocidad de cada una de las máquinas, a un lado se muestra una gráfica en la que es posible observar, para este caso los porcentajes de utilización de las pc's.

El Transcend contiene también un software llamado SmartAgent, el cual se instaló en algunas máquinas para poder observar las siguientes características desde la máquina de monitoreo (es decir la que contiene el Transcend):

- Datos de la persona que utiliza la máquina
- Área en la que se encuentra
- Nombre de dicha máquina

Este software usa controladores que necesitan poca memoria (6KB) y evita la necesidad de tener una dirección IP en cada máquina, permite un descubrimiento rápido de máquinas y actualización de información, además minimiza el tráfico en una red con backbones y ruteadores.

Desventajas de esta versión de transcend

Aunque el Enterprise Manager utiliza TCP/IP para comunicarse con dispositivos de la red, si se tiene instalado IPX en una PC, el paquete puede encontrar los dispositivos que utilizan IPX y agregarlos a la subred; pero si únicamente se tiene IPX detectará los dispositivos pero no los podrá administrar.

Esta versión no puede desplegar una gran cantidad de subredes. Por lo que al definir las subredes se deberán especificar los tres primeros octetos completos.

ICONO	DESCRIPCION
	LinkBuilder FMS, FMSII y 10Bti
	SoftHub DOS V2.0 o más
	LANplex 2500
	Dispositivos Generic MIB I/II SNMP

Tabla 3. Lista de los dispositivos que reconoce el Transcend en la FI.

En la *Tabla 3* se muestran las presentaciones que brinda el Transcend Enterprise Manager, de los dispositivos que reconoce, ya sea automáticamente o manualmente.

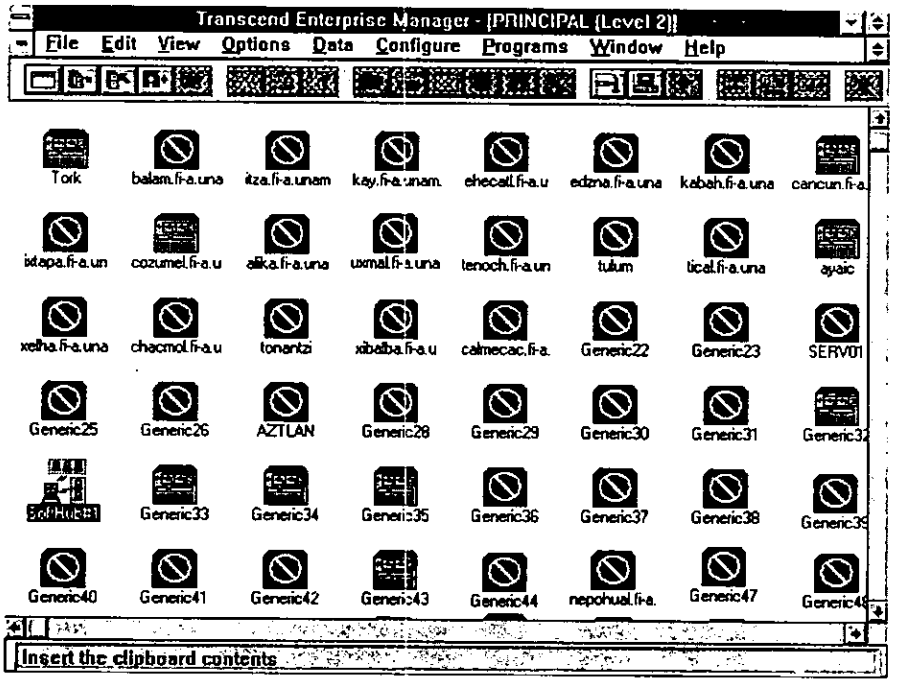


Figura 20. *El color de cada uno de los dispositivos se representa dependiendo del estado en el que se encuentre el dispositivo,como se explicó en el capitulo anterior.*

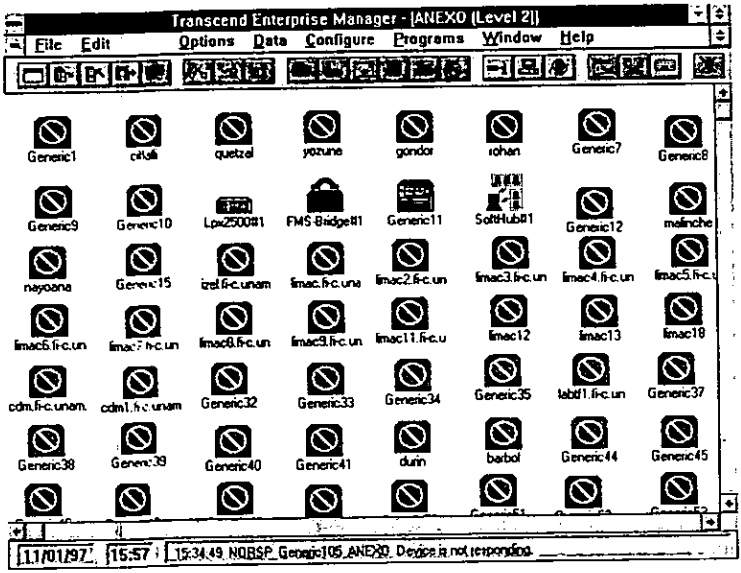


Figura 21. Dibujos de los dispositivos que reconoce el Transcend, entre ellos se pueden observar el softhub, switch y concentradores que se encuentran en el Anexo.

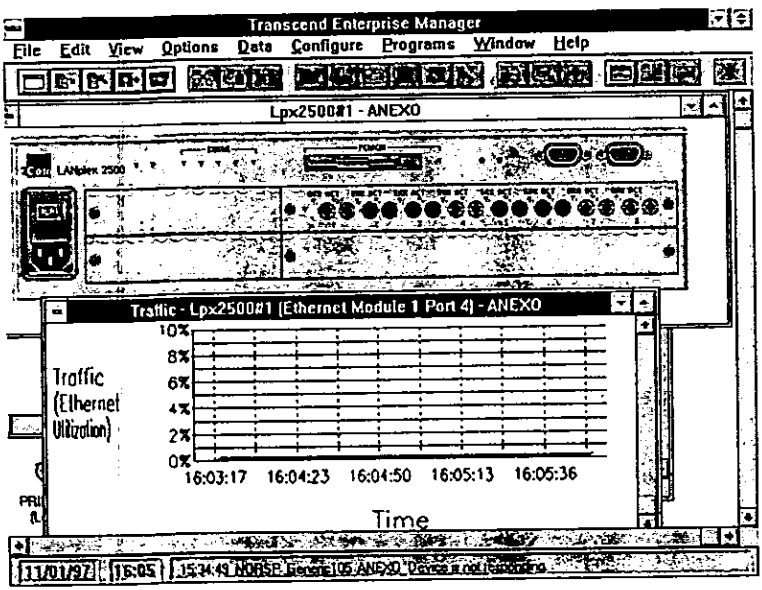


Figura 22. En la parte superior de esta figura se muestra la imagen del switch LanPlex 2500 que se encuentra localizado en UNICA del edificio del Anexo. En la parte inferior se muestra la gráfica del comportamiento de uno de los puertos del mismo.

LANalyzer

Esta herramienta ha sido el complemento para la inspección del uso de la red, ya que como se explicó anteriormente, es una herramienta basada en sistema microsoft Windows para monitoreo y análisis de tráfico sobre redes Ethernet y Token ring. Dicha herramienta ha sido de gran utilidad ya que al igual que el transcend se puede obtener un monitoreo diario o periódico que nos ha servido para detectar problemas específicos de la red, como el uso de equipos, filtración de paquetes o tráfico, detección de direcciones y usuarios en cierto momento.

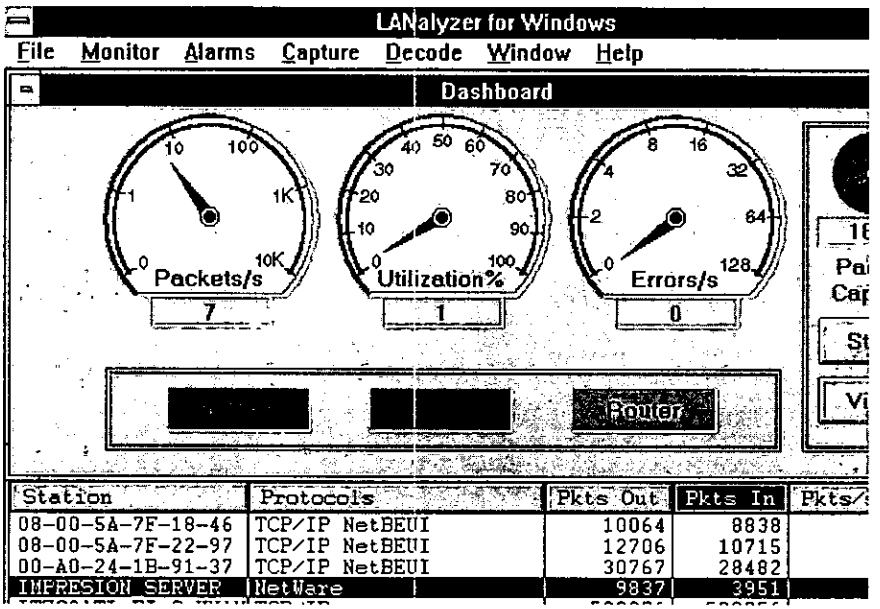
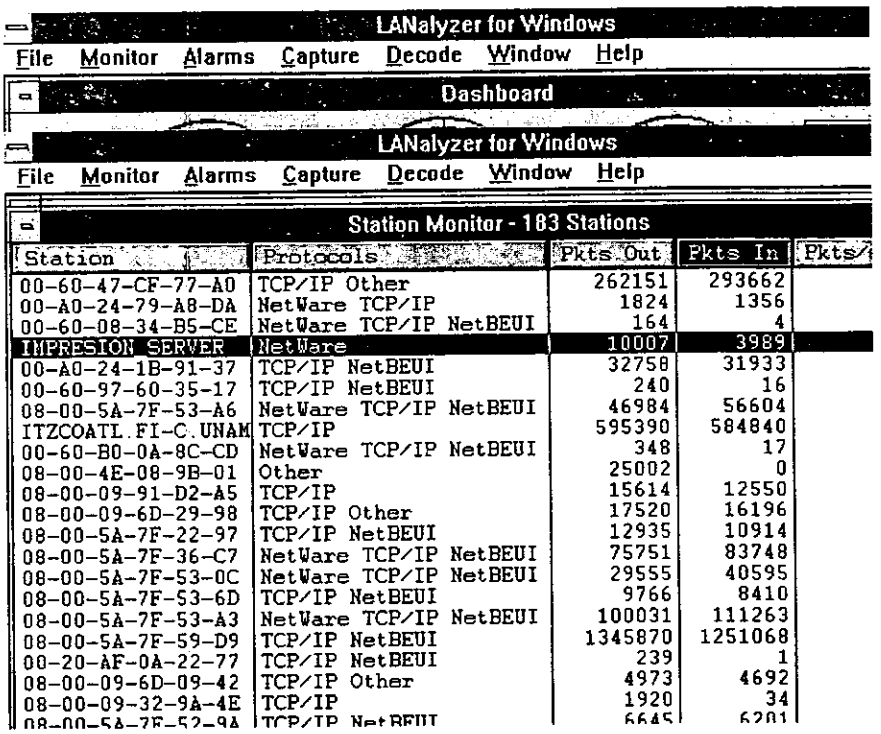


Figura 23. Pantalla principal del sistema LANalyzer

Otra de las ventajas de este sistema ha sido que es un producto de software único que se instala en una estación Netware. Haciendo posible (que es muy recomedable) tener un sistema de monitoreo local, es decir, en cada zona se puede instalar este sistema para que el administrador de la zona pueda saber en el momento que lo desee cual es el estado de la red. Y detectar y resolver en cualquier momento algún problema que pudiera surgir en la red.

En forma similar al Trancend, LANalyzer analiza la red desplegando estadísticas de red en tiempo real por medio de medidores, gráficas y tablas. También monitorea a través de un Monitor de estación el cual despliega una tabla con una lista de las estaciones activas en la red y sus estadísticas relacionadas.



Station	Protocols	Pkts Out	Pkts In	Pkts/
00-60-47-CF-77-A0	TCP/IP Other	262151	293662	
00-A0-24-79-A8-DA	NetWare TCP/IP	1824	1356	
00-60-08-34-B5-CE	NetWare TCP/IP NetBEUI	164	4	
IMPRESION SERVER	NetWare	10007	3989	
00-A0-24-1B-91-37	TCP/IP NetBEUI	32758	31933	
00-60-97-60-35-17	TCP/IP NetBEUI	240	16	
08-00-5A-7F-53-A6	NetWare TCP/IP NetBEUI	46984	56604	
ITZCOATL.FI-C.UNAM	TCP/IP	595390	584840	
00-60-B0-0A-8C-CD	NetWare TCP/IP NetBEUI	348	17	
08-00-4E-08-9B-01	Other	25002	0	
08-00-09-91-D2-A5	TCP/IP	15614	12550	
08-00-09-6D-29-98	TCP/IP Other	17520	16196	
08-00-5A-7F-22-97	TCP/IP NetBEUI	12935	10914	
08-00-5A-7F-36-C7	NetWare TCP/IP NetBEUI	75751	83748	
08-00-5A-7F-53-0C	NetWare TCP/IP NetBEUI	29555	40595	
08-00-5A-7F-53-6D	TCP/IP NetBEUI	9766	8410	
08-00-5A-7F-53-A3	NetWare TCP/IP NetBEUI	100031	111263	
08-00-5A-7F-59-D9	TCP/IP NetBEUI	1345870	1251068	
00-20-AF-0A-22-77	TCP/IP NetBEUI	239	1	
08-00-09-6D-09-42	TCP/IP Other	4973	4692	
08-00-09-32-9A-4E	TCP/IP	1920	34	
08-00-5A-7F-52-9A	TCP/IP NetBEUI	6645	6201	

Figura 24. Monitor de estación con una lista de las estaciones activas

LANalyzer usa alarmas indicadoras de mensajes que alertan las condiciones no usuales u ocurrencia de eventos en la red. Además analiza el rendimiento de la red mediante la capturación y decodificación de paquetes de red, los cuales los muestra a través de una ventana de buffer de captura, como se muestra en la Figura 25.

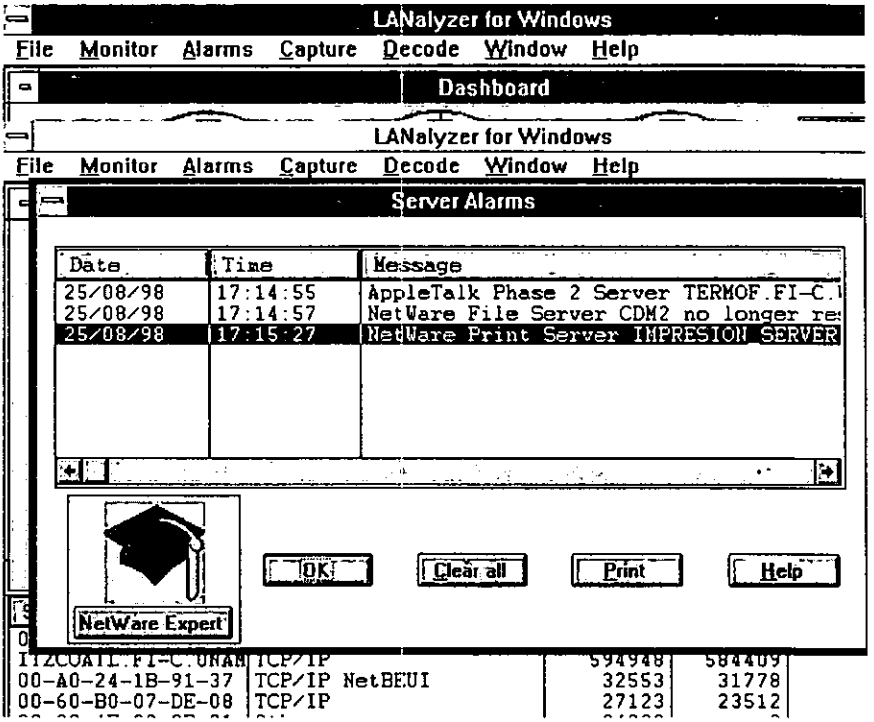


Figura 25. Alarmas

- Entre otras actividades, como ya se mencionó, LANalyzer monitorea los paquetes de red y el tráfico hacia y desde estaciones específicas, capturando paquetes de ciertos tipos de protocolos y paquetes basados en la presencia o ausencia de errores

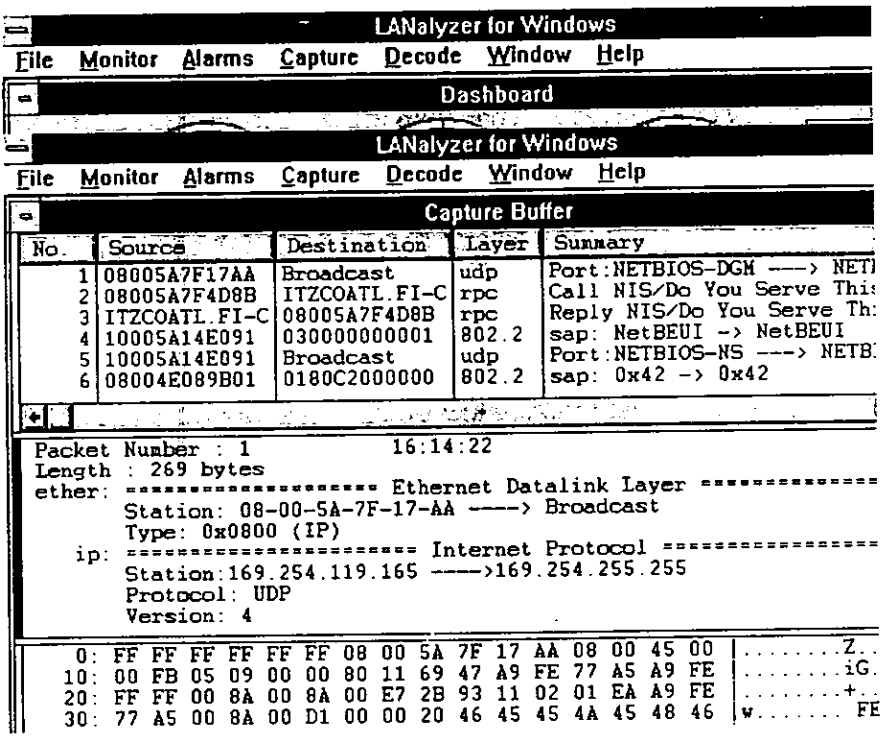
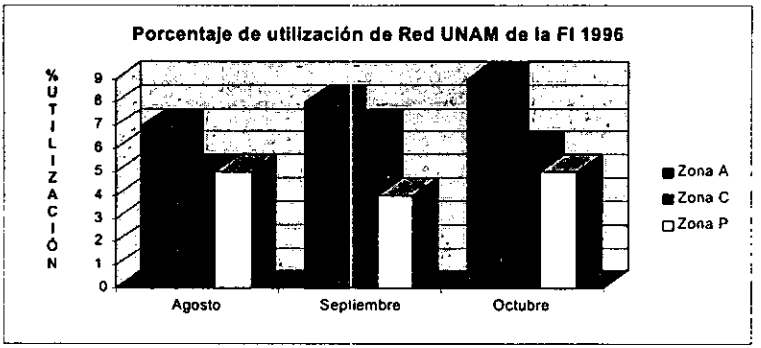


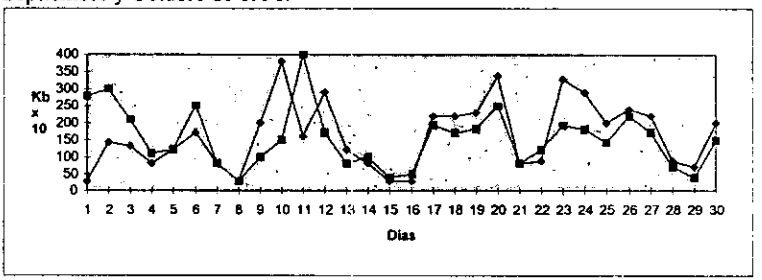
Figura 26. Captura de paquetes

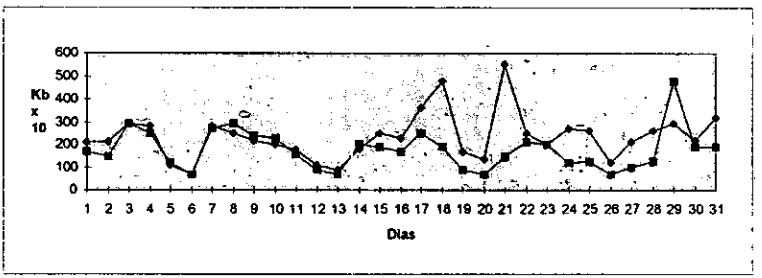
Dada la necesidad de saber el grado de utilización de la red, en el año de 1996 se solicitó a la DGSCA estadísticas de uso y tráfico, a lo que DGSCA respondió que tardarían un poco porque su generación era complicada[8]. Pero finalmente, se obtuvo dicha información. A continuación se presentan las gráficas resultantes:

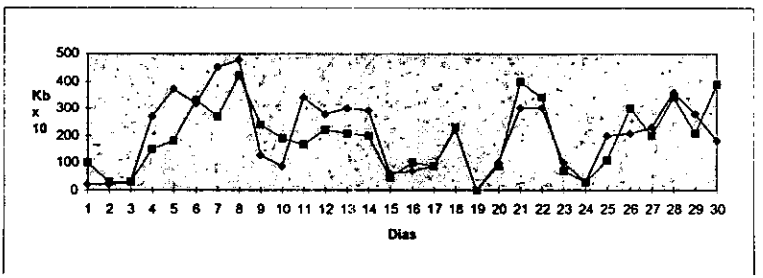
[8] Esta información fue del conocimiento al Comité Asesor de Cómputo el 23 de octubre de 1996.



Agosto, Septiembre y Octubre de 1996:



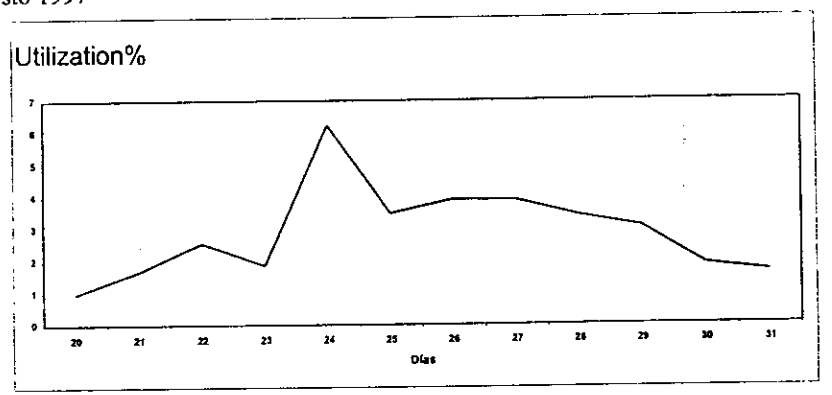




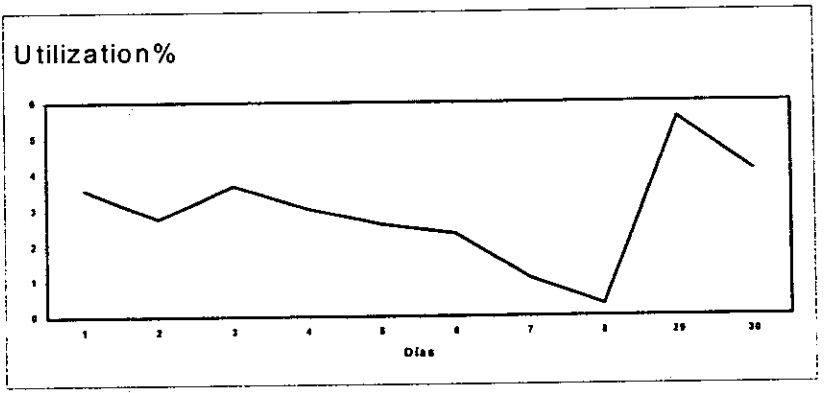
Estas gráfica nos muestran que de nuestra red, sólo se utiliza aproximadamente un 10%, cuando podemos utilizar hasta un 40%, y como consecuencia el flujo de información que se maneja no es excesivo como para saturar la red.

Para verificar que el monitoreo, recientemente puesto en marcha, por parte de la Facultad es confiable, se generaron también una serie de reportes[9]: Dichos reportes son el resultado de los dos sistemas de monitoreo los cuales en forma complementaria nos ayudaron para presentar los siguientes reportes.

Agosto 1997

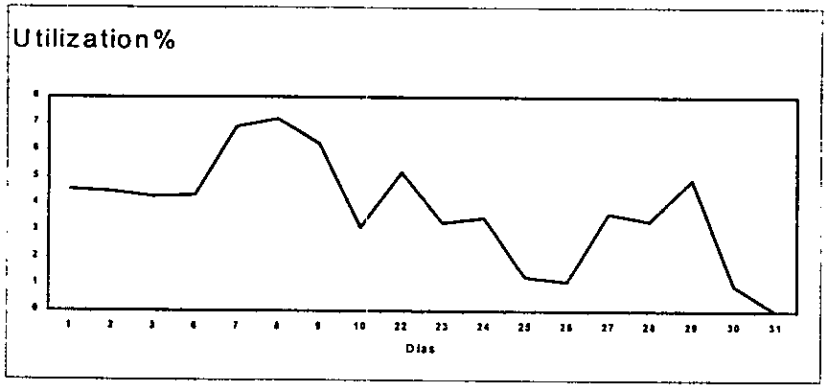


Septiembre 1997

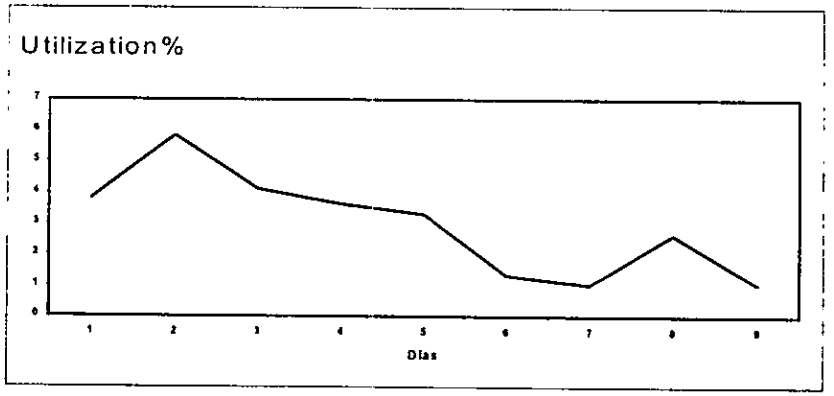


[9] Sólo se tienen datos de la Zona A, porque sólo en esta zona se cuenta con la autorización de realizar pruebas.

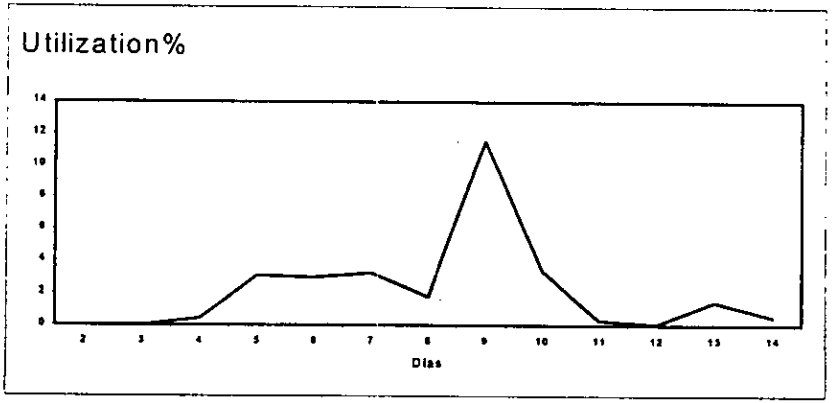
Octubre 1997



Diciembre 1997



Enero 1998



Como se puede notar, existen días y meses en los que no se tiene información, pero son en general los datos de un semestre de clases. Esto nos hace reflexionar que falta motivar el uso intensivo de la Red UNAM.

3.2.5 Consideraciones previas para la propuesta de administración

Con base en lo expuesto anteriormente, podemos obtener la siguiente tabla, que es una de las bases para establecer lineamientos de seguridad.

Recursos de la fuente			Tipo de usuario del que hay que proteger el recurso	Posibilidad de Amenaza	Medidas que se implementarán para proteger al recurso de la red
Área	Nombre	Imp. Recurso*			
	Rep. F.O.	10	Personas externas y alumnos	Robo, daño físico y desconexión (Alto)	Cajas Metálicas y con candado, sólo cuenta con acceso el administrador de red de la división y administrador general
	HUB's	8	Personas externas y alumnos	Robo, daño físico y desconexión (Alto)	Cajas Metálicas y con candado, sólo cuenta con acceso el administrador de red de la división y administrador general
	Servidores	7	Personas externas y alumnos	Robo, daño físico	Enjaulado de Equipo bajo llave
	Pc's	5	Personas no autorizadas y externas	Robo, daño físico, virus	Para las salas de trabajo y departamentos, las puertas de acceso bajo llave cuando se encuentren fuera de servicio, acceso controlado por credencial únicamente para salas y revisión de discos.
	Estaciones de trabajo	6	Personas no autorizadas y externas	Robo, daño físico	Para las salas de trabajo y departamentos, las puertas de acceso bajo llave cuando se encuentren fuera de servicio y acceso controlado por credencial únicamente para salas.
	Impresoras	4	Personas no autorizadas y externas	Robo, daño físico	Para las salas de trabajo y departamentos sólo personal autorizado
	Información	10	Personas no autorizadas y externas	Alteración, robo, Virus	Personal autorizado con permiso de sistema operativo.
	Software	4	Personas no autorizadas y externas	Alteración, Virus	Personal autorizado con permiso de sistema operativo.

Tabla 4. Hoja de trabajo para desarrollar un planteamiento de seguridad

En la *Tabla 4* se analizó el nivel de importancia, del equipo con que se cuenta. En la tabla siguiente se presenta el número de hub's y repetidores de fibra óptica por zona. Esto con la finalidad de contar con mayores elementos para la propuesta de administración que es el fin que se persigue.

Zona A (datos hasta el 22 de marzo de 1998)

Área	Repetidor de F.O.	Hub 24	Hub 12	Hub 8	Hub Coax.	Total de equipo
Edif. Principal ala oriente	1	4	2	1	1	9
Edif. Principal ala poniente			1	1		2
Unica Principal	1	1			1	3
USECAD			3	1	1	5

Zona B

Área	Repetidor de F.O.	Hub 24	Hub 12	Hub 8	Hub Coax.	Otros	Total de equipo
Edif. DIE	1	6	2				9
Edif. DIMEI	1	4	1			2 (Hub UTP 16 puertos)	2

Zona C

Área	Repetidor de F.O.	Hub 24	Hub 12	Hub 8	Hub Coax.	Otros	Total de equipo
UNICA Anexo	1	3				1 (Switch F.O. 6 Puertos)	5
DCB (Torre)			1				1
DCB (ADM)			1				1
DCB (Prof.)	1	2	1				4
CDM	1		4				5
Civiles	1	1	2				4
Termofluidos			2				2
Biblioteca		4					4

También podemos hacer un análisis de riesgo para saber que recursos convienen proteger, y cuáles son más importantes que otros.

Aquí los riesgos se clasifican por nivel de importancia y gravedad de la pérdida. Donde *Ri* es la estimación del riesgo de perder el recurso, y *Wi* la estimación de la importancia del recurso, y *Wri* es el riesgo evaluado del recurso. Y tenemos como resultado la tabla que contiene dicho análisis de riesgo de seguridad de la red:

Zona A

Recursos de la fuente			Riesgo de los recursos de la red (Ri)	Importancia de los recursos (Wi')	Importancia total de los recursos (Wi)	Riesgo evaluado (Ri*Wi)
Edificio	Nombre	Cantidad				
2	Repetidor de F.O.	1	8	1	1	8
	Hub 24	5	7	0.8	4	28
	Hub 8	1	7	0.8	0.8	5.6
3	Hub 12	1	7	0.8	0.8	5.6
	Hub 8	1	7	0.8	0.8	5.6
	Estación de trabajo	1	8	0.7	0.7	5.6
1	REP. F.O.	1	10	1	1	10
	Hub 24	1	7	0.8	0.8	5.6
	Hub 16	1	7	0.8	0.8	5.6
	Hub 12	1	7	0.8	0.8	5.6
	Hub 8	3	7	0.8	2.4	16.8
	Estación de trabajo	27	8	0.7	18.9	151.2

Tabla 5. Análisis para la Zona A

Zona B

Recursos de la fuente			Riesgo de los recursos de la red (Ri)	Importancia de los recursos (Wi')	Importancia total de los recursos (Wi)	Riesgo evaluado (Ri*Wi)
Edificio	Nombre	Cantidad				
9	Repetidor de F.O.	1	8	1	1	8
	Hub 24	9	7	0.8	7.2	50.4
	Hub 12	1	7	0.8	0.8	5.6
8	Repetidor de F.O.	1	8	0.7	0.7	5.6
	Hub 24	4	7	0.8	3.2	22.4
	Hub 12	1	7	0.8	0.8	5.6
	Estación de trabajo	18	8	0.7	12.6	100.8

Tabla 6. Análisis para la Zona B

Zona C

Recursos de la fuente			Riesgo de los recursos de la red (Ri)	Importancia de los recursos (Wi')	Importancia total de los recursos (Wi)	Riesgo evaluado (Ri*Wi)
Edificio	Nombre	Cantidad				
10	Repetidor de F.O.	1	8	1	1	8
	Hub 24	1	7	0.8	0.8	5.6
	Hub 12	2	7	0.8	1.6	11.2
	Estación de trabajo	16	8	0.7	11.2	89.6
11	Repetidor de F.O.	1	8	1	1	8
	Hub 12	4	7	0.8	3.2	22.4
	Estación de trabajo	16	8	0.7	11.2	89.6
12	Hub 12	2	7	0.8	1.6	11.2
	Estación de trabajo	2	8	0.7	1.4	11.2
13	REP. F.O.	1	8	1	1	8
	Switch 6	1	10	1	1	10
	Hub 24	3	7	0.8	2.4	16.8
	Estación de trabajo	5	8	0.7	3.5	28
14	Hub 12	2	7	0.8	1.6	11.2
17	Repetidor de F.O.	1	8	1	1	8
	Hub 24	4	7	0.8	3.2	22.4
	Hub 12	2	7	0.8	1.6	11.2
	Estación de trabajo	5	8	0.7	3.5	28

Tabla 7. Análisis para la Zona C

Zona M

Recursos de la fuente			Riesgo de los recursos de la red (Ri)	Importancia de los recursos (Wi')	Importancia total de los recursos (Wi)	Riesgo evaluado (Ri*Wi)
Edificio	Nombre	Cantidad				
P.M	Router	1	8	1	1	8
	Hub 24	2	7	0.8	1.6	11.2
	Hub 12	1	7	0.8	0.8	5.6
	Estación de trabajo	1	8	0.7	0.7	5.6

Tabla 8. Análisis para la Zona M

De este análisis podemos obtener el riesgo general de cada zona (Rg); que es el resultado de la sumatoria del riesgo evaluado de cada recurso (Ri*Wi) entre la sumatoria del peso o importancia total de cada uno de ellos (Wi). Es decir:

$$Rg = \Sigma(Ri*Wi)/\Sigma Wi$$

Así pues tenemos que el riesgo por cada zona es:
Zona A: 7.72
Zona B: 7.54
Zona C: 7.73
Zona M: 7.41

Como se puede notar, el riesgo en seguridad de la red es grande, y por ello se debe implementar una política que ayude a superar en todo esta deficiencia.

Es importante mencionar que este análisis no es sólo por esta ocasión, sino por el contrario, debe realizarse por lo menos cada año, y en caso de modificar elementos de la red o de adquirir equipo adicional.

Una tabla complementaria al análisis de riesgo de seguridad de la red es la hoja de trabajo para otorgar acceso a recursos del sistema y la red, esta hoja sirve para documentar las restricciones de seguridad o de acceso a las que esté sujeto cada usuario.

Recursos de una red		Tipo de Acceso L=Lectura, E=Ejecución	Permiso de sistema operativo UNIX:rwx
Número	Nombre		
1	Sistema Operativo (UNIX)	L y E	R, X
2	Comandos	L y E	R, X
3	FTP	L y E	R, X
3	TELNET	L y E	R, X
3	Lenguajes de programación	L y E	R, X
4	CSHRC	L y E	R, W, X
4	EXRC	L y E	R, W, X
4	FORWARD	L y E	R, W, X
4	LOGIN	L y E	R, W, X
4	Netscape	L y E	R, W, X
4	Profile	L y E	R, W, X
4	Oracle *	L y E	R, W, X
4	Sybases *	L y E	R, W, X

*El permiso para la utilización de estos paquetes los asigna el administrador de la red para las personas que así lo requieran

4. Guía para Mejorar la Administración de la Red de la Facultad de Ingeniería.

4.1 Política de seguridad

La política de seguridad en la red que a continuación se presenta, es un documento que describe los intereses de seguridad de la red de la Facultad de Ingeniería.

Como se puede notar en el capítulo anterior, la Red de la Facultad de Ingeniería cuenta con cinco zonas, por lo tanto cada una de ellas tiene diferente administración de red, y con ello diferentes metas y objetivos. Sin embargo, se busca que con el apoyo de esta guía se puedan establecer mecanismos de seguridad que cubra cada uno de estos objetivos y metas[1]. Los siguientes temas a tratar son los puntos que así se han considerado de suma importancia para establecer las pautas para una mejor administración en la red, como lo son establecer una política de seguridad en la red, actualización del software en uso, actualización en la tecnología, optimización de los recursos, entre otras.

4.1.1 Aspectos importantes

La política de seguridad en la red debe ser aceptada y aplicada por los usuarios y administradores de la misma.

Se debe asegurar que todos conozcan su propia responsabilidad para mantener la seguridad.

Para cada tipo de problema asignar a alguien que lo pueda manejar de manera responsable.

Elevar el nivel de seguridad actual de la red

En el capítulo anterior se realizó un análisis del riesgo de la seguridad de los recursos y debido al alto riesgo que existe en la red de la FI se proponen las siguientes medidas para que el riesgo de la seguridad disminuya.

Alcanzar al menos el nivel C2, para en un futuro tratar de llegar al nivel máximo de seguridad (nivel A), el cual incluye todos los componentes de los niveles inferiores que son los siguientes:

[1] Muchas de las cuestiones de política de seguridad que se plantean están basadas en la RFC 1244.

Nivel B3: Dominio de seguridad, utilizar hardware de manejo de memoria para proteger el dominio de seguridad contra accesos no autorizados. La terminal del usuario debe estar conectada al sistema a través de una ruta de acceso confiable.

Nivel B2: Protección estructurada, etiquetar los dispositivos como discos, cintas y terminales.

Nivel B1: Protección etiquetada, el dueño del archivo no puede modificar los permisos de un objeto que esté bajo control de acceso obligatorio.

Nivel C2: Registrar una auditoría por cada acción que ocurra en el sistema.

Nivel C1: Sistema de protección de seguridad discrecional, los usuarios deben identificarse ante el sistema mediante su login y su contraseña.[2]

Este nivel cuenta con un proceso estricto de diseño, control y verificación; el diseño debe verificarse matemáticamente, y debe realizarse un análisis de los canales cubiertos y de distribución confiable[3]. Para ello se recomienda seguir los pasos que a continuación se describen a detalle.

4.1.2 Procedimientos para incrementar el nivel de seguridad en la red

Todos los recursos importantes de la red, como servidores, backbones, vínculos de comunicación, host, deben estar ubicados en un área fisicamente segura que sólo tengan acceso los administradores (de la red o de las salas de cómputo, según el caso). Y para el caso de las salas de cómputo, regirse por las reglas previamente establecidas.

- Debido a que cada edificio o División cuenta con un administrador de red es conveniente que cada uno de ellos realice planes y procedimientos para salvaguardar los recursos de la red contra pérdida y daño. Pero a su vez todos deben realicen procedimientos u operaciones similares, con el fin de apegarse a la política de seguridad que se recomienda. Además de examinar periódicamente la política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

Como se pudo observar en el capítulo anterior, la **Tabla 1** se recomienda para hacer este análisis de la red, ya que es una hoja de trabajo que canaliza ideas conforme los lineamientos que se manejan en la política de red.

[2] Ver más detalles en el capítulo 2.

[3] La *distribución confiable* significa que el hardware y el software hayan estado protegidos durante su traslado para evitar violaciones de los sistemas de seguridad.

Recursos de la red			Tipo de usuario del que hay que proteger el recurso	Posibilidad de amenaza	Medidas que se implementarán para Proteger al recurso
Número	Nombre	Importancia			

Tabla 1. Hoja de trabajo para establecer lineamientos

Recordando que:

- Número de recursos de red: es un número de identificación interna de los recursos que van a ser protegidos (si se aplica).
- Nombre del recurso de red: es la descripción en lenguaje común de los recursos. La importancia del recurso puede estar en una escala del 0 a 10.
- Tipo de usuario del que hay que proteger al recurso: a los usuarios se les puede designar internos, externos, o grupos de nombres.
- Posibilidad de amenaza: Puede estar en una escala numérica del 0 al 10.
- Medidas que se implementaran para proteger el recurso de red:

Análisis del riesgo de la seguridad de la red

El análisis de riesgo y la evolución de la amenaza se debe realizar cada semestre para saber el avance que se ha tenido al aplicar medidas de seguridad y el riesgo que se pudiera tener. Este análisis se debe realizar como se ha mostrado en el capítulo anterior, recordando que se deben determinar los siguientes dos factores:

- Estimación de perder el recurso (Ri)
- Estimación de la importancia del recurso (Wi)

- La Tabla 2 nos recuerda el formato que debe seguir nuestro análisis para que nuestra política de red no sea obsoleta en poco tiempo.

Recursos de la red		Riesgo de los recursos de la red (Ri)	Importancia del recurso (Wi)	Riesgo evaluado (Ri*Wi)
Número	Nombre			

Tabla 2. Hoja de trabajo que ayuda a registrar datos.

Y como se ha mencionado con especial cuidado, este análisis debe realizarse por lo menos cada año y en caso de modificar elementos de la red o de adquirir equipo adicional.

También debe cuidarse el registro para otorgar acceso a recursos del sistema y la red, ya que sirve para documentar las restricciones de seguridad o de acceso a las que esté sujeto cada usuario.

Recursos de una red		Tipo de Acceso	Permiso de sistema operativo
Número	Nombre	L=Lectura, E=Ejecución	UNIX:rwx
1	Sistema Operativo (UNIX)	L y E	R, X
2	Comandos	L y E	R, X
3	FTP	L y E	R, X
3	TELNET	L y E	R, X
3	Lenguajes de programación	L y E	R, X
4	CSHRC	L y E	R, W, X
4	EXRC	L y E	R, W, X
4	FORWARD	L y E	R, W, X
4	LOGIN	L y E	R, W, X
4	Netscape	L y E	R, W, X
4	Profile	L y E	R, W, X
4	Oracle *	L y E	R, W, X
4	Sybases *	L y E	R, W, X

*El permiso para la utilización de estos paquetes los asigna el administrador de la red para las personas que así lo requieran

4.1.3 Consideraciones para mejorar la política de seguridad de la red

En la medida de lo posible periódicamente se debe determinar el valor y delicadeza de la información guardada en las computadoras ya que la revelación de información, nos ha demostrado que es una amenaza fatal en la red.

Como se ha hecho notar, debido a la estructura de la red, se debe identificar quién está autorizado para conceder acceso a los servicios de la red y determinar que tipo de acceso puede conceder a los usuarios, ya que si se presenta un problema en alguna división o edificio, se tiene el nombre (o nombres) del administrador de la red o en su defecto de quien lo sustituya en determinado momento.

Es importante que el comité mencione explícitamente a cada uno de los administradores las responsabilidades que acatarán tanto ellos como los usuarios, abordando los siguientes puntos:

¿Quién está autorizado para usar los recursos?

Todos los usuarios de la red de la FI están autorizados para utilizar sin distinción cada servicio y recurso de la red, es decir, no se asignan permisos especiales a cada uno de los cinco grupos que existen en la red.

Uso adecuado de los recursos

Se debe entender como uso adecuado de los recursos, aquellas acciones que no interfieran en forma destructiva hacia los demás usuarios. Es decir no se permiten acciones como compartir o introducirse en cuentas ajenas, descifrar dichas contraseñas, interrumpir algún servicio, por ejemplo, una base de datos, correo electrónico, acceso a impresoras, introducción o activación de virus en archivos, no modificar archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura, y en términos generales la alteración de la información en la red.

No se debe considerar como interferencia o violación de información a los sondeos de seguridad que realice el administrador de la Red.

¿Quién está autorizado para conceder acceso y aprobar el uso de los recursos de la red?

La persona que tiene la capacidad y autoridad para conceder acceso y aprobar los recursos asignados es el administrador de cada División, pero a su vez coordinados por el Administrador General (persona designada por la Secretaría General de la Facultad), el cual sugerirá los lineamientos de seguridad o de trabajo para la red.

Derechos y responsabilidades

Es necesario que tanto el administrador del sistema como el usuario tengan conocimiento de sus derechos y responsabilidades en cuanto al uso de la red.

Derechos y responsabilidades del administrador del sistema

- El administrador podrá examinar los directorios y archivos de un usuario, únicamente en caso de peligro de la seguridad o prevención de la política de seguridad de la red.

  Se deberán conceder sólo los privilegios suficientes para cumplir con las tareas necesarias.

Para crear cuentas y finalizar accesos se recurrirá a las utilerías del sistema operativo UNIX[4], o en el sistema que se opere actualmente.

Al crear cuentas, se recomienda que sea de la forma más sencilla, con la finalidad de reducir errores en su creación, además se debe realizar una documentación del proceso para que en caso de faltar el administrador correspondiente, el administrador general o persona autorizada realice este proceso de igual forma que el administrador responsable de la División.

Por lo que corresponde a la contraseña inicial (en el caso particular de las contraseñas de las cuentas del grupo "FACULTAD") se recomienda evitar que esté en función del nombre del usuario, o parte de éste, o alguna contraseña generada por un algoritmo que pueda adivinarse con facilidad. Ya que el CERT [5] calcula que 80% de todos los problemas de seguridad en redes son creados por contraseñas inseguras

Se recomienda desactivar las cuentas en las que no haya habido acceso durante cierto tiempo (por ejemplo durante un mes), con la finalidad que el usuario solicite nuevamente la activación de su cuenta.

Considerar que algunas contraseñas (del grupo FACULTAD, por ejemplo), cambien su contraseña en el tiempo que consideren adecuado. Existen utilerías en Unix, como password+ y npasswd que pueden usarse para probar la seguridad de las contraseñas.

La utilería npasswd es un remplazo compatible para el comando passwd. Incorpora un sistema de verificación de contraseñas que inhabilita las contraseñas sencillas, y puede encontrarse en ftp://ftp.uga.edu/pub/security/npasswd.tar.gz.

Elaborar un reporte semestralmente al administrador general, de las novedades, problemas o lineamientos de seguridad que pudieran establecerse; con el fin de globalizar la seguridad en la red.

- Los administradores tienen el derecho de Examinar el tráfico de la red y del host, así como de realizar un monitoreo de la red, en cuanto a conexiones y tiempo de las mismas, y en casos excepcionales de ciertos lugares de la red.

- Un administrador tiene la capacidad de suspender una cuenta que no se pegue a las normas establecidas.

- Examinar periódicamente la política de seguridad de la red para ver si han cambiado los objetivos y las circunstancias de la red.

- Realizar semanalmente la inspección del funcionamiento de la red en cuanto a tráfico de la red, duplicidad de direcciones IP, localización de las mismas, prevención de

[4] Se considera a unix como ejemplo, pero puede ser cualquier otro.

[5] Computer Emergency Response Team - Equipo de Respuesta de Emergencias de Cómputo

caída de la red, entre otros, con las herramientas que se han implementado para este proceso. Dichas herramientas son[6]: el Transcend Enterprise Manager for Windows de 3Com, (pero se propone que se adquiera la nueva versión[7]) y una herramienta auxiliar para una inspección local es el LANalyzer con la cual se complementa una reporte parcial, es decir, este reporte consiste en el monitoreo de la zona, incluyendo equipos que no estén conectados a red UNAM pero que están conectados a nuestra red interna o local.

- Para el caso del sistema operativo unix, almacenar la información de conexiones en archivos de registro especiales (syslog), ya que la mayoría de los usuarios tienen horarios de trabajo regulares y se conectan y desconectan casi a la misma hora todos los días y por lo tanto una cuenta que muestre actividad fuera del horario "normal" del usuario puede ser una intrusión. Deben revisarse los registros producidos por dichas herramientas para detectar cualquier mensaje de error desacostumbrado producido por el software del sistema. Por ejemplo, un gran número de intentos fallidos de conexión en un periodo corto puede indicar que alguien está tratando de adivinar contraseñas. También debe inspeccionar el número de intentos de registro de conexión en las cuentas delicadas como root y sysadm.

  En unix el comando ps enlista los procesos que se están ejecutando en ese momento. Puede usarse este comando para detectar[8] programas no autorizados que quizá hayan sido iniciados por un intruso. También se puede combinar los comandos ls y find en un script de shell para revisar las configuraciones de propiedades de permisos y privilegios de archivo. Asimismo, se puede guardar la salida de esta actividad de inspección en listas que se pueden comparar y analizar mediante las herramientas diff, awk o perl. Las diferencias en los permisos de archivos importantes pueden indicar modificaciones no autorizadas en el sistema. También, para tener un mayor control se puede utilizar el comando INET que es prácticamente el administrador del sistema.

- Si detecta algún acceso no autorizado, deberá ser reportado al administrador general de la red para proceder con la falta cometida.

Qué hacer con la información delicada

En la Facultad de Ingeniería, existen algunos lugares en los cuales se cuenta con información sumamente confidencial (por ejemplo USECAD), es recomendable utilizar

[6] Estas herramientas se describirán mas a detalle en la sección de Monitoreo de la red.
[7] En caso de adquirirla, no será necesaria la utilización del LANalyzer como aquí se menciona.
[8] El administrador del sistema debe inspeccionar con frecuencia y regularidad a lo largo de todo el día. Puede resultar muy fastidioso inspeccionar en horarios fijos, pero pueden ejecutarse comandos de inspección a cualquier hora. Ya que si se inspecciona con frecuencia se puede familiarizar rápidamente con la información normal, lo cual ayudará a detectar información inusual.

encriptación, compactación y respaldo de datos además de la asignación de un lugar físico aislado de personas externas o no autorizadas como mecanismos de seguridad.

Derechos y responsabilidades del usuario

- Es un derecho que el usuario tenga privacidad en su información.
- Es responsabilidad del usuario respaldar su información.
- Se considera como abuso en términos de usar la red aquello que perturbe el trabajo a los demás usuarios, así como a la utilización de recursos con fines no académicos lucrativos.
- No se permite que los usuarios compartan cuentas o permita a otros usar la suya (por propia seguridad de los dueños de la cuenta).
- No rebelar su cuenta en forma temporal, para permitir que otros trabajen en un proyecto utilizando su cuenta.
- Los usuarios que tienen acceso a la red "indefinido" (Grupo Facultad), deben de cambiar su cuenta, cuando menos cada semestre meses.
- Conocer y cumplir la normatividad de las salas de computo (UNICA) y el uso del WEB.
- Hacer buen uso de los equipos de cómputo, software y datos que le son proporcionados. Es preciso aclarar que cada usuario es responsable de sus acciones, esto al margen de los mecanismos implantados.
- Si existiera algún proyecto académico o administrativo que necesitara mayores recursos de los asignados (ver capítulo 3), y que sean plenamente justificados, se deberá solicitar al administrador responsable de la división.

4.1.4 Publicación e interpretación de la política de seguridad

La política que se presenta debe ser interpretada por los administradores de la red, que se hagan responsables de interpretar, repasar y revisar el documento por lo menos cada dos meses.

Distribuir la información de la política de seguridad de red por medio de listas de correo, sesiones informativas, reuniones personales con el administrador, folletos, revista de la FI, boletines, etc., para darla a conocer a la comunidad.

4.1.5 Plan de acción cuando se viole la política de seguridad

Se considerará que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado

Cuando se viole algunas de las disposiciones en la política de seguridad, se debe determinar si ésta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto.

En cualquiera de estos casos se tomará nota del usuario responsable, cancelándose el acceso a la red por un semestre, y si existiera reincidencia suspenderle totalmente su acceso.

Por otra parte, los intentos deliberados de violar las redes de otro sitio (cuando se tiene acceso a Internet) constituye una violación de la política de la red de la Facultad.

4.2 Identificación y prevención de problemas de seguridad

Como se pudo observar la política de seguridad presentada define lo que necesita protegerse, pero no se señala explícitamente cómo deberán protegerse los recursos y el enfoque general para mejorar los problemas de seguridad como parte de nuestra administración. En esta sección se abordarán los procedimientos generales que deberán implementarse para evitar problemas en la seguridad.

4.2.1 Actualización de la información

Para estar al tanto de las novedades en seguridad de redes, software, hardware, entre otras, se recomienda identificar algunas agencias con las que se debe hacer contacto en caso de incidentes de seguridad, además de los requerimientos adicionales, en nuestro caso, sería conveniente inscribirse en las listas de correo o grupos de noticias en los que se discuten temas de seguridad que sean de nuestro interés.

Se debe recordar que se requiere tiempo para mantenerse al día con la información de las listas de correo y grupos de noticias.

Listas de correo

Las listas de correo son mantenidas por servidores de listas en Internet. Cuando se une a una de ellas, puede comunicarse con los demás usuarios a través del correo electrónico.

Para enviar respuestas u opiniones acerca de un tema, se puede enviar correo electrónico a la lista. Todos los que estén en la lista de correo recibirán el mensaje. La solicitud para unirse a una lista de correo se envía a otra dirección, la cual es "diferente" de la dirección de correo electrónico de la lista. La solicitud de suscripción debe enviarse a la dirección de solicitudes y no a la dirección de correo electrónico de la lista. Los miembros de la lista, que pueden ser miles, no apreciarán recibir solicitudes para unirse a una lista de

correo. Algunos administradores de listas de correo compilan una lista especial de preguntas frecuentes (FAQs), las cuales constituyen un buen lugar para empezar a buscar más información.

Las listas de correo pueden ser moderadas o no moderadas. En las moderadas, el dueño de la lista actúa de moderador y descarta las respuestas que no estén de acuerdo con los objetivos de la lista.

Se dispone de gran variedad de administradores de listas. Algunos son automáticos y otros se procesan a mano. Si se tiene dudas de cómo suscribirse o retirarse de una lista, enviar el siguiente comando, en el que nombrelista representa el nombre de la lista de la cual desea información:

INFO <nombrelista>

En las listas no moderadas no existe proceso de selección. En consecuencia, la proporción entre señal y ruido puede ser muy baja. Si se decide que esa lista de correos no es la adecuada, enviar una solicitud de "eliminación de suscripción" a la dirección electrónica de solicitudes de lista (y no a la lista en sí). Esta solicitud debe incluir lo siguiente en el cuerpo principal:

UNSUBSCRIBE listname.

El término proporción entre señal y ruido usado en correo electrónico se refiere a que la señal representa mensajes de correo electrónico reales y significativos; el ruido representa los mensajes inútiles, como los de suscripción y prueba, que obstruyen las comunicaciones normales entre quienes utilizan listas de correo.

Listas de correo de seguridad de Unix

El objetivo de la lista de correo de seguridad de Unix es notificar a los administradores de sistemas acerca de problemas de seguridad, antes de que éstos se hagan de dominio público, así como proporcionar información acerca de temas relacionados con la seguridad. Esta lista está abierta sólo a aquellas personas de las que pueda comprobarse que son los administradores principales de la red.

Para suscribirse a esta lista, la solicitud debe originarse desde el contacto del sitio listado en la base de datos WHOIS del Centro de Información sobre Redes de la Red de Datos de la Defensa (DDN NIC, Defense Data Network's Network Information Center), o desde la cuenta raíz de una de las máquinas principales de la red. Se debe incluir la dirección destinataria de correo electrónico que se desee en la lista. También se debe incluir la dirección de correo electrónico y el número telefónico del solicitante.

La dirección de correo electrónico para enviar la solicitud de suscripción es la siguiente:

security-request@cpd.com

Lista de VIRUS-L

En la lista VIRUS-L se habla de experiencias con virus de computación, software de protección y temas relacionados. La lista está abierta al público y está implementada como un compendio moderado. La mayoría de la información se relaciona con las computadoras personales, aunque parte de ella puede aplicarse a sistemas más grandes. Para suscribirse, se debe enviar un mensaje de correo electrónico a la siguiente dirección:

listserv%lehiibm1.bitnet@mitvma.mit.edu

o bien:

listserv@lehiibm1.bitnet

y en el cuerpo del mensaje incluir la siguiente línea:

suscribe virus-L "Nombre Apellido"

Si se desea recibir un compendio de la versión, en lugar de respuestas de correo electrónico individuales, incluir la siguiente línea:

set virus-L digest

Esta lista también está disponible a través del grupo de noticias Usenet, con el siguiente nombre:

comp. virus.

Es necesario que se adquieran licencias para el uso de antivirus, ya que es una de las amenazas más importantes que tiene la red, y como consecuencia se puede llegar a perder la información de los usuarios.

4.2.2 Protección de la información

Encriptación de Datos

Otra forma de proteger datos es por medio de la encriptación de contraseñas. La oportunidad de encriptar información para proporcionar un nivel de seguridad más alto en el sistema y sus datos es de interés para usuarios y administradores de sistemas en todas partes. Sin embargo, aun los datos encriptados pueden correr riesgos si no se vigila y capacita adecuadamente a los usuarios que deseen utilizar estas funciones.

Cuando un usuario se registra en el sistema (unix), el programa "getty" pide el nombre de usuario y después ejecuta el programa de conexión. Éste le pide la contraseña, pero no lo descifra. De hecho, el programa de conexión encripta la contraseña y luego compara ese

valor con el que está almacenado en /etc/passwd. Si son iguales, significa que el usuario suministró la contraseña correcta. Por lo que el administrador se puede apoyar en el comando "getty" para las contraseñas proporcionadas por el usuario, sin riesgo a que sean descifradas de manera fácil para otros[9].

Encriptación de archivos

Como se ha visto, la encriptación de contraseñas mediante un mecanismo que no se descifra fácilmente constituye un método relativamente seguro de evitar que usuarios no autorizados tengan acceso al sistema. Por lo que se refiere a los archivos es relativamente fácilmente encriptar archivos con el comando crypt(1). Si no se dan argumentos en la línea de comando, crypt pide la clave, lee los datos que se encriptarán a partir de la entrada estándar e imprime la información encriptada en la salida estándar. Sin embargo, lo ideal es que en la línea de comando se dé la información que se usará, como se ilustra en el siguiente ejemplo:

crypt key <clear> cipher

El comando anterior lee el archivo clear, encripta las pruebas con la clave de contraseña y guarda el texto encriptado resultante en el archivo cipher. Los archivos encriptados pueden verse o desencriptarse mediante una línea de comando similar, como se muestra a continuación:

crypt key <cipher> clear
crypt hey <cipher | pr | lp

En el primer comando del ejemplo anterior, el texto encriptado en cipher se desencripta mediante key y se guarda en el archivo llamado clear. En el ejemplo de la segunda línea de comando se usa crypt para desencriptar el texto y enviar el resultado de texto llano a pr para su formateo, y después a lp para su impresión. Los archivos generados por crypt pueden ser editados mediante de o vi, considerando que el sistema soporta archivos de edición encriptados.

El mecanismo exacto usado por crypt está bien documentado y en Internet se encuentran disponibles públicamente muchas versiones de este comando. El programa cript(1) no usa las mismas rutinas de encriptación que crypt(3), el cual se usa para la encriptación de contraseñas.

La clave de encriptación utilizada es el factor limitante para determinar el grado de esfuerzo para desencriptar los datos. Mientras más grande sea la contraseña, más complejo es el patrón de encriptación, y más tiempo se requiere para transformar la clave a la configuración interna usada por la máquina. Por ejemplo, el proceso de transformación está diseñado para durar cerca de un segundo, pero si se restringe la clave

[9] Ver más detalles de teoría en el capítulo 2.

a sólo tres letras minúsculas, los archivos encriptados pueden leerse gastando sólo una fracción substancial de cinco minutos en tiempo real de máquina.

Una forma de mejorar la posibilidad de proteger sus datos es comprimiendo los archivos antes de encriptarlos.

Procedimientos de Recuperación

Siempre que se instale una versión nueva del sistema operativo, no sólo se debe hacer respaldo de la imagen binaria del kernel del sistema operativo, sino también de los archivos usados para compilar y configurar dicho sistema. Lo mismo es válido para todo el software de aplicación de red.

Los respaldo del sistema de archivos son como una póliza de seguros. No sólo protegen en caso de fallas del disco y de otras partes del hardware, sino también contra eliminaciones accidentales y como medida de reserva cuando el sistema es penetrado. Cuando se sospeche que alguien ha irrumpido el sistema, quizá tenga que restablecerse desde el respaldo para protegerse de los cambios que pudiera haber hecho el intruso. Si no se puede detectar cuándo ocurrieron los cambios no autorizados, tendrá que examinarse numerosos respaldos.

Los respaldos diarios, así como los de incremento, pueden ser útiles para ofrecer la historia de las actividades del intruso. Al examinar los respaldos anteriores, se puede determinar cuándo se introdujo al sistema por primera vez. (Cuando se busquen rastros de archivos de intrusos, deben buscarse nombres de archivo que normalmente no aparecerán en el listado del directorio. En nuestro caso buscar archivos cuyo nombre empieza con punto "." o que tengan caracteres no desplegables. Estos archivos son más difíciles de detectar.)

Existen diversas estrategias de respaldo, lo cual implica la combinación de los siguientes métodos[10]:

- Respaldo total (o nivel 0): Se respaldan todos los datos, sin importar cuándo hayan sido modificados, ni aun cuando no lo hayan sido (se recomienda cuando se desee hacer un cambio de sistema o de versión de sistemas operativos).

- Respaldo de nivel 1: Respalda todos los archivos que han sido modificados desde el último respaldo de nivel 0. Es recomendable para cualquiera de los administradores de red, ya que sus respaldos siempre estarán actualizados.

- Respaldo de nivel 2: Respaldo incremental para referirse al respaldo de todos los archivos que hayan sido modificados desde el último respaldo (de nivel 0 o 1)

[10] Ver más detalles de teoría en el capítulo 2.

- Respaldo personalizado: Útil cuando se quiere respaldar en forma selectiva unos cuantos archivos y directorios, y no esperar al respaldo programado.

Los respaldos de la información son necesarios para depurar y salvaguardar datos de interés. Una opción de ello es la utilización de cintas, es importante que este respaldo tenga continuidad, para que en algún momento se puedan desechar los respaldos que ya no sean necesarios, y así hacer un mejor uso de este recurso.

4.3 Monitoreo de la red

Como se analizó en el capítulo 3, el sistema de monitoreo de la red se está llevando a cabo con dos softwares (LANalyzer y Trnascend) y debido a la versión que se utiliza en el Transcend no es posible ver más detalles de la red, por lo que se recomienda actualizar este software a la versión 5.0, de la cual se describen a continuación sus características generales y la ayuda que dará a cada uno de los administradores de las divisiones de la FI.

Esta es una tarea de la administración de la red que no se debe descuidar, ya que es la herramienta principal que nos indica en cierto momento las anomalías que pudieran presentarse. Además es un indicador que ayuda para proponer nuevas opciones de ampliación, actualización ó reestructuración de la red.

Transcend Enterprise Manager V.5.0 para Windows 95

Este software permite un fácil uso de administración gráfica para un amplio rango de dispositivos de 3COM, desde ruteadores y switches hasta concentradores y pc's. Los mapas jerárquicos de código de colores permiten una visión exacta de la red y permite una fácil y rápida localización de fallas.

Con la adquisición de esta versión de software se adquieren los siguientes beneficios:

- Es para Windows 95: Actualmente todos los equipos con los que cuenta la FI cuentan con Windows 95 instalado, este producto al ser de 32 bits brinda más opciones de administración para una gama más amplia de dispositivos a monitorear.

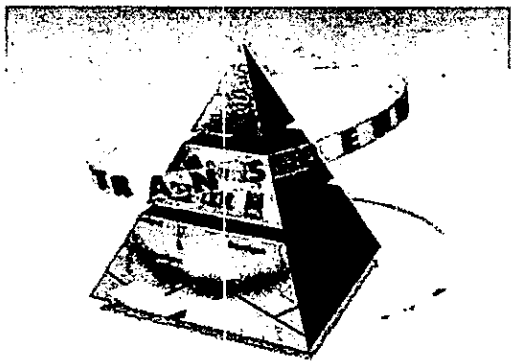
- -Ambiente más amigable: Es posible realizar una observación de los mapas de cada subred que se tenga configurada con sus respectivos estados y gráficas con mas opciones de acceso para cada una, además de todas las opciones que se han expuesto anteriormente.

Este software ofrece una administración en tres niveles:

- Red: Toma la forma de un mapa topológico jerárquico el cual representa las redes IP y IPX que contienen concentradores, switches y estaciones finales interconectadas con ruteadores.

- Grupo: Grupos virtuales de estaciones finales Pc's con el software Workgroup PC Links. Estos grupos representan grupos geográficos, administrativos o cualquier otro grupo que el usuario desee diseñar.

- Dispositivo: Descripción de la vista interna de una red de pc's con vistas gráficas de una amplia gama de productos como son LinkBuilder (dispositivo con el que cuenta la F.I.) LinkSwitch, SuperStack.



La versión 6.1 del Transcend para Windows, está disponible en dos partes:

- Transcend Enterprise Manager for Windows, el cual está diseñados para interredes globales y redes LAN grandes.

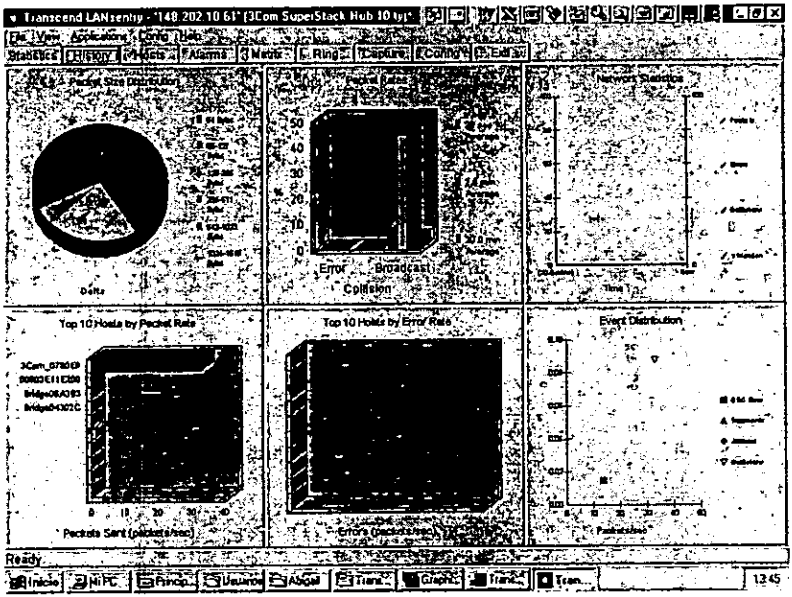
- *Transcend Workgroup Manager for Windows,* la cual está hecha para las necesidades de una red pequeña.

En cuanto a monitoreo y análisis el software de administración Transcend provee dos herramientas:

- Administrador LANSentry
- Vista de estados

Administrador LANSentry

Esta herramienta polea dispositivos de una red remota para recibir datos de red, los cuales procesa y despliega para permitir monitorear el estado del segmento, su rendimiento en ese momento y recientes sucesos. Para análisis más profundos, es posible correr la aplicación RMON para ver datos estadísticos e históricos, configurar condiciones de alarmas, monitoreo de conversaciones entre estaciones en la red, y capturar y desplegar paquetes específicos.



Vista de estados

Estos estados administran dispositivos de 3Com y grupos de dispositivos con observación de estados de estados, MAC y reporte de WEB.

Nota: Las vistas de estados y sus aplicaciones son soportadas únicamente por el software de administración Transcend corriendo en una estación NT. No la soporta Windows 95 ni está integrado en el software de administración Transcend Workgroup.

Reporte de estados (Status watch)

- Se utiliza para analizar el rendimiento operacional de los ocmponentes de la red. Por ejemplo, utilización de anillos FDDI.
- Detecta problemas operacionales del os dispositivos de la red. Por ejemplo, temperatura alta del sistema.
- Grafica o despliega datos en tiempo real mostrando estado operacionales.
- Monitorea interfaces de ruteo para corroborar problemas de ruteo de IP y determinar la integridad de las interfaces WAN.

Reportes de MAC's

- Vista de todas las direcciones MAC' asociadas con cada dispositivo.
- Monitorea la actividad de las direcciones MAC. Nuevas Mac's, las que se mueven, agregan o duplican de un grupo, a través de la información del último poleo.
- Localizar las estaciones terminales de trabajo que están conectados en la red mediante la búsqueda de direcciones MAC y de IP.

- Deshabilitar interfaces de switch seleccionadas.
- Deshabilitar dispositivos de switch seleccionados.
- Localizat direcciones IP duplicadas.

4.4 Actualización de tecnología y dispositivos

Debido al crecimiento de la red de la FI, se recomienda la actualización de la red Ethernet que se tiene actualmente por una red Gigabit Ethernet[11], ya que se mejoraran las conexiones de servidores a un switch; conexión switch a switch; y se mejora el backbone (columna vertebral). Esta propuesta se hace porque en este momento es la más adecuada, pero conforme pase el tiempo deberá irse adecuando a la tecnología que se requiera.

En cualquiera de los escenarios planteados, los sistemas operativos de Red (NOS; Network Operating Systems), las aplicaciones y los drivers (unidades de disco) de las tarjetas de interfase de red (NIC: Network Interface Card) permanecerán sin cambio en las estaciones.

4.4.1 Enlaces de Switch a switch

A continuación se presenta un ejemplo de cómo quedarían conectados los switches y los cambios que se requerirán para migrar a la tecnología propuesta.

En la Figura 1, se observan dos switches Ethernet que enlazan dos redes 10 Base T cada una con sus propios servidores y estaciones. La transmisión entre los switches de enlace de las dos redes es de 10 Mbps. Esta configuración puede ser mejorada si cambiamos los switches Ehternet por switches Gigabit Ehternet 100/1000 Mbps, como se muestra en la Figura 1. En esta configuración, la transmisión de datos entre los switches Gigabit Ehternet será de 100 Mbps, a estos switches se conectarán los servidores de la red con tarjetas de interface de red (NIC) Gigabit Ehternet, lo que hará que el trabajo entre los servidores y el switch se lleve acabo a 100 Mbps. Al switch Gigabit Ethernet se conectarán los otros hubs o repetidores a 10/100 Mbps. Esta configuración permitirá una mejor respuesta de los servidores a las estaciones de trabajo.

[11] Ver apéndice C

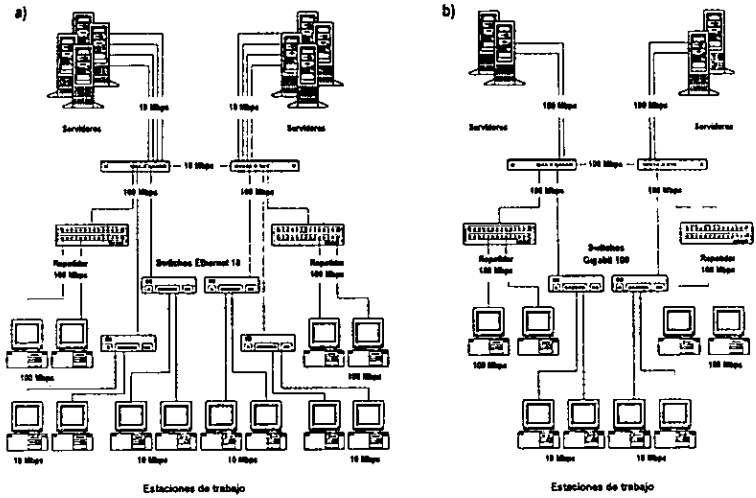


Figura 1. a) Switches Ethernet, b) Switches Gigabit Ethernet

4.4.2 Mejorar el backbone

En la **Figura 2a**, se observa un backbone (columna vertebral) 10 Mbps con un switch Fast Ehternet. Este backbone permite comunicar estaciones de trabajo a través de switches o hubs (concentradores) a 10/100 Mbps. El backbone puede modificarse y mejorarse si se cambia el switch Fast Ehternet por un switch Gigabit Ethernet, permitiendo la conexión con los switches 10/100 Mbps (véase **Figura 2b**).

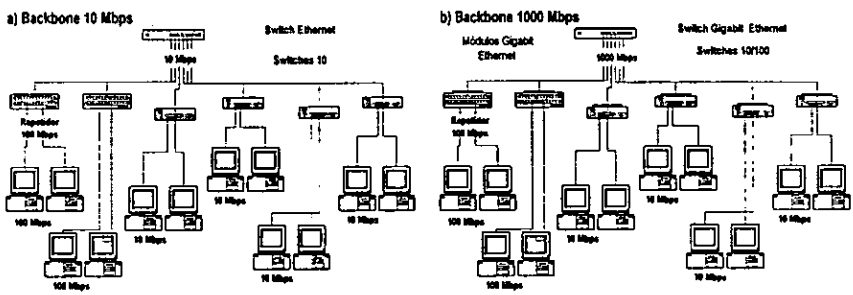


Figura 2. a) Backbone 10 Mbps, b) Backbone 1000 Mbps

Al switch Gigabit Ehternet pueden conectarse servidores con tarjetas de red Gigabit Ehternet.

Finalmente, el costo de entrenamiento, mantenimiento y solución de problemas para Gigabit Ehternet será muy bajo en relación con otras tecnologías, si se toma en cuenta que la red de la FI o institución tiene su base en la tecnología Ethernet, la cual es casi idéntica a Gigabit Ethernet.

Además de los costos otra ventaja es que Gigabit Ethernet es más rápida que otras tecnologías como son Ethernet, Fasth Ethernet, Token Ring, FDDI y ATM.

Esta actualización no solo se refiere a swithes, sino en general al equipo que conforma la red, que como se sabe, la tecnología que en su momento es actual, hasta la fecha tiene una duración de vida útil de aproximadamente 2 o 3 años, esto no significa que en los años siguientes ya no sean útiles, sino más bien ya no son las adecuadas para las nuevas necesidades de los usuarios.

La propuesta de cambiar switches, surge de la necesidad, y después de haber realizado el análisis correspondiente, de dar una mayor eficiencia de respuesta entre a las estaciones. Ya que en general, la conexión y equipos de la red son relativamente nuevos.

4.5 Herramientas de apoyo en el crecimiento de la red.

4.5.1 PROXY SERVER

Considerando el crecimiento de la red y sus alcances, podemos notar que las direcciones IP asignadas inicialmente a la red de la Facultad, en cierto momento ya no podrán satisfacer las necesidades de los usuarios, por ello, una de las propuestas en las que se hace mayor énfasis es la instalación de un Proxy Server en los lugares requeridos, para que con una dirección IP, varios usuarios puedan tener acceso a la red más grande del mundo, Internet.

Puede ser que en el transcurso del tiempo se asignen más direcciones a la Facultad, pero esta medida se toma como una medida de contingencia en los lugares donde se pueda ver que existe una limitación en cuanto a direcciones IP se refiere.

Durante la instalación de Microsoft Proxy Server, se creará una lista de direcciones IP que conforman la red privada. La dirección IP externa estará excluida de esta lista.

El archivo que contiene la LAT[12] se encontrará en el servidor, con el nombre Msplat.txt. Por default el archivo se encontrará en c: \Msp\Clients. Se instalará también un programa para clientes dentro de este directorio.

El programa de instalación Microsoft Proxy Server configurará el subdirectorio \Clients en el servidor para ser compartido con el nombre Mspclnt. Los usuarios podrán

[12] Tabla de Direcciones Locales (Local Adress Table), ver teoría más a detalle en el capítulo 2.

conectarse al \\Servername\Mspclnty y después ejecutarán el programa de instalación de clientes. Este programa de instalación configura la computadora cliente como cliente de WinSock Proxy Service, y también se configurará el usuario de Internet como cliente de Web Proxy Service.

En algunas situaciones, será necesario proporcionar acceso a cuentas a la dirección IP interna del servidor. Para llevar a cabo esta acción, es necesario crear un archivo LAT para una cuenta y copiarla al Msplat.txt. Sin embargo esto puede ser en forma temporal, dado que cada cuenta de Msplat.txt es reescrita en intervalos regulares por el servidor. Cualquier cambio local realizado es perdido cada vez que el servidor actualiza el archivo Msplat.txt.

Para evitar la pérdida de la cuenta, se debe crear un archivo LAT local, llamado Locallat.txt y colocarlo dentro del directorio Mspclnt. La cuenta estará en ambos archivos Msplat.txt y Locallat.txt si están presentes. De esta manera se podrán añadir rangos de direcciones IP que conformaran a la red privada.

El LAT consiste de una serie de direcciones IP, cada par de direcciones define un rango de direcciones IP (de la dirección inferior a la dirección superior) o una sola dirección (si ambas direcciones son iguales).

Requerimientos de instalación.

Hardware

Microsoft Proxy Server puede ser instalado en una computadora que contenga un disco duro configurado como file allocation table (FAT) o NTFS. Para un mejor funcionamiento, se recomienda que al menos uno de los discos del servidor este configurado como un NTFS volume.

Antes de instalar Microsoft Proxy Server, verificar que las tarjetas de red estén instaladas y configuradas. Para tener una configuración segura, el servidor debe tener al menos una tarjeta conectada a la red interna, más un adaptador de red, un módem o adaptador integrated services digital network (ISDN) conectado a internet.

Los programas que deben estar instalados antes de instalar Microsoft Proxy Server, son los siguientes:

- Windows NT Server 4.0
- Microsoft Internet Information Server 2.0
- TCP/IP
- Windows NT Server 4.0 Service Pack

El servidor puede ser configurado como un servidor stand-alone, un primary domain controller (PDC), o backup domain controller (BDC).

1. Para la instalación de Microsoft Proxy Server se deben verificar los requerimientos de instalación, antes mencionados.
2. Del directorio Ntupdate, abrir un subdirectorio de acuerdo a la arquitectura del procesador del servidor y ejecutar el programa update.exe para instalar Windows NT Server 4.0 Service Pack. Después de instalarse el Service Pack, inicializar el servidor y registrarse como supervisor.
3. Ejecutar el programa **Setup**. Dar click en el cuadro Welcome para continuar y un cuadro de diálogo de **CD Key Number** aparecerá.
4. Registrar el número de identificación del producto, teclear el número en el cuadro **CD KEY** y dar click para continuar. A continuación aparecerá una cuadro de dialogo de Change folder.
5. Para el cambio de directorio dentro el cual Microsoft Proxy Server será instalado, dar click **Change Folder** y completar el cuadro de diálogo. Para aceptar el directorio por default, saltarse este paso. Después aparecerá el cuadro de diálogo: **Installation Options**.
6. El cuadro de diálogo **Installation Options** contiene los siguientes componentes a instalar:
   - Proxy Server
   - Herramientas de administración
   - Documentación
7. Estos componentes pueden ser seleccionados o no para su instalación. Por default todos los componentes son seleccionados. Cuando estén apropiadamente selecionados los componentes, dar click para continuar. Después aparecerá una cuadro de dialogo de **Microsoft Proxy Server Cache Drives**.
8. En el cuadro de dialogo de **Microsoft Proxy Server Cache Drives**. Son listados los drives locales del servidor.
9. Para asignar un disco para almacenar cached data, seleccionar un drive de la lista y teclear un número en el cuadro **Maximun Size (MB)**, y aceptarlos con un click en la opción **Set.**

   Repetir como sea necesario para asignar drives adicionales para almacenar cached data.

   Durante la configuración de caché drives se debe, al menos, colocar un drive y 5 MB o más para caching. Se recomienda colocar al menos 100 MB o .05 MB por cliente de Web Proxy Server.

   Asignar espacio de un drive al caché en incrementos de 5 MB. Si se asigna cualquier número al cache este no podrá ser dividido por 5, la asignación es alrededor o menor de 5 MB, enseguida dar un click para continuar.
10. Aparecerá un cuadro de diálogo en **Local Address Table Configuration**. Para crear una tabla de direcciones IP en la red interna, dar click en el botón **Contruct Table**.
11. Seleccionar la tarjeta de red del servidor donde se encuentran las direcciones IP que son incluidas en el LAT, sleccionar **Load From NT Internal Routing Table** y completar esta opción.
    - Si se desconoce cual de las tarjetas del servidor está conectada a la red privada, seleccionar **Load Know addres ranges from all IP interface cards.**
    - Pero si se sabe cual de las tarjetas del servidor está conectada a la red privada y cual a internet, seleccionar **Load Know addres ranges from the follewing IP interface cards** para levantar solamente las direcciones IP asociadas con las tarjetas internas

conectadas al servidor. Posteriormente, en la lista de tarjetas de red, seleccionar el cuadro de verificación por cada tarjeta interna conectada, y limpiar el cuadro de verificación por cada tarjeta externa conectada.

12. Cuando se haya completado el cuadro de diálogo del **Contruct Local Addres Table**. La caja de dialogo **Local Address Table Configuration** retornará con una lista de pares de direcciones IP que serán desplegadas en el cuadro **Internal IP Ranges.**
13. Verificar que los accesos en el cuadro **Internal IP Ranges** sean correctamente identificados por la red interna. Agregar cualquier par de direcciones Ip necesarias hasta que todas las direcciones de la red interna sean definidas.
    - Para Añadir un rango de direcciones IP a la lista, debajo de **EDIT** teclear un par de direcciones en las cajas de **FROM** y **TO**, y después dar click al botón **ADD**.
    - Para añadir una sola dirección IP a la lista, debajo de **EDIT** teclear la misma dirección en ambas de **FROM** y **TO**, y después dar click al botón **ADD**.
    - Para suprimir una sola dirección o par de direcciones IP de la lista, seleccionar ésta del cuadro de dialogo **Internal IP Ranges**, y después dar click al botón **REMOVE**.
14. Cuando la configuración del LAT esté lista, dar click en el botón OK, y aparecerá el cuadro de dialogo **Client Installation/Configuration**.
15. Utilizar las opciones que se encuentran debajo de Winsock Proxy Client para especificar como el programa de instalación de clientes configurará WinSock Proxy Clients del servidor.
    - Seleccionar Machine, DNS Name o IP Addresses. Si se elige Machine o DNS Name, verificar el nombre correcto, sino, asignar un nombre apropiado.
    - Si el cuadro de verificación Enable Acces Control es seleccionado, el servicio de seguridad WinSock Proxy se habilitará, y solamente a esos clientes se les asignarán permisos para ocupar el servicio WinSock Proxy sobre el servidor. Si el cuadro de verificación no esta seleccionado, por default todos los clientes podrán hacer uso del WinSock Proxy.
16. Utilizar las opciones que se encuentran debajo del Web Proxy Client para especificar como el programa de instalación de clientes configura el Web Proxy Clients del servidor.
    - Debajo de Web Proxy Client seleccionar "Set Client Setup to Configure Browser Proxy Settings" para que el programa de instalación de clientes configure a los usuarios browser como un Web Proxy Clients (si el browser es Netscape Navigator o Microsoft Internet Explorer).
      Si se selecciona esta opción, verificar que el nombre mostrado en el cuadro Proxy To be Used by Client sea correcto. Si es necesario asignar el nombre correcto.
      También, si se selecciona esta opción el valor Client Connects to Proxy Via port mostrará el número de puerto de Web Proxy Clients que será configurado para su uso.
    - Cuando el cuadro de verificación Enable Access Control es seleccionado, Web Proxy service segurity es habilitado. Cuando este cuadro de verificación es borrado, el Web Proxy Service no validará la conección de usuarios. Por default, este cuadro de validación es seleccionado.
17. Cuando el cuadro de **Client Installation /Configuration** esta completo dar click para finalizar.

Configuración del Web Proxy Service

Selección de Método de Autentificación

Hay tres tipos de métodos de autentificación , que pueden ser usados por Web Proxy Service:

- Anónimo
- Básico
- Windows NT Pregunta/Respuesta

Configuración de los métodos de autentificación de los servicios WWW y Web Proxy

1. En el administrador de servicio de Internet, dar doble click en el nombre del servidor que se encuentra al lado del servicio **WWW**. Aparecera un cuadro de dialogo **WWW Service Properties**. Asegurar que la etiqueta Service este seleccionada.
2. Debajo de Password Authentication, seleccionar uno o más métodos de autentificación.
   - Permitir Anonimo
   - Básico (limpiar texto)
   - Windows NT Pregunta/Respuesta
3. Dar click en **Ok**.

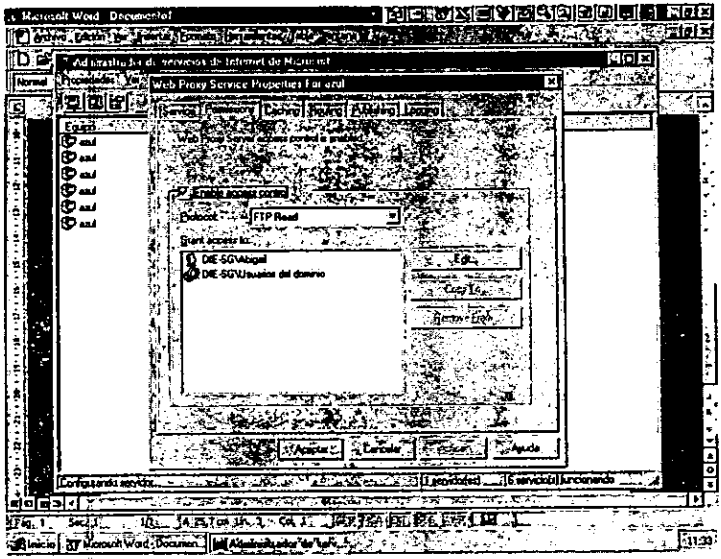
Este procedimiento es sólo par un servidor, en caso de haber más servidores, hacer el mismo proceso para cada uno de ellos.

Conceder permisos a usuarios de Proxy

- Si se habilita el método de autentificación anónimo en el servicio WWW, todos los usuarios tendrán acceso y no será necesario habilitar permisos en el Proxy.
- Si se deshabilita el método de autentificación anónimo en el servicio WWW y se habilita el básico o Windows NT Pregunta/Respuesta, se deberán habilitar los permisos antes que los usuarios puedan accesar a Internet ocupando Web Proxy Service

Los permisos del Proxy determinarán cuales usuarios o grupos pueden accesar al Internet utilizando un protocolo a través del Web Proxy Service sobre el servidor. Los permisos serán concedidos separadamente para cada protocolo. Los protocolos disponibles en Web Proxy service son:

- FTP Read.
- Gopher
- WWW
- Seguro



Antes de asignar permisos Proxy, es recomentable utilizar el administrador de usuarios para crear grupos de usuarios que contienen cuentas de usuarios quienes necesitan un protocolo o un grupo de protocolos. Posteriormente se podrá dar permisos a grupos y no sólo a usuarios individuales.

Con estas serie de pasos, podemos configurar proxies en los lugares donde sea requerido, para poder así satisfacer las necesidades de comunicación entre los usuarios.

4.5.2 INTRANETS

Es un concepto "nuevo", pero de gran utilidad, este concepto ha sido manejado en su mayoría de veces por las empresas privadas, que persiguen obtener la mejor utilidad y con ello elevar las ganancias de su empresa. Parecería que en nuestro caso, no sería útil, pero revisando un poco en detalle podemos observar que también podemos obtener ganancias.

Gracias a Internet, y con un costo moderado, se puede organizar de manera más eficiente toda la información de la Facultad, de tal forma que profesores, alumnos, y personal administrativo puedan consultar bases de datos o información de interés desde su PC. Para ello se requiere implementar una Intranet.

Los componentes de hardware y software que requiere una intranet son:

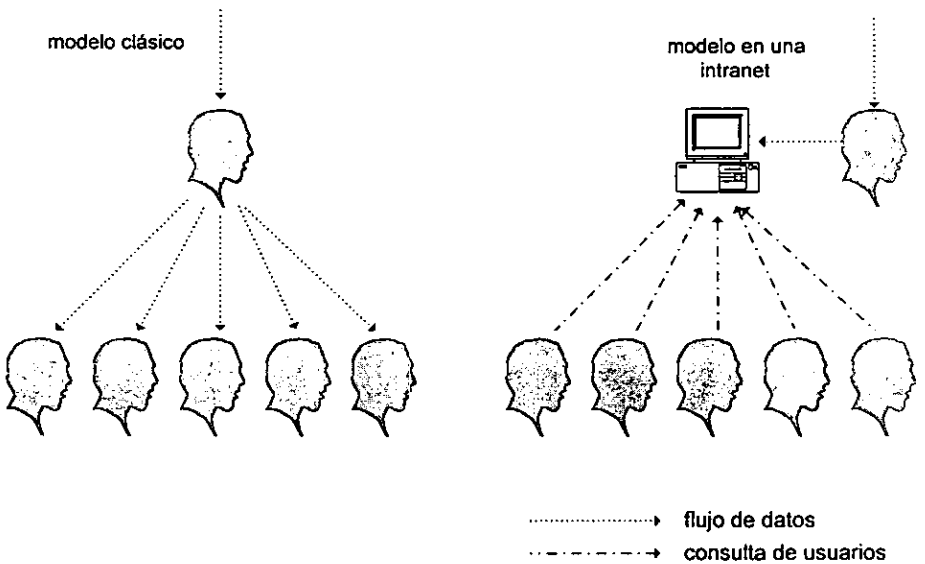
Servidor de Intranet, software para dicho servidor, protocolo TCP/IP, visualizadores (o browsers), firewall.

En cuanto a software se refiere, existen tres proveedores de herramientas para hacer intranets que son: Oracle, Microsoft y Lotus Notes, de los cuales se recomienda trabajar con Microsoft ya que el Windows 98 ya incluye el explorer 4.0 que se requiere para la elaboración de intranets, así como, el IIS (Internet Information Server) y Exchange Server (servidor de correo electrónico) SQL, ODBC, DSN y Páginas de servidor activas (active server pages), VBScript o Java.

La idea básica de Intranet tiene ciertamente vertientes peligrosas, ya que a priori no queda claro cómo proteger la privacidad de los usuarios de la misma, al tiempo que se les permite realizar transferencias con el exterior. Es por ello que el aspecto de la seguridad es vital en este tipo de instalaciones. Por ejemplo, cualquier conexión desde fuera de la Intranet hacia dentro que no tenga una autorización debe ser automáticamente bloqueada, para evitar que un intruso se cuele en nuestros archivos es por ello que se requiere de un firewall.

Mejorando el flujo de información

Los avisos, circulares, notas o informes... todo se puede enviar por correo, con un considerable ahorro en tiempo y dinero. Por otra parte, gracias a su velocidad todo el personal podrá mantenerse en contacto casi continuo, y así mejorar su rendimiento.
En segundo lugar hablábamos de estructurar la información.



En la Facultad existen jefes de división, o de departamento, que tienen personas a su cargo. Por dar una cifra razonable, imaginemos que cada jefe dispone de diez personas

trabajando con él. En nuestro caso, cada jefe ha de enviar la información en cuestión diez veces. La relación que se establece entre jefes y empleados está desequilibrada, ya que supone un cuello de botella para la transferencia de datos entre personas de la Facultad. Es decir si el tiempo que tarda un jefe en enviar la información a un empleado es X, habrá un empleado de los diez que recibirá su información al cabo de diez veces X tiempo, ya que el jefe va enviando los datos de uno en uno.

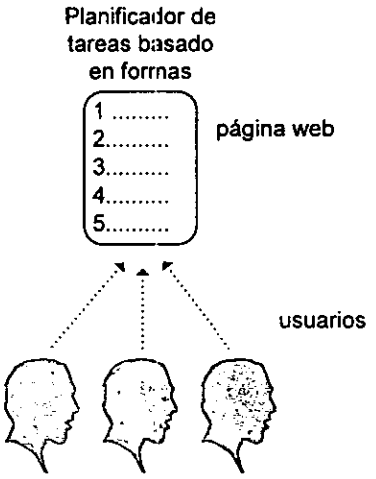
Aplicando el esquema clásico de circulación de datos en Intranets: el responsable de sección o departamento recibe la información que debe hacer llegar a sus empleados, pero no se la envía. En lugar de hacer esto, la sitúa en algún lugar accesible por todos los empleados a su cargo (habitualmente una home page de WWW). De esta manera, como cada empleado va a buscar la información, y nadie tiene que enviar los datos a todo el grupo de empleados, el flujo de datos es mucho más equilibrado. Lo que el empleado hace entonces es visitar la home page, y tomar la información que necesita.

Por ejemplo, se pueden poner todos los documentos que antes se enviaban a los empleados. Además de un considerable ahorro en papel (que puede ser más importante de lo que parece), esto supone mejorar la eficiencia. En la empresa tradicional, cuando un empleado pierde algún informe (cosa que sucede con relativa frecuencia), puede tardar varias horas o incluso días en tener uno nuevo disponible. Gracias a las Intranets se puede garantizar que lo tendrá en su pantalla en menos de cinco minutos.

Mejorando la coordinación interna

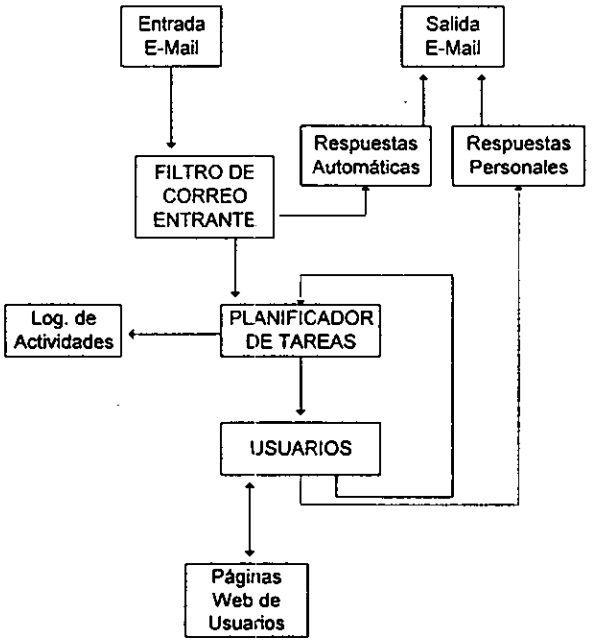
Eventualmente en la FI se problemas con los memorandums e información en general, ya que hay informes que se pierden, las tareas se repiten, etc. Por ello, no es extraño que a menudo existan situaciones sin sincronía. Por ejemplo, imaginemos la siguiente situación: se solicita que se haga un determinado trabajo, y por falta de coordinación, este trabajo es realizado por dos personas. Es evidente que aquí se ha desperdiciado potencial productivo, ya que una de las dos personas no debería haber hecho ese trabajo. Esta situación es relativamente frecuente, y no es más que falta de coordinación e intradepartamental que con las intranets se resolverá de manera considerable.

La solución que se adoptará es similar a la de invertir el flujo de datos, de manera que todo fluya de manera más natural y equilibrada. Se puede observar en la siguiente figura:



Además para solicitudes externas lo podemos manejar con correo electrónico y de la misma forma responder a la petición

De esta manera la FI en un futuro puede tener una estructura interna como la que se muestra a continuación:



El único punto de entrada que nos interesa es el de correo electrónico, ya que es el único que da acceso directo al interior de la Intranet.

Esta propuesta es con la finalidad de minimizar el tiempo de respuesta, y de mantener un mejor nivel de coordinación y sincronización interna. Además, las Intranets son probablemente una de las mayores contribuciones de Internet al mundo de la empresa, y no sólo a nivel tecnológico: su influencia va a ser tan grande, que probablemente se hable de un antes y un después de la revolución de las Intranets, del mismo modo que se habla del antes y el después de la aparición de las cadenas de montaje y de la producción en serie.

4.6 Administración física

Para finalizar, los puntos antes mencionados son de suma importancia para una mejor administración en la red. Pero no olvidemos que este mantenimiento no es sólo en hardware o software, también interviene el que comprende al área física de la red.

Existen diversas salas o laboratorios de cómputo, los cuales no siempre se encuentran en las mejores condiciones físicas. Consideramos que se debe incrementar el interés para dar un mayor confort a dichos centros, es decir, es recomendable que en las áreas donde operan más de 10 equipos de cómputo se instale un sistema de aire acondicionado que evite la concentración del calor emitido por los equipos que ahí se encuentren; lo que provoca desperfectos en su operación, teniendo como consecuencia un periodo de vida útil menor al estipulado por el fabricante en condiciones normales.

Así también es importante considerar que deben adquirirse equipos reguladores ininterrumpidos de energía que prevengan la interrupción del servicio, lo que provoca que se corra el riesgo de perder algún servidor, concentrador o simplemente la información que se procesa en el momento.

Conclusiones

La red de la Facultad de Ingeniería se ha visto consolidada, en cuanto a conexión se refiere desde 1996, dividiéndose en cinco zonas, cuatro de ellas ubicadas en Ciudad Universitaria y una más en el Centro de la Ciudad. Comunicándose así a todas las divisiones o secretarías que conforman la Facultad.

Los puntos de enlace con Red unam han sido en la zona A con la sala de UNICA, en la zona B con la División de Estudios de Posgrado y con la División de Ingeniería Mecánica e Industrial teniendo como punto intermedio al IIMAS. El otro punto de unión ha sido la DGSCA que envía la señal a la Zona C en la Sala Fundación UNAM, y a la Zona D en el Palacio de Minería.

La red de la Facultad cuenta con una tecnología ethernet; cableado estructurado categoría 5; sistemas operativos diversos como unix, windows nt; equipos diversos como concentradores utp, de fibra óptica o de cable coaxial; conmutador (switch); estaciones de trabajo, servidores de red, computadoras personales; software de comunicación como correo electrónico (telnet, ftp, etc.), software de edición gráfica (gimp); navegadores de internet (netscape); etc., y ante la problemática de dirigir, coordinar y vigilar el crecimiento de la red, se creó un comité de cómputo el cual, analizando las condiciones y situaciones de la red, estableció los reglamentos para uso de las salas de cómputo y para el uso del web.

Las direcciones IP fueron asignadas por la DGSCA para los cinco dominios; y fueron para la zona A la dirección 132.248.54.XX (fi-a.unam.mx), zona B 132.248.59.XX (fi-b.unam.mx), zona P 132.248.52.XX (fi-p.unam.mx), zona C 132.248.139.XX (fi-c.unam.mx) y para la zona D 132.248.138.XX (mineria.unam.mx). Para la administración de la red se cuenta con cinco administradores, uno por cada zona, la cual se realiza en diversas plataformas para su seguridad y administración y la política de red es aplicable por cada uno de ellos.

La red de la Facultad cuenta con una página web, que es la encargada de publicar información sobre sus actividades académicas y culturales. Toda creación de una página es regida por la "Normatividad y Lineamientos Generales para uso de Páginas Web en la Facultad de Ingeniería" a través del comité de administradores del web.

Como se puede notar en la breve descripción realizada, una administración en forma no se llevaba a cabo; por ello, el trabajo presentado tiene la finalidad de proponer opciones para su mejor operación.

Las propuestas que se presentan, en su mayoría están sustentadas en las pruebas realizadas en la Sala de Fundación UNAM y en la sala de cómputo de UNICA, por el permiso concedido de la Jefa de la Unidad de Cómputo de la Facultad, Ing. Elsa Barón Mayo.

Al inicio del análisis de la red, el monitoreo lo realizaba la DGSCA, por lo cual los resultados tardaban en llegar al administrador, y este último a su vez no podía tener un control constante del uso y fallas presentadas en cada una de las zonas de la red de la facultad. Ante esta problemática, y con las facilidades concedidas, se instaló un sistema de monitoreo con software de 3Com, el cual ayudó a tener una noción más clara del uso de la red pero debido a la versión que se instaló no era posible detectar con facilidad las máquinas que tenían problemas o que estuvieran ocasionando tráfico en la red, así como prevenir alguna falla en la misma, que es la principal finalidad al llevar a cabo un monitoreo.Y por esta razón, además de la instalación de dicho software fue necesario establecer un sistema de monitoreo local con otro software llamado LANalyzer, con el que se completaba la detección de máquinas, así como la cantidad de entrada y salida de paquetes, el porcentaje de utilización de la red, algunas direcciones IP con sus respectivas direcciones MAC y gráficas pero solo de manera local, es decir, observar el aprovechamiento de la red en una zona.

Este monitoreo fue un primer paso para conocer la situación de la red. Y con el apoyo de las tablas de análisis puede obtenerse una visón más amplia de dicha situación.

Esta implementación no fue suficiente, ya que no se había establecido una política de red que se diera a conocer a los usuarios y se les presentaran los recursos que se tienen de la red, ubicación de edificios (croquis o planos) de cada zona y documentación en general de la estructura de la red (conceptos de red) entre otros.

Con base en la situación de la red, se propusieron algunos mecanismos para mejorarla en todo.

Inicialmente se propone una política de seguridad, en la cual se establecen los lineamientos a seguir, basándose en un análisis matemático de la red (llamada hoja de trabajo para el análisis de riesgo de seguridad). El primer punto es determinar quien está autorizado para usar los recursos, para conceder acceso y aprobar su uso, como segundo paso se procede a delimitar las responsabilidades de los usuarios y del administrador; aquí se dan recomendaciones para la información delicada (o confidencial), como la encriptación de datos (acompañados de una compactación), o encriptación de contraseñas para evitar que en tráfico de la red puedan ser leídas y como consecuencia violadas. También se propone un plan de acción cuando se viole la política.

Por otra parte, se recomienda que dicha política sea publicada e interpretada para evitar confusiones y sobre todo que sea del conocimiento de todos los usuarios, no se descartan las normatividades en operación, sino por el contrario se mantienen y se refuerzan con lo propuesto, tratando siempre de salvaguardar la seguridad en la red. Este documento es muy importante ya que es la base para cualquier aclaración o modificación a dicho reglamento.

Esta política como parte de la administración, establece una inspección del uso del sistema; que de alguna forma ya se ha implementado con la configuración de dispositivos para monitoreo y la instalación del software para dicho fin; pero debido a la versión con la que se cuenta actualmente, en todo el análisis que se realizó, se detectó que existen

algunos inconvenientes para llevar a cabo de una manera eficiente y óptima el monitoreo de la red.

Al detectar dichas deficiencias se propone actualizar el software de 3COM con una versión reciente, lo cual permitirá detectar cualquier falla en la red, de una manera más fácil y sencilla, ya que cuenta con mas gráficos que permiten analizar a detalle la utilización de la red, detectar direcciones IP y MAC con rapidez así como prevenir la caída de algún nodo, servidor o incluso, dependiendo del problema, desactivar automáticamente el puerto de algún concentrador si la máquina a la que está conectado pudiera estar ocasionando conflictos en la red, además si se realiza algún cambio de equipo en un futuro próximo, el mismo software detecta los últimos dispositivos que hay en el mercado a la fecha. Incluso ya no sería necesario tener dos sistemas de monitoreo.

Este monitoreo es una opción de dos, ya que también puede realizarse con el sistema operativo unix, el cual, por lo ya estudiado no hace un análisis tan completo como los sistemas instalados para tal fin.

La administración no termina en un monitoreo de la red, porque: ¿qué se puede hacer si no se tiene una actualización?.. también se propone que se dedique un poco de tiempo para mantenerse al día con la información de las listas de correo y grupos de noticias, ya que se adquieren tips sobre los temas que pudieran ser de suma importancia, como son la actualización de antivirus, software de comunicación en la red, equipos para actualizar y explotar de la mejor forma el uso de la red, etc. Además también se deben considerar las licencias para el uso de software de vital importancia como los antivirus y softwares de trabajo más utilizados por el personal de la Facultad.

También en cuanto a seguridad se plantea que se cuente con un método de recuperación y respaldos, ya que es muy importante en momentos de contingencia, y con ello se evita la pérdida de datos en la red.

Para mantener la seguridad no basta con establecer una política de red, sino también es conveniente que se establezcan todos los elementos necesarios para llegar a tal fin, como son desde una actualización de tecnología hasta actualización en procesos. Es decir, la Facultad siempre se ha distinguido por ser una de las escuelas que se ha ido manteniendo a la vanguardia del desarrollo tecnológico, en nuestro caso necesitaríamos actualizarnos en nuestra tecnología de comunicación, es decir, la facultad cuenta con la tecnología ethernet y puede emigrar muy fácilmente a gigabith ethernet como lo son en conexiones de servidores a switch, conexión switch a switch y sobre todo mejorar el backbone.

Por otra parte, considerando el continuo crecimiento de usuarios y enlaces en la red, pudimos percatarnos de que llegará el momento en que no podamos contar con más direcciones IP de las asignadas inicialmente, para solucionar este problema se sugiere instalar un servidor proxy en las áreas que se requiera, como son departamentos, secretarías o salas de cómputo. Para que con una sola dirección IP tengan acceso un grupo de máquinas (pc's) a los recursos de internet o correo electrónico, sin tener que contar con una dirección única para poder tener comunicación al exterior, y así optimizar al máximo las direcciones IP.

También es necesario tener equipos de apoyo en casos de falta de suministro de energía eléctrica, que llegan a ocasionar daños de importante relevancia a los equipos, así como considerar la posibilidad de adquirir switches para que el o los concentradores dedicados por zonas no sean los únicos responsables de enviar señal, ya que como pudimos observar en nuestra hoja de análisis la red, es muy vulnerable cuando falta alguno de los concentradores, con esto y atendiendo la política de red se puede disminuir el índice de riesgo de nuestra red, el cual de acuerdo al análisis elaborado es muy alto.

Un punto que consideramos de sumo interés, y para el cual no se pudo realizar alguna prueba, fue la instalación de una intranet; que nos ayudaría a que se tuviera mayor comunicación entre las autoridades, y por qué no, entre el mayor número de miembros de la Facultad, es decir, por el tipo de actividad que se desarrolla en la Facultad en muchas ocasiones las tareas que se llevan a cabo administrativamente se realizan con mucha demora, y esto se debe a que no existe una buena comunicación (intercambio de datos por medio de las computadoras, aprovechando la instalación de la red). Una intranet ayudaría a evitar retraso en la información ya que una orden o requerimiento de una secretaría, departamento o dirección estaría presente casi en el momento. Desde luego que esto se va a poder llevar a cabo de una manera mas eficiente haciendo hincapié y concientizando a todo el personal (principalmente al que maneja mucho papeleo administrativo) del uso de la misma (intranet), para evitar demoras y gasto de papel, así como de los mas importante tiempo.

Es importante considerar dentro de esta administración la remodelación o mejoración de las condiciones de las salas o laboratorios de cómputo de la Facultad, para que los equipos que operan en ellos tengan la vida útil que se espera.

Un último punto a considerar, por su grado de importancia, es el constante cambio que sufre la red de la Facultad, estos cambios se dan por las nuevas formas y tipos de redes que parecen día con día, además que la red con el paso del tiempo se vuelve insuficiente para las necesidades reales de la Facultad.

Por lo que se recomienda la creación de un software para controlar y administrar, los elementos que conforman la red (pc's, concentradores, servidores y estaciones de trabajo), este software se puede integrar dentro de la red, de esta manera los administradores puedan hacer actualizaciones, en el momento que se registre un cambio en los dispositivos de la red.

Apéndice A

Cableado estructurado

Es necesario dejar claro que el cableado estructurado es un punto muy importante en el diseño de una red. Por ello, a continuación se presentan aspectos interesantes relacionados con el tema:

La norma EIA/TIA-568 es la norma de cableado estructurado para edificios y que está internacionalmente aceptada, además está en revisión y evolución continua, abarcando la topología física, tipos de cables, longitud de los cables, conectores y la "conectorización (conexión).

Por lo que se refiere a la topología física permitida en el cableado estructurado, es la de estrella. Y la estructura del cableado (ver Figura 1) lo conforman:

- Area de trabajo
- Cableado horizontal
- Cableado de administración (clóset de cableado)
- Cableado vertical (cableado central)
- Cableado de equipamiento (clóset de edificio) y
- Cableado del campus (entrada al edificio)

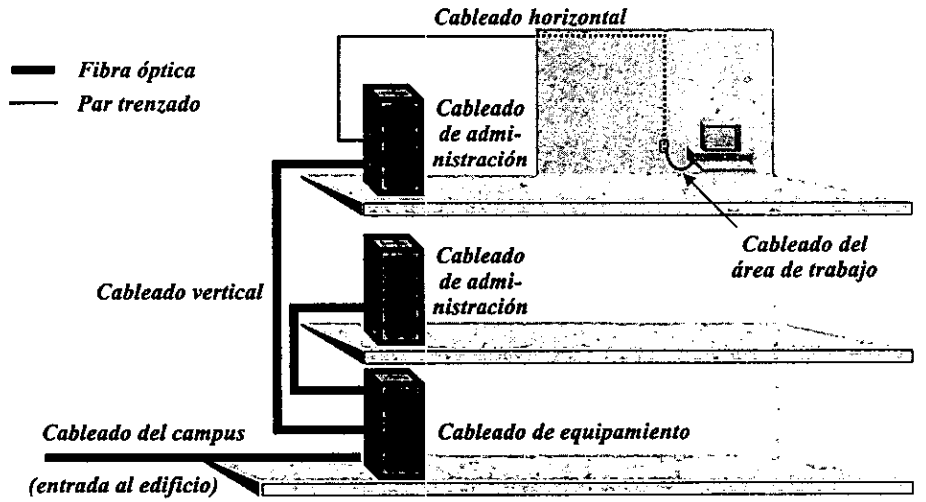


Figura 1. Estructura del cableado

Área de trabajo:

- *Par trenzado (igual que el horizontal)*
- *De la salida al equipo*
  - *Computadora (RJ-45)*
  - *Teléfono (RIJ-11 o RJ-45)*

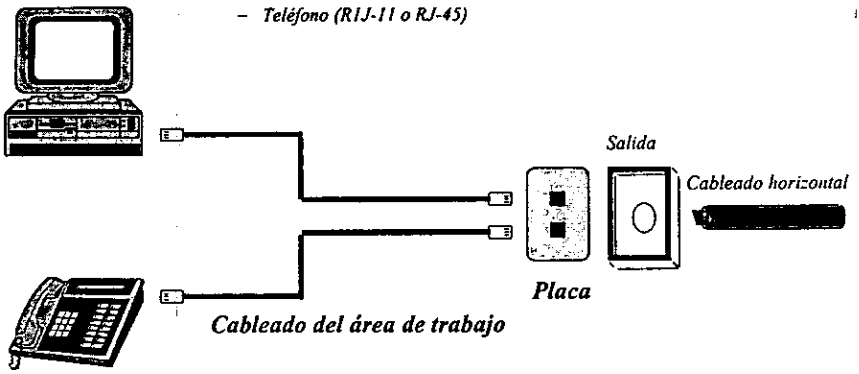
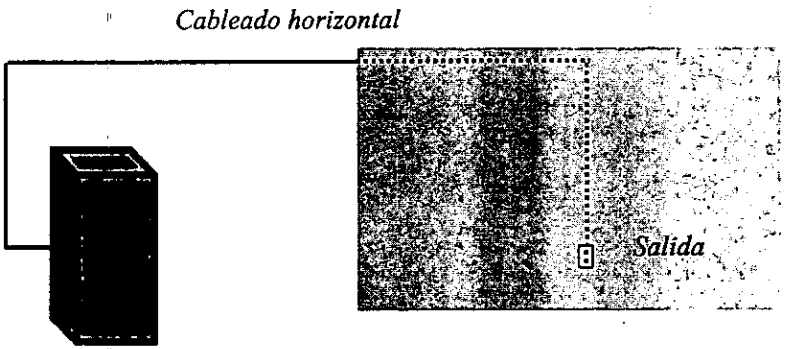


Figura 2. Cableado del área de trabajo

Cableado horizontal:

- *Par trenzado (igual que el del área de trabajo)*
- *Del clóset de cableado a la salida*
- *Opcionalmente puede pasar por un centro de distribución*



Clóset de cableado

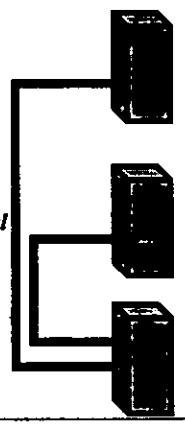
Características del cableado de administración (Patch panel)

- Par trenzado o fibra óptica
- Entre el cableado horizontal y el vertical, entre el vertical y el del equipamiento, o entre el del equipamiento y el del campus
- Flexibilidad para cambios y arreglos

Existen hubs que pueden realizar esta función por software ("port switching")

Cableado vertical (central o "riser")

- *Fibra óptica*
- *Del closet de cableado del edificio al closet de cableado de cada piso*
- *Enlaza todos los cableados del edificio a un centro único*



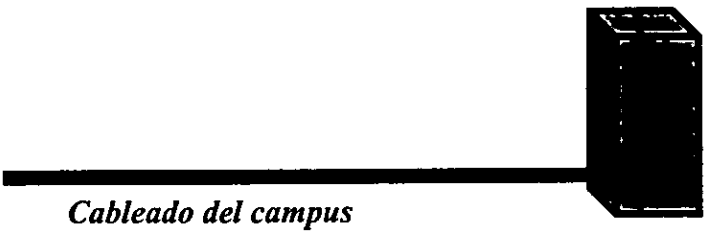
Cableado de equipamiento

El cableado del equipamiento está conformado por:

- Par trenzado o fibra óptica
- Entre el cableado de administración y los racks de los equipos de comunicaciones

Cableado del campus (entrada al edificio)

- *Fibra óptica*
- *Entre el closet de cableado del edificio y los closets de cableado de otros edificios*



Cableado del campus

Es necesario tener presente que para los closets de cableado, hay al menos un closet de cableado por cada piso, y por lo menos un closet de cableado general o principal por cada edificio.

Por lo que se refiere a los tipos de cables, los utilizados son:

- Par trenzado (UTP categoría 3, 4 y 5; y STP)
- Fibra óptica (62.5/125 μ)
- El cable coaxial sólo se puede utilizar en conexiones punto a punto dentro de los racks.

Y para tener una idea de las longitudes máximas permitidas de los cables, tenemos la siguiente tabla:

	Cableado Vertical	Cableado de administración	Cableado horizontal
Fibra óptica (62.5/125μ)	≤ 1,500 mts. ≤ 2,000 mts.	≤10 mts	≤490 mts
UTP (100 o)	≤ 800 mts. (voz) ≤ 100 mts. (datos)	≤10 mts	≤90 mts
STP (150 o)	≤ 100 mts.	≤10 mts	≤90 mts

Finalmente, por lo que respecta a la conectorización, es fundamental seguir los estándares. Porque aún utilizando cables y conectores de alguna categoría, la instalación puede quedar fuera del estándar si la conectorización no se realiza de acuerdo a dicho estándar, o por utilizar herramientas inadecuadas. También es importante que en todo caso se deba preservar el trenzado de los pares.

La conectorización es un aspecto en donde incide el mayor número de falla iniciales y de mantenimiento, pero en el cual se pueden utilizar módulos de inserción.

Apéndice B

Configuración de Dispositivos para Monitoreo

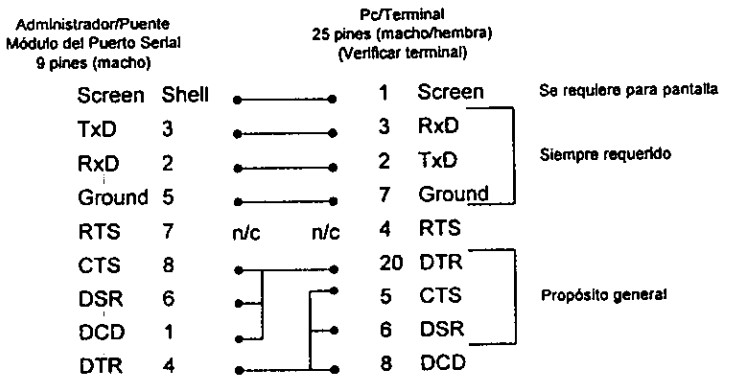
Configuración del módulo de administración del Concentrador

Como se mencionó en el capítulo dos, los puentes son dispositivos de interconexión de redes locales para distintos protocolos y arquitecturas, para ello debe existir una configuración que permita la comunicación entre dos o más redes (locales o remotas). Es decir, se deben establecer los parámetros con los cuales el puente se encontrará en condiciones para su operación.

A continuación se da un ejemplo de cómo se configuró el puente del concentrador (FMSII), que se encuentra ubicado en los laboratorios de UNICA en la División de Ciencias Básicas, (Sala de Fundación UNAM).

Se tiene un puente de administración que forma parte de un concentrador (FMS II), para poder accesarlo se requiere: una terminal o emulador VT100, un conector DB9 a DB25 y una dirección IP.

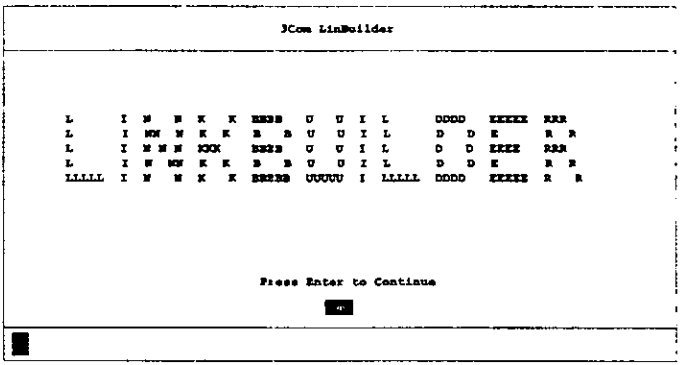
Las características del conector de DB9 a RS-232, según su conexión son las siguientes:



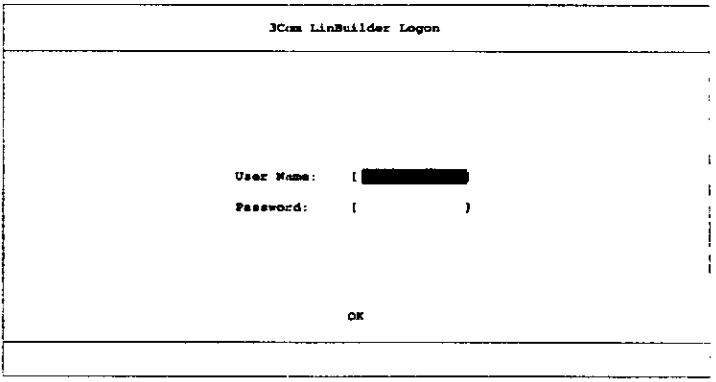
Contando con la interfaz de comunicación se procede a configurar la terminal con las siguientes características: Emular la terminal, para nuestro caso fue VT500, como una VT100, a 9600 baudios, control de flujo bidireccional, control DCD deshabilitado, tamaño de caracter 8, paridad ninguna, y bit de paro 1.

Contando con la interfaz y terminal, se procede a realizar la conexión directa, y en la pantalla de la terminal, pulsar **[Return] [Return] go**

Cuando se haya establecido comunicación entre la terminal y el puente se mostrará la siguiente pantalla:



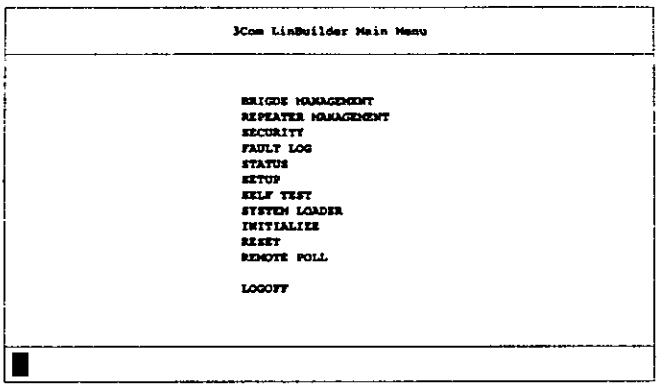
y para iniciar propiamente la configuración del dispositivo presionar [enter], después del cual, aparece nuevamente la pantalla que a continuación se presenta:



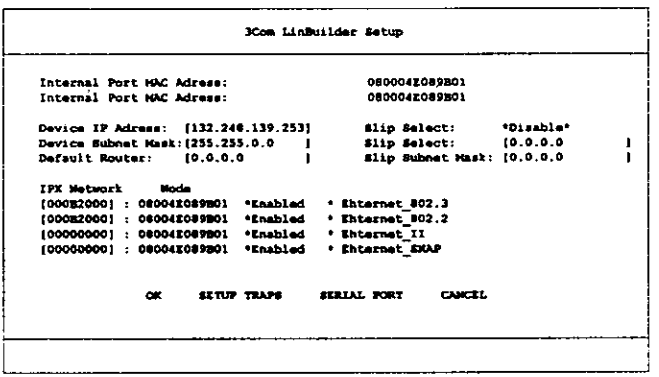
Para accesar a este módulo de administración se tienen tres niveles (referente al tipo de información a la que se tiene permitido). El primero es **monitor,** en el cual se accesa, pero no se pueden cambiar los parámetros de configuración una vez establecidos, el segundo es **manager,** en el cual se pueden cambiar parámetros de operación, pero no se puede: adicionar o eliminar usuarios, eliminar software, crear o cambiar enlaces o inicializar el equipo. Y el tercero es **security,** que permite el acceso a cualquier pantalla o información del equipo, y como consecuencia, realizar cualquier cambio, que en los

niveles anteriores no lo permitan. El password es el mismo nombre que el User name (o nivel).

Para nuestro caso, el nivel de interés es **security**, el cual contiene las siguientes opciones:



Es obvio que nuestro interés, para este punto, es la opción SETUP, en cuya pantalla se asignan los parámetros necesarios para el buen funcionamiento del dispositivo.



La dirección IP asignada fue: 132.248.139.253 y la máscara de subred 255.255.255.0, es importante mencionar que ningún otro parámetro predeterminado, para nuestro caso, se modificó.

Se sugiere que si es la primera vez que se configura un dispositivo como el presentado, es necesario reinicializarlo, y para ello no debe estar en uso la red, ya que se podrían perder algunos datos de los que en ese momento estuvieran trabajando.

Apéndice C

Opciones de segmentación de tráfico

Se tienen dos opciones de segmentación de tráfico, el primer se denomina Micro-segmentación con workgroup switches (switches departamentales) y la segunda, Macrosegmentación con backbone switches (swiches troncales):

Para el primer caso (Figura 3), los switches departamentales segmentan el tráfico entre diferentes grupos de trabajo, y permiten la conexión de una estación por puerto (un solo nodo conectado a un puerto del switch). Además permiten la conexión de servidores locales a alta velocidad.

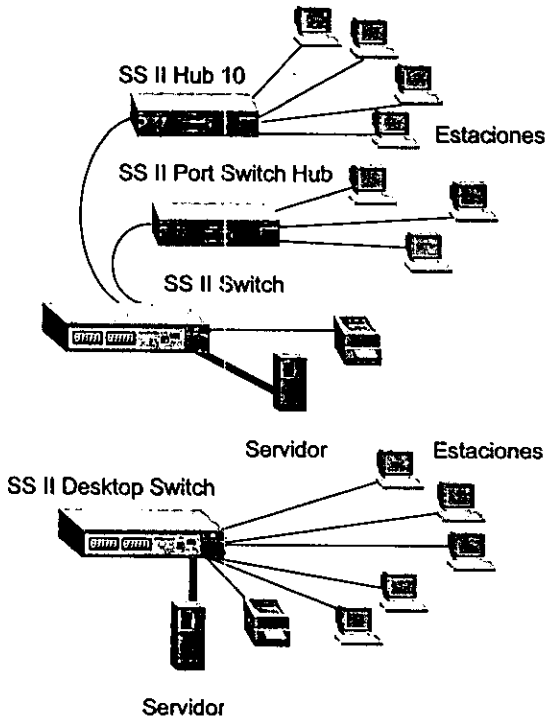


Figura 3. Switches departamentales

Para el segundo caso (Figura 4), los switches troncales segmentan el tráfico entre diferentes switches departamentales conectados a puertos de alta velocidad, además permiten la conexión de un concentrador por puerto (una sola red conectada a un puerto

de baja velocidad del switch). Así también permiten la conexión de servidores centrales a alta velocidad.

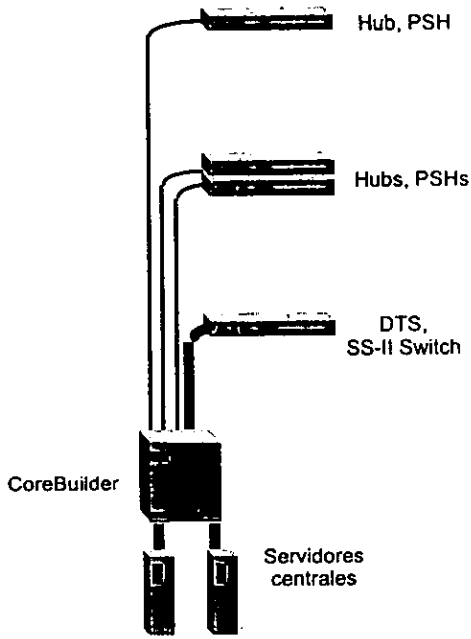


Figura 4. Switches troncales

Comparación entre ambos tipos de switch

1er. Caso:

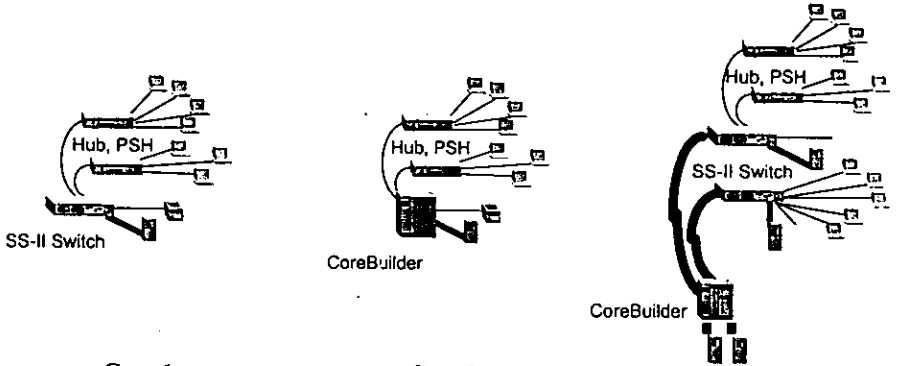
- Con muy pocas redes conviene utilizar un switch departamental

2°. Caso:

- Con un número medio de redes conviene utilizar un switch troncal

3er. Caso:

- Con muchas redes conviene utilizar switches departamentales en cada piso y un switch troncal para enlazarlos

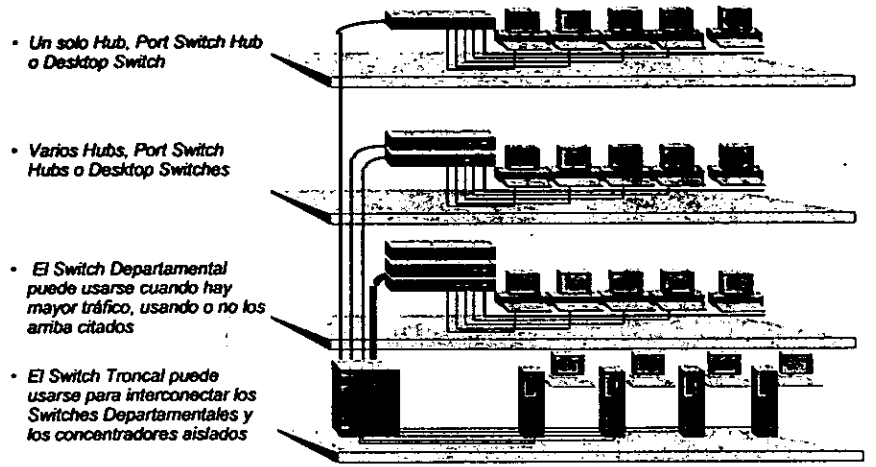


Caso 1 **Caso 2** **Caso 3**

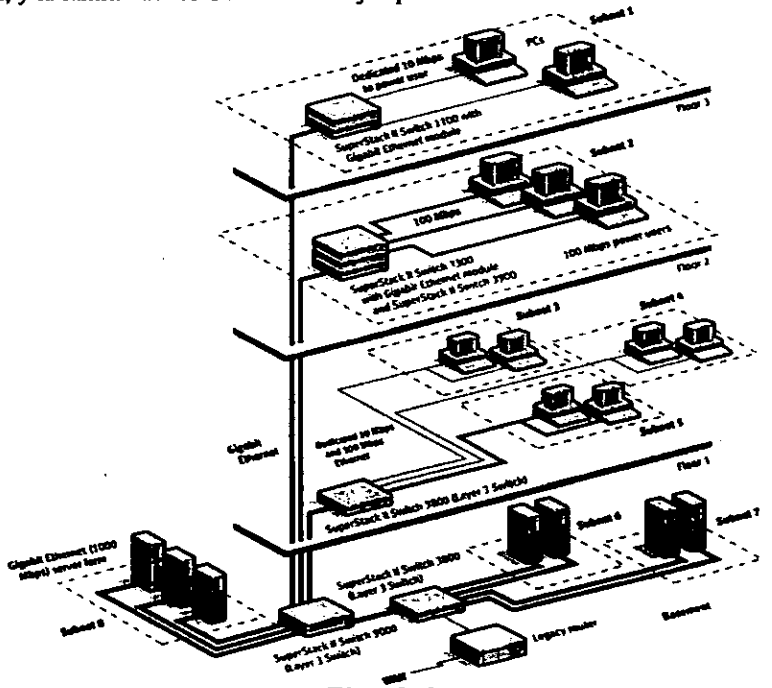
Guías generales en ambiente de oficina

• *Hasta 24 nodos:*	*Hub, Port Switch Hub, Dual Speed Hub o Desktop Switch*
• *Hasta 48 nodos:*	*Port Switch Hub, Dual Speed Hub o Desktop Switch*
• *Hasta 500 nodos en menos de 5 pisos:*	*Workgroup Switch con Hubs, Port Switch Hubs o Desktop Switches*
• *Hasta 8,000 nodos en 5 a 10 pisos:*	*Backbone Switch con Hubs, Port Switch Hubs y/o Desktop Switches*
• *Hasta 90,000 nodos o más de 10 pisos:*	*Backbone Switch con Workgroup Switches y Hubs, Port Switch Hubs o Desktop Switches*

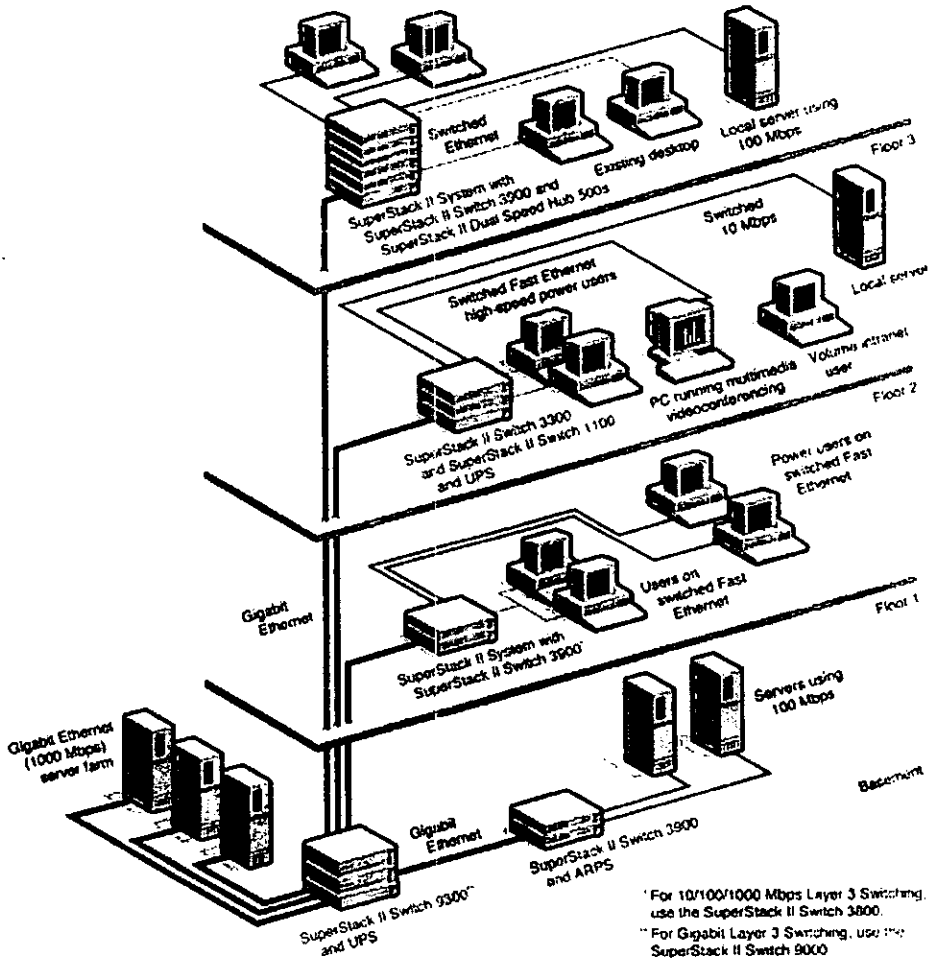
Combinación de swicthes troncales y departamentales



En la actualidad podemos disponer de switches con la tecnología gigabit ethernet, ya sea como departamentales o como troncales; entre ellos se encuentran la familia de los Super Stack II, y la familia de los CoreBuilder. Ejemplos:



Ejemplo 1


Switched Ethernet
Existing desktop
Local server using 100 Mbps
Floor 3
SuperStack II System with SuperStack II Switch 3900 and SuperStack II Dual Speed Hub 500s
Switched 10 Mbps
Local server
Switched Fast Ethernet high-speed power users
Volume ethernet user
PC running multimedia videoconferencing
SuperStack II Switch 3300 and SuperStack II Switch 1100 and UPS
Floor 2
Power users on switched Fast Ethernet
Gigabit Ethernet
Users on switched Fast Ethernet
SuperStack II System with SuperStack II Switch 3900*
Floor 1
Servers using 100 Mbps
Gigabit Ethernet (1000 Mbps) server farm
Basement
Gigabit Ethernet
SuperStack II Switch 3900 and ARPS
SuperStack II Switch 9300** and UPS
* For 10/100/1000 Mbps Layer 3 Switching, use the SuperStack II Switch 3800.
** For Gigabit Layer 3 Switching, use the SuperStack II Switch 9000

Ejemplo 2

GLOSARIO DE TÉRMINOS DE RED

10 BASE 2 Implementación de Ethernet de 10 Mbps en cable coaxial delgado. Su máximo segmento es de 200 metros.

10 BASE 5 Implementación de Ethernet de 10 Mbps en cable coaxial grueso. Su máximo segmento es de 500 metros.

10 BASE F Especificación para red Ethernet de 10 Mbps en fibra óptica.

10 BASE T Estándar de transmisión de Ethernet sobre MIT a 10 Mbps.

100 BASE FX Especificación para correr Ethernet 100 Mbps sobre fibra óptica.

100 BASE T Estándar de transmisión sobre MIT de velocidad 100 Mbps.

100 BASE T4 Especificación para correr Ethernet 100 Mbps sobre cable 3,4 y 5 MIT de 4 pares.

100 BASE TX Esquema que ofrece 100 Mbps sobre cable categoría 5 MIT. Address. En redes, la palabra dirección se refiere a un distintivo único para cada nodo de la red.

Administrador Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman superusuario.

Ancho de banda Relación de velocidad para la transmisión de datos medidos en Kbps (kilo baudios por segundo) y que representa la capacidad del canal de comunicación para transportar datos.

ANSI Organización encargada de la documentación de los estándares en Estados Unidos.

API Pequeños programas desarrollados para apoyar la interacción del sistema principal con las aplicaciones específicas.

Application Server Computadora destinada a brindar los servicios de una aplicación específica a los usuarios de una red.

ARCNet Red de computadoras y recursos compartidos creado por Datapoint muy popular en los años setenta, cuyas

	características eran: bajo costo, cableado en estrella y velocidad hasta 2.5 Mbps.
ARP	Proceso en donde se asigna al número de la tarjeta una dirección formato TCP/IP.
ARPA	Agencia militar de Estados Unidos encargada de proyectos tecnológicos como las redes computacionales militares.
ARPANET	Proyecto del Departamento de Defensa de los Estados Unidos que utiliza protocolos tipo X.25 donde la cantidad de información (paquetes) no es fija. La dividieron en dos: Milnet para uso militar e Internet para uso público.
ASCII	Código utilizado para representar los caracteres de escritura en formato binario (7 bits para 128 caracteres o el modo extendido de 8 bits para 256 caracteres).
Asíncrona	Forma de transmisión de datos donde no se necesita señal adicional de reloj. La señal contiene la información de cuándo cambia cada dato.
AT	Tecnología de 16 bits, utilizada en la tercera generación de computadoras personales 286.
ATM	Tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad, con tecnología de paquetes retrasados. Se considera la arquitectura del futuro en comunicaciones digitales.
AUI	Conexión utilizada para poder cambiar de tipo de cables en topologías Ethernet.
Average seek/access time	Intervalo promedio de tiempo desde que el sistema solicita datos hasta que dispositivo los tiene disponibles.
Backbone network	Red de Infraestructura. Red que actúa como conductor primario del tráfico de datos de la red. Comúnmente recibe y manda información a otras redes.
Backup incremental	Una copia de seguridad en donde se incluyen únicamente los archivos que se han modificado y etiquetado como modificados.
Backup completo	Respaldo o copia de seguridad con toda la información contenida en el servidor del sistema.

Backup diferencial Copia de seguridad o respaldo que se realiza copiando sólo las diferencias entre la copia anterior y el contenido actual del servidor.

Backup server Servidor dedicado a realizar las copias de seguridad y restaurar los datos borrados por error de toda la información de la red.

Baud rate Unidad de velocidad igual a un bit por segundo.

BIOS Porción de firmware de una computadora que maneja el flujo de señales entre el sistema principal y los dispositivos periféricos. Controla puertos, memoria, teclado y dispositivos primarios.

BPS Bits por segundo. Velocidad de transmisión serial.

Bridge Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.

Broadcast Transmisión abierta. Mensajes que se mandan sin destino específico.

CABLE NIVEL 3 Cable tipo MIT 2 pares que soporta 10 MHZ.

CABLE NIVEL 4 Cable tipo MIT que soporta 20 MHZ.

CABLE NIVEL 5 Cable tipo MIT 4 pares que soporta 100 MHZ.

Carrier o portadora Señal eléctrica que permite la modulación de otra señal que contiene la información. Se utiliza para la transmisión remota vía la infraestructura de comunicaciones.

CCITT Comité Consultivo Internacional de Telegrafía y Telefonía. Encargado de los estándares internacionales de comunicación.

Cliente Producto o presentación de front end (directamente con el usuario) que interactúa con otros servidores o productos de back end (sin presentación directa con el usuario). El cliente realiza solicitudes y presenta los resultados. No realiza los procesos ni los cálculos, eso se los deja a los programas de back end que son más poderosos pero no tienen la capacidad de comunicarse directamente con el usuario.

CoDec Codificador/decodificador. Dispositivo que convierte dos señales en ambas direcciones. De tipo A hacia B y de tipo B hacia A.

Colisión Definido como un exceso en portadora eléctrica. Sucede en Ethernet cuando dos o más estaciones hablan al mismo tiempo y las señales de datos se pierden.

Communication Server Computadora destinada a dar los servicios de comunicaciones de la red.

Concentrador Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.

Conectividad Estado que permite la transferencia de datos entre dos computadoras.

CSMA/CD Censor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.

Data Address Localización física dentro del dispositivo de almacenamiento.

Data Base Server Servidor que contiene las bases de datos y los programas que saben la forma de mover dicha base de datos.

DB25 Conector de 25 contactos comúnmente, dispositivo entre un equipo terminal (DTE) y la red.

Dial Up Circuito de comunicación que se establece vía telefónica.

Dirección Destino En el lenguaje de redes es la computadora que envía los datos de una transmisión.

Dirección Fuente En el lenguaje de redes es la computadora que recibirá los datos en una transmisión.

DLC Protocolo para el manejo de datos a través de líneas de comunicación.

Dominio Grupo de computadoras de la red que está administrada y

controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.

E0 Término utilizado para referirse a los canales de ISDN de 64 Kpbs en estándar americano.

E-mail Correo que se establece vía electrónica mediante Internet. Cada persona tiene una dirección asignada en su computadora de tal manera que puede enviar y recibir mensajes.

Emulación Imitación de la forma de comportarse de un equipo (en la emulación de terminal, la computadora imita el comportamiento de una terminal de red).

Encriptamiento Proceso basado en operaciones lógicas binarias para disfrazar un dato y evitar que sea leído por otra fuente distinta al destino.

Estación Computadora que puede realizar procesos.

Ethernet Estándar de red más popular e implementado. Utiliza CSMA/CD con una velocidad de 10 Mbps.

Fast Ethernet Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.

FAT Archivo que utiliza DOS para saber la ubicación física de los archivos en un medio de almacenamiento.

FDDI Estándar de transmisión de datos vía fibra óptica hasta de 100 Mbps con topología parecida a Token Ring/Token Passing.

Firewall Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.

FRAME Cuadro. Forma en que se organiza la información. Normalmente cuenta con tres partes: encabezado (control, fuente y destino), campo (datos a enviar), y CRC de verificación (bits para corregir errores).

Frame Relay Paquetes retrasados. Protocolo de comunicación asíncrono

	con dispositivo especial que atrasa el envío de grupos de información para mandarlos en paquetes de tamaño fijo.
FTP	Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.
Full Duplex	Característica de un canal de comunicación en el que dos terminales pueden mandar y recibir información simultáneamente.
Gateway	Dispositivo que permite conectar dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.
GIF	Formato de intercambio gráfico. Muy usado en Internet.
Half duplex	Característica de un canal de comunicación en el que dos terminales mandan y reciben información turnándose, una a la vez.
Hipertexto	También llamado Texto Virtual. Se refiere a la capacidad de recibir información en múltiples dimensiones. Una línea de texto puede llevar a otro texto, una imagen o una melodía.
Host	Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.
ICMP	Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.
IEEE	Agrupación de ingenieros que, entre otras funciones, documenta todos los desarrollos tecnológicos.
IEEE-802.1	Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
IEEE-802.2	Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI) llamado LLC.
IEEE-802.3	Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).

IEEE-802.4	Define cuadros Token Bus tipo ARCNET.
IEEE-802.5	Define hardware para Token Ring.
IEEE-802.6	Especificación para redes tipo MAN (de área metropolitana).
IEEE-802.7	Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.
IEEE-802.8	Especificación para redes de fibra óptica tipo Token Passing/FDDI.
IEEE-802.9	Especificaciones de redes digitales que incluyen video.
IEEE-802.11	Estándar para redes inalámbricas con línea de vista.
IEEE-802.12	Comité para formar el estándar de 100 base VG que sustituye CSMA/CD por asignación de prioridades.
IEEE-802.14	Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.
Interfaces	Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.
Internet	Red de redes con base en TCP/IP y acceso público mundial.
Internetworking	Término usado para referirse a la interacción entre varias redes.
Interoperabilidad	Término referente a la capacidad de diferentes redes para comunicarse entre sí.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.
IPX	Protocolo definido para redes Netware que tienen direcciones en tres campos (nodo, red y socket), lo cual le permite mantener varios enlaces entre redes y procesos en varios servidores.

IRQ	Canal de interrupción. Línea directa entre el microprocesador y la tarjeta periférica para que ésta solicite atención del CPU.
ISA	Arquitectura de 16 bits para tarjetas y dispositivos. El más común en las computadoras personales.
ISDN	Red pública utilizada para trasmitir varios tipos de información, texto, imágenes, sonido, etcétera.
ISO	Organización que especifica estándares de calidad internacionales.
ISO 9001	Modelo de calidad para empresas de diseño, fabricación e instalación de equipo.
Kernel	Parte del sistema operativo que actúa directamente con el hardware al más bajo nivel.
Lan Manager	Sistema operativo de red creado por Microsoft.
Lan Server	Versión de Lan Manager para servidores con funciones avanzadas.
Layer	En el lenguaje de redes se refiere a cada uno de los subsistemas que interactúan en los procesos de la red.
Link	Término utilizado para referirse a los componentes lógicos y físicos que permiten la comunicación entre dos sistemas.
LLC	Controla las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI).
Login	Proceso de entrada a la red utilizado como término para indicar que la estación está dentro de la red.
Logon	Proceso de entrada a un host. Utilizado para indicar que en realidad el trabajo se desarrolla en el host.
MAC	Capa de control de acceso a medios. Capa del modelo de comunicación OSI, que es la encargada del control lógico del medio físico.
MAN	Red de Área Metropolitana.
MAU	Dispositivo utilizado en topologías de estrella física para generar un círculo lógico. Todos se conectan a él, y él

	asigna quién tiene el Token Passing o derecho de transacción.
MIME	Especificación para redes y transmisiones multipunto.
MIT	Cable de par trenzado sin blindaje.
Módem	Modulador-Demodulador. Dispositivo que convierte señales binarias a tonos transmisibles por vía telefónica.
Motherboard	Tarjeta principal que contiene los lugares donde se alojarán todos los dispositivos físicos de la computadora.
MOTIF	Interfaz gráfica para XWindows UNIX.
MPS	Multi Procesamiento Simétrico. Capacidad de algunos servidores para llevar procesos en varios microprocesadores y distribuir la carga de trabajo.
Multitasking	Capacidad de un equipo de llevar más de una tarea a la vez.
NetBios	Interfaz estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
Netware	Sistema operativo de red desarrollado y propiedad de Novell.
NFS	Sistema de archivos de red. Genéricamente es un sistema que permite el acceso a un servidor de archivos.
NLM	Grupo de programas que se pueden cargar directamente en el servidor de Netware y responde a los comandos de consola del servidor.
Nodo	Estación de trabajo con identificación propia que puede ser fuente y destino en la red.
NFSNET	Red que agrupa varias universidades y tiene una velocidad T1 1.544 Mbps.
OS/2	Sistema operativo de IBM diseñado para tener funciones de 16 bits (286).
OSI	Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.
Output	Salida de datos se llama a los procesos de una computadora

	que entregan datos a otro dispositivo o directamente al usuario.
Overhead	Tiempo de proceso necesario para que se ejecuten los comandos antes de que un dispositivo esté listo para dar acceso.
Packet	Unidad de información a transmitir. No contiene dirección ni destino, tan sólo ruta (el siguiente punto a llegar).
PCI	Estándar de bus para periféricos que típicamente utiliza DMS tipo F y Fast IO bidireccional. Desarrollado por Intel.
PCMCIA	Estándar de bus para tarjetas periféricas de computadoras portátiles.
PDN	Redes públicas de conmutación de paquetes.
Peer-to-peer	Igual a igual. Forma de comunicación de red donde cada uno tiene las mismas tareas en el proceso.
Pines	Contactos eléctricos. Pequeñas líneas salientes de metal que permiten el contacto físico entre diversos componentes de hardware.
Ping	Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.
Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.
RAS	Servicio de acceso remoto a la red.
RDI	Red digital de servicios integrados. Clase de servicios para transmitir varios tipos de información, texto, imágenes, sonido, etcétera, mediante la red pública.
Repetidor	Dispositivo que transmite y amplifica la señal de la red.
RG11	Cable coaxial grueso usado en Ethernet.
RG58	Cable coaxial delgado de 50 ohms usado en Ethernet.
RG62	Cable coaxial delgado de 62 ohms usado en ARCNet.
RJ11	Conector para MIT 2 pares.

RJ45	Conector para MIT 4 pares.
Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje.
RS232	Interfaz serial entre DTE y DCE.
SAC	Concentrador que en una red FDDI tiene conexión de círculo.
SCSI	Estándar desarrollado para conectar dispositivos periféricos y a microcomputadoras con una velocidad máxima de 5 Mbps. Utiliza cable de 50 hilos.
SCSI D	Conector diferencial de 50 contactos utilizado para conectar dispositivos de longitud hasta 25 metros.
SDLC	Estándar en las arquitecturas SNA para transmisiones punto a punto.
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
Sincronía	Forma de transmisión de datos donde se necesita señal adicional de reloj para que el transmisor y el receptor funcionen a la misma velocidad.
SLIP	Protocolo para TCP/IP vía serial.
SMS	Servicios en Netware para el manejo de almacenamiento de back ups y discos.
SNA	Arquitectura de protocolos para redes.
SNMP	Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.
SOLARIS	Sistema operativo UNIX desarrollado por SunSoft.
SPX	Trabaja en el cuarto nivel de OSI. Brinda apoyo a IPX garantizando la llegada y controlando las secuencias.
STP	Cable de par trenzado con blindaje o aislamiento magnético.

Supervisor Usuario de la red con autoridad para realizar las tareas de alto nivel de cliente-servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman administrador.

TCP/IP Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.

TELNET Utilería de TCP/IP que permite un logon remoto sobre un host.

Tiempo de acceso Intervalo entre el tiempo de una solicitud de datos por el sistema y el tiempo en que el dispositivo los tiene disponibles.

Tiempo Real Dominación de aquellos procesos que suceden simultáneamente o con una diferencia imperceptible de tiempo. Internet ofrece tiempo real dentro de muchos servicios donde a la ejecución de una acción existe una respuesta inmediata (llegada de correo electrónico).

Token Passing Estafeta. Método de comunicación en red en el que cada elemento debe recibir el permiso para hablar o la estafeta.

Token Ring Red local en la que el permiso para transmitir es secuencial o en anillo.

Topología Descripción de las conexiones físicas de la red, el cableado y la forma en que éste se interconecta.

TP Cable de pares trenzados.

Transciever Dispositivo de Ethernet que permite el cambio de medio físico a cable.

Transductor Dispositivo que convierte una energía a otro tipo. Un foco convierte energía eléctrica en luminosa y calórica.

UNIX Sistema operativo multiusuario desarrollado en los años setenta y que se caracteriza por ser portátil y versátil.

Upgrade Término utilizado en software referente al cambio de programas hacia los más recientes, nuevos y mejorados.

UPS Fuente de poder que se activa cuando la señal de corriente alterna se pierde para evitar que los servidores se apaguen

	de manera abrupta.
Usuario	Persona que trabaja con la estación de trabajo. El que realiza tareas de acceso a los recursos de la red pero no los modifica substancialmente. Tiene derechos de uso pero no de mantenimiento mayor.
UUCP	Protocolo que permite conectar dos sistemas UNIX.
VESA	Desarrollado por varios fabricantes de interfaces de video. No soporta DMA de alta velocidad y utiliza un bus típicamente de 24 bits, 16 ISA más 8 de comunicación directa y Fast PIO bidireccional.
WAN	Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.
WEB site de WWW	Servidores de Internet que contienen la información disponible para los usuarios de esa red.
Workstation	Computadora que puede realizar procesos robustos de front end. Permite sacar máximo provecho a sus recursos de red.
X.21	Protocolo usado en las redes telefónicas digitales para voz y datos en transmisión síncrona Full Duplex.
X.25	Protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.
X/WINDOWS	Protocolo cliente-servidor de ambiente gráfico para UNIX. Originalmente desarrollado en el proyecto Athena por el MIT.

BIBLIOGRAFÍA

CAPÍTULO I

Libros

TANENBAUM, Andrew S. Redes de ordenadores, 2a. ed. Pretice Hall, México 1991.

SATALLINGS Willian, ISSDN and Broadband ISDN, 2ª. ed. Mac Millan, New York 1989.

HOPPER. Temple and Williamsom, Diseño de redes locales, 1ra ed, Addison Wesley, México D.F.

HALSALL, Fred., Data Communication computer network and open systems, 3ra de, Addison Wesley, E.U.A. 1993.

BLACK Uyless, Computer Networks Protocols, Standars and interfaces, 1ra de., Pretice Hall,
E.U.A. 1987.

SALLINGS William, Local and Metropolitan area networks, 4ta de., MacMillan Publishing Company,
E.U.A 1983.

DEITEL Harvey M., Introducción a los sistemas operativos, 2da de, Addison Wesley, E:U.A. 1990.

Varios autores, DAY Michael, Larry Budnick, LAN Operating Systems, New Riders Publishing, 1993.

HALSALL Fred, Data Comunications Computer Networks and Open Systems, Addison-Wesley, 1993.

Revistas

ALDACO Yolanda, "Porque frame relay sobrevive a ATM", RED, Mayo 1997, 24-32

CAPÍTULO 2

Libros
KARANJIT Siyan y Chris Hare, Firewalls y la seguridad en internet, Segunda edición, Prentice Hall Hispanoamericana, S.A., México, 1997.

Revistas
GUTIÉRREZ Jesús, "Tecnología Gigabit Ethernet: Redes de alto rendimiento con mayor velocidad", RED. Año VII, No. 84, Septiembre 1997, 4-12.

Internet

What is a firewall?
http://nematic.ieo.nctu.edu.tw//handbook72.html
08/10/97

Firewall
http://www.ora.com/refrence/dictionary/terms/f/firewall.htm
08/10/97

La WWW, una telaraña que se teje a pena luz del día
http://www.re.com.mx./julio96/interjul96.html
08/09/97

Ascend secure acces firewall technology Overview
http://www.crchq.com/products/ascend/firewall.html
08/09/97

Chossing a firewall
http://www.zed.ca/firewall.html
1996

Firewall Definitions
http://www.cyberpass.net/~bhule/fwalldef.htm
08/09/1997

Guardian firewall- System Description:
http://www.anr.co.il/guardian/lanhi.htm
08/09/1997

10 razones por las que una aplicación gateway es el método cortafuego más seguro
http://www.esegi/pasarela.html
21/09/1997

Vg-AnyLan Consertium Membership Information:

htp://www.iol.unh.edu/co...anylan/vg_membership.html
1994

Interphase 100VG-Any LAN Product Family
htp://www.iphase.com/products/technology/100VG/
1995

Proxy Server
htp://www.microsoft.cpm.proxy/guide/whatsnew.asp
1998

Seguridad Informática
htp://www.cybercenter.cl/segurida.htm
08/09/1997

CAPÍTULO 4

Revistas

Gutiérrez, Jesús. Tecnología gigabit ethernet, redes de alto rendimiento con mayor velocidad, RED. Septiembre 1997, 4 12

Internet.

Proxy server
htp://www.microsoft.com/proxy/default.asp
1996

Intranet
http://www.coverlink.com/concepto.htm
1996 Coverlink.

GLOSARIO

MARTÍNEZ Victor René, "Glosario de términos", RED. AñoV, No. 61, Octubre 1995,20-22.