PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO

Unidad de Ingeniería de Sistemas

Disertación de Grado previa la obtención del título de Ingeniero en Sistemas

"Manual de Configuración e Instalación de Redes WAN y LAN dirigidas a INTERNET e INTRANET Aplicado a la Pontificia Universidad Católica del Ecuador – Sede Ambato"

Disertación de grado de:

Inés Lucía Moncayo Urbina
Xavier Eugenio Miño Rodríguez

Director de Disertación

Ing. David Guevara

Ambato, 1999

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO

Disertación de Grado previa la obtención del título de Ingeniero en Sistemas

"Manual de Configuración e Instalación de Redes WAN y LAN dirigidas a INTERNET e INTRANET Aplicado a la Pontificia Universidad Católica del Ecuador – Sede Ambato"

Director de Disertación: _____

Ing. David Guevara

Revisores de Disertación: _____

Ing. Patricio Chambers

_____

Ing. Wigberto Sánchez

Inés Lucía Moncayo Urbina
Xavier Eugenio Miño Rodríguez

Ambato, 1999

DEDICATORIA

A Dios, quien ha guiado mis pasos en todo momento.

A mis padres, quienes gracias a su esfuerzo me han ido forjando día a día con todo el cariño, amor y comprensión.

Lucía Moncayo

A Dios, a quien le debo todo lo que soy.

A mis padres, quienes con sus sabios consejos y múltiples sacrificios han logrado guiarme por muy buenos senderos.

Xavier Miño

AGRADECIMIENTO:

Al culminar con éxito el presente trabajo de investigación, queremos agradecer a Dios, por darnos la fuerza y fe necesaria para seguir por la vida.

A nuestros padres, quienes nos han ayudado a culminar con éxito nuestra carrera.

Un agradecimiento especial a nuestros profesores quienes han dedicado tiempo y esfuerzo permitiendo la correcta formación del presente trabajo.

Y a todos los que pusieron su granito de arena para ayudarnos a cristalizar nuestros objetivos.

Lucía Moncayo y Xavier Miño

Manual de Configuración e Instalación de Redes WAN y LAN dirigidas a INTERNET e INTRANET Aplicado a la Pontificia Universidad Católica del Ecuador – Sede Ambato

INDICE GENERAL

CAPITULO III: EVALUACION LOGICA DE LA RED

PARTE II: ADMINISTRACION DE REDES WAN Y LAN

CAPITULO IV: CREACION DE POLITICAS Y PROCEDIMIENTOS DE REDES WAN Y LAN

INDICE DE GRAFICOS

PREFACIO

El inicio de la informática y su evolución hasta nuestros días, creó la necesidad de conectar computadoras entre si y compartir información de manera rápida y eficiente, iniciándose el desarrollo de las Redes de Area Local (Local Area Network o LAN) que se encuentran confinadas a un único departamento, grupo de trabajo o edificio; así como las Redes de Area Extensa (Wide Area Network o WAN), de proporciones globales, permitiendo interconectar redes de área local que se encuentran en lugares distantes unas de otras.

La conexión entre redes LAN ha alcanzado niveles impresionantes, formando una gran red WAN, conocidas como INTERNET, integrando redes de distintas características que se encuentran ubicadas en escuelas, bibliotecas, oficinas, hospitales, agencias gubernamentales, institutos de investigación y otras entidades. Esto implica entre otras cosas que la seguridad llega a ser un problema, aumentando la necesidad de autentificar y autorizar el acceso de los usuarios que utilizan estos servicios.

Así como Internet integra redes a nivel mundial, existe redes de información de alcance limitado diseñadas con el fin de compartir datos entre computadoras a través de una redes LAN o WAN que se encuentre dentro del control de una sola entidad o institución, conocidas como INTRANETS.

La configuración de una red LAN, WAN, INTERNET e INTRANET incluye que todos los recursos de hardware y software estén configurados y distribuidos de tal manera que

se aproveche al máximo dichos recursos teniendo como beneficio un mejor rendimiento de los equipos.

En una institución como la Pontificia Universidad Católica del Ecuador Sede Ambato, el tipo de información que transita en la red requiere además que se cuente con reglas claras de administración y seguridad para evitar que dicha información pueda perderse o ser substraída por personas no autorizadas, provocando la mala utilización de los equipos y su información.

El propósito de esta investigación es conseguir que el lector comprenda lo que significa tener y/o construir una red, qué elementos la componen y cómo se integran. Los conceptos presentados en este trabajo son tomados de libros, revistas e INTERNET, debido a que se encuentran ya creados no es el objeto de esta investigación definirlos nuevamente, su contenido se estructuró de tal manera que el lector se introduzca paulatinamente en el tema y al avanzar en la lectura, llegue a comprender qué es y cómo funcionan las redes y cada uno de los elementos que la componen, tomando como ejemplo la red construida en la PUCESA.

Al iniciar el presente estudio en el capítulo I se desarrollan algunos conceptos básicos que nos permitirá conocer y comprender algunos términos que son indispensables para introducirse en los conocimientos sobre redes. En el capítulo II se ofrece una guía de funcionamiento de instalación física de una red: sus componentes y aplicaciones; la que nos ayudará a poseer un criterio formado de cómo armar dicha red. En el capítulo III continuando con ésta guía describimos las aplicaciones o programas necesarios para la

configuración lógica de una red y correcta integración de sus componentes, así como sus características y servicios ofrecidas por las mismas.

Como conclusión o resumen del trabajo realizado en los capítulos anteriormente descritos incluimos en el capítulo IV la organización , administración , creación y redacción de políticas y reglamentos que pueden ser manejados por la red de la PUCESA, los cuales nos hemos basado en los reglamentos actuales del laboratorio de informática de la universidad.

Se incluye en cada capítulo una sección la cual se ha denominado "¿COMO SE APLICA EN LA RED DE LA PUCESA?" en donde se describe la forma de cómo la teoría se aplica a la práctica, en este caso la red de la PUCESA.

El análisis de la red instalada en la actualidad en la PUCESA, y todos los puntos que implican el mantenimiento, administración y configuración de equipos, su funcionamiento, aplicación, el software necesario para la correcta integración de los servicios; son un ejemplo de lo que representa construir una red, la misma que tomaremos como modelo para nuestra investigación.

La preparación de políticas, procesos y un sistema de información estructurado en páginas WEB conteniendo todo el material recolectado será un complemento que constituirá una herramienta de consulta rápida del trabajo realizado.

El sitio WEB producto de este trabajo se estructurará basándonos en el contenido de todo el texto y será construida utilizando Front Page, el mismo que es una aplicación de

edición de código HTML utilizada en Internet. En este estudio no se incluye el funcionamiento, formato, creación y estructuración de lo que representa construir un sitio web de este tipo, ya que estos temas se incluyen en el trabajo de disertación de grado "Guia de Administración Implantación y desarrollo de sitios y servidores Web aplicadas a la Internet de la escuela de sistemas de la Pontificia universidad Católica del Ecuador sede Ambato", desarrollado a la par con este estudio.

En la página Web, en la sección de anexos se incluye una "Guía de instalación y administración de Internet Information Server" que será una herramienta importante para la configuración lógica de una red. Así también, se presenta algunos videos que muestran los componentes de una red de fibra óptica que servirá para futuras reestructuración de dicha red.

El presente trabajo está dirigido a personas que posean un conocimiento básico sobre lo que es una red de computadoras y su funcionamiento, permitiendo determinar las razones por las cuales se puede armar una red ; comprender todos y cada uno de los componentes que la forman, llegando a una conexión a Internet o a una Intranet.

I. DIAGNOSTICO Y SITUACION ACTUAL DE LA RED DE LA PUCESA

La Pontificia Universidad Católica del Ecuador – Sede Ambato, en la actualidad es una de las Instituciones educativas de renombre en la localidad, la misma que posee un Laboratorio de Informática que sirve como herramientas didácticas proveyendo servicio de Internet y es base para que los estudiantes de la escuela de Ingeniería en Sistemas usen para su aprendizaje y otras actividades relacionadas.

El Laboratorio en la actualidad está dividido en tres secciones: *COMPAQ, IBM, Novell.*

Los dos primeros están gobernados por un Servidor Clon con un procesador Pentium y 64 MB en memoria RAM, Windows NT como Sistema Operativo y Windows 95 en las estaciones de trabajo, las dos secciones obtienen el servicio de INTERNET a través de un servidor COMPAQ Prosignia 500 con LINUX en sistema Operativo.

La sección de Novell está gobernada por un Servidor Clon con Novell de Sistema Operativo. Las tres secciones tienen una topología en estrella para lo cual utilizan tres HUBS, dos de 16 puertos y uno de 12 puertos los mismos que se encuentran conectados en forma de cascada. Para la conexión a INTERNET se utiliza un Modem y un Router que se encuentran conectados al servidor LINUX; todo el conjunto se comunica a través del protocolo TCP/IP, el más usado para el tipo de topología que emplean e Internet, como se muestra en la figura 1.

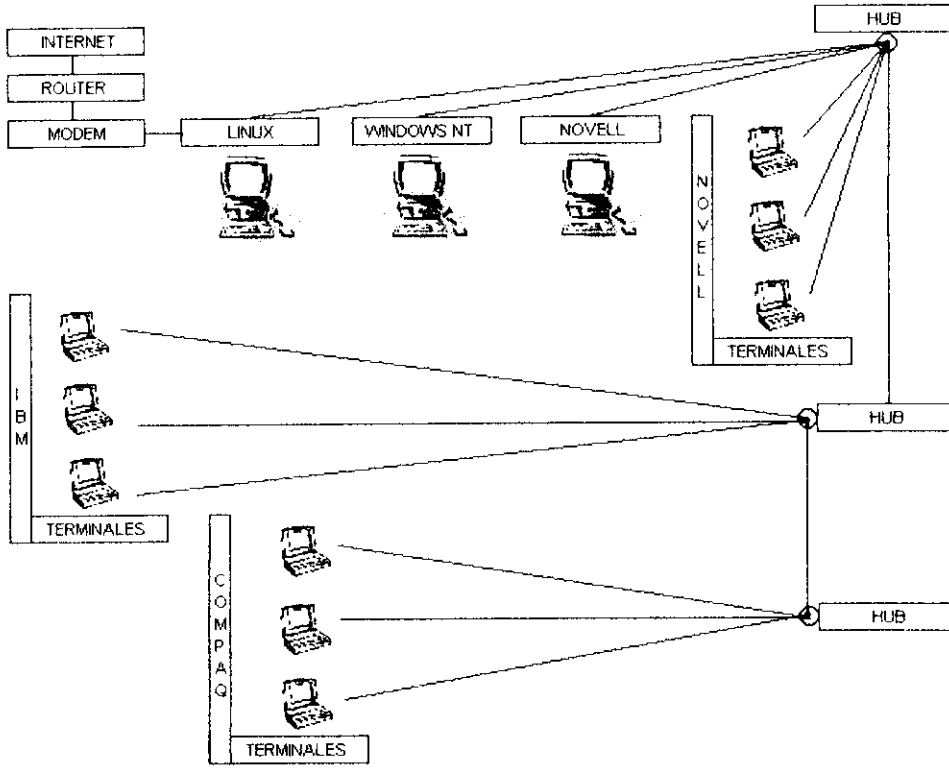


Figura 1. Distribución Red de la Pontificia Universidad Católica del Ecuador Sede Ambato

A lo largo de este estudio, se empleará esta información como ejemplo de la teoría que presentaremos sobre cómo se estructura una red dirigida a Internet e Intranet. La lista de equipos que posee la PUCESA se encuentra detallado en el ANEXO I.

PARTE I

INSTALACION Y CONFIGURACION DE REDES WAN Y LAN, DIRIGIDAS A INTERNET E INTRANET

INTRODUCCION

Con el creciente desarrollo tecnológico, se ha creado la necesidad de compartir información más eficientemente, permitiendo que las computadoras se puedan conectar entre sí, formando en un principio lo que se denomina hasta hoy como Redes de Area Local o LAN, las mismas que son en concepto un conjunto de computadoras conectadas entre si para compartir información, utilizando protocolos o medios de comunicación ubicadas en una misma área física, empleando para este propósito medios físicos directos como cables de comunicación: coaxial o par trenzado, que por lo general no pueden extenderse muchos metros.

Con el tiempo dichas necesidades fueron aumentando en cuanto a comunicación y se llegó al punto que las redes LAN de computadoras que se encontraban separadas por muchos kilómetros de distancia requería que compartan información más fácilmente, por lo cual aprovechando la tecnología existente en aquella época - el teléfono - se encontró la forma de comunicar estas redes de computadoras a un nivel mundial.

En ese momento se inició lo que hoy llamamos Internet, que es una red mundial de computadoras que se comunican usando un lenguaje común el cual se denomina TCP/IP (Transfer Control Protocol/Internet Protocol), Protocolo de Transferencia de Control / Protocolo Internet. Es similar al sistema telefónico internacional: nadie posee ni controla todo el sistema, pero está conectado de tal manera que funciona como una red muy grande.

Para ofrecer una interfaz gráfica y sencilla al recorrer y consultar los documentos de Internet contamos con la World Wide Web (WWW o simplemente Web). Dichos documentos así como los vínculos entre ellos, componen una red o "web" de información. Los archivos o páginas Web están interconectados a otras páginas que pueden utilizar textos o gráficos especiales que se denominan hipervínculos. Las páginas pueden estar compuestas por imágenes, texto, o elementos multimedia como sonidos y videos. Estas páginas se pueden encontrar en equipos situados en cualquier parte de la red por consiguiente del mundo. Cuando se conecta con Web, se dispone del mismo acceso a la información en todo el mundo.

De la misma forma trabaja lo que se denomina Intranet que hace referencia a cualquier red TCP/IP que no esté conectada a Internet pero que utilice estándares y herramientas de comunicación de Internet para suministrar información a los usuarios de la red privada. Por ejemplo, una organización puede instalar servidores Web a los que los empleados sólo pueda tener acceso para publicar boletines informativos de la organización, cifras de ventas y otros documentos de la organización. Los empleados pueden acceder a la información mediante exploradores Web. Los servidores Web pueden configurarse para suministrar una Intranet con las mismas características y servicios que se encuentran en Internet.

Por todo lo anotado es necesario tener una guía que permita comprender cómo funcionan tanto el software como el hardware de una red y tener acceso a los servicios de la misma forma como se posee en Internet para el mundo o dentro de una sola organización (Intranet), como es el caso de la Pontificia Universidad Católica del

Ecuador – Sede Ambato la misma que posee una red que puede ser adaptada para ambas funciones.

El presente estudio ofrece una guía que permita comprender cómo se configura, instala y evalúa una red sea esta WAN o LAN para que los servicios indispensables para Intranet e Internet estén listos al ser aplicados. Al globalizarse el concepto de Internet es indispensable que nosotros tengamos el conocimiento de cómo funcionan todos los elementos y componentes que forman una red para tener acceso a Internet o al potencial de una Intranet.

CAPITULO I

CONCEPTOS GENERALES

1.1 COMUNICACION ENTRE COMPUTADORAS

Las computadoras comparten información utilizando medios de comunicación de datos, entre los que se incluyen los cables de cobre, fibra óptica y ondas de radio, para el intercambio de datos y dispositivos de control remoto. Aquí se enumeran algunas de las aplicaciones que se pueden realizar en la comunicación de datos:

a) Intercambio de archivos.
b) Intercambio de correo electrónico.
c) Transacciones remotas de negocios, como la actualización de un inventario desde un terminal punto de venta.
d) Actividades bancarias, como cuando los usuarios acceden a su cuenta personal del banco desde un cajero automático.
e) Gestión y supervisión, en las cuales se controlan los dispositivos remotos como los censores, y se recogen los datos de lectura.

Hay dos formas de desplazar información de un sitio a otro. Las técnicas de comunicación *paralelas* que usan múltiples caminos o cables entre dos puntos, como una autopista de varios carriles y los métodos de comunicaciones *serie* que utilizan un simple cable, como la vía de un puente. Un canal paralelo podría constar de 8, 16, 32 o incluso 64 cables uno al lado del otro para la transmisión de información. Por ejemplo, un procesador de 32 bits posee un bus de datos interno (camino de transmisión) que puede enviar simultáneamente 32 bits de un lugar a otro. Si se considera que un código de 8 bits representa un carácter alfabético, es posible enviar 4 caracteres a la vez. A diferencia de una línea serie, que sólo posee

un cable para la transmisión, de manera que los bits deben alinearse en un único archivo y transfiere como un flujo sobre el cable, después se montan de nuevo en bloques apreciables de bits al final de la recepción. Por consiguiente, las transmisiones de datos sobre cables telefónicos son considerablemente más lentas que las que se producen en el interior de un microprocesador o sobre el cable paralelo que conecta una impresora a una computadora. Las configuraciones típicas para la transmisión de datos se muestran en la figura 2.

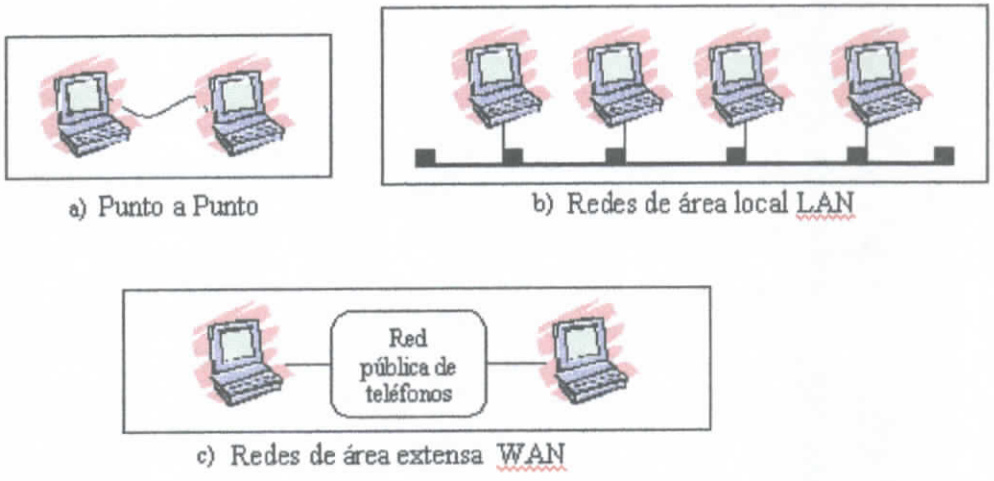


Figura 2. Transmisiones de comunicaciones de datos.

Las características de estas configuraciones son las siguientes:

a) **Punto a punto.-** Es una conexión existente entre dos sistemas de computadoras, o una computadora y un periférico, como una impresora o un modem.

b) **Red de Area Local (LAN, Local Area Network).-** Es un servicio de comunicación de datos compartido. Varias computadoras pueden unirse a la

red, pero, en la mayoría de los casos, solo pueden transmitir una en un momento dado. Los datos se empaquetan y transmiten en flujos serie.

c) **Red de Area Extensa (WAN, Wide Area Network).-** Normalmente envuelve a la red telefónica de una compañía nacional o internacional de telecomunicaciones. Los datos se transmiten por la línea en flujos serie.

Se realiza una conexión punto a punto con un cable paralelo o serie. Un cable paralelo incluye múltiples cables que transmiten bits de datos en paralelo, pero está limitada por distancias debido a que los bits tienden a desincronizarse con la distancia. Una conexión paralelo está limitada a unos 10 pies o 3 metros.

En todos los casos aquí tratados, la interfaz entre los sistemas debe ser la misma o tener la traducción apropiada si se necesita conversión de códigos, formatos, tramas y protocolos entre sistemas. Incluso si dos computadoras intercambian archivos con éxito, las aplicaciones en el sistema de recepción pueden no ser capaces de abrir un fichero o de utilizar sus datos. No obstante, esto se relaciona más con el sistema operativo y la interoperatividad de la aplicación, que con la comunicación de datos.

Se define a la *interoperatividad* como la capacidad de que diferentes sistemas de computadoras, redes, sistemas operativos y aplicaciones trabajen juntos y compartan información.

Para referirse a los caminos de comunicación de los datos a menudo se utiliza los *canales o circuitos* que es el enlace entre dos dispositivos a través de los cuales

fluyen los datos. Los dos términos son similares, pero su origen es diferente. Un canal, como un canal de TV o de radio, implica que existan canales paralelos y que cada canal forme un flujo separado de datos. Tiempo o frecuencia separan los canales. Se entiende mejor un circuito (en términos que aquí se trata) como el cable que conecta un teléfono al sistema de conmutación de la compañía telefónica, donde se conecta con otros cables de teléfonos. Un circuito forma un camino especializado a través del sistema de conmutación mientras dura la llamada. En un sistema de *banda base* (aplica los pulsos de tensión directamente al cable y usa todo el espectro de señal de ese cable), transmite un canal sobre un cable, mientras que un sistema de *banda ancha* (las señales de radio de múltiples canales se modulan con distintas frecuencias "portadoras" separadas y donde se subdivide el ancho de banda en diversos canales de comunicación que ocupan un rango de frecuencias específico), puede transmitir múltiples canales sobre un cable con el uso de técnicas de multiplexación; para presentar una perspectiva de la multiplexación, considere una autopista llena de automóviles que deben cruzar un puente. El puente posee un único carril, con lo que los automóviles solo pueden cruzarlo en una sola fila. Un director de tráfico indica al automóvil del primer carril que cruce el puente, luego se lo indica al del segundo carril, al del tercer y así sucesivamente. El proceso comienza de nuevo después del último carril. De esta manera, se permite que los automóviles de cada carril accedan al puente de la misma forma. La *multiplexación* usa una técnica similar para permitir a múltiples usuarios compartir una única línea de comunicación hacia una facilidad remota. La línea consiste en una línea dedicada entre dos puntos y los paquetes de datos de cada usuario equivalen a los automóviles que cruzan el puente.

El sistema receptor de una transmisión pone los datos en un búfer o área de almacenamiento, luego transfiere los datos al procesador o los envía al disco para almacenarlos. Si el búfer se llena con los datos que llegan, el sistema receptor debe indicarle al emisor que pare temporalmente la transmisión para evitar la sobrecarga. A este proceso se denomina *control de flujo*.

Para transmitir texto, se debe delimitar el flujo de datos para diferenciar la estructura orientada a byte (caracteres) original. Por ejemplo en las comunicaciones *asíncronas*, cada carácter se codifica como una cadena de bits separados por un bit de comienzo de carácter y otro de parada. Algunas veces se utiliza un bit de paridad para detección y corrección de errores. Por el contrario, en las comunicaciones *síncrona* es más eficiente, ya que no se necesitan bits de comienzo y parada.

Los datos transmitidos están sujetos a la corrupción producida por interferencias externas, atenuaciones y otros problemas asociados con los servicios de transmisión. Las técnicas de detección y corrección de errores pueden detectar los datos falseados y solicitar una retransmisión. El hardware de comunicación subyacente de área extensa aprovechan el hecho de que los servicios de transmisión están en gran parte libres de errores y no realizan la verificación de los mismos. Esto mejora las prestaciones. Es entonces el sistema receptor quien determina si el dato ha desaparecido o se ha corrompido, y solicita una retransmisión si ha sido así. El receptor o los nodos a lo largo del camino de comunicación no necesitan verificación de errores ni reconocimiento de datos constantemente.

Un sistema de comunicaciones está constituido por un ancho de banda, que mide el rendimiento de los datos. La medida se da normalmente en bits por segundo (bps, Bits per Second). Los circuitos de teléfono analógico transmiten en el rango de los kilobits por segundo (miles de bits), mientras que las LANs transmiten en el rango de megabits por segundo (millones de bits). Los nuevos sistemas de fibra óptica en redes públicas telefónicas transmiten en el rango de gigabits por segundo (miles de millones de bits). Los datos transmitidos a través del sistema telefónico están limitados a 64 Kbits/seg., sin embargo, las líneas digitales están disponibles para transmitir a velocidades mucho mayores.

La mayoría de las LANs y WANs transmiten información en *paquetes o datagramas*, como se denominan a menudo. Un paquete es una agrupación de datos con información de encabezamiento que contiene las direcciones fuente y destino, información de la corrección de errores, números de secuencias y otra información. Los paquetes tienen un tamaño limitado, así para transmisiones extensas de datos, como puede ser la transferencia de un archivo grande, los datos se reparten y se colocan en dos o más paquetes. Empaquetar datos de esta forma ofrece diversas ventajas:

a) Las interferencias en la red pueden afectar sólo a un paquete específico, no a toda la transmisión. Sólo se resiente el paquete afectado.
b) Los paquetes son entidades independientes que transportan datos, los que se pueden transmitir por múltiples caminos a través de una red de tipo malla. Esto permite que se encaminen por el mejor camino y se evite la congestión.

c) En redes compartidas, no se puede permitir que una estación envíe transmisiones largas congestionando la red. Los paquetes pequeños ofrecen la posibilidad de que muchas estaciones transmitan conjuntamente sus paquetes por la red.

1.2 ¿QUE ES UNA RED?

Una Red de computadoras es un sistema de comunicaciones de datos que enlaza dos o más computadoras y dispositivos periféricos. Como se muestra en la figura 3 la red consta de un cable que une las Tarjetas de la Interfaz de Red o NICs (Network Interface Cards) a cada uno de los dispositivos.

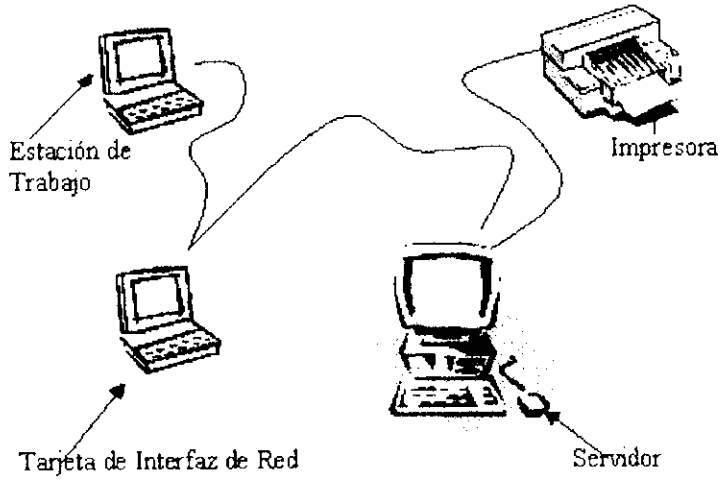


Figura 3. Componentes de una Red.

Un componente de una red son las *Tarjetas de Interfaz de Red o NIC's* que es un adaptador instalado en una computadora ofreciendo un punto de conexión a la red. Cada NIC se diseña para un tipo de red específica.

Como se muestra en la figura 4, presentamos la configuración lógica de un sistema de comunicaciones de red. En esta configuración, las aplicaciones utilizan el software subyacente de comunicación de redes para que intercambien información con otros servidores o aplicaciones.

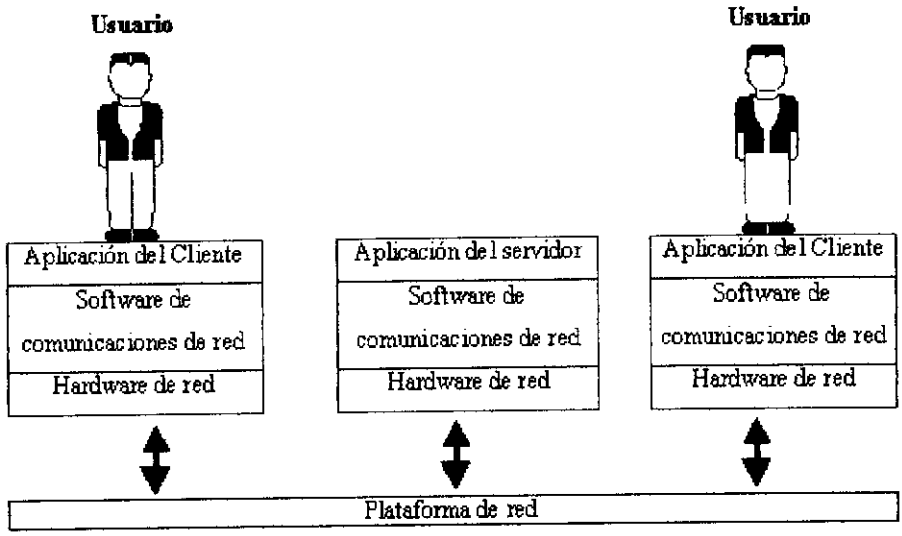


Figura 4. Modelo de comunicación de Red.

Como se muestra en la figura 5, en la parte izquierda se representa la configuración básica de una red de área local o LAN departamental. En la parte derecha, se han conectado distintas LANs departamentales para formar una inter-red, que permite a más usuarios comunicarse y compartir recursos unos con otros.

Una WAN es una inter-red que puede utilizar la Red Pública Telefónica Conmutada (PSTN, Public Switched Telephone Network) o algún otro servicio público para enlazar redes sobre límites metropolitanos, estatales o nacionales.

Para proporcionar conexiones para las computadoras se utilizan los *modems* (moduladores/demoduladores) que son dispositivos de equipos de comunicación de datos utilizadas sobre la Red Telefónica Pública Conmutada PSTN. Los modems convierten (modulan) las señales digitales de computadoras en señales analógicas que se pueden transmitir a lo largo de las líneas telefónicas. Un modem en el otro extremo del enlace demodula la señal convirtiéndola de nuevo a bits digitales. Se convierte el pulso eléctrico digital, que representa aun 0 o un 1, a una forma de onda analógica en un extremo de la transición y otro modem se vuelve a convertir a digital en el extremo receptor. El modem se controla con ordenes enviadas desde un paquete de comunicación de datos y éste maneja el marcado y la respuesta del teléfono. También controla la velocidad de transmisión, que va de 300 bits/seg. a 9600 bits/seg. Si se utiliza compresión, son posibles velocidades de hasta 28000 bits/seg. con las últimas normas, aunque se desarrollan velocidades más altas.

Los modems para computadoras están disponibles en modelos internos y externos. Un modems interno es una placa de circuito o adaptador que se ajusta a una ranura (slot) de una computadora. Un modem externo es una pequeña caja que permanece exterior a la computadora y se conecta a su puerto de comunicación serie.

Cuando un modem llama a otro, el modem destino contesta y se produce un intercambio de señal, que establece los parámetros para una sesión de

comunicación. El proceso de negociación determina la velocidad de señalización máxima disponible entre los dos modems así como el uso de compresión. La utilización de líneas telefónicas impone algunas restricciones en la velocidad de transferencia de datos.

1.3 ¿POR QUE ESTABLECER UNA RED DE COMPUTADORAS?

Las razones para establecer una red de computadoras se perfilan en los siguientes puntos, en las cuales se aclara qué es una red y qué puede hacer en una organización:

a) **Compartición de archivos y programas.-** Las versiones de red de muchos paquetes populares de software están disponibles, con un ahorro considerable de costos cuando se compara con la compra de copias de licencias individuales. Los archivos de programas y datos se almacenan en un servidor de archivos y acceden a ellos muchos usuarios de la red.

b) **Compartición de recursos de red.-** Los recursos de red incluyen impresoras, trazadores gráficos y dispositivos de almacenamiento. La red ofrece un enlace de comunicación que permite a los usuarios compartir estos dispositivos.

c) **Compartición de base de datos.-** Un sistema gestor de bases de datos es una aplicación ideal para una red. Una característica de red llamada Bloqueo de Registro permite que múltiples usuarios accedan simultáneamente a un

archivo sin corromper datos. El Bloqueo de Registro asegura que dos usuarios no editen el mismo registro a la vez.

d) **Expansión económica de la base del PC.-** Las redes proporcionan una forma económica de aumentar el número de computadoras en una organización. Se pueden enlazar económicas estaciones de trabajo sin disco a una red que utilice la unidad de disco duro del servidor para el arranque y almacenamiento.

e) **Grupos de trabajo.-** Una red ofrece un medio de crear grupos de usuarios que no se localicen necesariamente en el mismo departamento. Los grupos de trabajo facilitan nuevas estructuras colectivas planas, donde las personas de diversos y remotos departamentos pertenecen a proyectos de grupos especiales.

f) **Correo electrónico.-** El correo electrónico permite que los usuarios se comuniquen fácilmente entre ellos. Los mensajes a los buzones se pasan para que el receptor los lea en el momento oportuno.

g) **Software de grupos y de flujo de trabajo.-** Se diseñó específicamente el software de grupos y el software de flujo de trabajo para las redes y para aprovechar las ventajas de los sistemas de correo electrónico que ayudan a los usuarios a colaborar en proyectos, programas y procesamiento de documentos.

h) **Gestión centralizada.-** Una red ofrece un camino a los servidores centralizados y a sus datos, junto con otros recursos. Cuando los dispositivos se localizan en un lugar las modernizaciones de hardware, las copias de seguridad de software, el mantenimiento y la protección del sistema son mucho más fáciles de gestionar.

i) **Mejora de la estructura corporativa.-** Las redes pueden cambiar la estructura y gestión de una organización. Los usuarios que trabajan en un departamento concreto y para un director específico sin la necesidad de estar en la misma área física. Pueden tener sus oficinas en áreas donde se necesite más su experiencia. La red los une con sus directores y compañeros de departamento. Esta disposición es útil para los proyectos especiales donde individuos de distintos departamentos, como investigación, producción y marketing, necesitan trabajar estrechamente unos con otros.

1.4 ¿QUE ES INTERNET?

Internet es una malla mundial de computadoras y redes de computadoras interconectadas. La Malla se refiere al hecho de que Internet es una red de redes. Integra redes de área local (LANs) ubicadas en escuelas, bibliotecas, oficinas, hospitales, universidades, institutos de investigación y otras entidades, en una única gran red de comunicaciones extendida por todo el mundo. Las conexiones subyacentes incluyen a la red de enlace telefónico, a los enlaces por microondas tanto terrestres como para satélites, y a las redes de fibra óptica. La red normal no se puede idear en cualquier momento, ya que constantemente se añaden nuevas

computadoras y redes, y los caminos electrónicos para la información cambian continuamente.

Aunque los investigadores pensaron en un principio en Internet, como una red de comunicaciones, principalmente militar, hoy día la utilizan millones de personas en oficinas, educación o simplemente para comunicaciones. Internet ofrece servicios de correo electrónico, así los usuarios se pueden enviar mensajes unos a otros. También proporciona muchas formas de servicios de información, tanto públicos como privados, que los usuarios pueden hojear libremente.

Internet se podría comparar con el servicio de información privada ECUANET, SATNET o W.NET. Los usuarios inician la sesión para acceder a los recursos de una red de sistemas de computadoras que proporcionan un conjunto de servicios dentro de límites específicos. Internet es más que un soporte de comunicaciones para acceder a muchos servicios distintos. Es una estructura con vínculos a muchas redes públicas y privadas. El acceso a estas redes puede ser libre y sin restricciones, en función de los privilegios de acceso o de cuánto se esté dispuesto a gastar. El sistema nacional y mundial de telecomunicaciones, tanto público como privado, da soporte a la red.

Internet surge de un proyecto inicial del Departamento de Defensa de Estados Unidos, la Red de la Agencia de Proyectos Avanzados de Investigación (ARPANET, Advanced Research Projects Agency Network), que se introdujo en 1969 como un proyecto pionero para examinar las redes de conmutación de paquetes. ARPANET proporcionaba los enlaces entre los investigadores y los

centros de computadoras remotas. En 1983, la parte militar de comunicaciones de ARPANET se separa y convierte en MILNET (Red Militar), aunque el cruce de comunicaciones fue todavía posible. ARPANET se desmanteló oficialmente en 1990.

El Consejo de Actividades Internet (IAB, Internet Activities Board) coordina el diseño, la ingeniería y la gestión de Internet en dos comités principales:

a) **Grupo para Tareas de Ingeniería Internet (IETF, Internet Egineering Task Force).-** Especifica los protocolos y recomienda las normas.
b) **Grupo para Tareas de Investigación Internet (IRTF, Internet Research Task Force).-** Investiga nuevas tecnologías y hace las recomendaciones sobre ellas al IETF.

1.5 ¿COMO FUNCIONA INTERNET?

Internet funciona integrando varios conceptos y características que las definimos a continuación:

a) **Conexión a Internet TCP/IP.-** Internet utiliza, aunque no exclusivamente, el Protocolo de control de Transmisión/ Protocolo Internet (TCP/IP). También usa otros protocolos, pero TCP/IP es la clave de la interoperatividad en Internet. TCP/IP es un protocolo abierto de comunicación que se encuentra normalmente disponible en la mayoría de los sistemas de computadoras. Los protocolos definen las reglas de comunicación. TCP/IP y se diseño

específicamente para la interconexión de diferentes tipos de equipos de computadoras. Primero se utilizó en ARPANET (Red de la Agencia de Proyectos Avanzados de Investigación) y ahora está disponible para casi todos los sistemas operativos de computadora como una característica incorporada o como una opción que se puede añadir.

Internet consta de miles de caminos de comunicación interconectados (la malla) que los paquetes pueden atravesar. Estos caminos son las actuales conexiones de red, líneas telefónicas dedicadas, enlaces de satélites y otra serie de posibilidades. En su conjunto, cada computadora en Internet puede conectarse potencialmente a las otras computadoras de Internet.

Una de las razones de por qué Internet es tan popular se debe a que sus usuarios poseen muchas computadoras y sistemas operativos. Con TCP/IP, es posible la interconexión de estos sistemas.

b) **Acceso a Internet.-** Para utilizar los servicios de Internet, primero se necesita entender cómo conectarse a ella. Muchos usuarios de Internet se conectan a ella a través de su compañía, una institución de educación u otra organización. Una red en casa puede proporcionar un camino a estos servicios. La compañía u organización recoge a menudo el costo de las llamadas y accede a los recursos disponibles en otras redes de Internet. Por ejemplo, las agencias de gobierno poseen libre acceso para asegurar que determinados recursos de Internet no estén disponibles para los usuarios domésticos.

Se puede obtener acceso a Internet a través de proveedores comerciales que poseen sus propios sistemas anfitriones conectados a Internet o se puede conectar directamente a Internet, en cuyo caso su computadora se convierte en un anfitrión.

En cuanto a los componentes físicos, se necesita una computadora con un modem. Si se conecta con un suministrador de servicios, necesitará un programa de emulación de terminales. Si se conecta directamente a Internet, necesitará ejecutar la serie de protocolos TCP/IP.

Si se está considerando interactuar en Internet, los proveedores le ofrecerán algo más que servicios de correo. Sólo con el acceso al correo, se puede intercambiar correo con otros usuarios pero eso es todo. Con capacidades interactivas, se puede acceder a servicios que permiten buscar información, charlar con otros usuarios y transferir archivos. Sin embargo, si el servicio de correo es todo lo que necesita de Internet y una conexión con otro servicio de correo, como Compuserve, MCIMail, Hotmail o Yahoo está conectado, puede simplemente aprovecharse de las conexiones que estos servicios ofrecen en Internet para intercambiar correo sobre ella.

La dirección IP determina dónde y cómo constituye la conexión Internet, puede ser tanto una pasarela, como un anfitrión a acceso o incluso su máquina, como se describe a continuación:

- **Pasarela:** Proporciona servicios de Internet a un usuario, pero este usuario nunca se situará en Internet por sí mismo.
- **Anfitrión de inicio de sesión:** Un servicio que le permite entrar en Internet e interactuar con ella, pero su máquina normalmente nunca está en Internet, si lo está el anfitrión de inicio de sesión. Se accede al anfitrión de entrada al sistema con un modem. Los costos mensuales y de acceso se pagan al proveedor. Los otros usuarios de Internet no ven su máquina como un anfitrión.
- **Su máquina:** Esta categoría implica que su máquina es un anfitrión en Internet y puede permitir a otros usuarios el acceso a los servicios que les proporcione.

c) **Direccionamiento en Internet.-** Toda computadora en Internet posee un nombre y una dirección numérica específica. El nombre se utiliza para simplificar el acceso de las personas, los equipos y las computadoras de comunicación utilizan la dirección numérica. Normalmente, el nombre no forma parte del Protocolo Internet IP, es una traducción del número que realiza el Servicio de Nombres de Dominios (DNS, Domain Naming Service). Los nombre en Internet simplifican el direccionamiento del correo electrónico y el acceso de los usuarios a otros sistemas de Internet.

La dirección numérica es un valor numérico de 4 bytes (32 bits) que identifica tanto a una red como a un anfitrión local o nodo de la red. Cada dirección IP debe ser única y constar de cuatro números decimales separados por puntos, como 191.245.10.3. si se establece una red interna TCP/IP, la asignación de

las direcciones numéricas es arbitraria dentro de una compañía u organización, pero si se proyecta conectar una computadora como un anfitrión a Internet, se necesitará obtener un número registrado.

Todos los nombres Internet poseen los dos elementos mostrados aquí:

Local@dominio

Estos nombres se utilizarán cuando se direccionan mensajes de correo electrónico o cuando se conecta con otros sistemas de la red. La orden FTP (File Transfer Protocol) o Protocolo de Transferencia de archivos se utiliza para conectarse con otros sistemas.

Un nombre Internet consta de varias palabras separadas por punto como se define en el Servicio de Nombres de Dominios (DNS). El nombre del dominio pasa a formar parte de la dirección de cada anfitrión en la red TCP/IP. Se combina con el nombre de la organización y con un tipo de código que representa el tipo de organización que se trata. Aquí se listan los tipos de códigos más comunes:

.com Organización comercial

.edu Institución educativa

.gov Organización del gobierno

Un nombre Internet completo para una compañía ficticia llamada Conjunto, Inc. Sería *Conjunto.com.* Si la compañía posee oficinas en diversas ciudades, la ciudad se añadiría al nombre para diferenciar las oficinas. Por ejemplo, los siguientes nombres representan oficinas de Conjunto en Ambato y Quito. Obsérvese que los nombres de las ciudades se abrevian, para reducir el número de pulsaciones que deben realizar los usuarios cuando necesitan escribir a menudo estos nombres.

am.conjunto.com

qu.conjunto.com

Si la compañía quiere diferenciar sus departamentos, se pueden añadir abreviaciones para los nombres de los departamentos, como a continuación se indica:

am.pro.conjunto.com

qu.mktg.conjunto.com

Las compañías y organizaciones son las responsables de sugerir el nombre. Una vez que el nombre está definido, la organización lo registra en Internet. Entonces se le asigna un Servicio de Nombre de Dominios (DNS) al anfitrión de la nueva red. Después se obtiene una pasarela para el correo electrónico y se puede decidir si se quiere que los usuarios de la red accedan a su sistema como a un anfitrión.

Los usuarios individuales de la red TCP/IP también necesitan un nombre. Es una buena idea que las organizaciones normalicen, desde el principio, su estrategia de nombres para el correo electrónico. Por ejemplo, primero la inicial del nombre y después el apellido. Obsérvese que el que los caracteres estén en mayúsculas o minúsculas ya que puede ser importante en algunos sistemas o con algunas aplicaciones. Para direccionar un mensaje de correo electrónico, se añade el nombre de correo electrónico al nombre del anfitrión de Internet como aquí se muestra:

Nombre-de-usuario@anfitrión

Donde nombre-de-usuario (username) es la identificación o buzón de receptor y anfitrión (host) es la computadora y/o anfitrión o nombre de dominio. Por ejemplo, lo que sigue a continuación es la dirección de Carlos Mera en Conjunto,Inc.:

Cmera@conjunto.com

1.6 SERVICIOS INTERNET

Una vez que se ha obtenido acceso a Internet a través del proveedor de servicios o de su propia conexión, puede iniciar la sesión, empezar con la edición de órdenes. Primero se describe *Telnet*, por que es la orden que se usa al inicio de sesión. A continuación de describen los servicios disponibles en Internet:

a) **Inicio de sesión (logon) Telnet.-** Es el protocolo o la orden que permite iniciar una sesión en sistemas remotos. Esta orden está disponible en todo sistema que tenga el soporte TCP/IP instalado. Si se ha conectado con un proveedor de servicios, la orden estará disponible en su sistema. Algunos sistemas poseen una orden *rlogon* equivalente. Simplemente se escribe el nombre del anfitrión, aparece el indicador del sistema (prompt) de Telnet y se puede escribir *help* para visualizar la información sobre la utilización de la orden.

b) **FTP (Protocolo de Transferencia de Archivos, File Transfer Protocol).-** Es el programa que se usa para la transferencia de archivos entre anfitriones. Recuerde que si se conecta a un anfitrión del proveedor se servicio, sólo puede transferir archivos a o desde allí. Luego se usa un programa de transferencia local de archivos para llevarlos a su máquina. Las utilidades que hacen esto se añaden por regla general al servicio proporcionado por el anfitrión.

También se puede usar FTP para acceder a cuentas anónimas (anonymous), que son cuentas de anfitriones abiertas al público y que proporcionan información a la que se puede acceder, por lo general, sin costo. Internet contiene una gran cantidad de información disponible en las cuentas anónimas de FTP. Se obtendrán documentos de investigación, software libre, acceso a debates y otras informaciones. Localizar la información es el reto. Un servicio denominado *Archie* puede ayudarle. Mantiene bases de datos

dedicadas con la información disponible en Internet, que se pueden consultar para encontrar la información.

Hay un completo conjunto de órdenes que se pueden usar una vez que se ha iniciado una sesión FTP. Frecuentemente se usa FTP como un verbo en la literatura de Internet, alguien podría decir "FTPme el archivo". Se puede escribir *help* para obtener más información.

c) **Correo electrónico, servicios de conversación y noticias.-** El correo electrónico es probablemente el servicio más activo en Internet. Hay una serie de utilidades que se pueden usar para crear mensajes de correo, algunas de la cuales están libremente disponibles en Internet. El componente clave es el mecanismo de distribución, que es el protocolo que el sistema de correo electrónico utiliza para enviar mensajes. El protocolo de correo electrónico de TCP/IP es el Protocolo Básico de Transferencia de Correo (SMTP, Simple Mail Transfer Protocol). Aunque el protocolo sea SMTP, la interfaz de usuario puede tener cualquier aspecto que los desarrolladores elijan. Un sistema de correo basado en SMTP en un equipo permite que los usuarios envíen y reciban mensajes a o de los usuarios de un sistema UNIX o con cualquiera en Internet, sin tener que pasar por una pasarela especial que traduzca el mensaje.

Si todo lo que se quiere hacer es intercambiar correo con otros usuarios, se puede pasar por diversos proveedores de servicios y sistemas de Tablón de Anuncios (Bulletin Board) que realicen este intercambio. Si el proveedor

posee una pasarela, no necesita preocuparse de la utilización de un sistema de correo compatible con Internet. Por ejemplo, si se usa CompuServe, simplemente se escriben los mensajes mediante la utilización del sistema de correo electrónico de CompuServe y después se dirige a un usuario final en Internet.

Las siguientes redes proporcionan servicios de distribución de correo electrónico Internet. Algunas son asociaciones libres de usuarios conectados, mientras que otras son organizaciones lucrativas:

- **UUCP mail network:** Red UNIX de enlace telefónico que suministra correo y noticias de USENET (UUCP, Protocolo de Copia entre Sistemas UNIX – to – UNIX CoPy protocol).
- **FidoNet:** Una red DOS de enlace telefónico que proporciona correo y Echomail, un servicio parecido a las noticias de USENET.
- **BITNET (Because It's Time Network):** Una red de computadoras de campus patrocinada por la Fundación Nacional de Ciencias.
- **MCI Mail:** Un servicio de distribución de correo ofrecido por MCI Corp.
- **CompuServe:** Permite servicios de intercambio de correo con Internet.
- **Genie:** Proporciona servicios de intercambio de correo con Internet.

d) Correo privado mejorado.- El Correo Privado Mejorado (PEM, Privacy Enhanced Mail) proporciona correo electrónico autentificado y confidencial. El emisor firma electrónicamente el correo con el uso de los métodos de

cifrado de clave pública. El receptor puede después verificar la firma mediante la utilización de una clave pública. Internet adopta los protocolos PEM.

El volumen de información disponible en Internet se encuentra escalonado. Debido a que Internet es una asociación libre formada por muchas redes y muchas fuentes de información, no hay una forma fácil de determinar la ubicación de la información. Los siguientes servicios se han hecho populares y han ampliado los servicios que proporcionan:

- **ARCHIE:** Es un servicio que permite localizar rápidamente la información en los anfitriones anónimos de FTP. Se accede a ARCHIE a través de sesiones Telnet, consultas de correo electrónico u otros métodos.

- **GOPHER:** Es un sistema de búsqueda y recuperación de documentos distribuidos desarrollado por la Universidad de Minnesota. Oficialmente se define como un Protocolo básico cliente – servidor que se puede utilizar para editar y buscar la información contenida en una red de anfitriones distribuida. Los usuarios de Gopher pueden visualizar la información extendida sobre muchos anfitriones diferentes. La información aparece en forma jerárquica, o los usuarios pueden solicitar un índice de los temas equivalentes.

e) **Servicio de Información de Area Extensa (WAIS).-** WAIS (Wide Area Information Service) es un servicio de búsqueda y recuperación que proporciona realimentación que se puede utilizar para refinar futuras búsquedas. WAIS posee servidores que mantienen índices de los documentos de Internet.

f) **Malla Extensa Mundial (World Wide Web) o W3.-** Proporciona servicios de localización de información mediante la utilización de enlaces de hipertexto que conectan un documento con otro. Cuando se utiliza el servicio, simplemente se siguen los enlaces entre documentos.

g) **Servicios de conversación (CHAT).-** Son sesiones de comunicaciones en tiempo real que se pueden mantener con uno o más usuarios de Internet al mismo tiempo. Durante la sesión, se pueden escribir mensajes que verán otros participantes o tan sólo cruzarse de brazos y leer los mensajes escritos especiales como política, aviación, computadoras, salud, finanzas y muchos otros, o puede crear sus propias sesiones. Existen dos servicios disponibles:

- **Conversación (talk):** Un servicio interactivo de comunicaciones uno a uno.
- **IRC (Conversación de Transmisión Internet, Internet Relay Chat):** Un servicio interactivo de comunicaciones de muchos a muchos.

h) **Grupo de noticias Usenet.-** Es un grupo de sistemas que intercambian noticias y abarcan universidades, agencias del gobierno, oficinas y usuario

domésticos. No hay control central. Se parece al sistema de tablón de anuncios o al de conferencia, en el que hay temas o correo en desarrollo que algún usuario puede ver y responder. Las categorías incluyen computadoras, noticias, ciencia, ocio, y por supuesto, conversación. Noticias (news) de USENET es un servicio de transmisión de noticias de Internet que distribuye información, por lo general sobre Internet, a todos los anfitriones. La red USENET incluye todas las computadoras que consiguen noticias de USENET. Si sólo se contrata el servicio de correo, también se tendrá la oportunidad de obtener acceso a este servicio.

1.7 ¿QUE ES INTRANET?

Internet es una red de redes. Intranet es una red más pequeña y restringida con la integración de estándares de Internet dentro de la empresa para explotar al máximo la información y la inversión en tecnología. Los beneficios de Intranet son las siguientes:

a) Permite a los grupos de trabajo y departamentos de las empresas de sus clientes compartir información más fácil y efectivamente en los siguientes puntos:

- Fácil acceso y uso de información publicada en una Intranet.
- Eficiencia en la consulta de información disponible en Intranet.
- Máximo aprovechamiento de los sistemas existentes.
- Integración de los sistemas de información.

Ejemplos:

- El organigrama corporativo actualizado en todo momento.
- Políticas de recursos humanos.
- Calendarios de eventos.

b) Sus clientes obtienen mayor productividad, ya que las aplicaciones están integradas, haciéndolas más fáciles de usar. Con Intranet toda la información se accede a través de una sola forma, ofreciendo ventajas como:

- Compartir los mismos recursos para almacenar e intercambiar información.
- Facilitar el desarrollo de aplicaciones para trabajo en grupo.
- Definir una plataforma de mensajería como medio par el intercambio de información.
- Permitir a sus clientes la comunicación y colaboración en tiempo real.

Ejemplos:

- Compartir bases de datos de clientes, contactos o proveedores.
- Foros de discusión
- Procesos de aprobación de créditos.

c) Le permite a sus clientes obtener un mayor retorno a su inversión, utilizando programas existentes. Esto le permite a usted ofrecer servicios de consultoría, instalación, conexión, etc., permitiendo:

- Proveer un ambiente único e integrado para el desarrollo de aplicaciones independientes de la plataforma en la se trabaje.
- Aprovechar sus datos existentes.
- Integrar los diferentes sistemas donde la información es compartida desde una única interface de trabajo.

Ejemplos:

- Procesamiento de ordenes.
- Procesamiento de reclamos.
- Asignación de actividades.
- Integración de información que reside en otras plataformas.

d) Ayuda a sus clientes a mantener el control de ambientes distribuidos como Intranet, a través de sus distintos componentes; permitiendo:

- Reducción de costos asociados con el soporte a usuarios.
- Manejo de Intranet a través de Internet, incluyendo la administración del sitio web y la distribución de su contenido.
- Análisis del uso de los sitios web para medir aumentos en productividad.

1.8 ¿COMO SE APLICA EN LA RED DE LA PUCESA?

La Red que posee el laboratorio informático cumple con los requisitos mencionados para justificar su creación. Aquí se presenta un resumen de lo anotado anteriormente aplicado a la PUCESA el cual permite:

a) **Intercambio de archivos.-** Enviar y recibir archivos entre los diferentes terminales que están integrados en la red.

b) **Transacciones remotas de datos.-** Recibir archivos a través de Internet, al estar conectada la red a Internet se puede transmitir archivos desde servidores remotos utilizando los protocolos comunes de Internet como son FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos) o HTTP (Hiper Text Transfer Protocol, Protocolo de Transferencia de HiperTexto); de la misma forma se especifican directorios FTP o hipervinculos en las páginas WEB de la PUCESA que permitan la transferencia de archivos, la PUCESA podría transferir archivos a otras personas que se encuentren enlazadas a Internet.

c) **Compartir recursos de red**.- Los terminales de la PUCESA cuentan con sistemas operativos que permiten compartir recursos como unidades de disco, impresoras, etc. Esto permite que otras terminales tomen estos recursos como propios, llamadas unidades virtuales para ser direccionadas y trabajadas directamente.

d) Compartir Archivos.- De la misma forma, el sistema operativo permite que se compartan directorios o secciones específicas de las unidades que se pueden tomar como unidades virtuales en otros terminales permitiendo conservar la confidencialidad de áreas de los medios de almacenamiento en las que otros equipos no pueden acceder.

e) Grupos de Trabajo.- El Sistema operativo de red permite crear grupos de trabajo donde los miembros de cada grupo poseen derechos especiales y específicos de acuerdo a los criterios de cada grupo; los que no pertenecen al grupo solo pueden tener algunos derechos restringidos por el creador del grupo o administrador de la red.

f) Correo Electrónico.- La red de la PUCESA cuenta con un servidor de correo electrónico que permite a los usuarios y estudiantes tener acceso a un buzón de correo para recibir y enviar mensajes tanto dentro de la PUCESA como a Internet.

g) Gestión Centralizada.- Se puede hablar de una gestión centralizada de la información ya que cuenta con un servidor único en el cual se manejan todos los servicios de red como son correo electrónico, definición de usuarios, etc.; manejo de base de datos el mismo que se encuentra ubicado en una sección de servidores, ubicado en la oficina de administración del laboratorio, éste crea y regula todas las reglas que se manejan el laboratorio.

Internet, posee todos los servicios que permiten a la empresa:

a) Navegar en la Malla Extensa Mundial (WWW).

b) Servicios de Conversación (CHAT).

c) Servicios de Noticias (USENET).

d) Conexión, direccionamiento y acceso a Internet (TCP/IP, Login) .

e) Protocolo de Transferencia de Archivos (FTP).

f) Protocolo de Transferencia de Hipertexto HTTP.

g) Intercambio de correo electrónico MAIL.

Las propiedades y características expuestas anteriormente califican a la red de la PUCESA como una Intranet cumpliendo con los estándares de Internet: compartir recursos, archivos e información, aprovechando y haciendo más eficiente el uso de los recursos del laboratorio.

CAPITULO II

EVALUACION FISICA DE LA RED

2.1 EVALUACION DE LA CONFIGURACION DE LAS COMPUTADORAS

En este capítulo se describirá y evaluará todos los componentes físicos de las computadoras que posee los laboratorios de la PUCESA para la instalación de una red LAN y WAN, dirigidas a Internet e Intranet. Nos enfocaremos principalmente en las redes LAN y WAN, ya que son el motivo de nuestro estudio.

2.1.1 TIPOS DE REDES

Una red puede ser inicialmente pequeña y después crecer con la organización. Los diferentes tipos de redes se describen a continuación:

a) **Segmento de red o subred.-** El hardware o una dirección concreta de red definen normalmente un segmento de red. Por ejemplo, en el entorno Windows NT , un segmento de red incluye todas las estaciones de trabajo pertenecientes a un grupo de trabajo. Cada segmento posee su propia dirección de red. Todas las computadoras enlazadas a un segmento, reciben las mismas transmisiones de señal como grupo de red.

b) **Red de Area Local (LAN, Local Area Network).-** Es un segmento de red con grupos de trabajo y servidores enlazados, o un conjunto de segmentos de red interconectados, por lo general dentro de la misma área, como por ejemplo un edificio.

c) **Red de campus.-** Es una red que abarca otros edificios dentro del área de un campus o de un parque industrial. Los distintos segmentos o LANs existentes en cada edificio se conectan con cables soporte. Por regla general la organización es propietaria del terreno y es libre de tender tanto cable como necesite, ésta es otro tipo de LAN.

d) **Red de Area Metropolitana (MAN, Metropolitan Area Network).-** Una red que se extiende sobre áreas de ciudades o municipios, y que se interconecta mediante la utilización de facilidades proporcionadas por la compañía de telecomunicaciones local, ésta es un tipo de WAN.

e) **Red de Area Extensa (WAN, Wide Area Network).-** Redes que cruzan grandes fronteras internacionales enlazados con los servicios públicos y privados de telecomunicaciones, además de los enlaces por satélites y microondas.

f) **Red corporativa.-** Interconecta todos los sistemas de computadoras dentro de una organización, independientemente del sistema operativo, protocolos de comunicación, diferencias de aplicaciones o ubicación geográfica. Puede ser por lo tanto una LAN, MAN o WAN. La red se ve a sí misma como una plataforma sobre la cual se conectan muchos tipos de dispositivos distintos. Se emplean diversas técnicas para ocultar las diferencias entre sistemas, así los usuarios pueden acceder a cualquier recurso de forma transparente. Por ejemplo los productos Middleware ocultan protocolos y las diferencias de las aplicaciones.

La red corporativa normalmente es un *sistema de información distribuida,* en el cual se localizan recursos y datos por toda la organización. En este entorno, se necesitan servicios de directorio que ayuden a los usuarios a localizar a otros usuarios, recursos y datos. La seguridad es también un tema importante. Una vez que una red conecta una compañía entera, los gestores de departamentos o grupos de trabajo se deben preocupar por restringir el acceso a los datos. Las bases de datos se pueden dividir y distribuir a emplazamientos remotos para que los usuarios de estas zonas tengan los datos disponibles más fácilmente y así reducir los costos de acceso sobre enlaces caros de WAN. Este método necesita técnicas de reproducción o sincronización para asegurarse de que las bases de datos poseen la misma información. Estas redes pueden clasificarse como LAN o WAN dependiendo de los mecanismos de interconexión que se empleen y las áreas físicas donde se encuentren.

2.1.2 REDES DE AREA LOCAL (LAN)

Es el método principal de transmisión de datos entre computadoras de equipos de escritorio en muchas organizaciones hoy en día. Conecta las computadoras de un grupo de trabajo, departamento o edificio. En contraste, una inter-red es una colección de LANs dentro de un edificio, grupo de edificios o área de campus.

Las LANs que emplean métodos de conexión por cable usan tanto cables coaxiales como de par trenzados. Un cable coaxial se tiende normalmente

entre las computadoras de una oficina mediante la utilización de una configuración serie. Los sistemas de cable de par trenzado conectan cada computadora a una caja central llamada concentrador (hub). Si la red es grande, un concentrador se puede conectar a otro.

Distintas limitaciones de la red pueden hacer que se desplieguen varias redes separadas, luego se conectan con el uso de dispositivos como repetidores, puentes y encaminadores. Estas limitaciones incluyen la distancia del cable, una restricción en el número de estaciones de trabajo o simplemente la incapacidad de conectar fácilmente computadoras dispersas. Los dispositivos usados en redes son las siguientes:

a) **Repetidor (Repeater).-** Alarga la distancia de un segmento de cable mediante la ampliación de la señal.

b) **Puente (Bridge).-** Interconecta dos tipos de LAN distintas, como una Ethernet a una en anillo con testigo.

c) **Encaminador (Router).-** Proporciona una forma de interconectar muchos segmentos de redes diferentes y controlar el tráfico por los múltiples caminos existentes entre esos segmentos.

Las LANs son sistemas de comunicación compartidos que proporcionan conexiones para cientos de usuarios potenciales. Se necesita un mecanismo para asegurarse que solo una estación de trabajo transmita datos por el cable

en un instante dado. A estos mecanismos se les denomina *métodos de acceso* y existen varios, como se describen a continuación:

a) **Acceso Múltiple con Detección de Portadora (Carrier Sense Multiple Access).-** Las estaciones escuchan para saber si se usa el cable y sólo transmiten si éste está disponible.

b) **Paso con testigo (Token passing).-** Las estaciones toman posesión de un testigo electrónico y sólo transmiten mientras lo poseen.

c) **Prioridad bajo demanda (Demand on priority).-** Un concentrador central determina qué estación puede acceder al cable y puede otorgar prioridades a unas estaciones sobre otras, dependiendo de la sensibilidad al tiempo de los datos que se quiere transmitir.

d) **Bus ranurado**.- Está disponible un flujo continuo de ranuras (como un tren de furgones), en los que cualquier estación puede situar datos para transmitírselos a otra.

Existen también las *LANs por Infrarrojos,* que son redes inalámbricas. Se utiliza una señal infrarroja, parecida a la señal entre dos estaciones. La luz infrarroja esta por debajo del espectro de luz visible. Las estaciones de trabajo deben estar dentro de la línea de actuación del transmisor de infrarrojos, lo que les da algo de movilidad. Algunas LANs por infrarrojos funcionan con

señales que rebotan fuera de las paredes en un modelo disperso. No obstante, estas LANs incluyen distancias limitadas.

2.1.3 REDES DE AREA EXTENSA (WAN)

Una WAN constituye un sistema de comunicación que interconecta sistemas de computadoras geográficamente remotos. Enlaza las computadoras situadas fuera de las propiedades de una organización (edificios o campus) y atraviesa áreas públicas que están reguladas por autoridades locales, nacionales e internacionales. Generalmente, el enlace entre lugares remotos se realiza a través de la red pública de teléfono, pero una organización podría crear sus propios enlaces WAN mediante microondas, satélites u otras tecnologías de comunicación.

Una WAN es una red con proporciones potencialmente globales. Si se emplean facilidades públicas, una WAN involucrará Compañías de Telecomunicaciones para el Intercambio Local (LECs, Local Exchange Carriers), Compañías de Telecomunicaciones para el Intercambio a Larga Distancia (IXCs, Interexchange Carriers) y Compañías de Telecomunicaciones de lugares remotos.

Como lo describimos anteriormente encontramos *Redes corporativas extensas* que son redes de área extensa que interconecta los recursos informáticos de una organización a través de áreas locales o extensas, sin tener en cuenta los sistemas operativos, los protocolos de comunicación o las

plataformas. Habitualmente, las gestiona una autoridad central. Las organizaciones pueden construir diferentes tipos de redes:

a) **Red privada.-** Consiste en un equipo de conmutación y de comunicaciones que es propiedad de una organización interconectada mediante líneas de comunicación alquiladas o propias (como sistemas de microondas). Las líneas privadas facilitan a la compañía el mantenimiento de la seguridad y el control sobre el tráfico que atraviesa la línea; en cambio, los servicios contratados a un proveedor garantizan la calidad de la línea y la disponibilidad.

El servicio de línea digital normalizado es el canal T1, que proporciona velocidades de transmisión de 1,544 Mbits/seg. las líneas T1 pueden transportar voz y datos mediante el uso de dispositivos multiplexores, de modo que se usan frecuentemente para proporcionar conexiones telefónicas entre lugares remotos pertenecientes a una organización. Una línea T1 puede proporcionar 24 canales de voz o datos en un ancho de banda de 64 Kbits/seg.

Las redes construidas con líneas alquiladas T1 (1,544 Mbits/seg.) o T3(45 Mbits/seg.), son adecuadas en algunas condiciones, en función de los presupuestos, los requisitos de la transmisión y la distancia entre los puestos tal y como se describe a continuación:

- El costo de las líneas alquiladas se incrementa con la distancia, así que sólo son apropiadas dentro de ciertas áreas geográficas.
- Cuatro o más horas diarias de tráfico WAN entre dos emplazamientos podrían justificar el alquiler de una línea privada, pero los costos debidos a la distancia afectan a este cálculo.
- Las redes privadas construidas con líneas alquiladas son adecuadas para la interconexión de unos pocos emplazamientos, pero inadecuadas para la interconexión de muchos emplazamientos distintos que tengan niveles de tráfico relativamente bajos.
- Dentro de la misma línea alquilada se pueden multiplexar llamadas orales y transmisiones de datos, en ocasiones, puede justificarse que una organización use este tipo de líneas, cuando existe mucho tráfico de voz y de datos entre dos lugares.

Una red privada que conectase cuatro posiciones separadas, podría tener un aspecto como el de la figura 7.

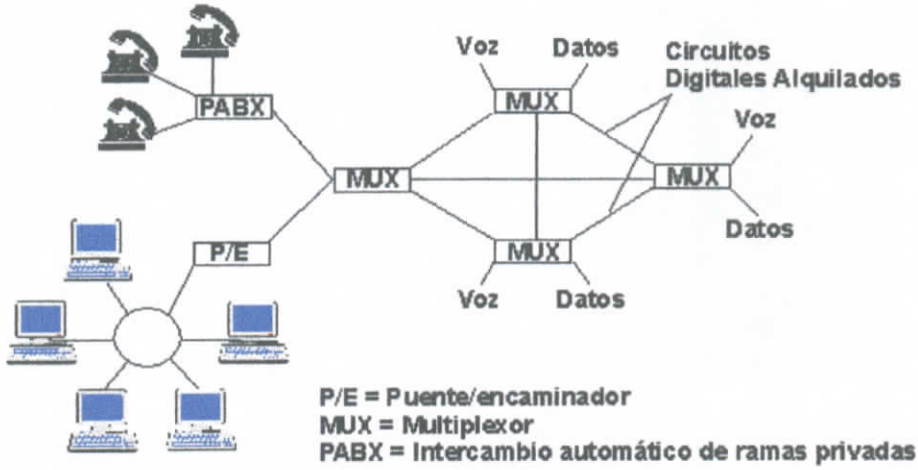


Figura 7. Red Privada que conecta cuatro lugares remotos

Los cuatro lugares puede que se localicen dentro de la misma Area Geográfica Local para Acceso y Transporte (LATA, Local Access and Transport Area), con lo que las líneas alquiladas las aportaría la Compañía de Telecomunicaciones para el Intercambio Local (LEC, Local Exchange Carrier). Si se sobrepasan los límites de la LATA, se involucraría a las LECs de los puertos local y remoto, a través de la Compañía de Telecomunicaciones para el Intercambio a Larga Distancia que los conectará (IXC).

b) **Red pública.-** De las Redes Públicas de Datos (PDN, Public Data Network) se ocupan las compañías de telecomunicaciones, sean o no de Valor Añadido (VAC, Value-Added Carrier). La VAC proporciona todos los enlaces de datos que el cliente necesita y éste paga una factura. La conmutación se hace en la red de la compañía . Las redes públicas son las mejores para el enlace de muchos lugares remotos y para el enlace de sitios que no existe bastante tráfico entre ningún par de ellos como para que se justifique una línea alquilada dedicada. Además, si la distancia entre las posiciones de dos clientes es tan grande como para que el costo de una línea alquilada se haga prohibitivo, la mejor opción también será una red pública de conmutación de paquetes. Una Red Pública de Datos o PDN proporciona servicios tanto de conmutación de paquetes como de circuitos, como se describe a continuación:

- **Servicios de conmutación de circuitos:**

  - Estos servicios proporcionan un camino fijo entre dos puntos que se configura previamente al intercambio de información.
  - También aportan circuitos dedicados con una anchura de banda conocida y garantizada.
  - Cuando se selecciona al circuito, se producen pequeños retrasos.
  - La transmisión de datos comienza sólo cuando el circuito se ha estabilizado. Ambos sistemas finales deben estar preparados para efectuar el enlace, al igual que sucede en una conexión telefónica.
  - Las líneas caídas pueden detener toda transmisión, o requerir la intervención del usuario para rodear el problema.

- **Servicios de conmutación de paquetes:**

  - Los paquetes de información se encaminan a través de la malla de redes, de acuerdo con la dirección de destino que figura en su cabecera.
  - Los paquetes viajan a través de puertos compartidos, por lo que se pueden producir ligeros retardos, especialmente si son de longitud variable.

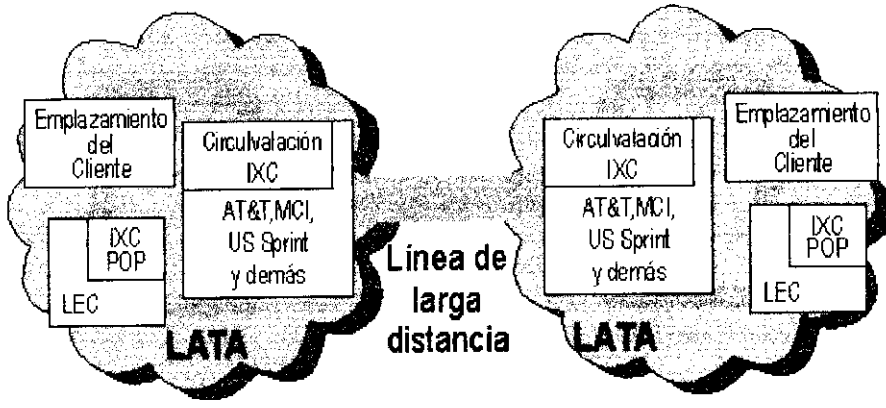
- No hay ningún retraso asociado a la elección de un circuito, sino que los circuitos lógicos orientados a la conexión se pueden definir a priori.
- Si se posee capacidades de ancho de banda variable, puede soportar el tráfico de ráfagas.
- La fuente puede transmitir en cualquier momento. No es necesario haber prefijado una sesión.
- La red evita de forma automática las líneas caídas o los nodos. En las redes públicas hay muchas rutas "alternativas"que pueden ocuparse del tráfico de los caminos que fallen.

La decisión acerca de qué método usar, la conmutación de circuitos o la de paquetes, se basa en la calidad de retraso que es tolerable para que se produzca entre el emisor y el receptor. En un sistema orientado a mensajes que se ocupa de correo electrónico y archivos de datos, se hace aceptable un retardo de segundos, minutos e incluso horas, y los sistemas de conmutación de paquetes son más baratos. Para las aplicaciones en tiempo real del tipo de procesamiento de transacciones en línea y otros requisitos interactivos, se hacen esenciales los sistemas de conmutación de circuitos y el tipo de circuito dependerá de la cantidad de tráfico y el número de posiciones que deban conectarse. Si sólo está involucrado un usuario, una línea de enlace telefónico a alta velocidad puede ser aceptable, pero si hay múltiples usuarios que requieren acceso a una posición central al mismo tiempo y de modo

continuo, podría ser necesario construir una red privada o usar facilidades de conmutación de circuitos que proporcionen conexiones casi instantáneas entre dos emplazamientos.

Si se usa una PDN, se evitan los problemas inherentes al control de las líneas y configuración del propio equipo de conmutación. Una PDN también se ocupa de cualquier problema que haya con la red y puede garantizar la distribución de los datos a través de una vasta malla de líneas conmutadas.

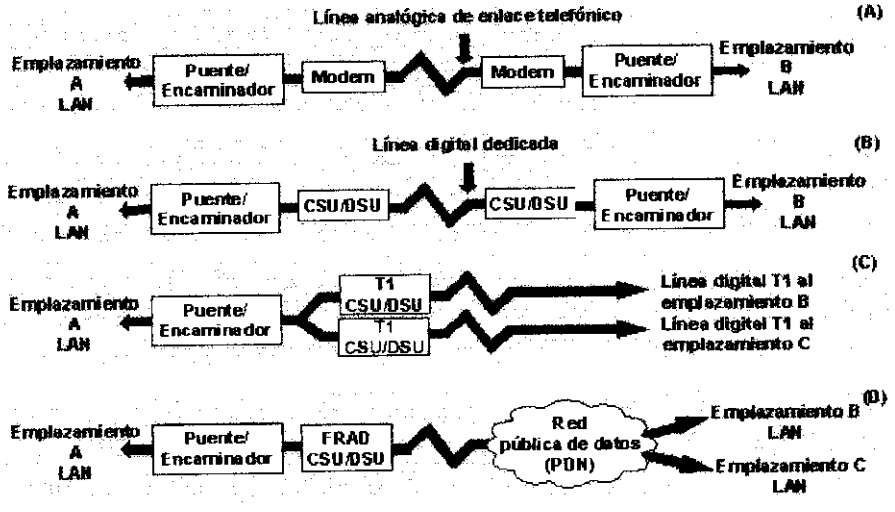
Como se muestra en la figura 8 se representa la topología de una conexión de área extensa.



IXC = Compañía de telecomunicaciones para el intercambio a larga distancia
LEC = Compañía de telecomunicaciones para el Intercambio Local
POP = Punto de presencia
LATA = Area Local para Acceso y Transporte

Figura 8. Facilidades para distancias locales y grandes para conexiones WAN

Un LATA se corresponde habitualmente con la geografía de un código de área telefónica. Una Compañía de Telecomunicaciones para el Intercambio Local (LEC) que fuera una de las Compañías Regionales de Operaciones Bell (RBOCs, Regional Bell Operating Companies) trabajaría dentro de un área LATA. Aunque dentro de la misma LATA podrían operar también compañías que no fuesen de operaciones Bell. Se quiere que haya una LEC para que proporcione una facilidad de Punto de Presencia (POP, Point-of-Presence) a las Compañías de Telecomunicaciones para el Intercambio a Larga Distancia (IXC), como AT&T, MCI y US Sprint, y así los clientes podrían elegir la IXC que requieran. Algunas compañías de larga distancia ofrecen facilidades de desvío, de forma que sus clientes puedan conectarse directamente a sus servicios de larga distancia en lugar de hacerlo a través de una LEC. En el Ecuador una de las compañías autorizadas para el transporte e intercambio de información es TELEHOLDIN. Como se muestra en la figura 9 se representa el equipo físico para las conexiones de una WAN.



FRAD = Dispositivo de acceso Frame Relay.

Figura 9. Estrategias de conexión de WAN

Un encaminador o un puente hace converger al tráfico desde la red local sobre la conexión de área extensa. Conectado al puente o al encaminador hay un modem para las líneas analógicas o una Unidad de Servicio de Canal/Unidad de Servicio de Datos (CSU/DSU, Channel Service Unit/Data Service Unit) para las líneas digitales. En (A), los modems conectan dos LANs a través de líneas remotas telefónicas analógicas. En (B), una CSU/DSU conecta dos líneas remotas a través de una línea digital. En (C), se interconectan múltiples sitios a través de líneas digitales T1 separadas. En (D), una única conexión a una red pública Frame Relay proporciona conexiones a múltiples posiciones remotas, mediante las facilidades de conmutación de la compañía de telecomunicaciones y los servicios de paquetes de la red de retransmisión de tramas. Nótese que en (C) y (D), también puede emplearse un multiplexor de voz/datos para transmitir tanto voz como datos a través de las mismas líneas.

También existen *servicios de las Compañías de Telecomunicación para las conexiones WAN*. Estos servicios consisten en líneas de enlace telefónico, líneas dedicadas y servicios de conmutación de circuitos o paquetes. La velocidad de transmisión de las líneas de enlace telefónico analógicas está en el rango entre 1200 y 28800 bits/seg (dentro de los estándares existentes). Los servicios dedicados digitales de conmutación están en el rango entre 56Kbits/seg y 45 Mbits/seg., con servicios de transmisión de celdas como el Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode) que

actualmente presta servicios a las velocidades de T3 de 45 Mbits/seg. A continuación, se dan las aplicaciones típicas:

a) Las transferencias de correo electrónico que requieren velocidades de transmisión de 2400 a 9600 bits/seg.
b) Los programas de control remoto necesitan velocidades entre 9600 y 56000 bits/seg.
c) Las interacciones remotas con las aplicaciones basadas en LAN precisan velocidades entre 9600 y 384000 bits/seg.

Para hacerse una idea del tipo de rendimiento que se necesita, hay que multiplicar estas velocidades por el número de usuarios que tengan que acceder al enlace simultáneamente.

Los servicios que poseen dichas compañías son las siguientes:

a) Servicios analógicos de enlace telefónico.- Las líneas de enlace telefónico usan modems que pueden proporcionar velocidades de transmisión de hasta 28000 bits/seg, a través de líneas de conmutación. Como las líneas son de conmutación, sólo se incurre en cargas durante el tiempo de conexión.

Los servicios de enlace telefónico son ideales para los enlaces ocasionales. Pueden ofrecer enlaces para transferencias de correo electrónico entre dos emplazamientos de la compañía o permitir a los

usuarios, del lugar o móviles, que se conecten con la base de datos de la compañía. En el caso de las conexiones de control remoto, el usuario enlaza la red de la compañía y toma el control de la computadora perteneciente a la LAN. La computadora conectada a la LAN, realiza el procedimiento, pero envía las pantallas obtenidas al usuario remoto y acepta entradas del teclado del mismo. Esta técnica minimiza la cantidad de tráfico que se transfiere a través del enlace remoto.

b) **Líneas privadas.-** Las líneas digitales se pueden obtener de las compañías de telecomunicación de varios modos y, típicamente, se alquilan por meses. Hay un cargo por la configuración inicial, y el resto de los pagos dependen de la distancia. Si la línea conecta posiciones de dos LATAS separadas, se involucra a la Compañía de Telecomunicaciones para el Incremento Local (LEC) de cada una de las áreas locales para el acceso y transporte, junto con la compañía de telecomunicaciones de larga distancia. Como se mencionó previamente, ésta situación podría cambiar, ya que compañías de larga distancia como MCI trabajan para proporcionar a sus clientes enlaces directos para las conexiones de larga distancia, en lugar de que los enlaces se realicen a través de las LECs.

Cambiando de escala, T1, Fractional T1 y T3 proporcionan velocidades de transferencia de datos en el rango de los megabits. Una línea T1 transfiere 1,544 Mbits/seg., Fractional T1 es adecuada para aquellos que no necesiten una línea T1 completa, pero que se anticipan así a

posibles necesidades futuras. Proporcionan 24 canales de 64 Kbits/seg. cada uno. Un cliente podría comenzar con un cierto número de líneas Fractional T1 y aumentarlo hasta una línea T1 completa, cuando lo necesite. La compañía de telecomunicaciones configura la línea T1 completa, pero hace que esté disponible sólo el ancho de banda contratado, hasta que se necesite más. Una línea T3 equivale a 28 líneas T1.

Las líneas digitales dedicadas se suelen usar para transportar voz, imágenes y multiplexación para mezclar voces y datos en las mismas líneas digitales. De esta forma, un cliente puede alquilar la línea T1 completa, y usar algunos de los canales para llamadas de voz entre dos emplazamientos de la compañía. El ancho de banda remanente se usa para los datos. Se requiere un multiplexor para que mezcle las señales de las fuentes de voz, imágenes y datos, y las transforme en un solo flujo de datos que cruce las líneas T1. En el otro extremo de la línea, habría un demultiplexor que separaría cada canal individual.

No todas las líneas alquiladas son dedicadas. Una organización podría alquilar temporalmente una línea de alta velocidad para uso ocasional, como la transferencia de archivos a fin de mes, o de video conferencias semanales. Este tipo de servicios se contratan de antemano con las compañías de telecomunicaciones. Sin embargo, los servicios digitales de conmutación que se discuten a continuación, han reducido la necesidad de este tipo de líneas.

c) Servicios de conmutación de circuitos.- Básicamente, este servicio no es muy diferente al de una llamada telefónica. Se configura un canal dedicado entre los dos puntos, durante el intervalo de la llamada. Durante este tiempo, se proporciona una cantidad específica de ancho de banda. Los usuarios pagan sólo por el tiempo en el que están conectados, y pueden llamar a diferentes sitios. Estos servicios se suelen denominar servicios de *marcar bajo demanda*. Habitualmente las llamadas sufren un cierto retardo de configuración asociado a este tipo de servicios; sin embargo, los nuevos equipos de conmutación han reducido este tiempo de configuración a microsegundos. En muchos casos, un tiempo de configuración breve no supone problema.

Se suelen usar las líneas de conmutación de circuitos como líneas de seguridad para las líneas dedicadas de alta velocidad en los siguientes casos:

- En el caso de que falle una línea alquilada dedicada, se conectan una o más líneas de conmutación de circuitos para que se ocupen del tráfico entre dos emplazamientos, hasta que se reconecte la línea dedicada.
- En caso de que una línea llegue a saturarse, se conectan líneas de conmutación de circuitos para que se ocupen de la excesiva carga de tráfico. Esta estrategia proporciona a los administradores de la red un camino económico para enlazar posiciones, sin necesidad de adquirir una cantidad excesiva de servicio dedicado.

Una técnica que combine líneas de conmutación de circuitos con multiplexores inversos, proporciona ancho de banda bajo demanda. Con esta técnica, se añaden enlaces adicionales cuando se incrementa el ancho de banda. Los multiplexores inversos de cada extremo dividen y recombinan las señales de múltiples líneas de baja velocidad.

Un servicio de conmutación común es *switched-56*, que opera a 56 kbits/seg. y requiere un switched-56 CSU/DSU especial en cada uno de los emplazamientos. Los servicios switched-56 tenían originalmente la finalidad de proporcionar una línea de seguridad alternativa a las líneas alquiladas de alta velocidad del tipo T1. Si una línea fallaba, una línea switched-56 establecería rápidamente una conexión alternativa. Todavía pueden usarse para esto, pero además se emplean para manejar picos de tráfico, transmisiones de fax, copias de seguridad, transferencias de correo electrónico voluminosas y conexiones de LAN a LAN. Las tarifas se suelen calcular por minutos.

Para velocidades de transmisión de datos más altas, las compañías del tipo de AT&T ofrecen servicios con switched 384k y switched T1. Se requiere que el cliente instale previamente el servicio de Red Digital de Servicios Integrados (ISDN, Integrated Service Digital Network).

d) **Red Digital de Servicios Integrados (ISDN).-** Es un servicio que proporciona todos los servicios digitales en el bucle local, que es el cable que corre entre la casa o el negocio del usuario, y la oficina de

conmutación de la compañía de telecomunicaciones de intercambio local. Este bucle es en gran medida aún, un cable par trenzado de cobre que soporta transmisiones analógicas. ISDN se ofrece en áreas selectas, y se usa del mismo modo que los servicios telefónicos. Al mismo tiempo que se proporcionan servicios digitales de conmutación de circuitos de alta velocidad, entre un cliente y la compañía telefónica, también ofrece un rango de servicios de integración de voz y datos a partir del cual se construyen muchas otras ofertas. Por ejemplo AT&T ofrece dos servicios switched 384k y switched T1, que se requieren para que el usuario configure un interfaz ISDN entre su posición y la compañía telefónica. Además, la red Frame Relay es una ampliación de ISDN.

La ISDN básica, conocida como Interfaz de Velocidad Básica (BRI, Basic Rate Interface) posee tres canales: dos proporcionan 64 Kbits/seg. y un tercero de señalización proporciona 16 Kbits/seg. La interfaz de velocidad principal proporciona servicios a aquellos que lo necesiten. Consta de 23 canales de voz o datos a 64 Kbits/seg. En ambas interfaces, el canal de señalización se ocupa de la importante función de configurar las llamadas. Con esto se consiguen velocidades de configuración de microsegundos y señalización fuera de banda, con lo que se mantienen los canales de datos libres para las transmisiones.

e) **Servicios de conmutación de paquetes.-** Proporciona una malla de conexiones a través de la cual viajan los paquetes de datos, hasta

alcanzar su destino. Los datos del sistema fuente se separan y se dividen en paquetes de tamaño predefinido. Hay dos tipos de servicios para la distribución de paquetes:

- **Un servicio orientado a la conexión:** Cada paquete es una entidad independiente que sigue su propio curso a través de la red, dependiendo del mejor camino disponible o de las decisiones que tomen los conmutadores a lo largo del camino. Como los paquetes pueden seguir distintas rutas, pueden llegar desordenados a su destino, y el sistema destinatario tiene que resecuenciarlos.

- **Un servicio orientado a circuito:** Se establece a través de la red una conexión lógica o camino. El camino está predefinido, con lo que mejora la eficiencia y la sobrecarga debida a los paquetes. Dado que el camino se fija de antemano, los paquetes llegan en orden, con lo que no hay secuenciarlos nuevamente.

Existe un protocolo *X.25* que define conexiones a una Red de Datos Públicos con Conmutación de Paquetes (PSPDN, Packet-Switched Public-Data Network). El protocolo define las conexiones físicas de la red y las de enlace de datos. Las redes X.25 trabajan a velocidades de hasta 64 Kbits/seg. Realizan una amplia comprobación de errores en cada nodo para asegurarse de que los datos se difundan correctamente a través de las poco fiables líneas telefónicas. En los países desarrollados,

las líneas son extremadamente fiables, así que está aumentando el uso de servicios rápidos que suprimen la comprobación de errores en los nodos. La red Frame Relay es un servicio de este tipo.

f) **Servicios Frame Relay.-** Es una innovación que emergió a partir de las especificaciones ISDN. Es un servicio orientado a circuitos, aunque también se trata como un servicio rápido de paquetes. Perfecciona las técnicas de conmutación de paquetes mediante la eliminación del procesamiento al nivel de red asociado al X.25. Típicamente, las redes de retransmisión de tramas poseen un rendimiento en el envío de datos de 1,544 Mbits/seg. aunque se tratan de implementar velocidades aún mayores.

La sobrecarga del X.25 se suele comparar con frecuencia con Frame Relay. Por ejemplo, en X.25, cada nodo del camino del paquete debe recibir la totalidad del paquete y realizar un test de errores sobre el mismo, antes de enviarlo. Los nodos de Frame Relay simplemente consultan en el encabezamiento del paquete cuál es su dirección de destino, e inmediatamente lo envían, en algunos casos incluso antes de haberlo recibido por completo. Frame Relay no requiere el uso de las tablas de estado que el X.25 emplea en cada nodo intermedio para el trato de la gestión, el control de flujo y la comprobación de errores. Los nodos finales detectan los fragmentos perdidos y solicitan su retransmisión.

g) **Servicios de conmutación.-** El mayor problema de cualquier servicio de conmutación es cómo ganar acceso a la facilidad de la compañía de telecomunicaciones que proporciona el servicio. Las conexiones entre dos usuarios cualquiera, uno de una LAN local y otro de una LAN remota, no están previstas en las redes públicas del emplazamiento del cliente, pero sí en el equipo de conmutación de la compañía de telecomunicaciones. Los clientes deben alquilar líneas dedicadas de tipo T1 o T3, con suficiente capacidad para comunicar el tráfico de datos locales multiplexados a la facilidad de conmutación de la compañía de telecomunicaciones, o usar líneas de conmutación como Switched-56 o las interfaces ISDN para acceder a la facilidad.

En principio, podría parecer poco coherente alquilar una línea dedicada para acceder a la facilidad de conmutación de la compañía de telecomunicaciones, si se posee una cuenta cuál es el propósito de estas facilidades, pero hay que tener presente que la distancia hasta la red de la compañía de telecomunicaciones es relativamente cualquiera a través de grandes distancias, con tarifas que son mucho menores que el costo de construcción de una red privada que salvase estas distancias grandes.

El problema, y lo que encarece a los servicios WAN actuales, es el requisito de que los clientes encaminen el tráfico a través de las facilidades de la Compañía de Telecomunicaciones para el Intercambio Local (LEC, Local Exchange Carrier) de su área, donde es recogido por las compañías de telecomunicaciones de larga distancia, a través de la

facilidad de Punto de Presencia (POP, Point of Presence). MCI y otras compañías que cubren grandes distancias planean aliviar esta situación construyendo facilidades alternativas en las mayores áreas metropolitanas.

Los actuales sistemas nacionales e internacionales de teléfonos son incapaces de manejar los cada vez mayores requerimientos de transferencias de multimegabits de datos para la informática de gran ancho de banda y los sistemas multimedia, éstas podrían ser algunas de las tecnologías y servicios que soportarán en el futuro las redes globales de datos, voz e imágenes. La cantidad del tráfico de datos en las redes, se incrementará a medida que lo hagan la potencia y la velocidad de los sistemas informáticos. Cuando la demanda crezca, las redes de datos llegarán a ser tan frecuentes y transparentes como lo son las redes de voz. La Red Optica Síncrona (SONET, Synchronous Optical Network) es una red transparente que posibilita esto. Define un estándar de multiplexación para la transmisión a través del cable de fibra óptica con velocidades en el rango entre 51 Mbits/seg. y 2488 Mbits/seg.

El Modo de Transferencia Asíncrono (ATM) transporta datos en las redes SONET. Multiplexa células de datos (paquetes de tamaño fijo) que proceden de diversas fuentes de la red física (SONET). ATM proporciona trayectos de comunicación virtual a través de la red SONET. Un circuito virtual orientado a la conexión entre dos puntos puede alcanzar velocidades de 45 Mbits/seg. a 622 Mbits/seg., aunque

la limitación habitual de las compañías de telecomunicaciones es de 45 Mbits/seg. La conmutación ATM es habitual en el nivel LAN de los concentradores cableados. También es frecuente su uso como una técnica de conmutación de las redes de telecomunicación internacionales y globales.

Por encima de ATM está la Red de Servicios Integrados de Banda Ancha (B-ISDN, Broadband-Integrated Services Digital Network). ATM es la base de B-ISDN. B-ISDN es un sucesor de ISDN que define cómo proporcionar la comunicación entre casa y oficinas a base de conmutación de circuitos, en incrementos de 64 Mbits/seg. B-ISDN usa la tecnología ATM y la red física SONET para difundir datos con una velocidad de transferencia entre 155 Mbits/seg. y 622 Mbits/seg., junto con diversos servicios al cliente. Otra oferta de las posibles es el Servicio de Conmutación de Datos Multimegabits (SMDS, Switched Multimegabits Data Service), que fue desarrollado por Bellcore, una división de investigación de las compañías regionales de operaciones Bell. SMDS se diseñó para que proporcione redes de datos públicas y privadas dentro de las áreas metropolitanas.

2.1.4 ENTORNOS DE RED

El sistema operativo y los protocolos que proporcionan servicios de comunicación y de red, definen el entorno de una red. Existen dos tipos básicos de sistemas operativos de red:

a) **Par a par.-** Este es un sistema operativo que permite a los usuarios compartir recursos en sus computadoras y acceder a los recursos compartidos en otras computadoras. Par a par implica que todos los sistemas poseen el mismo rango en la red. Ningún sistema es esclavo de otro.

b) **Servidor dedicado.-** En un sistema operativo de servidor dedicado, como Netware de Novell, una o más computadoras actúan exclusivamente como servidores de archivos dedicados y no realizan otras tareas.

A continuación se exponen algunos entornos genéricos de sistemas operativos de red:

a) Redes SNA par a par de IBM que ejecutan protocolos APPC/APPN.
b) Sistemas operativos UNIX par a par que ejecutan protocolos TCP/IP.
c) Sistemas Operativos de servidor dedicado para NetWare de Novell que ejecutan protocolos de comunicación SPX/IPX.
d) Entornos par a par de Windows NT y Windows para Grupos de Trabajo, que ejecutan protocolos de comunicación NetBios/NetBEUI o TCP/IP.

Para entender los entornos operativos de red, es útil compararlos con los entornos de procesamiento centralizado de computadora central (Mainframe)

y minicomputadora. En una red, los clientes acceden a programas y archivos en servidores centrales o servidores de pares, pero ejecutan estos programas en su propia memoria. Un sistema de computadora central o minicomputadora gestiona las tareas de procesamiento de los terminales unidos a ella. A éstos se les denomina a menudo terminales tontos debido a que no incluye procesador o memoria propios. Cada nuevo usuario que inicie la sesión en un sistema centralizado obtiene una parte de su capacidad de procesamiento y de este modo disminuyen las prestaciones.

Las redes son sistemas de procesamiento distribuido donde múltiples servidores y estaciones de trabajo realizan el procesamiento. En otras palabras, se puede ver toda la red como un conjunto de dispositivos de procesamiento. Los servidores son por regla general los dispositivos de mayor potencia de procesamiento de la red. Las redes y aplicaciones que reparten el procesamiento entre una estación de trabajo frontal (front-end), establecen relaciones cliente - servidor. El servidor ofrece tareas como almacenamiento y recuperación de archivos, gestión, compartición de impresoras y seguridad.

2.1.5 COMPONENTES DE UNA RED

Una red de computadoras consta tanto de hardware como de software. El hardware incluye tarjetas de la interfaz de red y el cable que las une. Los componentes software incluyen sistemas operativos, protocolos de

comunicación y controladores de la tarjeta de la interfaz de red del servidor, como se describen a continuación:

a) **Sistema operativo de red**.- En una red par a par, cada nodo de red ejecuta un sistema operativo con el soporte de conexión de red incorporado, el cual permite que los usuarios compartan archivos y periféricos. Normalmente también se incluyen características de seguridad y de gestión. El sistema operativo de red para una red dedicada, se ejecuta en servidores o estaciones de trabajo autónomos que ejecutan el software del cliente que se comunica con el servidor.

b) **Servidores**.- Los sistemas operativos de red modulares como NetWare de Novell pueden proporcionar alguno de o todos estos servicios en uno o más servidores, depende de qué componentes modulares elija instalar el administrador. Un servidor ofrece los siguientes servicios a los usuarios de la red:

- **Servidor de archivos:** Proporciona servicios de almacenamiento y recuperación de archivos, incluidas las utilidades de seguridad que controlan los derechos de acceso a los usuarios.

- **Servidor de correo electrónico o pasarela:** Ofrece servicios de correo electrónico de corporación extensa o local y traducción entre distintos sistemas de correo.

- **Servidor de comunicaciones:** Permite los servicios de conexión en sistemas de computadora central o de minicomputadora, o en sistemas y redes de computadoras remotas por medio de enlaces de área extensa.

- **Servidor de bases de datos:** Un servidor dedicado que gestiona las peticiones y respuestas del usuario de la base de datos.

- **Servidor de archivos:** Un sistema dedicado a copias de seguridad y almacenamiento de archivos en la red.

c) **Sistemas clientes (nodos o estaciones de trabajo).-** Estos sistemas clientes se unen a la red por medio de tarjetas de la interfaz de red. El sistema operativo que se ejecuta en la estación de trabajo puede incluir el software ya incorporado para soportar las tarjetas, o puede ser necesario cargar el software del cliente. El software del cliente redirecciona las peticiones de red de los usuarios o las aplicaciones al servidor.

d) **Tarjetas de la Interfaz de Red (NICs).-** Las estaciones de trabajo de las computadoras pertenecientes a redes Ethernet, anillo con testigo, ARCNET y a otras necesitan la instalación de una tarjeta de la interfaz de red. Hay algunas computadoras que ya incorporan estas interfaces. El cable de red se une a la parte de atrás de la NIC.

e) **Sistema de cableado**.- El sistema de cableado de red es el medio que conecta juntos servidores y estaciones de trabajo. No necesario el cable en las redes inalámbricas por radio o infrarrojos.

f) **Recursos y periféricos compartidos.-** Los recursos y periféricos compartidos incluyen dispositivos de almacenamiento unidos al servidor, unidades de disco óptico, impresoras, trazadores gráficos y otros equipos disponibles que utiliza cualquier usuario autorizado de la red.

2.1.6 TIPOS DE CONFIGURACIONES FISICAS Y TOPOLOGIAS DE RED

Para conectar una red, se necesitan tarjetas de la interfaz de red y cable (a menos que se considere la red inalámbrica). Hay diversos tipos de tarjetas de interfaz y esquemas de cableado.

El tipo de cable utilizado define las redes, la composición del cable o topología, las velocidades de transferencia de datos, los protocolos de comunicación y el método utilizado por los nodos para el acceso y el uso de la red (métodos de acceso). Es posible construir una inter-red que conecte una serie de redes mediante puentes, encaminadores y pasarelas.

Los tipos de redes más populares son Ethernet (de cable coaxial o de par trenzado), anillo con testigo, ARCNET y la Interfaz de Datos Distribuidos por Fibra (FDDI). La velocidad de transferencia de datos de un tipo de red es

por regla general un factor determinante. ARCNET trabaja a 2 Mbits/seg. anillo con testigo de 4 a 16 Mbits/seg. Ethernet a 10 a 100 Mbits/seg. y FDII a 100 Mbits/seg. En el pasado, el tipo de cable utilizado por un tipo de red fue un factor determinante, pero hoy día, la mayoría opera sobre cable de par trenzado adaptable y económico. FDDI utiliza cable de fibra óptica que incrementa el rendimiento de redes más rápidas.

Para permitir unir segmentos de red de tipos de redes similares o no se utilizan los puentes y encaminadores Los sistemas operativos del servidor NetWare de Novell, Windows NT, VINES de Banyan y otros han incorporado el puenteado y el encaminamiento. Cada NIC instalado en el servidor crea un segmento de red independiente y el sistema operativo gestiona el tráfico entre las redes.

2.1.6.1 TIPOS DE CABLES

El medio utilizado para transferir señales entre nodos de red es por regla general el cable de metal aislado, pero los métodos de comunicaciones inalámbricos y de fibra óptica tales como radio e infrarrojos ofrecen otras alternativas. Existen varios tipos de cables que se describen a continuación:

a) **Cable coaxial.-** Este tipo de cable, similar en la construcción al cable de TV por cable, fue uno de los primeros tipos de cables utilizados por las redes. Proporciona velocidades de

transferencia de datos relativamente altas (10 a 20 Mbits/seg.), a bajo costo y algo de inmunidad ante interferencias externas.

El cable coaxial se utiliza en la conexión de redes con topología en bus, como Ethernet (con cable coaxial RG-58) y ARCNET (con cable coaxial RG-62). El cable consta de un núcleo de hilo de cobre rodeado por un aislante. Todo ello se envuelve con hilos de cobre trenzado u hojas metálicas, lo que sirve de pantalla entre las señales externas y la radiación procedente de las señales internas. Una cubierta exterior de plástico rodea al conjunto.

Este tipo de cable consta de un núcleo de cobre sólido rodeado por un aislante, una especie de combinación entre pantalla y cable de tierra y un revestimiento protector exterior, según se muestra en la figura 10. En el pasado, el cable coaxial permitió una transmisión más alta (10 Mbits/seg.) que el cable de par trenzado, aunque las recientes técnicas de transmisión sobre par trenzado igualan e incluso superan la velocidad de transmisión por cable coaxial. Sin embargo, los cables coaxiales pueden conectar los dispositivos de la red a distancias más largas que los de par trenzado.

b) Cable de fibra óptica.- Este tipo de cable también crece en popularidad, debido a sus altas velocidades de transferencia y

seguridad (no emite señales y se pueden detectar los cables "pinchados").

El cable de fibra óptica utiliza fotones en la transmisión de las señales digitales. Un cable de fibra óptica se fabrica con vidrio puro, que no impone resistencia alguna al paso de los fotones a su través. El cable de cobre está sujeto a los siguientes problemas:

- Las *transmisiones* de la señal a largas distancias se encuentran sujetas a atenuaciones, que consiste en una pérdida de la amplitud o intensidad de la señal, lo que limita la longitud del cable.
- La *capacitancia* es una característica no deseada que puede producir distorsión sobre el cable. Cuanto mayor es la longitud del cable o el espesor del aislante, mayor es la capacitancia y la distorsión resultante.
- La *diafonía* constituye la mayor fuente de ruido en cables de par trenzado. Se origina por la pérdida de la señal entre cables adyacentes.

El cable de fibra óptica es resistente a la interferencia electromagnética y no genera radiación por si solo. El cable de cobre irradia energía, que puede recogerse. Las escuchas

ilegales pueden detectarse debido a la variación de la intensidad de la señal que viaja por el cable.

Este cable utiliza luz para transmitir las señales a través de una hebra de vidrio muy transparente. El núcleo óptico consiste en dióxido de silicio puro. Las señales de las computadoras se envían a través de este cable mediante la conversión de los 1s y 0s en códigos ópticos. En un extremo de un cable de fibra óptica se sitúa un diodo emisor de luz y un fotodetector percibe el destello de luz en el otro extremo, convirtiéndolo en una señal eléctrica.

c) **Cable de par trenzado.-** El cable de cobre de par trenzado ha ganado popularidad debido a su bajo precio y fácil instalación. Los nuevos estándares para grado de datos estimulan las velocidades de transferencia de datos hasta y por encima de los 100 Mbits/seg.

El cable de par trenzado consta de dos hilos de cobre aislados que se trenzan uno alrededor del otro. Los hilos se encuentran trenzados por pares, de forma que cada par forma un circuito que puede transmitir datos. Un cable consta de un haz de uno o más pares trenzados rodeados por un aislante. El Par Trenzado sin Apantallar UTP (unshielded twisted pair) es usual en la red telefónica, y el Par Trenzado Apantallado STP (shielded twisted

pair) proporciona protección frente a la diafonía. Precisamente es el trenzado el que previene los problemas de interferencia. Son posibles velocidades de transmisión elevadas (100 Mbits/seg.) si se ha instalado cable de grado de datos (de categoría 5). El cable de par trenzado debe mantenerse durante todo el recorrido entre los puntos extremos de la conexión. El cable de par trenzado se utiliza usualmente en redes con topología Ethernet, en anillo con testigo y otras. Se dispone de cable de par trenzado en las siguientes categorías:

- **Categoría 1:** Cable tradicional de par trenzado sin apantallar para teléfono, adecuado par la transmisión de voz pero no de datos. La mayoría del cable telefónico instalado antes de 1983 entra en esta categoría.
- **Categoría 2:** Cable de par trenzado sin apantallar certificado para la transmisión de datos hasta 4 Mbits/seg. este cable incluye cuatro pares.
- **Categoría 3:** Admite una velocidad de transmisión de 10 Mbits/seg., requisito para redes en anillo con testigo (4 Mbits/seg) y Ethernet 10Bse-T a 10 Mbits/seg. Este cable incluye cuatro pares y tres rizos por pie.
- **Categoría 4:** Certificada la transmisión a 16 Mbits/seg., lo que constituye la calidad mínima aceptable para redes en anillo con testigo a 16 Mbits/seg. El cable incluye cuatro pares.

- **Categoría 5:** Define al cable de cobre de 100 ohmios de cuatro pares trenzados, que puede transmitir datos a 100 Mbits/seg., lo que constituye un requisito para nuevas tecnologías basadas en Ethernet y en el modo de transferencia asíncrono ATM. El cable incluye una baja capacitancia y exhibe un bajo nivel de diafonía.

Como se muestra n la figura 10, se describen los tipos de cables genéricos utilizados en los sistemas de comunicación de red.

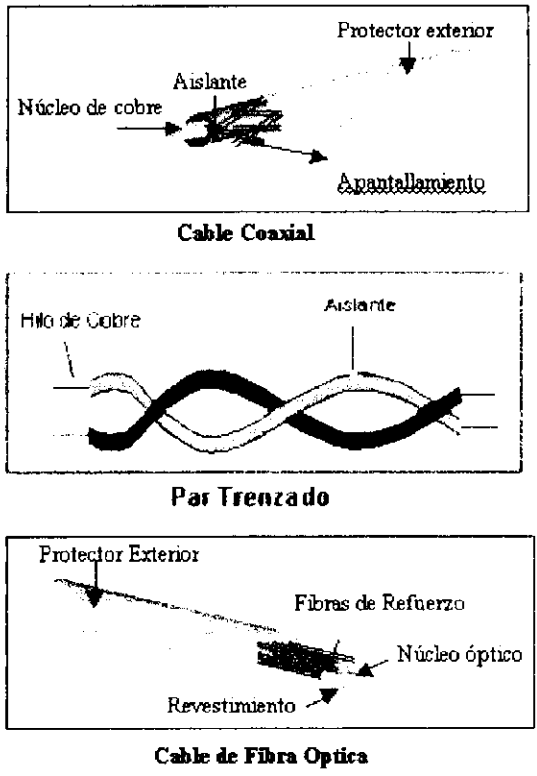


Figura 10. Tipos de Cables para comunicación de red

d) Cable estructurado.- Es un sistema de cableado preplanificado que está pensado para hacer frente a las reconfiguraciones y el crecimiento. La Asociación de Industrias Electrónicas EIA y la

Asociación de Industrias de Telecomunicaciones TIA desarrollaron una norma para el cableado de telecomunicaciones en edificios comerciales denominada Normativa 568 de Cableado para Edificios Comerciales de EIA/TIA. Esta norma proporciona un sistema de cableado uniforme que es apto para los entornos y los productos de diferentes vendedores.

El cableado estructurado conforma una infraestructura con caminos para las partes críticas de la red. El sistema incluye cables, conectores de comunicación, enchufes, conectores, adaptadores, baluns (equilibrado – no equilibrado), sistemas de paneles de parches y componentes electrónicos. Idealmente, proporciona un medio para la transmisión de datos, video, voz y otros tipos de información. Los sistemas de cableado estructurado están basados en normas. Están definidas las distancias, las topologías y las especificaciones físicas de forma que se cumplan los requisitos de cableado que luego se puedan presentar; de esta forma, es posible realizar el cableado de un edificio sin conocer de antemano los equipos de comunicación de datos que lo utilizarán. El tendido de los cables es sencillo de administrar y los fallos son fáciles de localizar.

Los métodos inalámbricos permiten la informática móvil, tanto interior como exterior, dependiendo del método utilizado. Aunque disminuyan las velocidades de transmisión y sea

necesaria una línea de actuación (infrarrojos), los métodos inalámbricos ofrecen ventajas y ahorro de costos en los casos donde no es necesario el cableado. Las conexiones de red móvil para usuarios remotos se hacen populares con las técnicas de paquetes de radio y celulares.

2.1.6.2 ARQUITECTURA DE RED

La topología, el método de acceso al cable y los protocolos de comunicación utilizados definen la arquitectura de una red. Antes de que cualquier estación de trabajo pueda acceder al cable, debe establecer sesiones de comunicación con otros nodos en la red. El método de acceso al cable de una red define cómo una estación de trabajo establece el acceso a medios compartidos y así puede transmitir información. Los *protocolos* son las reglas y procedimientos que los sistemas utilizan para comunicarse unos con otros sobre la red.

Las arquitecturas de red definen como se enlazan juntos los equipos de computadoras y otros dispositivos para formar un sistema de comunicaciones que permita a los usuarios compartir información y recursos. Hay arquitecturas de red propietarias como la Arquitectura de Sistemas de Red o SNA (System Network Architecture) de IBM y la Arquitectura de Red Digital o DNA (Digital Network Architecture) de DEC, y hay arquitecturas abiertas como el Modelo de

Interconexión de Sistemas Abiertos u OSI (Open System Interconnection) definido por la Organización Internacional de Normalización o ISO (International Organization for Standatization).Las arquitecturas de red se caracterizan por los niveles. Si la norma abierta, proporciona un camino para que los fabricantes diseñen software y hardware interoperables con los productos de otros fabricantes. Sin embargo, el modelo OSI ha quedado como un modelo, en lugar de cómo una norma internacional completamente aceptada. Debido a la extensa variedad de normas de factor existentes, la mayoría de los fabricantes simplemente han decidido adoptar los diversos protocolos que se usan en al industria antes de ajustarse a una norma.

Las capas especifican los distintos servicios y funciones de los niveles en una "pila de protocolos". Los protocolos definen cómo tiene lugar la comunicación, por ejemplo los flujos de datos entre sistemas, la detección y la corrección de errores, el formateado y empaquetado de datos y demás utilidades. La estructura básica se muestra en la figura11.

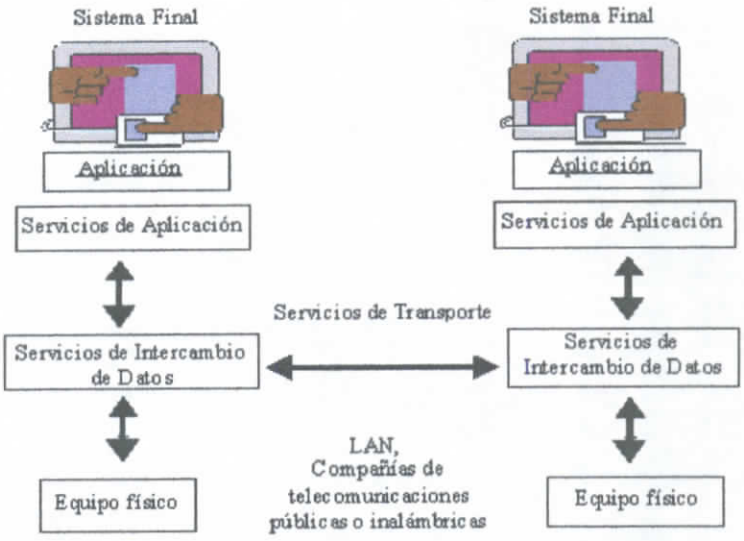


Figura 11. Arquitectura de red

La comunicación es el principal objetivo de cualquier arquitectura de red. En el pasado, un fabricante estaba más preocupado en asegurarse de que sus propios protocolos podían comunicarse, que de haber abierto la arquitectura para que así otros fabricantes pudiesen producir productos compatibles. Compatibilizarlos era a menudo difícil. En cualquier caso, los protocolos especifican un conjunto de reglas y procedimientos que definen cómo tiene lugar la comunicación en los distintos niveles de funcionamiento. Los niveles definen las conexiones físicas, entre las que se incluyen el tipo de cable, el método de acceso y la topología, y cómo se envían los datos sobre la red. Además, son protocolos que establecen las conexiones y mantienen las sesiones de comunicación y, todavía más son protocolos que definen cómo las aplicaciones acceden a las funciones de

comunicación de los niveles inferiores de red e interoperan con las aplicaciones de los otros sistemas unidos a la red.

Como ya se ha mencionado, el modelo OSI se ha convertido en el modelo con el cual se comparan todos los otros protocolos y arquitecturas de red. El propósito del modelo OSI es coordinar las normas de comunicación entre fabricantes. Aunque muchos fabricantes han seguido con sus propias normas, otros, como DEC e IBM, han integrado OSI en sus estrategias de conexión de red junto con normas de Internet como TCP/IP.

Mientras se conectan LANs en redes corporativas extensas la interoperatividad será la principal preocupación. Se utilizan distintas técnicas para realizar esto, entre las que se incluyen la utilización de múltiples protocolos en un único sistema o de técnicas que ocultan los protocolos con un nivel de Middleware. El Middleware también puede proporcionar una interfaz que permita el intercambio de información entre diferentes aplicaciones en distintas plataformas. Con la utilización de estas técnicas, los usuarios pueden acceder, desde sus aplicaciones de equipos de escritorio, a los productos de múltiples vendedores.

A continuación se describen los componentes que definen la arquitectura de red:

a) Topologías.- Se puede considerar una topología de red como un mapa de la distribución de cables. La topología define cómo se organiza el cable en las estaciones de trabajo individuales y desempeña un papel importante en la decisión que se tome sobre el cable. Una red puede tener una topología lineal, en anillo o en estrella. Se debe considerar la topología de una red cuando se tomen decisiones sobre qué tipo de red instalar. Como se describe aquí, la topología equivale a cómo se instalará el cable a través de las paredes, suelos y techos de un edificio.

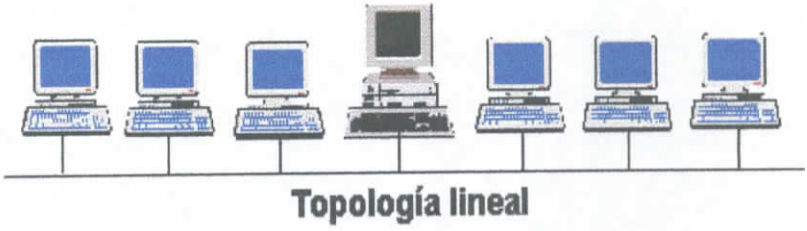


Figura 12. Topología lineal

Como se muestra en la figura 12 una *topología lineal* consta de un único cable que se extiende de una computadora a la siguiente en un modo serie. Los extremos del cable terminan con una resistencia. Las redes coaxiales de Ethernet utilizan topología lineales. Aunque es fácil de instalar, una rotura en cualquier parte del cable inutiliza toda la red.

Figura 13. Topología en estrella.

Se muestra figura 13 una *topología en estrella*, todos los cables parten de una única localización, como un servidor de archivos o un armario central de cableado. Las topologías en estrella necesitan un cable por cada estación de trabajo, pero un cable roto sólo desconecta la estación enlazada a él. Las redes Ethernet 10Base-T y en anillo con testigo usan topologías en estrella, aunque internamente, en anillo con testigo es una red en anillo.

Figura 14. Topología en anillo

Se muestra en la figura 14 una *topología en anillo*, el cable de red se conecta circularmente y las señales viajan en un anillo. Las topologías en anillo físico son raras. Anillo con testigo y ARCNET son redes en anillo lógico.

b) **Método de acceso al cable.-** Describe cómo una estación de trabajo establece el acceso al sistema de cables. Cuando la tarjeta de la interfaz de red obtiene el acceso al cable, comienza el envío de paquetes de información en un formato de trama como flujos de bits sobre la red.

Los sistemas de cable lineales como Ethernet utilizan el método de Acceso Múltiple con Detección de Portadora/Detección de Colisión (CSMA/CD, Carrier Sense Multiple Access/Collision Detection), donde una estación de trabajo accede al cable pero se retira si otra estación de trabajo intenta el acceso al mismo tiempo. Una estación de trabajo transmite una señal y cada uno de los otros nodos de la red la oye, pero solo el nodo direccionado presta atención. Si dos nodos transmiten al mismo tiempo, se produce una colisión y ambos se retiran, esperan una cantidad aleatoria de tiempo y lo intentan de nuevo. Las prestaciones se degradan cuando el tráfico de la red es pesado, debido a estas colisiones y a las retransmisiones. Las redes en anillo normalmente utilizan un método de paso de testigo en el cual una estación sólo pasa a utilizar la red cuando está en

posesión del testigo. Considérese un testigo como un billete o paso temporal para utilizar la red. Cuando una estación de trabajo esta lista para transmitir, debe esperar que el testigo esté disponible y entonces cogerlo. Esto evita que dos máquinas utilicen el cable simultáneamente.

c) **Protocolos de comunicación.-** Los protocolos de comunicación son las reglas y procedimientos utilizados en una red para comunicarse entre los nodos que establecen el acceso al sistema de cable. Los protocolos controlan dos niveles de comunicación diferentes. Los protocolos de nivel superior definen cómo se comunican las aplicaciones y los protocolos de nivele inferior y cómo se transmiten las señales por un cable. Hay protocolos entre estos niveles que establecen y mantienen sesiones de comunicación, se pueden comparar con los protocolos diplomáticos, donde los diplomáticos de rangos diferentes negocian los protocolos de red, los fabricantes pueden diseñar y fabricar fácilmente productos de red que trabajen en sistemas de múltiples vendedores.

2.1.6.3 DISPOSITIVOS DE CONEXION DE REDES

Los sistemas de cableado de red poseen limitaciones de distancia debido a la pérdida de señal y otras características eléctricas. Se puede extender la distancia de un segmento de red si se añade un repetidor,

que regenere la señal eléctrica y doble la longitud permitida del cable. Un repetidor puede no permitir añadir más estaciones de trabajo a una red ampliada que las definidas en las especificaciones de red. A menudo se usa un repetidor para conectar la estación de trabajo de un almacén o sucursal con la oficina principal.

Los segmentos de red separados se pueden unir con un puente (bridge). Un puente es un dispositivo autónomo o que puede existir en los servidores de la red. Por ejemplo, se puede realizar un puente en un servidor de NetWare si se instalan dos tarjetas de red. Los puentes incluyen la capacidad de mantener el tráfico local y transferir solo los paquetes destinados a otros segmentos sobre el enlace. Esto ayuda a reducir el exceso de tráfico de la red. Un encaminador (router) proporciona un nivel de interconectividad mayor que el ofrecido por los puentes. Un encaminador puede leer la información de direccionamiento de un paquete que le ayude a determinar el mejor camino posible que le llevará a su destino, cuando una red tenga muchos enlaces o caminos distintos.

Los concentradores (hubs) o centros de cableado se utilizan para construir sistemas de cableado estructurado. Un concentrador es una disposición central en el esquema de cableado configurado en estrella. Típicamente, el concentrador posee un bus que acepta conexiones Ethernet, anillo con testigo, FDDI u otros tipos de módulos. Estos módulos incluyen múltiples puertos para las estaciones de trabajo de

la red. Normalmente, los concentradores se instalan en un departamento y todas las computadoras de ese departamento se conectan a él. Después, los concentradores de departamento se conectan a los concentradores corporativos lo que forma un esquema de cableado jerárquico.

2.1.6.4 METODOS DE CONEXION MAN Y WAN

Las Redes de Area Metropolitana (MAN, Metropolitan Area Network) y las Redes de Area Extensa (WAN, Wide Area Network) proporcionan conexiones entre diversas zonas geográficas. Las MANs son por lo general redes de fibra óptica de alta velocidad, que conectan segmentos LAN dentro de un área metropolitana. Un método alternativo es la utilización de los esquemas de conexión de red privada, como los sistemas de microondas. Las antenas de microondas se instalan en el tejado de los edificios y se apuntan unas a otras para establecer un enlace inter red.

WANs ofrecen conexiones por todo el país o mundiales por medio de satélites y líneas telefónicas. Las corporaciones grandes que poseen oficinas regionales o por todo el mundo utilizan WANs para interconexión de redes. Los circuitos dedicados se alquilan a las compañías de telecomunicaciones de larga distancia para proporcionar conexiones durante todo el tiempo entre los sistemas. En cambio, las conexiones de conmutación de circuitos o de conmutación de

paquetes, que operan a menor costo y ofrecen mayor flexibilidad, están disponibles para aplicaciones de utilización y conexión. El actual paradigma de red es la red multiprotocolo (heterogénea) y de múltiples vendedores, antes que el entorno de los sistemas abiertos, donde todos los vendedores fabrican equipos compatibles. Las redes heterogéneas se construyen por toda la corporación y se conectan distintas gamas de sistemas, incluidos LANs de departamentos y grupos de trabajo, además de sistemas colectivos de computadora central y minicomputadora. En este entorno, los administradores de la red se enfrentaban a la tarea de hacer que los distintos sistemas interoperasen. Para realizar esto, se dio soporte a diversos protocolos de comunicación e incluso se usaron productos Middleware, que ocultan los protocolos a los usuarios y aplicaciones.

Aunque los recursos informáticos de la red física se distribuyen entre los departamentos y divisiones de una compañía, la responsabilidad y gestión de estos recursos están a cargo de un gestor de la red corporativa. Esto se debe a que la red corporativa se diseñó para ayudar a toda la organización a conseguir sus objetivos, entre los cuales se incluye que cualquier usuario de cualquier parte de la organización comparta datos y recursos. Las LANs departamentales pueden mantener todavía su autonomía, así los gestores locales pueden definir derechos de seguridad y proteger los datos locales de usuarios no autorizados. No obstante, el gestor corporativo dirige los

departamentos hacia la meta común de la integración de toda la compañía.

La nueva red se construye con concentradores, sistemas de cableado estructurado, soportes multiprotocolos colapsados y conexiones de área extensa de alta velocidad que permite a los usuarios de zonas remotas al acceso a las redes colectivas con poca demora. Las estaciones de trabajo pueden operar con Prestaciones de 100 Millones de Instrucciones por Segundo (MIPS, Millon Instructions Per Second) con cientos de megabytes de RAM o gigabytes de espacio de memoria disponible en disco. El rendimiento del servidor crece para satisfacer las altas demandas de los usuarios. Es cada vez más frecuente la utilización de servidores de muy alta velocidad que usan procesadores múltiples que se ejecutan a 200 MHz y proporcionan 300 MIPS y mayores. Ahora, los sistemas de computadora central y minicomputadoras se ven como potentes servidores que se enlazan directamente a la red.

El soporte de múltiples protocolos de comunicación en las computadoras pertenecientes a la red ha resultado muchas de las diferencias de los niveles inferiores de comunicación. Ahora, los administradores se preocupan de elevar el nivel de interoperatividad del nivel de aplicación del modelo de protocolos OSI. El objetivo es permitir que los usuarios ejecuten diversas aplicaciones en una serie de plataformas para acceder a los datos de toda la red corporativa sin

preocuparse de otros temas como son la interfaz, traducción y conversión. El Middleware facilita el desarrollo de aplicaciones que creen el software para estos nuevos entornos y proporciona un nivel normalizado de programación, que oculte al programador la complejidad de las redes y de los protocolos de múltiples vendedores. Los niveles ofrecen Interfaces de Programación de Aplicaciones (APIs, Application Program Interfaces) de alto nivel.

El Entorno de Informática Distribuida (DCE, Distributed Computing Environment) desarrollado por la Fundación de Software Abierto, proporciona herramientas que ayudan a los administradores a integrar entornos heterogéneos. El entorno abierto colaborativo de Apple y la arquitectura de sistemas abiertos de Windows de Microsoft son estrategias para construir redes corporativas. Los entornos orientados a objetos, como Cairo de Microsoft, trabajan con el objetivo de proporcionar acceso a los datos por medio de las tecnologías orientadas a objetos. En un entorno orientado a objetos, se combinan datos y métodos para trabajar sobre un único objeto. La importancia de los objetos se debe a que se pueden usar sobre plataformas software y hardware. Los usuarios pueden acceder a los objetos en sistemas de otras localizaciones mediante el uso de una serie de interfaces de aplicación. Este planteamiento global permite que se desarrollen aplicaciones más fácilmente para el acceso a las bases de datos distribuidas.

Las plataformas de gestión centralizada son necesarias en estos entornos informáticos. Reducen el número de utilidades y paquetes de gestión que se deben aprender, y la gestión centralizada, lo que ayuda a reducir la cantidad de administradores necesarios.

2.1.6.5 SISTEMA DE RED ETHERNET

El sistema de red Ethernet fue originalmente creado por Xerox, pero desarrollado conjuntamente como una norma en 1980 por Digital Equipment Corporation, Intel y Xerox. Esta norma se conoció como DIX Ethernet, haciendo referencia a los nombres de quienes lo habían desarrollado. La norma 802.3 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define una red similar, aunque ligeramente diferente, que utiliza un formato alternativo de trama (una trama constituye la estructura de codificación de un flujo de bits transmitidos a través de un enlace). Puesto que la norma 802.3 de IEEE se ha adoptado por la Organización Internacional de Normalización ISO.

Ethernet presenta un rendimiento de 10 Mbits/seg., y utiliza un método de acceso sensible a la señal portadora, mediante el que las estaciones de trabajo comparten un cable de red, pero solo una de ellas puede utilizarlo en un momento dado. El Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones CSMA/CD se utiliza para arbitrar el acceso al cable.

El comité 802.3 de IEEE es el responsable de la definición del nivel físico en la pila de protocolos OSI. Este nivel se divide en dos subniveles denominados Subnivel de control de acceso al medio MAC y Subnivel de enlace de datos Data-link. Las redes CSMA/CD, en anillo con testigo y en bus con testigo pueden conectarse al nivel MAC, actuando el nivel de enlace de datos como puente que puede transferir paquetes entre redes si es necesario.

Todas las adaptaciones de la norma 802.3 del IEEE presentan una velocidad de transmisión de 10 Mbits/seg., con la excepción de 1Base-5, que permite la transmisión a 1 Mbits/seg. Pueden conectarse hasta 8.000 estaciones de trabajo en una única red de área local. Debido a que 10Base-5, 10Base-2 y 10Base-T son las topologías más populares. El primer nombre se refiere a la velocidad en Mbits/seg., y el último a los metros que admite en segmento (multiplicado por 100). Base hace referencia a banda base y Broad a banda ancha.

A continuación se describen las diferentes clases de cable coaxial utilizado en el sistema de red Ethernet:

a) **10Base-5.-** Cable coaxial con longitud máxima de segmento de 500 metros; utiliza métodos de transmisión de banda base.
b) **10Base-2.-** Cable coaxial (RG-58 A/U) con longitud máxima de segmento de 185 metros; utiliza métodos de transmisión en banda base.

c) **10Base-T**.- Cable de par trenzado con longitud máxima de segmento de 100 metros.

d) **1Base-5.-** Cable de par trenzado con longitud máxima de segmento de 500 metros y velocidad de transmisión de hasta 1 Mbits/seg.

e) **10Broad-36.-** Cable coaxial (RG-59 A/U CATV) con longitud máxima de segmento de 3.600 metros; utiliza métodos de transmisión de banda ancha.

f) **10Base-F.-** Sirve de soporte a redes soporte de fibra óptica de hasta 4 kilómetros con transmisión a 10 Mbits/seg. la EIA/TIA ha adoptado este cable para establecer conexiones cruzadas entre los edificios de un campus, en su normativa de cableado para edificios comerciales.

g) **100Base-X**.- Una nueva norma Ethernet que presenta un rendimiento de 100 Mbits/seg. y utiliza el método de acceso CSMA/CD sobre configuraciones jerárquicas de cableado de par trenzado.

h) **100 VG-AnyLAN.-** Una nueva norma Ethernet que presenta un rendimiento de 100 Mbits/seg. y utiliza el método de acceso de prioridad bajo demanda, sobre configuraciones jerárquicas de cableado de par trenzado.

La topología de las redes Ethernet 802.3, con excepción de las realizaciones 100 VG-AnyLAN, consiste en un bus lineal que utiliza el método de acceso CSMA/CD. En las realizaciones sobre cable

coaxial, las estaciones de trabajo se conectan en serie conectando los segmentos de cable entre cada estación. Los segmentos forman un único y extenso sistema de cableado, denominado línea troncal. La versión de cable trenzado de Ethernet (10Base-T) adopta una topología en estrella, en la que el cable trazado hacia cada estación es una rama que parte de un concentrador central de cableado.

El sistema de red Ethernet posee las siguientes características:

a) **Acceso Múltiple con Detección de Portadora y Detección de Colisiones CSMA/CD.-** Los adaptadores Ethernet realizan la transmisión de los paquetes sobre la red compartida cuando son los únicos que poseen el acceso al cable. La detección de colisiones se refiere al método utilizado para solucionar accesos simultáneos al cable. Cuando éste no se utiliza, dos estaciones pueden intentar acceder a él al mismo tiempo. Si ambas comienzan la transmisión de datos se produce una colisión, que puede causar la corrupción de los datos. En el protocolo CSMA/CD, existe un mecanismo que detecta la colisión, con lo que las dos estaciones esperan durante un intervalo aleatorio de tiempo e intentan de nuevo la transmisión.

   El método CSMA/CD es eficiente cuando el tráfico de la red es ligero. Al aumentar dicho tráfico se producirán más colisiones. Las estaciones de retiran y retransmiten de nuevo, pero si la red

sigue ocupada, este proceso continúa y crece, originando una caída de prestaciones y una lentitud percibida por los usuarios. Una solución consiste en reducir el número de estaciones en cada segmento de la LAN. Si se adopta la técnica de microsegmentación, que requiere la utilización de concentradores de conmutación, una única estación de trabajo ocupará cada segmento de la red, lo que elimina totalmente el fenómeno de contención.

La aparición de colisiones es un factor que impone un límite en la longitud de la línea troncal de un segmento Ethernet. La distancia máxima es de 2.500 metros. Las líneas troncales dentro de estos límites están sujetas a retardos en la propagación de la señal, que pueden originar un fallo en el mecanismo de detección de colisiones. Dos estaciones situadas en los extremos opuestos de un cable que no cumpla estos límites y que intenten acceder al cable al mismo tiempo podrían no darse cuenta del intento de acceso de la estación contraria. Un fallo en la detección de un acceso múltiple origina la corrupción de los datos y puede bloquear el segmento de la red.

b) Segmentación.- Es el proceso de división de un segmento Ethernet en dos o más segmentos, reduciéndose de esta manera el número de estaciones de trabajo conectadas a cada uno de los segmentos y mejorándose así las prestaciones. Generalmente, se

realiza la división de un segmento y se utiliza un puente o un encaminador para conectar los dos segmentos, gestionando así el tráfico entre las redes.

La segmentación se convierte en un tema importante al conectarse a la red nuevos usuarios, debido especialmente a aquellos usuarios que necesitan un ancho de banda alto. Las aplicaciones de video son las que requieren la mayoría del ancho de banda. Además, las imágenes en movimiento son sensibles al tiempo y deben tener prioridad, lo que reduce las prestaciones de las otras. Los usuarios de este tipo de aplicaciones pueden así compartir sus propios segmentos.

Netware, Windows para trabajos en grupo, Windows NT y sistemas operativos de red similares disponen de utilidades de encaminamiento incorporadas. Cada adaptador de red situado en un servidor forma un segmento separado de red. Cada tema operativo gestiona el tráfico entre los segmentos. Un servidor puede incluir dos tarjetas de interfaz de red instaladas, que trabaja con topologías Ethernet tipos bus y estrella. La elección de una u otra topología depende del diseño del entorno de oficina y del tipo de cable a utilizar.

El filtrado constituye una parte importante en el esquema de la segmentación. Una vez dividida una red con objeto de reducir el

tráfico y mejorar las prestaciones, se filtran los paquetes para reducir el tráfico en las redes no compatibles con esos paquetes. Un inconveniente a esta esquema de interconexión de redes es que los puentes y encaminadores introducen cierto retardo en la transferencia de paquetes entre redes. Los concentradores de conmutación pueden eliminar este problema de retardo.

c) **Concentradores de conmutación Ethernet.-** Amplía el concepto de segmentación, al ofrecer microsegmentación en un único dispositivo. De esta forma, una única estación de trabajo puede disponer de un enlace directo y no compartido con un servidor o con otro dispositivo, reduciéndose el fenómeno de contención y proporcionándose la velocidad máxima de 10 Mbits/seg. sobre la red. Las redes que poseen estaciones de trabajo de ingeniería o multimedia pueden beneficiarse del alto rendimiento posibilitado por los concentradores de conmutación.

Dichos concentradores de conmutación son dispositivos de baja latencia que realizan conmutación matricial. Muchos concentradores de conmutación también disponen de conexiones dedicadas de alta velocidad para servidores, como una interfaz a FDDI a 100 Mbits/seg. La razón para ello es que el rendimiento estándar de 10 Mbits/seg. en Ethernet es normalmente inadecuado para las necesidades de un servidor. La conexión de

un super servidor con multiprocesamiento, que trabaja a muchos millones de instrucciones por segundo a una red de baja velocidad es una operación ridícula. Si se analizan las cifras involucradas, FDDI puede proporcionar 100 Mbits/seg.

d) **Formatos de trama.-** Una trama Ethernet representa la estructura de un paquete de datos enviado a través de una red Ethernet. Describe la posición de las cabeceras, bits de datos y la carga útil de información del paquete. Comprender los tipos de trama es importante si se desea conectar un analizador de protocolos a una red para realizar una supervisión del tráfico de la misma. Es posible descubrir ciertos problemas en una red observando el contenido de los paquetes y reuniendo estadísticas al respecto.

Existen cuatro tipos de trama en Ethernet:

- **Ethernet_II:** El tipo de trama original de Ethernet. Asigna una única cabecera al paquete, el utilizado en las redes Apple Talk Phase I y las redes conectadas a sistemas DEC o a computadoras que utilizan el protocolo TCP/IP.
- **Ethernet 802.3:** El tipo de trama utilizado genéricamente en redes Netware de Novell.
- **Ethernet 802.2:** El tipo de trama utilizado por defecto en redes Netware 4.x de Novell.

- **Ethernet _SNAP:** El tipo de trama utilizado en redes AppleTalk Phase II.

Como se muestra en la figura 15, en la parte superior de la figura se indica la trama original de Ethernet_II, y en la parte inferior la trama IEEE 802.3. Los campos más importantes de las tramas se describen a continuación:

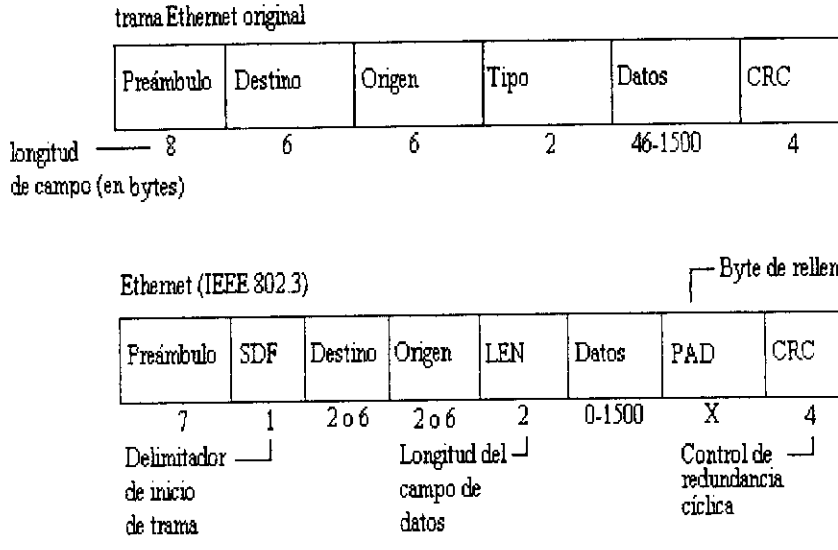


Figura 15. Tipos de trama en Ethernet

- **Preámbulo:** Este campo señala el comienzo de la trama.
- **Delimitador de Inicio de Trama SFD (Start Frame Delimiter):** Este campo proporciona un campo adicional que indica el comienzo de la trama Ethernet IEEE 802.3.
- **Destino y origen:** Estos campos mantienen la dirección original y de destino.

- **Longitud (LEN) del campo de datos:** Este campo indica la longitud de la porción de datos de la trama.
- **Control de Redundancia Cíclica (CRC, Cyclical Redundancy Chesksum):** Este campo mantiene un valor calculado por el emisor. El receptor realiza el mismo cálculo para ver si coincide con el valor del campo CRC. Si no es así, se considera que la trama se ha corrompido y se retransmite de nuevo.

El sistema de red Ethernet más utilizado en el cable coaxial es de *Ethernet 10Base-T (Par trenzado)*. Ofrece la mayoría de las ventajas de Ethernet sin las restricciones y el costo que impone el cable coaxial. Además, la topología en estrella o distribuida permite la conexión de grupos de estaciones de trabajo departamentales o situadas en otras zonas.

Parte de la especificación 10Base-T es incompatible con otras normas 802.3 del IEEE, de modo que es sencillo realizar una transición de un medio a otro. Es posible mantener las mismas tarjetas Ethernet al pasar de cable coaxial a cable de par trenzado. Además, pueden añadirse líneas troncales de par trenzado a las ya existentes, gracias a repetidores que admiten la conexión de líneas troncales de cable coaxial, fibra óptica y par trenzado. Muchos fabricantes presentan este tipo de dispositivos en sus líneas de productos Ethernet.

Las estaciones 10Base-T utilizan cable de Categoría 3, aunque categorías superiores de cable (como la categoría 5) permiten un crecimiento futuro que acepta tecnologías de transmisión más rápidas, como 100 Mbits/seg. La mayoría de las tarjetas 10Base-T tienen actualmente incorporado el receptor, conectándose directamente al cable RJ-45.

Los componentes que se describen forman parte típicamente de las redes 10Base-T. Manténgase en mente la idea de que un sistema no siempre necesita todos estos componentes:

a) **Tarjeta de interfaz de red.-** Es necesaria una tarjeta Ethernet con un conector tipo DIX de 15 patillas o RJ-45 10Base-T. Hay que añadir una PROM de arranque remoto si se instala la tarjeta en una estación de trabajo sin disco.

b) **Concentrador (HUB).-** El concentrador dispone a menudo de hasta 12 puertos. Normalmente dispone de un puerto de conexión a redes soporte de cable coaxial o de fibra óptica.

c) **Cable de par trenzado.-** 10Base-T utiliza cable de par trenzado con conectores RJ-45 de hasta 100 metros de longitud. Puede adquirirse cable a granel y conectores aparte para construir segmentos de distintas longitudes según las necesidades. Para ello se necesita una herramienta especial par RJ.

d) **Transceptor.-** El transceptor dispone de un conector RJ-45 en un lado y uno DB-15 en el otro. Por otra parte, la mayoría de las tarjetas actuales presentan un transceptor ya incorporado.

e) **Cable para el transceptor.-** Este cable se conecta al transceptor en la parte posterior de la tarjeta de interfaz de red.

f) **Cable conector al bloque de conexión.-** Si va a utilizarse el cable telefónico preexistente, un cable de 50 patillas Telco (que conecta al concentrador directamente a un bloque de conexión) simplifica la instalación. Esto hay que consultarlo con el fabricante del concentrador.

g) **Enchufe de pared.-** Se trata de un conector con una clavija RJ. Si también se necesita una conexión telefónica, pueden adquirirse placas dobles.

Hay que darse cuenta de que algunas especificaciones del cable 10Base-T son flexibles, dependiendo del fabricante. Como se muestra en la figura 17 se indica una conexión completa entre el enchufe de pared y el concentrador.

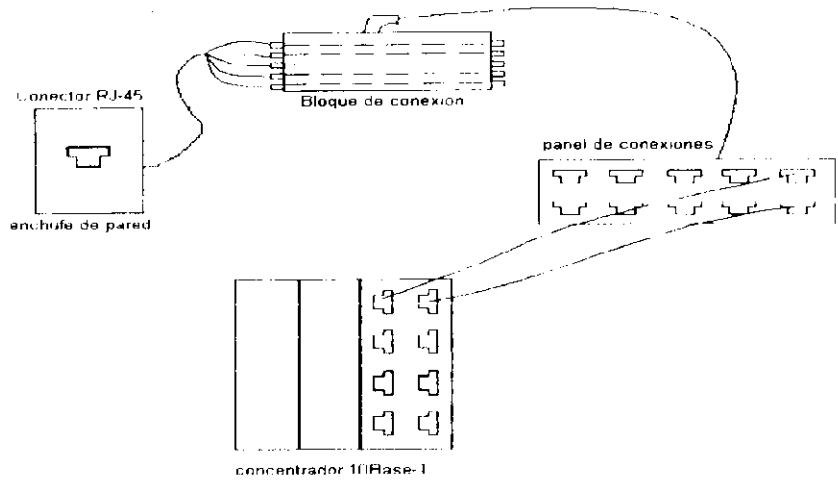


Figura 17. Configuración Ethernet 10Base-T entre el enchufe de pared y el concentrador

Las especificaciones 10Base-T se relacionan a continuación:

a) Utilice cable de par trenzado sin apantallar de categoría 3,4 o 5.

b) Utilice clavijas RJ-45 en el extremo de los cables. Las patillas 1 y 2 son transmisoras y las 3 y 6 receptoras. Cada par está cruzado de modo que el transmisor en un extremo se conecta con el receptor en el otro.

c) Un transceptor y un cable de transceptor de 15 patillas puede conectarse a cada una de las estaciones de trabajo. Algunas tarjetas disponen de transceptores incorporados.

d) La distancia que hay desde un transceptor a un concentrador no puede exceder los 100 metros.

e) Un concentrador normalmente conecta 12 estaciones de trabajo.

f) Pueden conectarse hasta 12 concentradores a un concentrador central par aumentar el número de estaciones en la red.

g) Los concentradores pueden conectarse a redes soporte de cable coaxial o de fibra óptica con objeto de formar parte de redes Ethernet extensas.

h) Pueden existir hasta 1024 estaciones en una red sin necesidad de utilizar puentes.

2.1.6.6 NORMATIVA 568 DE CABLEADO PARA EDIFICIOS COMERCIALES EIA/TIA

Un sistema de cableado estructurado constituye el resultado de un diseño planificado y realizado de manera que sea posible su acomodación a futuras necesidades de crecimiento, servicios y configuración. La Asociación de Industrias Electrónicas EIA y la Asociación de Industrias de Telecomunicaciones TIA han desarrollado una normativa para los sistemas de cableado de los edificios, denominada Normativa Comercial para Edificios Comerciales EIA/TIA 568. Esta norma proporciona un sistema uniforme de cableado y permite entornos y productos multiproveedores.

De acuerdo con los documentos EIA/TIA, la norma se ha diseñado con objeto de proporcionar las siguientes utilidades y funciones:

a) Un sistema de cableado genérico de comunicaciones para edificios comerciales.

b) Medios, topología, puntos de terminación y conexión, así como administración, bien definidos.

c) Un soporte para entornos multiproveedores y multiprotocolo.

d) Instrucciones para el diseño de productos de comunicaciones para empresas comerciales.

e) Capacidad de planificación e instalación de cableado de comunicaciones para un edificio sin otro conocimiento previo que los productos que van a conectarse.

La especificación EIA/TIA 568 se aplica a todos los esquemas de Cableado de Par Trenzado sin Apantallar (UTP, unshielded twisted pair) en topologías Ethernet, Token ring, PBX, Red digital de servicios integrados (ISDN) y otros tipos de topologías. EIA/TIA 568 presenta una serie de beneficios a sus clientes debido a que normaliza el cableado y la instalación de las redes, abriendo el mercado una serie de productos y servicios que compiten en el área del diseño, instalación y gestión de sistemas de cableado.

Cuando se estructura este sistema de cableado la especificación EIA/TIA 568 propone una topología jerarquizada en forma de estrella. Los cables adoptan esta topología desde el armario de comunicaciones hasta la toma de pared donde se conectan las computadoras de la red. todos los armarios de un piso se conectan a una sala de equipamiento,

y todos los pisos se conectan a la facilidad principal de conexiones cruzadas. El tamaño máximo del emplazamiento es de 3.000 metros, cubriéndose 1 millón de metros cuadrados de espacio de oficina, y hasta 50.000 usuarios individuales. El sistema completo puede observarse en la figura 18.

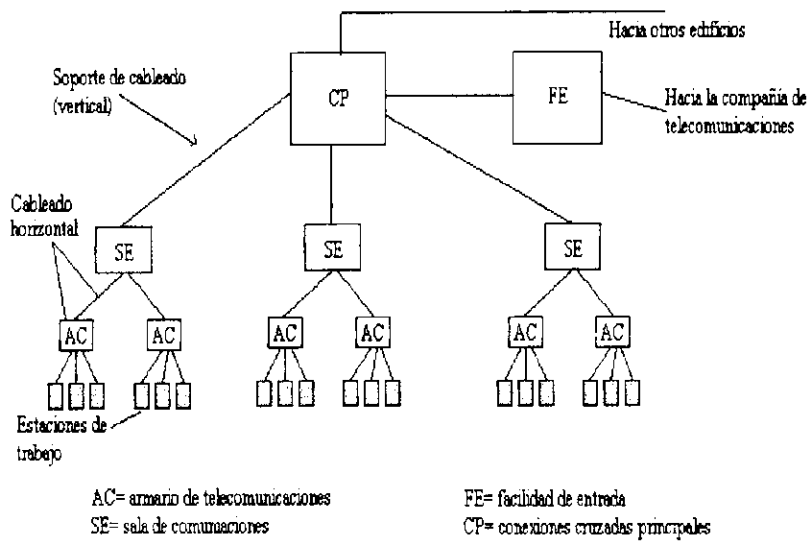


Figura 18. distribución jerarquizada de un sistema de cableado estructurado.

La arquitectura de cableado estructurado contiene cinco subsistemas que comprenden un sistema de cableado como el que se describe a continuación:

a) **Area de trabajo.-** Este subsistema consta de los elementos externos de comunicación (armarios y placas frontales), cableado y conectores necesarios par conectar el equipo de trabajo de área (computadoras, impresoras y demás) al

subsistema de cableado horizontal. Los zócalos o placas frontales típicas acomodan los conectores, como por ejemplo mediante clavijas modulares para teléfonos o datos, y clavijas modulares modificadas para transmisión de datos a baja velocidad. También pueden acomodar conectores BNC para cable coaxial y de fibra óptica.

b) **Cableado horizontal.-** Discurre entre cada toma de las estaciones de trabajo finales y el armario de comunicaciones. La distancia máxima horizontal desde éste hasta las tomas de comunicaciones es de 90 metros, independientemente del tipo de medio. Existen cuatro tipos de cable reconocidos en este sistema:

- Cables de par trenzado sin apantallar UTP de cuatro pares y de 100 ohmios.
- Cables de par trenzado apantallado STP de dos pares y de 150 ohmios.
- Cables coaxiales de 50 ohmios.
- Cable de fibra óptica con diámetros de núcleo de 62.5 micras.

c) **Armario de comunicaciones.-** Contiene el equipamiento necesario para la conexión de las estaciones de trabajo de la zona adyacente, conectándose a la sala de equipamiento. El

armario de comunicaciones es una facilidad especial que puede proporcionar conexiones para el cableado horizontal, así como conexiones con la facilidad de entrada. No existe límite en cuanto al número de armarios de comunicaciones permitidos.

d) **Sala de equipamiento**.- Proporciona el punto central de conexión para todos los armarios de comunicaciones dentro del sistema de cableado horizontal y la conexión con el soporte de cableado. La distinción principal entre las salas de equipamiento y los armarios de comunicaciones consiste en el equipamiento. La sala de equipamiento ofrece las terminaciones mecánicas para uno o más sistemas de cableado para comunicaciones.

e) **Red soporte de cableado.-** Discurre a través de los distintos pisos del edificio e interconecta las salas de equipamiento de cada piso. Estos cables se mezclan en las conexiones cruzadas principales proporcionadas por el centro de cableado del edificio. La red soporte de cableado puede estar formada por uno de los siguientes tipos de cable, cuyas limitaciones de longitud se representa en la figura 19:

- Cables UTP de 100 ohmios y cuatro pares.
- Cables STP de 150 ohmios y dos pares.
- Cables coaxiales de 50 ohmios.
- Cables de fibra óptica con un diámetro de 62.5 micras.

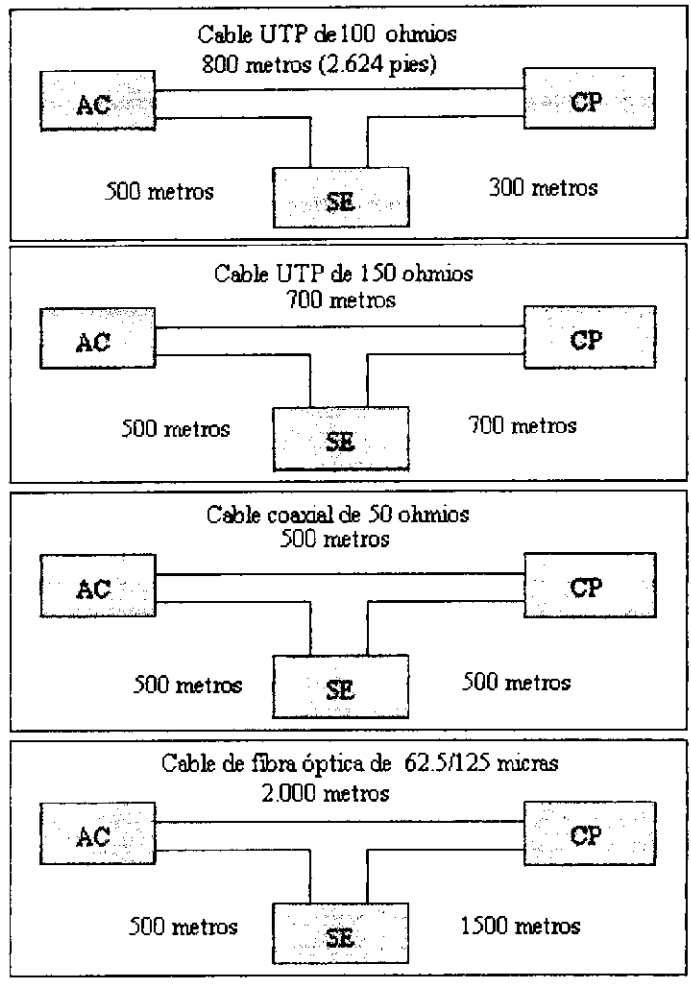


Figura 19. longitudes de cables en soporte de cableado de sistemas estructurados

f) Conexiones cruzadas principales.- Este elemento es el punto central de conexión entre el soporte de cableado del edificio y el cable que realiza la conexión con otros edificios.

g) Facilidades de entrada.- Ofrece el servicio de entrada al servicio de comunicaciones del edificio e incluye el acceso a

través del muro. Esta facilidad puede contener también conexiones a una red soporte de cableado de campus. Además, contiene el punto de demarcación de la red, que es la interconexión con las facilidades de comunicación ofrecidas por la compañía de intercambio local de telecomunicaciones. El punto de demarcación se encuentra normalmente a 12 pulgadas del punto de entrada de las facilidades de la compañía de telecomunicaciones al edificio, aunque ésta podría efectuarlo de otro modo.

h) Administración.- Este subsistema incluye las conexiones cruzadas e interconexiones entre los subsistemas de distribución. Es el punto en el que se gestiona los cambios del sistema de cableado estructurado.

Puede existir una cierta indecisión a la hora de optar por instalar un sistema de cableado estructurado EIA/TIA 568 o bien un sistema tradicional como Ethernet. EIA/TIA 468 presenta una serie de reglas rígidas y su instalación resulta más cara si se trata de una instalación de cierta magnitud, aunque es una normativa que permite expansiones futuras. Las redes tradicionales basadas en Ethernet 10Base-T. Los métodos tradicionales presentan un costo más atractivo en instalaciones pequeñas o bien en adaptaciones de instalación antiguas que ya está instalado el cable.

2.1.6.7 CONECTORES (SOCKETS)

Los conectores fueron en su origen mecanismos de comunicación local entre procesos que se utilizaban en el entorno UNIX. Evolucionaron a enlaces de red en las redes Protocolo de Control de Transmisión/Protocolo Internet TCP/IP. Un conector es básicamente un punto terminal en el enlace de comunicación entre dos aplicaciones. Los conectores que se extienden sobre la red conectan dos o más aplicaciones que se están ejecutando en distintas computadoras. Un conector se compone de dos direcciones:

a) **Dirección del puerto.-** Esta es la dirección del proceso o la aplicación que se esté ejecutando en una computadora.

b) **Dirección de protocolo Internet IP.-** Esta es la dirección de la estación de trabajo en la red TCP/IP.

Se muestra en la figura 20 el direccionamiento de un conector.

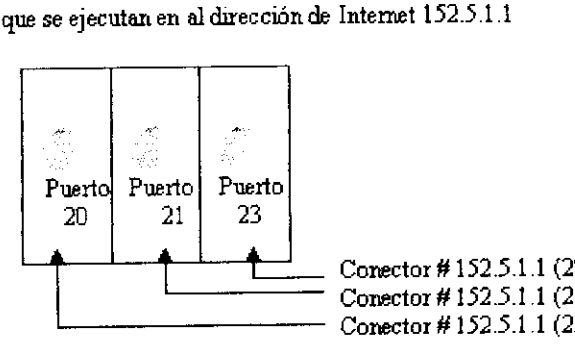


Figura 20. Direccionamiento en un conector

Los conectores proporcionan un canal de comunicación dúplex entre uno o más sistemas. Un puerto local se conecta con un conector remoto. Esto significa que el conector identifica a una computadora de la red y el puerto software dentro de esa computadora asociado con el proceso que está ejecutando la aplicación. Una vez que se ha abierto el canal, la información se envía o se recibe, y a continuación se desmantela el circuito. Existen conectores de datagrama y de flujo como se describe a continuación:

a) **Conector de flujo.-** Proporciona un enlace orientado a la conexión, de extremo a extremo, entre dos conectores mediante el fiable protocolo TCP. Los conectores de flujo ofrecen todas las facilidades de los enlaces orientados a la conexión, tales como la transmisión fiable de datos a través de circuitos que transmiten los datos en orden y proporcionan la confirmación de los datos recibidos.

b) **Conector de datagrama.-** Es un servicio no orientado a la conexión que utiliza el Protocolo Datagrama de Usuario (UCP, User Datagrama Protocol). Los servicios de datagrama son rápidos y eficientes, y son apropiados para los patrones de tráfico intenso en un corto período de tiempo propios de las LANs. El sistema emisor puede direccionar los datagramas con destino a varios conectores de diferentes computadoras de la red.

La Interfaz de Programación de Aplicación (API) de Windows es una especificación que se puede utilizar para escribir aplicaciones Windows que se vayan a ejecutar sobre redes TCP/IP, de forma que este API será de importancia para aquellos que deseen crear aplicaciones interoperativas.

También existen otros tipos de conectores como se describen a continuación:

a) **Conectores RJ-11 y RJ-45.-** Son clavijas típicas de teléfono, que se usan en Ethernet 10Base-T y otros sistemas de redes con cables de par trenzado. Hay dos tipos:

- **RJ-11:** Es un conector modular de cuatro hilos para teléfonos.
- **RJ-45:** Es un conector modular de ocho hilos para redes y algunos sistemas telefónicos.

b) **Conector BNC.-** Se usan para la conexión, la extensión y la terminación de redes de cables coaxiales como Ethernet y ARCNET. Como muestra la figura 21, hay varios tipos de conectores, como el conector en T de BNC, el conector cilíndrico de BNC y el terminador BNC.

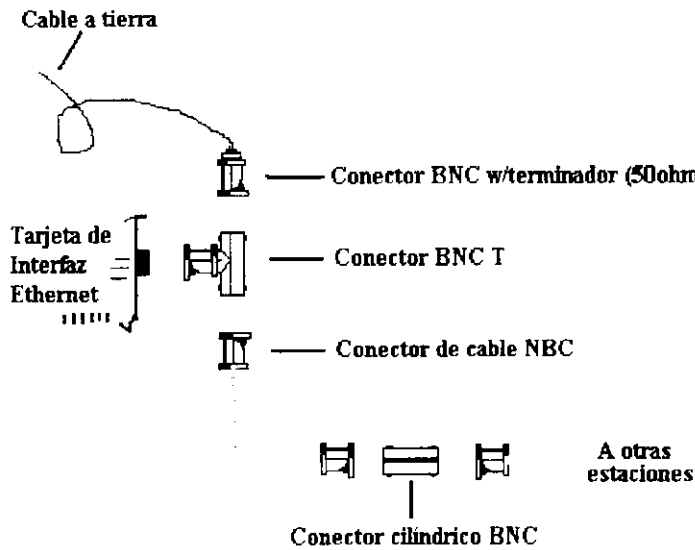


Figura 21. Componentes de una red Ethernet delgada

A continuación se definen los diferentes tipos de conectores:

- **El conector BNC:** Se une directamente al cable. Posee una clavija central que se suelda al hilo central del cable y una cubierta exterior donde se fija el hilo de protección de tierra. Los conectores BNC se colocan en los extremos de los conectores T, luego se trenza el alojamiento exterior para encerrarlo.
- **Los conectores en T de BNC:** Proporcionan la unión del cable a la tarjeta de la interfaz de red. Los cables se ramifican de los otros extremos de la T a las estaciones anterior o posterior en el cable de conexión.
- **El terminador BNC:** Posee una resistencia que se coloca en un extremo del cable coaxial. Cada extremo de

conexión del cable coaxial necesita un terminador y como mostró en la figura 21 es necesario colocar un conductor a tierra en un extremo.

- **El conector cilíndrico:** Se usa para la unión de dos segmentos de cable.

2.2 REVISION DE RUTEADORES Y HUBS

2.2.1 ENCAMINADORES (ROUTERS)

Los encaminadores son conmutadores de paquetes (o retransmisores a nivel de red Netware) que operan al nivel de red del modelo de protocolo de Interconexión de Sistemas Abiertos (OSI, Open Systems Interconnectión). Los encaminadores interconectan redes tanto en las áreas locales como en las extensas, y cuando existe más de una ruta entre dos puntos finales de la red, proporcionan control de tráfico y filtrado de funciones, como se muestra en la figura 22.

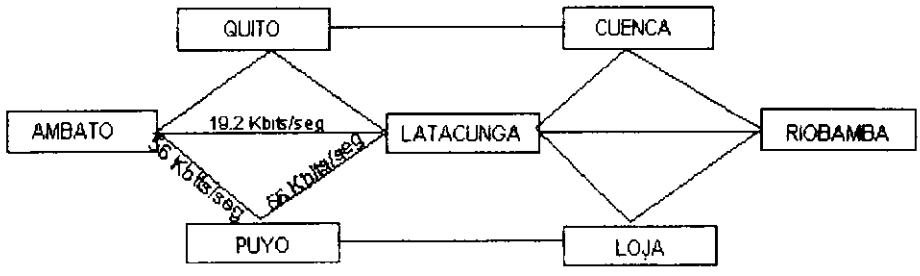


Figura 22. Esquema de trabajo de los encaminadores

Los encaminadores son críticos en las redes interconectadas grandes y de área extensa que usan enlaces de telecomunicación. Dirigen los paquetes a través de las rutas más eficientes o económicas dentro de la malla de redes, que posee caminos redundantes a un destino.

2.2.1.1 TRABAJO DE LOS ENCAMINADORES

Un encaminador examina la información de dirección de los paquetes y los envía hacia su destino a través de una ruta predeterminada. Los encaminadores mantienen tablas de los encaminadores adyacentes y de las redes de área local que hay dentro de la red. Cuando un encaminador recibe un paquete, consulta dichas tablas para ver si puede enviarlo directamente a su destino. En caso contrario, determina la posición de otro encaminador que pueda hacerlo avanzar hacia su destino.

El proceso de avance requiere la realización de un cierto procesamiento. Cuando el encaminador ha recibido la totalidad de un paquete, consulta la información de dirección HS y a continuación lo reenvía. Como consecuencia, el rendimiento se verá influido por las diferencias en los componentes del encaminador y en la arquitectura. Algunos sistemas operativos de red como Novell NetWare, soportan el encaminamiento en el servidor. Esto se logra mediante la instalación de dos o más tarjetas de interfaz de red. Sin embargo, las tareas de encaminamiento pueden hacer lento al servidor. En ese caso,

se hacen necesarios los encaminadores externos, para que liberen al servidor de dichas tareas y se ocupe sólo de los archivos.

Los encaminadores trabajan bien con un protocolo único como el Protocolo de Control de Transmisión / Protocolo Internet (TCP/IP) o bien con múltiples protocolos como Intercambio Secuencial de Paquetes / Intercambio de Paquetes entre Redes (SPX/IPX, Sequenced Packet Exchange/Internetwork Packet Exchange) y TCP/IP. Recuérdese que no se soportan todos los protocolos y que algunos de ellos no pueden ser encaminados. Sin embargo, estos últimos pueden transmitirse a través de las redes interconectadas usando técnicas de encapsulación.

Los encaminadores permiten segmentar una red en otras, para que se direccionen por separado. Los segmentos son más fáciles de gestionar. Cada segmento LAN posee su propio número de LAN específico, y cada estación de trabajo del segmento incluye su propia dirección. Esta es la información que empaquetan los protocolos del nivel de red.

2.2.1.2 PROCESO DE PAQUETES DE LOS ENCAMINADORES

Los encaminadores manipulan paquetes que poseen la misma dirección de red. Cuando un encaminador recibe un paquete, comienza un procedimiento que lo desempaqueta y determina dónde se debe enviar.

Un *paquete* es un envase de datos que se intercambia entre dispositivos sobre un enlace de comunicación de datos. Los datos intercambiados entre los dispositivos pueden adoptar las formas siguientes:

a) Mensajes y órdenes, como una petición de servicio.
b) Códigos de control para controlar la sesión, como los códigos que indican errores de comunicación y la necesidad de transmisión.
c) Datos, como el contenido de un archivo.

Varios subsistemas de comunicación del sistema de transmisión colocan la información en paquetes, luego se disponen dentro de flujos de bits en serie y se envían sobre el enlace de comunicaciones. Una de las principales razones par empaquetar y hacer tramas de información es que cualquiera de los errores que se produzcan en el enlace de comunicación sólo afectan a una parte pequeña y perceptible de la transmisión, la cual se retransmite fácilmente.

Para empezar el proceso de creación de un paquete el protocolo empieza en el nivel de aplicación como muestra la figura 23 en su parte izquierda. Un programa en el sistema A posee alguna información para enviar al sistema B. La información enviada desciende a través de la pila de protocolos, cruzará el cable y ascenderá a través de la pila de protocolos del sistema B. Esta

información toma la forma de una Unidad de Datos de Protocolo (PDU, Protocol Data Unit). Cuando la PDU se mueve a través de los niveles del sistema A, cada nivel agrega información específica a la PDU que está relacionada con los protocolos en ese nivel. Esta información agregada se destina al nivel par del sistema receptor. Por ejemplo, el protocolo del nivel de transporte en el sistema A añade ana secuencia numérica a la PDU.

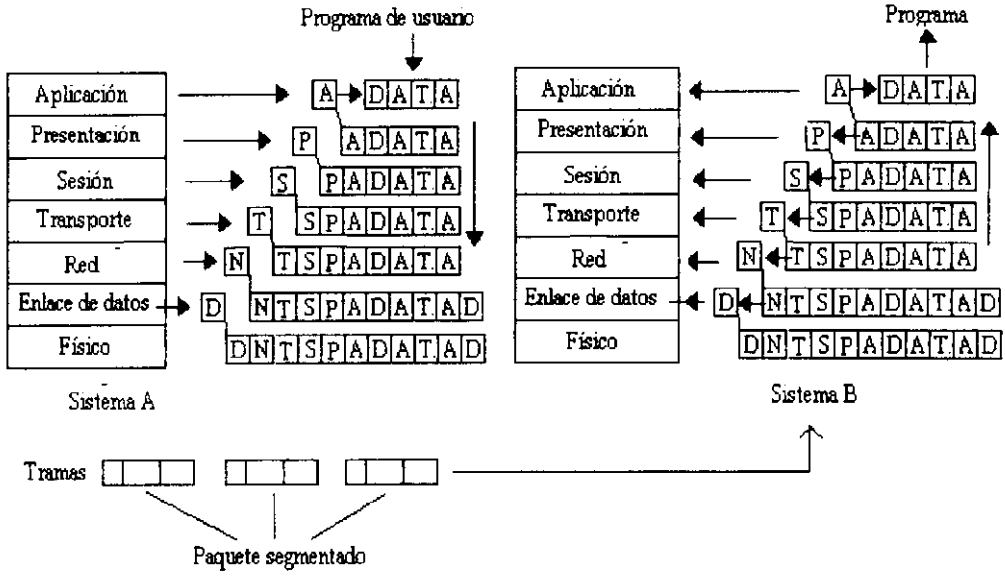


Figura 23. Ensamble, transmisión y desensamble de paquetes

El protocolo del nivel de transporte, del sistema B lee esta secuencia para volver a colocar los paquetes en secuencia.

El protocolo de comunicación define la estructura del paquete y el sistema de interconexión de red que se usa (como Ethernet a anillo con testigo) y define la estructura de la trama para la transmisión del flujo de bits. Cada nivel de protocolo agrega información destinada a

su nivel par en el otro sistema. Cuando la PDU alcanza el nivel físico, se transmite como un flujo de bits. En el hilo de cobre, los flujos de bits toman la forma de variaciones de nivel de tensión que representan unos y ceros binarios.

En general, un paquete es una colección de información que contiene datos y cabeceras. Las cabeceras incluyen las direcciones fuente y destino, así como la información de control para manejar apropiadamente los errores y el flujo de paquetes. Cada paquete es un bloque de información independiente que puede tener una dirección de destino diferente y en algunos casos, tamaños diferentes. Un paquete típico contiene 512 bytes de información, de modo que la transferencia de un archivo grande por la red necesita muchos paquetes.

Cuando los paquetes atraviesan la red, los puentes y encaminadores usan la información de las direcciones que contienen para dirigir los paquetes a su destino, o impedir su paso a las redes a las que no pertenecen, como se definen a continuación:

a) **Envío de paquetes:** Proceso realizado por un nodo de red cuando envía paquetes al siguiente nodo o al encaminador apropiado de la red.

b) **Filtrado de paquetes:** Forma de clasificar paquetes de forma que sólo se transmitan los paquetes de un tipo específico o con una dirección concreta.

A continuación se dan los procedimientos que sigue el encaminador, cuando trabaja con un paquete:

a) Se comprueba si el paquete posee algún error, con el uso del valor del código de paridad contenido en el paquete.
b) Se descarta la parte de la información del paquete que la añadieron los protocolos de nivel físico y de enlace de datos, tal como se muestra en la figura 24.
c) Se evalúa la información que añadieron, en la computadora fuente, los protocolos de la red.

La información de los protocolos del nivel de red contiene la dirección de destino, y en el caso de las redes que, al igual que TCP/IP, tengan un encaminamiento fuente, también contiene una lista de "saltos" que definen la "ruta mejor", previamente determinada, para cruzar la red.

El encaminador podría hacer una de entre las siguientes cosas:

a) El paquete podría estar dirigido al propio encaminador así que el encaminador evalúa cuál es la información remanente en el paquete.

b) Si un paquete posee un destino en la propia red, el encaminador simplemente lo envía.

c) Si la lista de filtros está disponible, el encaminador compara la dirección del paquete con los valores de la lista y lo descarta si es necesario. Esto hace que un paquete quede dentro o fuera de la red, en base a razones de seguridad.

d) Si el paquete contiene información procedente del encaminamiento fuente, en la que se contenga el nombre del próximo encaminador que está en la ruta hacia su destino, simplemente dirige el paquete hacia él.

e) Un encaminador mantiene una tabla de rutas que pueden emplear los paquetes para cruzar la inter-red.

f) Si un encaminador no conoce una ruta, o no puede encontrar la dirección de destino del paquete en su tabla de caminos, descarta el paquete y podría devolver un mensaje de error a la fuente.

g) Algunos paquetes (del tipo de los TCP/IP) contienen información acerca del número de saltos que han hecho en la red. Si un paquete sobrepasa un cierto número, el encaminador lo descarta ya que asume que está en un bucle. El encaminador podría devolver un mensaje de error a la fuente.

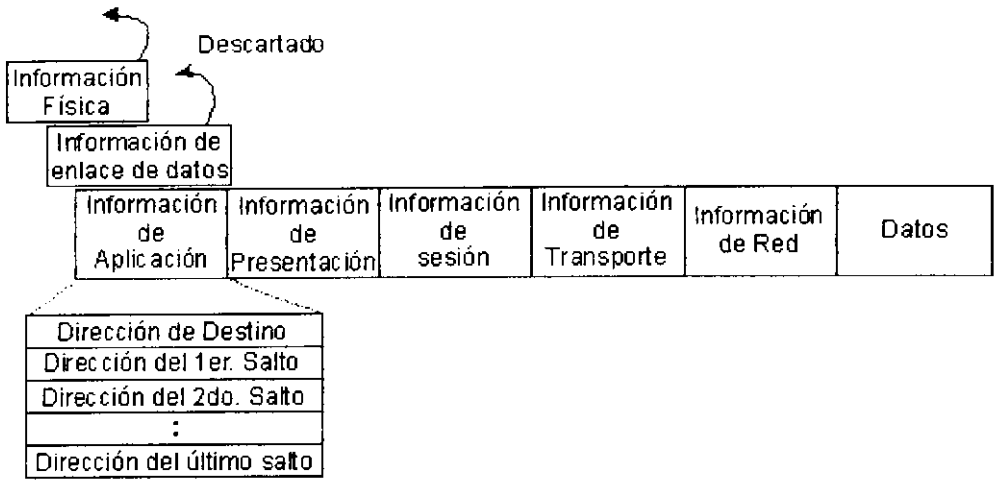


Figura 24.Procesamiento de paquetes realizado por los encaminadores

2.2.1.3 LA ELECCION DEL CAMINO MEJOR

Naturalmente, la interconexión de redes presupone que debe haber una cierta tolerancia a los fallos. Se crean varias rutas entre los encaminadores, para que exista un camino de seguridad en el caso de que falle un enlace. Algunas de estas rutas pueden usar una red de alta velocidad, como la Interfaz de Datos Distribuidos por Fibra (FCCI, Fiber Distributed Data Interface), dentro del campus o del área metropolitana, o líneas digitales directas (T1) para redes de área extensa. Los encaminadores pueden enviar los datos por la mejor de estas rutas, en función de cuál sea el costo por usarlas, la más rápida, la mas directa o la que ha especificado un administrador.

Los protocolos de encaminamiento eligen el mejor camino a través de una red en base a criterios tales como el número de saltos entre los

encaminadores de la red que tendría que hacer el paquete hasta alcanzar su destino. Además la mejor ruta debe evitar los caminos que cruzan segmentos LAN congestionados. Se puede dotar de prioridades al tráfico. Por ejemplo, los paquetes con prioridad alta se enviarían a través de enlaces de comunicación digital a una velocidad de 56 Kbits/seg., y los de baja, se enviarían a 19,2 Kbits/seg., a través de enlaces de telecomunicación. El administrador de la red puede decidir cuáles son las mejores rutas de la red, o en algunos casos, hace que sean los encaminadores los que elijan el mejor camino. Una red privada se forma con líneas alquiladas o de enlace telefónico y con encaminadores, tal como se muestra en la figura 25.

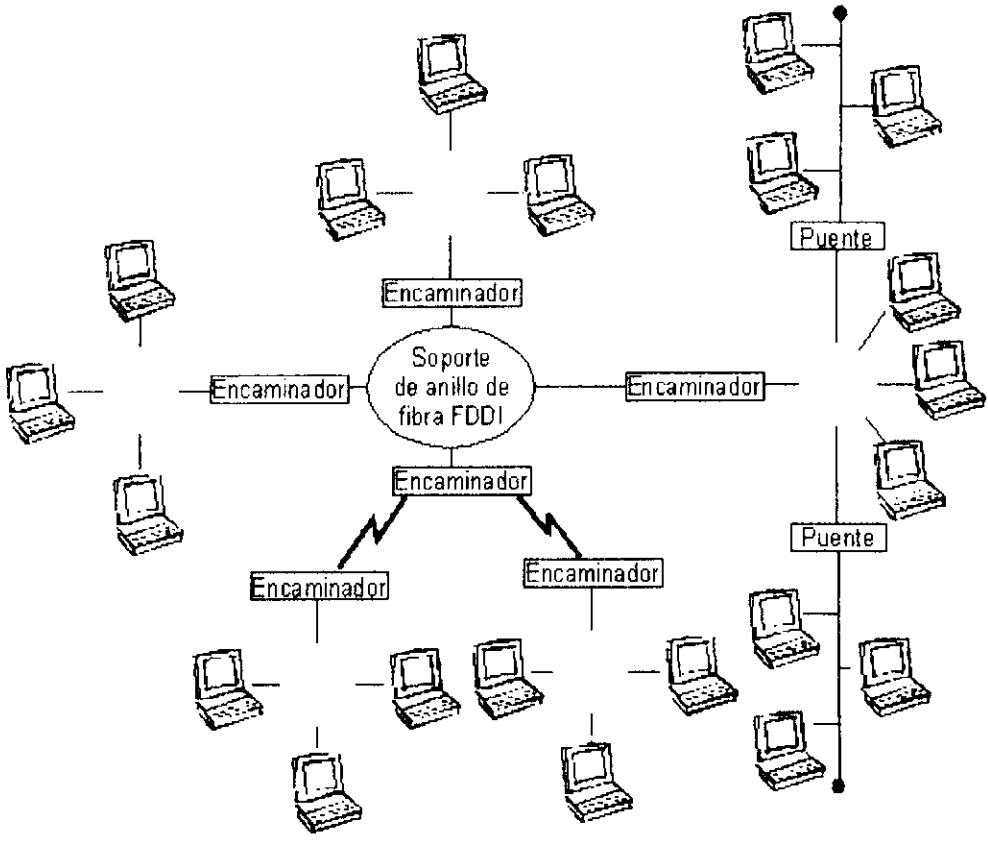


Figura 25. Encaminador perteneciente a una red soporte

Los encaminadores también se emplean para enlazar las redes con los soportes como aparece en la figura 25. En ese caso el tráfico local permanece en la LAN local, mientras que el tráfico entre redes o el de la WAN atraviesa el soporte de fibra óptica. FDDI para alcanzar su destino. Nótese que el soporte FDDI actúa como las rotondas de las carreteras, en el sentido de que el tráfico se mueve a su alrededor para alcanzar los nodos de las ramas.

2.2.1.4 LAS ESPECIFICACIONES DE LOS ENCAMINADORES

Normalmente, cuando una red es pequeña o está en un único edificio, se hace útil el uso de puentes. Estos pueden facilitar el tráfico entre los distintos segmentos de una red local muy ocupada. Nótese a la derecha de la figura 25 que se han conectado varias subredes a través de puentes, y que el conjunto de las mismas está conectado al soporte FDDI mediante un encaminador.

Si se trata de interconectar mediante puentes más de, aproximadamente diez subredes, se introduce demasiado tráfico entre ellas, y se provocan problemas del tipo de paquetes que acaban recorriendo bucles. Para la conexión de diferentes tipos de red, como una Ethernet a un soporte FDDI, o para conectar con enlaces WAN, es más adecuado el uso de encaminadores. Si una red establece protocolos múltiples, es necesario usar un encaminador multiprotocolo. Los encaminadores pueden distribuir la carga entre

múltiples líneas y proporcionan el control de las rutas que unen la compleja malla de encaminadores interconectados. También pueden reconfigurar una ruta si falla uno de sus enlaces.

Cuando se evalúan y se compran encaminadores, hay que cerciorarse de que todos los de la inter-red usan los mismos métodos para el encaminamiento y trabajan con los mismos protocolos. Algunos encaminadores utilizan técnicas de compresión de datos para el incremento del rendimiento de los paquetes. Para evitar problemas se debe intentar usar siempre el mismo encaminador en todos los puntos. Aunque generalmente los métodos de encaminamiento están estandarizados, un error al compararlos podría causar problemas que se tradujeran en la degradación de los resultados.

Los sistemas de gama alta ofrecen facilidades de tolerancia a los fallos tales como fuentes de alimentación redundantes y el reemplazamiento vivo de los módulos. Incluso, se llega a hacer difícil la configuración de los encaminadores, ya que hay que programar en el dispositivo facilidades como los protocolos múltiples, caminos redundantes, eficiencia y seguridad. Un buen programa de instalación puede facilitar la tarea. El Encaminador Multiprotocolo (MPR, Multiprotocol Router) de Novell simplifica en parte la configuración, ya que proporciona algunos de los parámetros por defecto válidos para las redes NetWare, tales como el tamaño de los paquetes, los temporizadores, y algunos otros.

paquetes por segundo. La latencia de almacenamiento y reenvío de los puentes y los encaminadores disminuye algo el rendimiento. MPR de Novell envía de 3.000 a 4.000 paquetes por segundo.

No hay necesidad de que el rendimiento, en paquetes por segundo, de los puentes y de los encaminadores sea mayor que las capacidades de las LANs a las que se conectan. Recuérdese además, que el tráfico que cruza el puente es menor que el local. Aunque las ráfagas de los sistemas de alto rendimiento pueden llegar a saturar incluso el ancho de banda del cable Ethernet normal, el mecanismo de contención del método de acceso por cable Ethernet añade la suficiente sobrecarga, con grandes volúmenes, como para mantener un tráfico bajo en el puente o en el encaminador. Normalmente, un encaminador o un puente que es capaz de procesar 5.000 paquetes de 64 bytes por segundo es adecuado para 10 Mbits/seg., una vez que se ha tenido en cuenta esta sobrecarga. Las redes en anillo con testigo poseen un punto de saturación similar. El cable contrae pos sí mismo el ancho de banda, más de lo que podría hacerlo un puente. Con un puente o encaminador que transfiera de dos a tres mil paquetes por segundo, se puede manejar adecuadamente. Nótese que el disponer de una velocidad de transferencia alta es menos importante en las conexiones WAN porque la propia WAN establece un rendimiento mucho menor que una LAN.

2.2.1.5 ENCAMINADORES MULTIPROTOCOLO

Una red multirprotocolo soporta diversos protocolos, tales como TCP/IP, IPX, AppleTalk, DECnet y otros. Los encaminadores multiprotocolo dan lugar a organizaciones que posibilitan la conexión de los recursos de la red directamente a la propia plataforma de la red. En función de las capacidades del encaminador, un encaminador multiprotocolo puede ejecutar software para el manejo de paquetes, de acuerdo con cada uno de los protocolos que soporta la red.

Las redes multiprotocolo proporcionan el medio para aunar los distintos protocolos en tan solo unos pocos. Los administradores pueden dirigir paulatinamente a los usuarios hacia los protocolos que soporta la compañía, y una vez que todos los usuarios hayan realizado la transformación, deshabilitar los protocolos viejos.

Por ejemplo Windows NT es un ejemplo de un sistema Operativo multiprotocolo ya que se puede definir varios protocolos de trabajo, este detecta con que protocolo está trabajando la aplicación específica y automáticamente le responde con el mismo protocolo siempre y cuando esté definido.

2.2.1.6 ENCAMINAMIENTO EN INTERNET E INTRANET

La arquitectura de encaminamiento de Internet (TCP/IP) es similar a la arquitectura de Interconexión de Sistemas Abiertos (OSI, Open

System Interconection). Existe una jerarquía de sistemas formada por subredes a las que se conectan los anfitriones (host) (computadoras de usuario, servidores y otros). Estas subredes se acoplan a los encaminadores, que son los que las conectan a las otras subredes dentro del sistema autónomo. Un sistema autónomo (también llamado sistema interior o dominio) es una colección de subredes y encaminadores que, generalmente, usan los mismos protocolos de encaminamiento y están bajo el mismo control administrativo.

Los Protocolos de pasarela interior como el Protocolo de Información de Encaminamiento (RIP, Outing Information Protocol) y el Primero en Abrir el Camino más Corto (OSPF, Open Shortest Path First) se usan para intercambiar información de encaminamiento dentro de un dominio. El OSPF es un protocolo de encaminamiento interior, muy similar al protocolo OSI IS-IS. En los límites de los dominios están los encaminadores fronteras, que conectan un dominio con otro. Estos encaminadores emplean los protocolos de encaminamiento exterior para intercambiar la información de encaminamiento. El Protocolo de Pasarela Exterior (EGP, Exterior Gateway Protocol) proporciona un medio para que dos encaminadores vecinos situados en los límites de sus respectivos dominios, intercambien mensajes e información. Existe una alternativa al EGP que es el Protocolo de Pasarela Frontera (BGP, Border Gateway Protocol) y que aporta algunas mejoras como la posibilidad de especificar políticas de encaminamiento.

2.2.2 CONCENTRADORES (HUBS)

En su forma más simple, un concentrador es un dispositivo que centraliza la conexión de los cables procedentes de las estaciones de trabajo. Existen concentradores pasivos y activos:

a) **Concentradores pasivos**.- Adoptan la forma de pequeñas cajas, que disponen de unos pocos puertos para la conexión de estaciones de trabajo dentro de una configuración en forma de estrella. Puede considerarse a un panel de distribución o a un bloque de conexión como un concentrador pasivo. El punto más importante es que no se realiza ampliación de señales. Un concentrador pasivo es 'únicamente un cuadro de unión que no requiere una conexión eléctrica.

b) **Concentradores activos.-** Los concentradores activos disponen normalmente de más puertos que los concentradores pasivos y regeneran las señales que viajan entre los dispositivos conectados, según muestra la figura 26. Requieren una conexión eléctrica. Los concentradores activos se utilizan como repetidores que proporcionan una extensión del cable conectado a una estación de trabajo.

Los concentradores activos simples poseen una sencilla tarea asignada: recibir señales de una estación y retransmitirlas fielmente a otra. La detección de colisiones se gestiona por las tarjetas de interfaz de red de las estaciones de trabajo individuales.

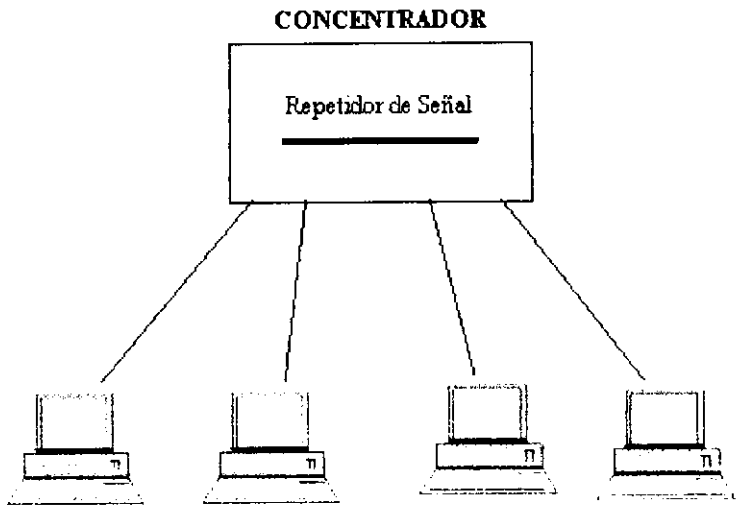


Figura 26. Un concentrador activo regenera las señales desde un dispositivo a otro

Típicamente, unos concentradores se conectan a otros, formando una jerarquía como la representada la figura 27 La configuración física se corresponde con un sistema de cableado estructurado. El cable de par trenzado de cobre es el más frecuentemente utilizado para e cableado horizontal de cada piso, y el cable de fibra óptica se utiliza a menudo en los recorridos verticales, aunque estos tipo de cable no se hallan definidos de una forma estricta. El cable de grado de datos puede proporcionar actualmente velocidades de transmisión superiores a 100 Mbits/seg., utilizado como cable de red soporte. El cableado estructurado es sencillo de instalar, gestionar y expandir. Sirve de soporte a las nuevas redes de alta velocidad y a futuras tecnologías, como por ejemplo el Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode). Los concentradores hacen que el cableado estructurado sea posible y proporcionan los siguientes beneficios:

a) Según se modifica la organización de la compañía, los cambios en la red serán fáciles de realizar a partir de sistemas de cableado estructurado construidos en torno a concentradores.

b) Las redes pueden expandirse de forma incremental mediante el cableado estructurado y concentradores.

c) Los concentradores se acomodan a numerosas opciones de red, como Ethernet, redes en anillo con testigo, FDDI y conexiones a redes de área extensa a través de Frame Relay, SMDS, ATM y otras.

d) Los concentradores proporcionan una gestión centralizada y recolección automática de información de la red.

e) Los concentradores proporcionan utilidades tolerantes a fallos, que mantienen el sistema de cableado en funcionamiento.

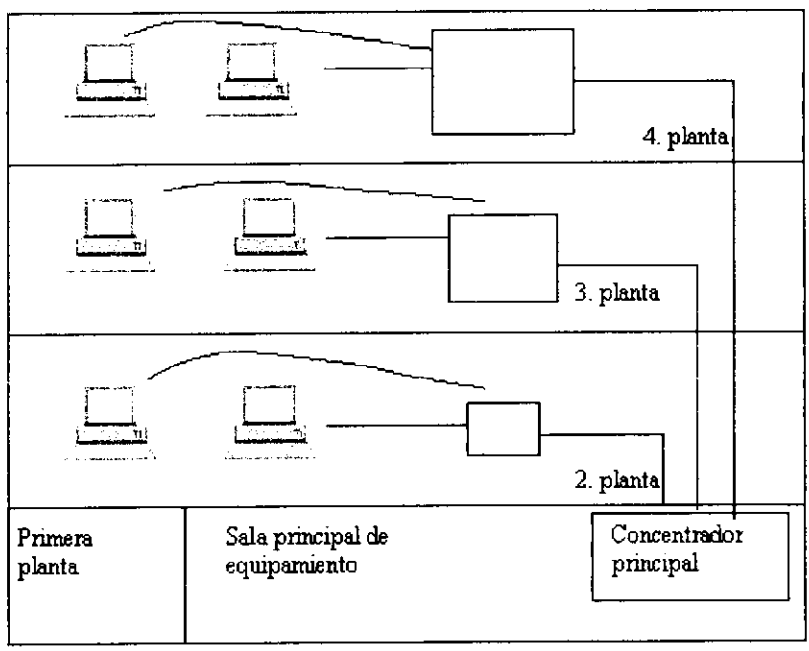


Figura 27. El cableado estructurado es semejante a un diseño jerarquizado en árbol

Una de las ventajas de la utilización de cable de par trenzado de cobre es la limitación impuesta a la distancia. Los concentradores reducen algo el problema, debido a que actúan como dispositivos repetidores. Por ejemplo, en una red Ethernet 10base-T, una estación de trabajo puede encontrarse al final de una configuración serie (daisy-chain) hasta con cuatro concentradores intermedios.

La topología de las redes de concentradores es típicamente una configuración en estrella. Sin embargo, en redes en anillo con testigo, las señales viajan sobre la red en circuito lógico, y en Ethernet las señales se difunden a todas las estaciones de trabajo desde el concentrador, presentando sus ventajas. Como cada cable conecta una única estación de trabajo, la ruptura de uno de ellos sólo afectará a la estación asociada. Gracias al concentrador, los gestores pueden realizar diagnósticos sobre un único recorrido de cable, con el objeto de determinar su flujo de tráfico o detectar problemas aislados.

2.2.2.1 CLASIFICACION DE LOS CONCENTRADORES

Es posible clasificar los concentradores en tres grupos principales. Estos grupos se definen básicamente atendiendo a la configuración de cableado estructurado, a la que las estaciones de cada planta se conectan mediante cableado horizontal y las plantas entre sí mediante cableado vertical. Las tres categorías son el concentrador para un grupo de trabajo, el concentrador intermedio y el concentrador corporativo, según se describen a continuación:

a) Concentradores para grupos de trabajo.- Conecta un grupo de máquinas dentro de su entorno inmediato. Por ejemplo, podría conectar ocho computadoras dentro de un departamento de artes gráficas. Dentro de una misma planta pueden coexistir distintos grupos de trabajo.

Una variación interesante del concentrador para un grupo de trabajo es el adaptador de concentración, que consiste en un cuadro de concentradores reducido a una tarjeta de interfaz que se conecta a un servidor. Se asume que dicho servidor se encuentra próximo al grupo de trabajo, en lugar de en una zona central de gestión. Un cable especial, que dispone de puertos de conexión para estaciones de trabajo, se extiende desde la tarjeta adaptadora. Alternativamente, un conector Telco de 50 patillas une la tarjeta a un panel de conexiones dentro de un armario de distribución. Pueden acoplarse diversos adaptadores de concentración a un único servidor y unirse mediante tiras de alambre, creando así un puente entre los puertos de las tarjetas. Novell ha definido la Arquitectura de gestión de concentradores HMA y un módulo de carga de Netware NLM denominado HubCon para realizar la gestión de los adaptadores.

b) Concentradores intermedios.- Se encuentra en el armario de distribución localizado en cada planta. Los cables se ramifican desde éste hasta los concentradores para grupos de trabajo. El

concentrador intermedio de cada planta se conecta a un cable vertical de red soporte que se extiende a través del conducto entre las plantas y se conecta con el concentrador corporativo. De forma alternativa, el concentrador intermedio podría disponer de un enlace directo de fibra óptica al concentrador corporativo.

Los concentradores intermedios son opcionales, pudiendo formar la base de una futura expansión hacia concetradores corporativos. Por ejemplo, un concentrador intermedio puede hacer acopio de todas las conexiones procedentes de las estaciones de trabajo en cada planta. Posteriormente, los concentradores intermedios de cada planta podrían unirse con un cable de red soporte, los concentradores intermedios pueden conectarse a un concentrador corporativo.

c) **Concentradores corporativos.-** Representa el punto de conexión central par a todos los sistemas finales conectados a los concentradores para grupos de trabajo. Los concentradores corporativos forman por sí mismos la red soporte o proporcionan la conectividad a ésta. Pueden proporcionar puenteado, encaminamiento y servicios de conexión de área. Dentro de un concentrador corporativo pueden situarse módulos de gestión avanzada.

Como se mencionó anteriormente, puede comenzarse con concetradores para grupos de trabajo, conectar éstos a través de concentradores intermedios y, posteriormente, conectar éstos últimos mediante una red soporte como FDDI, o bien utilizar un concentrador corporativo, que permitirá una mejor gestión, aceptar un mayor volumen de tráfico y ofrecerá un entorno más integrado que una red soporte FDDI.

Los concentradores corporativos deben diseñarse para cumplir requisitos críticos, fundamentales par una organización completa, y para ser compatibles con nuevas tecnologías como ATM.

2.2.2.2 CONCENTRADOR (HUB) INTELIGENTE

Los concentradores son zonas centrales de cableado que proporciona funciones de repetidor en redes como ARCNET y Ethernet 10 Base-T. El concentrador se utiliza como un lugar central donde conectar las estaciones de trabajo y de este modo gestionar más fácilmente la red. Los primeros concentradores fueron sencillos repetidores que sólo daban soporte a un único medio de transmisión. La configuración del cableado que soportaba se adecuaba a redes de área local para departamentos o grupos de trabajo de unos son aún productos viables para pequeñas LANs.

Los concentradores de segunda generación se llaman concentradores inteligentes debido a que incluyen características de gestión, como la capacidad de detectar fallos y recoger información sobre las actividades de la red y de los puertos individuales en el concentrador. La información se recoge y se devuelve a la estación de gestión central. La mayoría de los concentradores de segunda generación, admiten las utilidades de gestión del Protocolo Básico de Gestión de Red (SNMP, Simple Network Management Protocol).

A continuación se enumeran otras importantes utilidades de los concentradores inteligentes:

a) Incluyen planos posteriores con múltiples buses para soportar diferentes medios como Ethernet, anillo con testigo y FDDI.
b) Normalmente utilizan procesadores RISC de altas prestaciones que mejoran el rendimiento de los paquetes.
c) Permiten crear segmentos lógicos de LAN dentro de un único concentrador y tender puentes (bridges) a estos segmentos.
d) Pueden tener módulos instalables de gestión que proporcionan la capacidad de gestionar el concentrador desde una localización remota.
e) Poseen señalización fuera de banda que conecta estaciones de gestión remotas al concentrador por medio de líneas separadas, que permanecen activas incluso si falla la comunicación LAN.

Los concentradores de tercera generación han empezado a aparecer. Estos incluyen utilidades de gestión y control más sofisticadas, planos posteriores más rápidos, puenteado y encaminamiento mejorados entre segmentos, y la capacidad de microsegmentar la red de forma que una única LAN de soporte a una sola estación de trabajo. Los concentradores que surgen proporcionan conmutación del Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode) entre cualquiera de los puertos.

2.2.2.3 CONCENTRADOR (HUB) PASIVO

Un concentrador pasivo es una localización central para la unión de cables desde las estaciones de trabajo. Existen concentradores activos y pasivos. Un concentrador pasivo es una pequeña caja que dispone únicamente de unos cuantos puertos para la conexión de estaciones de computadoras en una configuración en estrella. También puede ser un panel de cableado o un bloque de conexiones. El aspecto importante es que no existe amplificaciones de las señales. Un concentrador pasivo es simplemente una caja de uniones que no requiere conexión eléctrica.

En contraste, un concentrador activo normalmente dispone de más puertos que el pasivo y regenera activamente la señal entre un dispositivo y otro. Los concentradores activos necesitan una conexión

eléctrica. Se usan como repetidores, con objeto de proporcionar una extensión del cable conectado a una estación de trabajo.

2.2.2.4 CONCENTRADORES DE CONMUTACION

Un concentrador de conmutación es un dispositivo que puede reducir la contención en las topologías de redes compartidas, mediante la disminución del número de nodos de un segmento utilizado técnicas de microsegmentación. En una red microsegmentada, un segmento de red de área local puede tener varios nodos como si fuesen uno solo. El concentrador de conmutación se encarga de gestionar las conexiones entre los nodos situados en diferentes segmentos de LAN que se necesiten comunicar. No se deben confundir las técnicas de conmutación con la conmutación de puertos, que es una función de gestión que utilizan los administradores cuando desean desplazar estaciones de trabajo de un segmento lógico a otro, por medio de un programa de administración, en lugar de mover físicamente los cables de un concentrador. Con técnicas de conmutación se pueden segmentar las LANs, de forma que el conmutador gestione el tráfico entre los segmentos, de forma similar a como lo haría un puente, pero sin el bajo rendimiento del mismo. Los concentradores de conmutación originales se diseñaron para el uso departamental y estaban construidos sobre su propia carcasa. Los concentradores de conmutación más modernos son unidades modulares y encajan en los concentradores corporativos.

Una red con 20 usuarios que esté desbordada por un exceso de tráfico, se puede dividir en dos segmentos conectados por un puente, reduciendo así la carga de tráfico y disminuyendo la contención de cada uno de los nuevos segmentos de LANs. Se supone que es posible mantener en el mismo segmento a todos los usuarios y los dispositivos que se suelen comunicar entre sí, de manera que se reduzca el tráfico entre segmentos. Si el problema no se resuelve, se puede dividir la LAN en cuatro segmentos, seis segmentos, y así sucesivamente. Un concentrador de conmutación realiza este tipo de segmentación. Contiene una serie de puertos, cada uno de los cuales está dedicado a un segmento de LAN.

El concentrador de conmutación maneja el tráfico entre segmentos a través de un conmutador matricial interno. El nivel de Control de Acceso al Medio (MAC) se encarga de gestionar toda la conmutación. Cuando llega un paquete al conmutador, se anota, se anota inmediatamente su dirección de destino y se establece una conexión con el segmento final adecuado. Los sucesivos paquetes se retransmiten a través del conmutador sin necesidad de almacenar y reenviar los paquetes como ocurre en los puentes.

La mayoría de los concentradores de conmutación son Ethernet, de forma que una única estación conectada por sí misma a un puerto podría conseguir enviar 10 Mbits/seg. al concentrador. Dado que no hay ninguna otra estación de trabajo que comparta el puerto, no se

producen contenciones y se puede conseguir toda la anchura de banda de los segmentos. Algunos fabricantes están trabajando también en concentradores de conmutación de alta velocidad con planos posteriores de conmutación en Modo de Transferencia Asíncrono (ATM).

ATM es una tecnología de transmisión de datos que posee el potencial suficiente para revolucionar el modo en que se construyen las redes de computadoras. Viable para redes de área local y extensa, esta tecnología proporciona una alta velocidad de transmisión de datos y soporta muchos tipos de imágenes. ATM aprovecha las ventajas de las altas velocidades de rendimiento de datos posibles en los cables de fibra óptica. En los sistemas de las compañías de telecomunicaciones, las realizaciones ATM de alta velocidad (155 Mbit/seg., a 622 Mbits/seg.) utiliza la red óptica síncrona, la cual se realiza en cable óptico y proporciona una norma genérica de telecomunicaciones mundiales.

ATM es una tecnología de banda ancha para transmisiones de voz, video y datos sobre LANs o WANs. Es una tecnología de retransmisión de celdas, esto implica que los paquetes de datos poseen un tamaño fijo. Se puede pensar en una celda como en una clase de vehículo que transporta bloques de datos desde un dispositivo a otro a través de un dispositivo de conmutación ATM. Todas las celdas contiene el mismo tamaño, al contrario d lo que ocurre en los sistemas

Frame Relay y LAN en los que los paquetes pueden tener distintos tamaños. El uso de celdas de igual tamaño proporciona un modo de predicción y garantía del ancho de banda para las aplicaciones que lo necesitan. Los paquetes de longitud variable pueden causar retardos de tráfico en los conmutadores, del mismo modo que los coches deben esperar que los camiones grandes giren en las intersecciones ocupadas.

El dispositivo de conmutación es el componente más importante en ATM. Puede de utilizarse como un concentrador dentro de una organización que retransmite rápidamente paquetes de un nodo a otro o puede servir como un dispositivo de comunicación de área extensa, que transmite celdas ATM entre LANs remotas a velocidades altas. Las convencionales como Ethernet, Interfaz de datos distribuido por fibra y anillo con testigo usan un medio compartido en el cual un solo nodo puede transmitir a la vez. Sin embargo, ATM proporciona conexiones cualquiera a cualquiera y los nodos pueden transmitir simultáneamente. Se multiplexa la información desde muchos nodos como un flujo de celdas.

NOTA. Un Conmutador ATM simplemente transmite celdas. Examina la cabecera e inmediatamente empieza a enviar la celda. Se elimina el tiempo consumido por los métodos de almacenaje y de envío que usan los encaminadores.

2.3. ¿COMO SE APLICA EN LA RED DE LA PUCESA?

Las redes de la PUCESA pueden ser definidas de acuerdo a lo que hemos estudiado en este capítulo de la siguiente forma:

a) Tipo de red.- Puede ser catalogada como:

- **Segmento de red:** Si tomamos por separado las secciones: IBM, Compaq o Novell, esto representa que las red de la PUCESA está compuesta por tres segmentos cada uno de estos compuestos por los terminales que se encuentran ubicados en cada una de las áreas divididas físicamente en tres aulas como se muestra en la figura 28.

- **Red LAN o de campus:** Tomando en total su estructura considerando que se encuentra en un área específica es este caso los predios universitarios que pertenecen a la Escuela de Ingeniería en sistemas, como se muestra en la figura 28

- **Red WAN:** Los momentos en los que entra en enlace permanente con INTERNET ya que en estos momentos cumpliría los requisitos para se una red de área extensa pudiendo ser diferenciada de una red corporativa ya que la INTERNET en si no pertenece a la PUCESA.

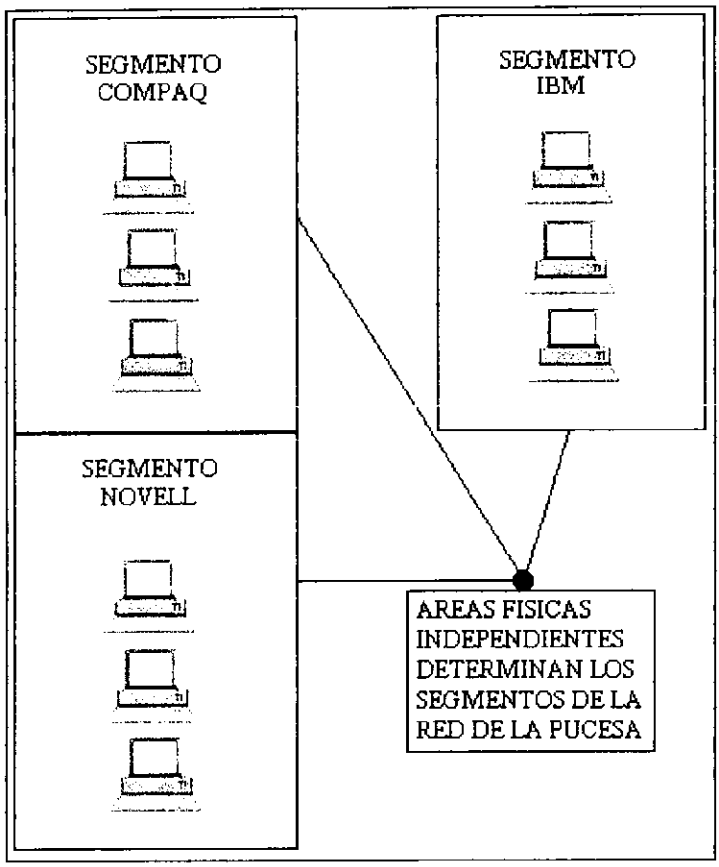


Figura 28. Segmentos de red de la PUCESA

- **Red metropolitana:** Pudiera ser considerada como una si el edificio de la Medalla Milagrosa se conectara con la Red de la Escuela de Sistemas por medio de comunicación locales, esto se podría conseguir conectando todos las computadoras del edificio de la medalla milagrosa a un servidor, éste a su ves a un modem y disponiendo de una línea dedicada, sea esta telefónica, microondas o por radios de onda corta y realizando un enlace entre servidores con el que se encuentra en el laboratorio de sistemas de la escuela de Ingeniería de sistemas.

- Pudiera ser Considerada como *Corporativa* si se tratara de que la red estuviera conectada con la red de la PUCE Quito, a través de los medios de comunicación y enlace conocidos y utilizando el mecanismo detallado para la posibilidad de integrar una red metropolitana.

b) Entornos de red.- La red de la PUCESA está compuesta por los dos tipos de entorno de red:

- **Par a par:** En los Servidores LINUX y Windows NT que ejecuta protocolo TCP/IP.
- **Servidor dedicado:** En el Servidor Novell.

c) Componentes de una red.- La red de la PUCESA cuenta con todos los componentes enumerados que forman una red como se describe a continuación:

- **Sistema operativo de red:** Consta de tres sistemas operativos de red como son : Windows NT, LINUX, Novell.
- **Servidores:** Cuenta con tres equipos servidores como se explica en la sección "Diagnóstico y situación actual de la PUCESA" el cual se lista en el ANEXO I.
- **Sistemas clientes:** Cuenta con terminales que contienen como sistema operativo Windows 95 y DOS.

- **Tarjetas de la interfaz de red:** Cada uno de los equipos tanto servidores como clientes poseen tarjetas de interfaz de red que permiten una conexión a la red.
- **Sistema de cableado:** El sistema de cableado es estructurado ya que posee el cableado multipar.
- **Recursos y periféricos compartidos:** Cuenta con Impresoras y todos los recursos en cada uno de las estaciones que son permitidas compartir por el sistema operativo que corre en cada una de ellas.

d) Ruteadores.- El encaminador de la PUCESA permite el enlace con INTERNET cumpliendo lo especificado en la sección de encaminadores. Este ruteador que se posee es un PTR que funciona como un Bridge.

e) Hubs.- Los hubs de la PUCESA son del tipo inteligente y existen tres, los mismos que controlan todo el tráfico de la red de la universidad.

f) Modem.- Se posee un modem el cual es utilizado para acceder al INTERNET. Es de tipo ATM que permite una conexión a una línea dedicada, es decir no se necesita una inicialización para la conexión en el momento de recibir una señal por parte de la línea telefónica, el modem se activa e inicia el proceso de comunicación. El modem se encuentra conectado a través de una línea telefónica con una empresa de comunicaciones especializada en la transmisión de datos como es Transteledatos, ésta a su ves realiza una conexión con una empresa distribuidora de Internet ACCESS Internet, la cual

está conectada con el mundo en este caso Internet como se muestra en la figura 29.

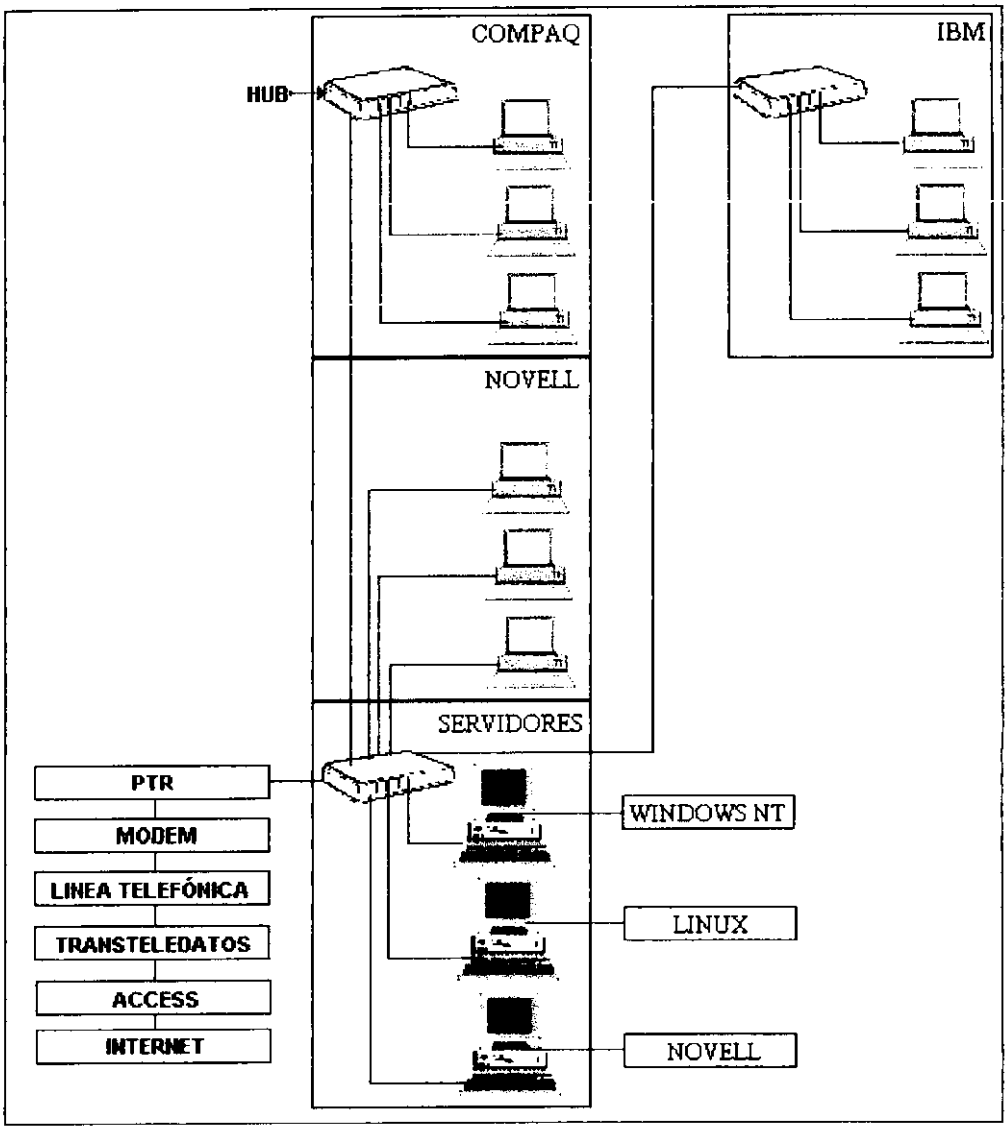


Figura 29. Red LAN de la PUCESA

g) Topologia de red.- La red se encuentra construida con una arquitectura Ethernet en estrella, armada con cableado estructurado utilizando un cable par trenzado de cuatro pares con conectores RJ-45.

Se posee un Rack en el laboratorio de IBM con un Patch Panel y un HUB, a los cuales llegan todos los cables de conexión de las computadoras de este segmento de red y de éste se derivan hacia el servidor; los otros segmentos de red (COMPAQ y NOVELL) no poseen estos aditamentos.

h) **Tarjetas de interfaz de red.-** Cada uno de los equipos tanto servidores como clientes poseen tarjetas de interfaz de red que permiten una conexión a la red. Estas tarjetas están diseñadas para soportar conectores RJ-45, también en algunos equipos encontramos que sus tarjetas de red soportan conectores tipo BNC.

i) **Protocolos de red.-** Como protocolo de red se utiliza TCP/IP, ya que para este tipo de topología es el más ideal, además que permite un libre acceso a través de un servidor a INTERNET si éste se encuentra enlazado.

j) **Recursos y periféricos compartidos.-** En este tipo de redes, se puede compartir tanto impresoras como recursos propios de los equipos como son las unidades discos duros, sean íntegras o parciales como las unidades de disco flexible.

CAPITULO III

EVALUACION LOGICA DE LA RED

3.1 MODELO DE INTERCONEXION DE SISTEMAS ABIERTOS

Podemos comprender cómo funcionan las redes de comunicación utilizando el Modelo de Interconexión de Sistemas Abiertos el cual se basa en los estándares tomados por la Organización Internacional de Normalización (ISO, International Organization for Standarization) la cual creó una norma que es el modelo de OSI (Open Systems Interconnection). Este define un modelo de niveles para un entorno de sistemas abiertos, donde un proceso que se ejecuta en una computadora puede comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicación de niveles OSI. La figura 30 representa un modelo OSI:

NIVEL 7	Aplicación
NIVEL 6	Presentación
NIVEL 5	Sesión
NIVEL 4	Transporte
NIVEL 3	Red
NIVEL 2	Enlace de Datos
NIVEL 1	Físico

Figura 30. Modelo de Interconexión de Sistemas Abiertos OSI

Durante una sesión de comunicación, los procesos que se ejecutan en cada nivel de la computadora se comunican unos con otros. El nivel inferior define los componentes físicos reales como conectores y cables, y la transmisión eléctrica de los bits de datos entre los sistemas. El nivel inmediatamente por encima define los métodos de empaquetado y direccionamiento de datos. Aún más arriba están los métodos para mantener activas las sesiones de comunicación. Finalmente, los

niveles más altos describen cómo las aplicaciones usan los sistemas subyacentes de comunicación para interactuar con las aplicaciones de otros sistemas.

El modelo OSI se usa para describir y definir cómo se comunican los distintos protocolos, como se muestra en la figura 31 se comparan varios protocolos en relación con el estandard OSI:

OSI	NetWare	UNIX	AppleTalk	LANManager
Aplicación / presentación	Protocolo principal de Netware	Sistemas de Clasificación de red (NFS)	AppleShare / Protocolo de clasificación AppleTalk (AFP)	Bloques de Mensaje del Servidor
Sesión	Conductores nominados / NetBios	SNMP / FTP / SMTP / Telnet	ASP / ADSP / ZIP / PAP	NetBios / Conductores nominados
Transporte	SPX	TCP	ATP / NBP / AEP / RTPM	NETBEUI
Red	IPX	IP	Protocolo de distribución de datagrama(DDP)	
Enlace de Datos	Controladores LAN / ODI / NDIS	Controladores LAN / Control de acceso al medio	Controladores LAN / Local-Talk / Ether-Talk / Token-Talk	Controladores LAN / NDIS
Físico	Físico	Físico	Físico	Físico

Figura 31. Comparación del modelo de protocolo

Los protocolos se cargan en una computadora como los controladores de software. Cada nivel de la pila de protocolos define un conjunto concreto de funciones. Una aplicación en el nivel más alto interactúa con el nivel de debajo cuando necesita enviar información a otro sistema de la red. La petición se empaqueta en un nivel y se pasa al siguiente, que añade la información de las funciones generadas en ese nivel, creando un nuevo paquete dentro del paquete. Posteriormente, se pasa este paquete al siguiente nivel y el proceso continúa, como se muestra en la figura 32 que indica la información que se relaciona con las funciones de cada nivel y que se añade al paquete cuando desciende por la pila del protocolo.

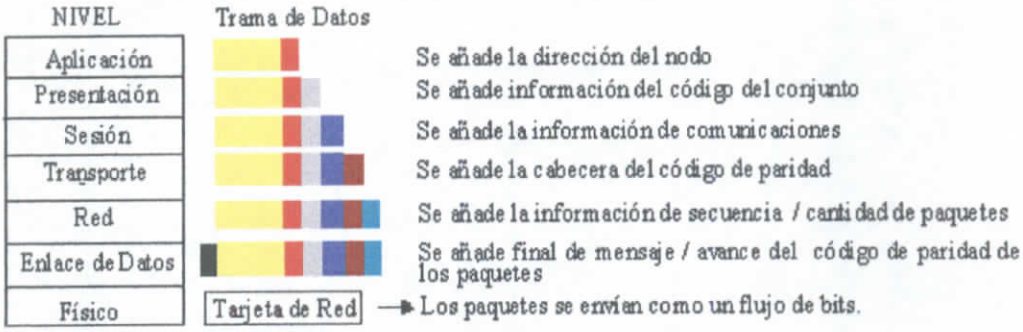


Figura 32. Información que se relaciona con las funciones de cada nivel y que se añade al paquete cuando desciende por la pila de protocolo

Cada nivel añade información al paquete del mensaje y el nivel correspondiente en la pila de protocolos del sistema de recepción lee esta información. De esta forma, cada nivel del protocolo se comunica con su nivel de protocolo par, para facilitar la comunicación.

Cada nivel define los procedimientos y las reglas que los subsistemas de comunicación deben seguir para comunicarse con sus pares de los otros sistemas. A continuación se enumeran algunos ejemplos de los procesos gestionados por los subsistemas de comunicación:

a) Interacción e intercambios entre aplicaciones, además de traducciones entre las diferentes sintaxis y representaciones de datos.
b) Gestión de intercambio de datos tanto en el modo dúplex como en el modo semi-dúplex.
c) Gestión de sesión orientada a la conexión (es decir, la supervisión y el mantenimiento de un canal de comunicación entre dos sistemas).

d) Procedimientos de encaminamiento y direccionamiento de red.

e) Controladores de red (es decir, la fragmentación de los datos para prepararlos para la transmisión).

f) Funciones de tarjeta de la interfaz de red (es decir, la transmisión de señales eléctricas, ópticas o de radio sobre los medios de la red).

Los desarrolladores de software utilizan protocolos normalizados para crear productos que interoperen con los de otros desarrolladores. Por ejemplo, los niveles inferiores definen técnicas de interacción del hardware. Un desarrollador que trabaja a este nivel diseña controladores de hardware y software de red que siguen las reglas definidas de ese nivel.

En una sesión de comunicación real, cada nivel de la pila de protocolos se comunica con su nivel par en el otro sistema; para ello, añade la información que necesita comunicar en un paquete que se pasa al siguiente nivel inferior del protocolo, como se mencionó previamente.

Se debe tener el hardware de red a nivel físico, disponible antes de que puedan tener lugar cualquiera de lo otros niveles de comunicación, por eso se describe primero el nivel físico. A continuación se describen los diferentes tipos de niveles:

a) Nivel físico.- Establece las características físicas de la interfaz como son los componentes y conectores mecánicos, los aspectos eléctricos como los valores binarios que representan niveles de tensión, y los aspectos funcionales entre los que se incluyen el establecimiento, mantenimiento y liberación del

enlace físico. Las interfaces de nivel físico más conocidas en las comunicaciones de datos incluyen RS-232 y RS-449 del Asociación de Industrias Electrónicas EIA (Electronic Industries Association), esta última sucesora de RS-232. El RS-449 permite distancias de cable mayores. Los sistemas de red de área local más conocidos son Ethernet, anillo con testigo y la Interfaz de Datos Distribuidos por Fibra (FDDI, Fiber Distributed Data Interface).

b) Nivel de enlace de datos.- Define las reglas para el envío y recepción de información a través de la conexión física entre dos sistemas. Este nivel codifica y sitúa los datos en tramas para la transmisión, además de ofrecer detección y control de errores, los niveles superiores pueden no necesitar gestionar tales servicios. Sin embargo, cuando se utilizan medios fiables, el rendimiento mejora si se realiza el control de los errores en los niveles superiores, en lugar de en éste. Los puentes operan en este nivel de la pila de protocolos. He aquí los protocolos genéricos que ocupan el nivel de Enlace de Datos:

- Control de Enlace de Datos de Alto Nivel (HDLC, High-level Data Link Control) y protocolos síncronos orientados a bit afines.
- Controladores LAN y métodos de acceso como Ethernet y anillo con testigo.
- Redes de área extensa de paquetes rápidos como Frame Relay y Modo de transferencia asíncrono (ATM, Asynchronous Transfer Mode).

- Especificación de la Interfaz del Controlador de Red (NDIS, Network Driver Interfaz Specification) de Microsoft.
- Interfaz Abierta de Enlace de Datos ODI (Open Data-link Interface) de Novell.

c) **Nivel de red.-** Define los protocolos para abrir y mantener un camino sobre la red entre los sistemas. Se relaciona con los procedimientos de transmisión y conmutación de datos, y oculta tales procedimientos a los niveles superiores. Los encaminadores operan en el nivel de red. Este nivel mira las direcciones del paquete para determinar los métodos de encaminamiento. Si se direcciona un paquete a una estación de trabajo de la red local, se envía directamente allí. Si se direcciona a una red de otro segmento, el paquete se envía al dispositivo de encaminamiento, que lo envía a la red. He aquí los protocolos genéricos que ocupan el nivel de red:

- Protocolo Internet (IP).
- Protocolo X.25.
- Intercambio de Paquetes entre Redes (IPX, Internetwork Packet Exchange).
- Protocolo Internet VINES (VIP) de Banyan.

d) **Nivel de transporte.-** Proporciona un alto nivel de control para trasladar la información entre sistemas, así se incluyen las utilidades más sofisticadas de gestión de errores, prioridades y seguridad. El nivel de transporte ofrece servicios de calidad y distribución segura mediante la utilización de los

servicios orientados a la conexión entre los sistemas finales. Controla la secuencia de paquetes, regula el flujo del tráfico y reconoce los paquetes duplicados. El nivel de transporte asigna la información empaquetada un número de seguimiento que se controla en el destino. Si el dato desaparece del paquete, el protocolo del nivel de transporte en el sistema receptor acuerda con el nivel de transporte en el sistema de transmisión que posee paquetes a retransmitir. Este nivel asegura que se reciben todos los datos y en el orden adecuado. Se puede establecer un círculo lógico, que es como una conexión dedicada, para proporcionar una transmisión fiable entre sistemas. Entre los protocolos del nivel de transmisión que no son OSI y que pueden proporcionar servicios orientados a la conexión, se incluyen los siguientes:

- Protocolo de Control de Transmisión (TCP, Transmission Control Protocol).
- Protocolo de Datagramas de Usuario (UDP, User Datagram Protocol) de Internet.
- Intercambio Secuencial de Paquetes (SPX, Sequenced Packed Exchange) de Novell.
- Protocolo de Comunicación entre Procesos VINES (VICP, VINES Interprocess Communication Protocol) de Banyan).
- NETBIOS/NetBEUI de Microsoft.

e) **Nivel de sesión.-** Coordina el intercambio de información entre sistemas mediante técnicas de conversación o diálogos. Los diálogos no son siempre necesarios, pero algunas aplicaciones pueden necesitar una forma de saber

dónde reiniciar una transmisión de datos si se perdió temporalmente una conexión, o puede necesitar un diálogo periódico que indique el final de un conjunto de datos y el comienzo de otro nuevo.

f) **Nivel de presentación.-** Forman parte del sistema operativo y de la aplicación que el usuario ejecuta en una estación de trabajo. En este nivel se da formato a la información para visualizarla o imprimirla. Los códigos se interpretan dentro de los datos, como pueden ser las secuencias de tabulación o gráficos especiales. También se gestiona el cifrado de datos y la traducción.

g) **Nivel de aplicación.-** Las aplicaciones acceden a los servicios de red subyacentes mediante procedimientos definidos. El nivel de aplicación se utiliza para definir una serie de aplicaciones que gestionan transferencias de archivos, sesiones de terminales e intercambio de mensajes (por ejemplo, correo electrónico). Aquí se listan los protocolos del nivel de aplicación OSI:

- Terminal virtual.
- Acceso y Gestión en la Transferencia de Archivos (FTAM, File Transfer Acess and Management).
- Procesamiento de Transacciones Distribuidas (DTP, Distributed Transaction Processing).
- Sistema de gestión de menajes (X.400).
- Servicios de directorio (X.500).

La figura 33 muestra cómo fluyen los datos a través de la pila de protocolos y sobre el medio desde un sistema a otro.

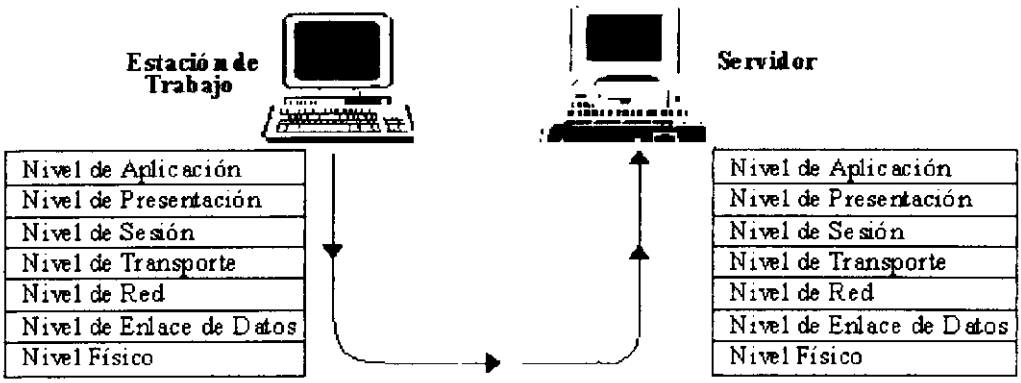


Figura 33. Los paquetes se ensamblan cuando descienden a través de los niveles de protocolo y se desensamblan cuando ascienden por los niveles de la pila

La figura 33 muestra cómo fluyen los datos a través de la pila de protocolos y sobre el medio desde un sistema a otro. Los datos comienzan en los niveles de aplicación y presentación, donde trabaja un usuario con una aplicación y presentación, un usuario con una aplicación de red, como un programa de correo electrónico, Las peticiones de servicio del nivel de presentación se pasan al nivel de sesión, que comienza el proceso de empaquetado de la información. Entre los dos sistemas se abre una sesión de comunicación orientada a la conexión para ofrecer transmisiones fiables. Una vez que se establece la sesión, los niveles de protocolos comienzan el intercambio oportuno de la información.

La configuración y evaluación lógica de la red se determina revisando el sistema operativo de red que corre tanto en el equipo servidor como en el equipo cliente.

3.2 EVALUACION DE LA CONFIGURACION DEL SERVIDOR CENTRAL

3.2.1 WINDOWS NT DE MICROSOFT

Windows NT de Microsoft está diseñado para permitir que los vendedores de software desarrollen aplicaciones que aprovechen los potentes nuevos equipos de escritorio, incluyendo aquellos que están diseñados alrededor de los procesadores Intel, DEC y demás. Windows NT amplia las características de Windows 3.1 y ofrece muchas facilidades que lo hacen ser único entre los demás sistemas operativos. Windows NT está dirigido a un amplio público como se describe a continuación:

a) Usuarios finales que necesiten resultados y la capacidad de intercambiar muchas aplicaciones.
b) Usuarios de los grupos de trabajo que necesiten compartir su sistema con otros usuarios, conectarse con otros computadores compartidos, intercambiar correo electrónico y planificar reuniones y compromisos de grupo.
c) Creadores de software que quieran desarrollar aplicaciones para ejecutarlas en sistemas que trabajen con Windows NT.
d) Administradores de red que necesiten un entorno de red seguro y que aproveche las ventajas de los nuevos sistemas de computadores multiproceso.

El último punto es especialmente importante. Windows NT no está restringido a los sistemas Intel como ocurre con DOS y Windows. Puede ejecutarse sobre cualquiera de los siguientes procesadores, y se plantea desarrollar el soporte para otros, como el Motorola Power PC:

a) Sistemas con procesador Intel 80386, 80486 y Pentium.
b) Sistemas de Computadoras con Repertorio Reducido de Instrucciones (RISC, Reduced Instruction Set Computer) MIPS R4000 de 64 bits.
c) Sistemas RISC de 64 bits basados en el DEC Alpha.
d) Sistemas Super Servidor que usan una combinación de procesadores y diseños de bus especiales patentados.

IBM está trabajando para hacer que Windows NT esté disponible en sus sistemas super servidor, lo cual incluye características tales como tolerancia a los fallos, Sistemas de Dispositivos Redundantes de Discos Baratos (RAID, Redundant Arrays of Inexpensive Disks), memoria correctora de errores y registros de errores hardware.

Windows NT es un sistema operativo de 32 bits con multitareas priorizadas y protección de memoria, además de soporte para el multiproceso simétrico y el trabajo en red, todo con un interfaz gráfico de usuario. La capacidad que posee Windows NT de acceder plenamente a los procesadores de 32 bits, permite trabajar con grandes números, direcciones de memoria e instrucciones. Por encima de todo se consigue rendimiento, que es el

resultado de haber potenciado la combinación de la capacidad de ejecución del procesador, la transferencia de datos y el acceso a memoria.

Cuando el sistema operativo puede hacer varias cosas a la vez se le denomina *Multitarea* y cuando el usuario u otra tarea puede interrumpir la ejecución de una tarea, en lugar de esperar a que termine por completo estamos halando de tarea *Priorizada*. Como la velocidad del procesador es tan alta, las actividades relacionadas con el hardware, como el acceso a disco, pueden parecer increíblemente lentas. Cuando un sistema operativo no priorizado accede al disco, el procesador espera mientras se accede al disco mecánico, con lo que se pierden ciclos de procesamiento. En Windows NT se pueden realizar múltiples tareas simultáneamente, así que si una tarea queda colgada al acceder a un dispositivo lento del tipo de un disco, el procesador puede volver su atención hacia otras tareas. Básicamente, no se pierde ningún ciclo de proceso.

La protección de memoria asegura que los múltiples programas se ejecuten en su propio espacio de memoria y no corrompan la memoria usada por las otras aplicaciones. Si falla una aplicación, el resto de ellas y el sistema operativo permanecen activos, de modo que los usuarios pueden cerrar sus trabajos y salir de forma adecuada.

El multiprocesamiento simétrico hace que Windows NT pueda aprovecharse de múltiples procesadores. A pesar de que los sistemas multiprocesadores existen desde hace tiempo, normalmente estos sistemas asignan tareas

dedicadas a cada procesador, como la entrada/salida de la red. Este multiprocesamiento asimétrico posee un procesador dedicado a cada tarea, implica que cada procesador permanece inactivo cuando termina su trabajo específico. El multiprocesamiento simétrico es más difícil de implementar, pero proporciona unos resultados superiores.

Las facilidades de red de Windows NT permiten la compartición de archivos del sistema propio con otros usuarios de la red y la conexión con directorios compartidos de otros sistemas. Las computadoras que ejecutan Windows para trabajo en grupo pueden participar en la red. Además, Windows NT viene con software y controladores que soportan conexiones con otros tipos de sistemas operativos, como las Computadoras centrales (Mainframes) de UNIX e IBM.

El producto Windows NT Advanced Server es una versión de Windows NT que aporta sofisticadas facilidades de servidor de archivos para grandes entornos de redes. Incluye facilidades adicionales para la protección de datos, como la duplicación automática de datos en discos secundarios.

3.2.1.1 SOPORTE PARA OTROS ENTORNOS

Integrado en Windows NT se halla el entorno Win32 que soporta aplicaciones NT de 32 bits. Además, NT incluye algunos otros subsistemas entorno. Estos subsistemas permiten que aplicaciones diseñadas para otros sistemas operativos se ejecuten bajo Windows NT. Se accede a ellos arrancando Command Prompt en el grupo Main

del Program Manager. Los subsistemas que se incluyen son los siguientes:

a) **El subsistema Máquina DOS Virtual (VDM, Virtual DOS Machine).-** Emula el entorno MS-DOS para que se puedan ejecutar aplicaciones DOS.

b) **El subsistema Máquina DOS Virtual Win16**.- Emula el entorno Windows (16 bits) de modo que pueden ejecutarse aplicaciones Windows 3.1. Las aplicaciones se ejecutan en un modo de emulación 80286.

c) **El subsistema OS/2.-** Permite que se ejecuten aplicaciones basadas en caracteres de MS OS/2 1.x. Este subsistema no se soporta en la computadoras MIPS o DEC Alpha.

d) **El subsistema POSIX.-** Ejecuta aplicaciones que se ajustan al estándar de la Interfaz de Sistema Operativo Portátil (POSIX, Portable Operating System Interface) para entornos de informática, tal como lo define el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

3.2.1.2 MEMORIA VIRTUAL

La memoria virtual es un medio de que las aplicaciones y el sistema operativo dispongan de más memoria de la que está físicamente presente en la computadora. Cuando la memoria comienza a escasear se realizan intercambios (swapping) con disco para que otros procesos tengan memoria. Por ejemplo, si un proceso posee en memoria información que no usa de forma habitual, esta información se copia en disco, con lo cual el espacio de memoria queda disponible para otro proceso.

3.2.1.3 EL SOPORTE DEL SISTEMA DE ARCHIVOS WINDOWS NT

El sistema de archivos original de Windows NT es el Nuevo Sistema de Archivos NT (NTFS, NT File System), pero Windows NT también soporta los sistemas de archivos antiguos, descritos aquí:

a) **Sistema de archivos Tabla de Localización de Archivos (FAT, File Allocation Table).-** Este es el sistema de archivos de DOS. Usa un formato de nomenclatura de archivos con nombres de ocho caracteres y extensión de tres. Windows NT puede acceder a unidades FAT, pero si el sistema se arranca en DOS, no se puede acceder a las unidades NTFS.

b) **Sistema de Archivos de Alta Resolución (HPFS, High Performance File System).-** Este es el sistema de archivos diseñados para OS/2 con el que se consiguen nombres de archivos largos. También posee facilidades de resolución que FAT no posee. Windows NT puede acceder a las unidades HPFS.

c) **NTFS.-** Este es el nuevo sistema de archivos de Windows NT. Proporciona nombres de archivos largos, protección y recuperación de datos, y seguridad a través de los permisos de directorio y archivo.

Si se instala Windows NT en un sistema nuevo, es más cómodo formatear todo el disco como NFS. En los sistemas ya existentes, se podría preferir guardar parte del sistema de archivos existente. Hay varias opciones de instalación:

a) Se puede guardar una partición existente de otro sistema operativo e instalar NTFS en otra partición separada. Cuando se inicializa el sistema aparece una pantalla que permite seleccionar el sistema operativo que se desea arrancar.
b) Se puede convertir la partición de inicialización existente en un volumen NFS.
c) Se puede reformatear una partición existente como NFS. Esto borra los archivos existentes en la partición.

3.2.1.4 PROTECCION DE ARCHIVOS Y DEL SISTEMA

Windows NT incluye varias facilidades que protegen los datos almacenados en su sistema de archivos frente a usuarios no autorizados y frente a posibles daños. Para proteger el sistema frente accesos sin autorización, todos los usuarios deben iniciar la sesión tecleando un número de cuenta y una clave. El administrador del sistema puede aplicar varias restricciones de acceso a las cuentas que, por ejemplo, deshabilitan la cuenta tras un período de tiempo o fuerzan a que los usuarios cambien sus claves.

Windows NT también proporciona mecanismos de protección del sistema de archivos que detectan y rechazan los sectores de disco erróneos y realmacenan transacciones que no se hayan escrito por completo debido a fallos en la alimentación. La información importante del sistema de archivos también se duplica en el disco para protegerla frente a fallos de sectores. El programa de instalación también crea un disco reparador que se puede usar para traer la copia de seguridad de Windows NT en el caso de que se haya corrompido la información de inicialización.

Windows NT también admite Fuentes de Alimentación Ininterrumpida (UPS, Uninterruptable Power Supplies) que aportan una corriente de seguridad procedente de baterías, cuando falla la corriente alterna. El sistema trabajará durante un cierto período de

tiempo, lo que permite que los usuarios cesen su trabajo en el sistema y escriban en disco toda la información de la memoria.

3.2.1.5 REDES

Los servidores de red de Windows NT son compatibles con los servidos de Microsoft Windows para trabajo en grupo, Microsoft LAN Manager y Windows NT Advanced Server. Las computadoras que trabajan con cualquiera de estos sistemas operativos pueden compartir directorios, archivos y recursos. Se incluye soporte para el Sistema Básico de Entrada Salida para Redes (NetBIOS, Network Basic Input Output System), la Interfaz de Usuario Extendido por NetBIOS (NetBEUI, NetBIOS Extended User Interface) y para Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP). También existe el soporte para conectarse con Novell NetWare a través de los protocolos de Intercambio Secuencial de Paquetes/Intercambio de Paquetes entre Redes (SPX/IPX, Sequenced Packet Exchange/Internetwork Paquet Exchange).

Windows NT emplea las Especificaciones de la Interfaz del Controlador de Red (NDIS, Network Driver Interface Specification) de Microsoft como una interfaz adaptadora de la red. Con NDIS, los vendedores de tarjetas de red simplemente tienen que crear controladores que sean compatibles con NDIS. Así, los usuarios finales pueden comprar tarjetas compatibles NDIS con la seguridad de

que trabajarán adecuadamente con Windows NT. NDIS soporta diversas tarjetas de interfaz con la red en el mismo sistema, con lo que el sistema puede acceder a diferentes tipos de redes.

3.2.1.6 JERARQUIA DE USUARIOS Y SEGURIDAD

Windows NT sigue las normas de seguridad de Protección de acceso controlado C2 del Departamento de defensa de los Estados Unidos. Las reglas C2 requieren que las computadoras implementen una política de seguridad e inspección de sucesos, no solo para el acceso de los usuarios de la red, sino también para los usuarios locales. La seguridad de nivel C2 de Windows NT proporciona lo siguiente:

a) Los usuarios poseen cuentas especiales que requieren que se acceda a ellas con claves de identificación. La cuenta sigue la pista de varias de las acciones realizadas por un usuario, con el propósito de realizar una auditoría, tales como inicios y abandonos de sesión y accesos a archivos. También se tienen en cuenta tareas de gestión tales como el cambio de las cuentas de usuario o la configuración de los servidores.
b) Los administradores y usuarios pueden controlar el acceso a los archivos, directorios y recursos (impresoras) de su propio sistema.
c) Los administradores del sistema pueden rastrear y ver los sucesos revisables.

d) A los usuarios se les prohibe examinar el contenido de la memoria.

Como Windows NT proporciona capacidades de compartición de archivos y recursos, la seguridad se ve afectada por el acceso de múltiples usuarios a una misma computadora. Los administradores y usuarios deben poder proteger los archivos compartidos de su propio sistema, frente a usos no autorizados. Sin embargo, la seguridad lleva aparejada una cierta cantidad de administración. Se deben aplicar permisos a los directorios y los administradores deben crear cuentas de usuarios a las que se accede mediante clave y proporcionar restricciones en el acceso.

La información relativa a las cuentas de inicio de sesión se almacena en la base de datos principal (denominada Gestor para la Seguridad de las Cuentas o SAM, Scutiry Account Manager) de cada sistema Windows NT. Cuando un usuario accede, se comprueba en el SAM del sistema al que accede su nombre de usuario y su clave.

Aunque la base de datos SAM aporta una seguridad adecuada a los sistemas Windows NT locales, existe una *relación de confianza*, el cual introduce algunos problemas de seguridad y mantenimiento en otras computadoras de la red que posean archivos y recursos compartidos. Por ejemplo, se pueden definir derechos de acceso para grupos de usuarios de la red, pero no para usuarios individuales que

necesiten acceder a un sistema desde otra computadora de la red. Aquí es donde desempeña su papel el Windows NT Advanced Server.

El producto Windows NT Advanced Server puede establecer relaciones de confianza con otras computadoras de la red. Esto quiere decir que una computadora pueda autentificar a un usuario y proporcionarle información de acceso acerca de los usuarios de otras computadoras. Así, los usuarios pueden iniciar la sesión en una computadora y acceder a otra, sin necesidad de iniciar la sesión separadamente en cada una de ellas.

Una característica interesante del sistema de seguridad es que la información de protección asignada a los archivos viaja con ellos. Por ejemplo, si se otorga a un usuario la capacidad de abrir un archivo pero no de modificarlo, se aplicarán los mismos derechos incluso si el dispositivo de almacenamiento se traslada a otro sistema.

3.2.1.7 IMPRESION

Si se conecta un sistema Windows NT a una red, se pueden compartir las impresoras del sistema con otros usuarios o acceder a las impresoras compartidas de la red. El Print Manager de Windows NT contiene todas las facilidades y funciones necesarias para instalar, configurar y compartir cualquier otra actividad de gestión de las impresoras.

El control del tipo de acceso a las impresoras que poseen los usuarios, viene dado por los permisos. Por ejemplo, los administradores pueden evitar o permitir que los usuarios accedan a una impresora y otorgar a algunos de ellos la capacidad de controlar los documentos de la cola del Print Manager. Los administradores poseen pleno control sobre las impresoras.

3.2.1.8 OPCIONES DE REGISTRO E INICIALIZACION

La persona que instala Windows NT en una computadora especifica la clave del administrador, con lo que posee el pleno control del sistema. Este usuario administrador puede crear cuentas protegidas por palabras clave, de forma que otros usuarios puedan registrarse en el sistema. Además, pueden asignarse derechos y permisos a cada cuenta de usuario para otorgar o restringir el acceso al sistema y sus archivos. Si un usuario inicia la sección en un sistema Windows NT y no puede acceder a ciertos archivos, es porque su cuenta incluye estas restricciones.

Cada usuario que inicia la sesión con su propia cuenta, puede modificar su propia cuenta, puede modificar el entorno para adaptarlo a sus necesidades. Por ejemplo cuando un usuario entra en el sistema puede rearrancar el entono y añadir nuevos iconos de inicialización para los programas que él usa. Cuando otro usuario acceda al sistema, no podrá ver los cambios que realizó el primer usuario y podrá crear

su propia configuración personalizada que el primer usuario no podrá ver. Sin embargo los administradores pueden crear configuraciones comunes que pueden ver los otros usuarios.

3.2.2 WINDOWS PARA TRABAJO EN GRUPO DE MICROSOFT

Windows para Trabajo en Grupo (Windows for Workgroups) de Microsoft es una versión para redes par a par del popular sistema operativo Windows. Facilita que la gente pueda conectar sus computadores, compartan información y trabajen juntos. Pueden enviarse mensajes de correo electrónico a los asociados, planearse reuniones de grupo, compartir archivos e impresoras, gestionar calendarios y trabajar juntos en proyectos de grupo.

Con Windows para trabajo en grupo, cualquier 80386 o modelo posterior puede actuar como un servidor y compartir sus recursos (archivos e impresoras) con otros usuarios de la red. Cualquier otro sistema conectando a la red y que esté ejecutando Windows para trabajo en grupo puede usar aquellos recursos compartidos como un cliente. Se puede ejecutar el programa en un sistema que ya esté conectado a una red, o se puede construir una nueva red mediante la adición de tarjetas de interfaz con la red. Un producto similar llamado Workgroup Connection for MS-DOS contiene todo el software que se necesita para conectar un PC cuyo sistema operativo sea MS-DOS, a un servidor Windows para trabajo en grupo.

Windows para trabajo en grupo proporciona a los programadores las características y herramientas que necesitan para escribir aplicaciones Windows que se beneficien de las capacidades de los grupos de trabajo. Esto garantiza que surjan muchas aplicaciones de red compatibles. Las aplicaciones podrán extenderse fácilmente para que soporten la funcionalidad del correo electrónico en Windows para trabajo en grupo. Por ejemplo, las hojas de cálculo, documentos, mensajes pueden enviarse a otros usuarios, simplemente conectándolos al correo de mensajes.

Este producto es compatible con otros productos Microsoft como Windows NT. También es compatible con las redes Novell Netware e incluye el soporte para el protocolo de comunicación intercambio secuencial de paquetes/Intercambio de paquetes entre redes (SPX/IPX). Los usuarios pueden acceder simultáneamente a las redes Microsoft y Netware. Los administradores y los usuarios pueden instalar y configurar Windows para trabajo en grupo en una única sección de arrastrar y soltar. Esto ahorra tiempo y problemas y reduce las necesidades de soporte de sobremesa.

El hecho de conectar computadoras en una red incluye algunas ventajas básicas:

a) Transferencia de archivos y rápidas y cómodas entre computadoras de red.
b) Almacenamiento de archivos y copias de seguridad centralizados.

c) Soporte para la Vinculación e Incrustación de Objetos (OLE) a través de la red, con lo que se consigue la actualización automática de la información de los documentos enlazados.

d) Correo electrónico y mensajería.

e) Compartición de impresoras, discos duros, unidades de CD-ROM y otros dispositivos periféricos.

f) Aplicaciones par grupos de trabajo.

Las facilidades y utilidades son parte de este paquete como se describen a continuación:

a) Microsoft Mail.- Es un servicio de correo electrónico que permite que los usuarios lean, compongan, envíen y respondan mensajes de correo electrónico, además de gestionar los mensajes que se reciben.

b) Schedule +.- Es una aplicación muy completa para la planificación gráfica que permite a la gente programar reuniones de grupo y gestionar electrónicamente sus calendarios diarios y listas de tareas.

c) Network DDE.- Proporciona un medio para que los usuarios creen documentos compuestos que compartan datos a través de la red.

d) Seguridad.- Ofrece características de seguridad que pueden impedir que usuarios no autorizados accedan a los recursos compartidos de la red. Los usuarios del sistema pueden compartir archivos e impresoras

con otros usuarios a dos niveles. Los otros usuarios de la red pueden o bien tener acceso completo al directorio, o bien permisos concedidos para leer usuarios claves específicas, relacionadas con el nivel de seguridad que deberían tener. Si se requiere una seguridad más sofisticada, se recomienda usar Windws NT o Novell Netware.

3.2.3 UNIX

En 1969 y los primeros setenta, Ken Thompson y Dennis Ritchie desarrollaron en los laboratorios AT&T Bell, el sistema operativo UNIX. Es un sistema multiusuario que soporta las redes interconectadas y los sistemas de archivos distribuidos como el Sistema de Archivos de Red (NFS, Network File System) de Sun Microsystems o la implementación del Sistema de Archivos Andrew (AFS, Andrew File System) de la Fundación de Software Abierto (OSF, Open Software Foundation). Después de que AT&T pusiera el sistema Unix a disposición de las universidades y facultades para que lo usaran en proyectos de investigación y programas de informática, se hicieron algunas variantes de este sistema operativo. La versión es la UNIX System V Release 4.2 (SVR 4.2) que incluye, entre otras, las mejoras de la Berkeley Software Division.

A continuación, se enuncian algunos de los mayores logros del sistema UNIX:

a) En los primeros ochenta, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y el Instituto Americano de Normalización (ANSI) definieron la Interfaz de Sistema Operativo Portátil para UNIX (POSIX, Portable Operating System Interface), con el fin de crear un estándar industrial UNIX, y un conjunto de interfaces de programación de aplicaciones para el desarrollo de aplicaciones portátiles. Todavía hoy, hay varios grupos de trabajo dentro del IEEE encargados de definir el estándar. La Organización Internacional para la Normalización (ISO, International Organización for Standardization) adoptó en 1988 las especificaciones originales.

b) Algunas compañías como Bull, Nixdorf, Philips, y Siemens fundaron el grupo X/Open para promocionar los estándares de UNIX abierto mediante la comprobación de su conformidad con otros productos.

c) IBM, DEC, Hewlett-Packard, Nixdorf, Siemens y otros centenares de miembros formaron en 1988 la Fundación de software abierto para el desarrollo tanto del sistema operativo distribuido OSP/1 UNIX, como el Entorno de Informática Distribuida (DCE, Distributed Computing Environment).

d) El UNIX System Laboratory (USL) de AT&T, Control Data, Data General, Informix, Intel, Motorola, NCR, Olivetti, Texas Instruments y cientos de otras compañías, fundaron el 1988 Unix Internacional, para promocionar el UNIX abierto a través de documentación disponible públicamente. Después de satisfacer sus objetivos, la organización se deshizo a finales de 1993.

e) IBM, Hewlett-Packard, SunSoft, Novell y otros, fundaron en 1993 el Entorno Genérico de Software Abierto (COSE, Common Open Software Environment) con el objetivo de cooperar en la consecución de un entorno común de sobremesa (interfaz gráfico de usuario) para UNIX que rivalizará con Microsoft Windows.

f) En 1991 Novell y el UNIX System Laboratory (USL) de AT&T se asociaron para crear Univell, una compañía con el propósito de desarrollar UnixWare, un sistema UNIX de sobremesa integrado en el soporte Novell NetWare. En 1993, Novell compró USL y formó el Grupo de Sistemas UNIX (USG, UNIX System Group) para la gestión de UnixWare. Eventualmente. Univell llegará a desarparecer.

Con la compra de USL, Novell alcanzó el control de UNIX SVR 4, ante la consternación de los demás vendedores. Sin embargo, en un intento de consolidar en la industria un sistema operativo UNIX común, Novell dio la patente de UNIX a la organización X/Open. X/Open concede la patente a aquellas implementaciones que sean compatibles con un conjunto de especificaciones definidas por el grupo COSE. Este conjunto de implementaciones llamadas COSE Spec1170 APIs, define interfaces de programación que promueve la portabilidad de aplicaciones entre dos sistemas operativos.

Una de las principales ventajas de UNIX es su amplio uso como la plataforma de desarrollo y sistema operativo de escritorio. Como se mencionó antes, AT&T permite que el código esté disponible en los ambientes académicos,

con lo que estimula su proliferación en muchas plataformas y el desarrollo de aplicaciones únicas. La mayor parte de este trabajo se hizo en la Universidad de California, en Berkeley, donde se realizaron diferentes versiones conocidas como las Distribuciones de Software de Berkeley (BSDs, Berkeley Software Distributions). UC Berkeley es responsable de la adición de los protocolos de conexión de redes Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) y de transportar UNIX al DEC VAX. Existe un cierto número de variaciones de UNIX, entre las que se encuentran XENIX de Microsoft. ULTRIX de DEC y Ejecutivo Interactivo Avanzado (AIX, Advanced Interactive Executive) de IBM, LINUX para redes.

El sistema operativo se popularizó en primer lugar en los entornos de ingeniería, diseño asistido por computador y científicos. Eventualmente encontró su camino en los negocios, la medicina, y muchos otros entornos. Otro factor que contribuyó a la popularidad de UNIX es que está escrito en el lenguaje de programación C. Debido a ello, UNIX es altamente portátil y contiene componentes del sistema escritos en un lenguaje de programación común bien conocido, que se pueden recompilar fácilmente para que trabajen en toda una gama de sistemas.

Hoy en día el mayor crecimiento y desarrollo de UNIX establece un lugar en sistemas más pequeños, del tipo de los basados en los procesadores Intel x86 y las estaciones de trabajo de bajo precio construidas a partir del *chip* Computadora con un Repertorio Reducido de Instrucciones (RISC). El gran número de versiones de UNIX ha frenado su aceptación en la Industria, pero

el creciente uso de Windows NT ha proporcionado un incentivo a los vendedores de UNIX para que creen productos compatibles e interfaces gráficos de usuarios para promocionar el entorno UNIX.

3.2.3.1 EL NUCLEO DE UNIX Y SU SISTEMA DE ARCHIVOS

UNIX consiste básicamente en un pequeño núcleo que ejecuta procesos, además de aplicaciones de usuario y servicios. El núcleo (kernel) de UNIX es un sólido corazón que cambia muy poco de un sistema a otro, mientras que el usuario puede añadir procesos a discreción. Este enfoque de diseño facilita que el usuario añada nuevos servicios o elimine los que ya no sean necesarios. Así además se fomenta la simplicidad, ya que no hay que volver a compilar la totalidad del sistema operativo. Los usuarios interactúan con el sistema operativo a través de un *shell*, que también es un proceso que acepta entradas del usuario y realiza diversas tareas. Como el shell es un proceso reemplazable, hay muchas variaciones, como el Bourne shell, el C shell y el Korn shell.

El sistema de archivos es jerárquico. Hay un directorio de raíz y un grupo de subdirectorios que dependen de él, cada uno de los cuales posee su propio conjunto de subdirectorios. Los archivos se almacenan en los directorios (o en los subdirectorios) y su nombre completo incluye la ruta completa en el árbol de directorios, aunque si el contexto actual es el directorio en el que está almacenado el

archivo, no es necesario especificar el camino completo. Los nombres de los dispositivos del tipo de los monitores y las impresoras se manejan de la misma forma que los archivos. Por ejemplo, un usuario podría dirigir la salida de un proceso o de un listado de archivo bien a un monitor, bien a una impresora, sin más que usar sus nombres en una orden. Una facilidad de encauzamiento proporciona un modo de dirigir la salida de una orden, como una clase, a otra orden.

3.2.3.2 UNIX EN EL ENTORNO DE REDES

El UNIX y los protocolos TCP/IP están estrechamente enlazados. Hoy en día, la mayor parte de las implementaciones UNIX incluyen TCP/IP y el soporte para Ethernet, lo que simplifica en gran medida la conexión de redes dentro de ese entorno. Además, el Sistema de Archivos en Red (NFS) de Sun Microsystems es el sistema de compartición de archivos que se distribuye, normalmente, de forma conjunta con UNIX, aunque OSF está implementando el Sistema de Archivos Andrew (AFS), que es superior en muchos casos. De esta forma, UNIX proporciona en un solo paquete la posibilidad de instalar en una computadora un potente sistema operativo que permite que los usuarios compartan archivos y ejecuten programas en las computadoras de otros usuarios, junto con un uno de los más comunes y potentes protocolos de red, de entre los existentes en la industria.

TCP/IP es un protocolo de red extremadamente útil y extendido. Fue desarrollado por el Departamento de Defensa de los Estados Unidos, como una forma de conectar muchos sistemas diferentes. TCP/IP incluye varias aplicaciones que facilitan la transferencia de archivos y el acceso entre dos sistemas. Como Telnet y el Protocolo de transferencia de archivos (FTP). Telnet es un programa para terminales remotos que permiten que un usuario controle un programa en un sistema anfitrión (host). FTP proporciona un medio para la transmisión de archivos entre dos sistemas. NFS permite que los usuarios accedan a archivos de sistemas remotos, de la misma forma que si fuesen parte del propio sistema. No se precisa ninguna orden o procedimiento extra para el listado de archivos, la consulta de sus contenidos, la creación de nuevos archivos o la copia en el disco rígido local. El sistema de archivos remotos está mapeado así que aparece como un disco local.

3.2.3.3 X WINDOW

Es una Interfaz Gráfica de Usuario (GUI, Graphical User Interface) normalizada y usada en sistemas UNIX. Una GUI es una interfaz controlada por medio del ratón y el teclado con menús despegables, botones en la pantalla, barras de desplazamiento y ventanas superpuestas par la ejecución de aplicaciones independientes. Ejemplos de otros entornos de GUI incluyen Macintosh de Apple, Windows de Microsoft y OS/2 Presentation Manager de IBM. Sin

embargo, el entorno X Window es un diseño cliente-servidor que funciona bien sobre enlaces remotos.

Con respecto a los programadores, X Window proporciona herramientas software e interfaces de programas de aplicación normalizadas para la creación de aplicaciones distribuidas basadas en gráficos. Las aplicaciones completadas son independientes del hardware, lo que significa que se pueden ejecutar en cualquier sistema que soporte el entorno X Window. El entorno completo frecuentemente se referencia simplemente como X.

X Window ejecuta programas en una o más ventanas en una pantalla representada como una mapa de bits. Los usuarios pueden ejecutar múltiples programas a la vez en cada ventana y cambiar de ventana mediante la pulsación en ellas con el ratón. Como se muestra en la figura 34 se dibuja el entorno X Window que se describe en la lista siguiente:

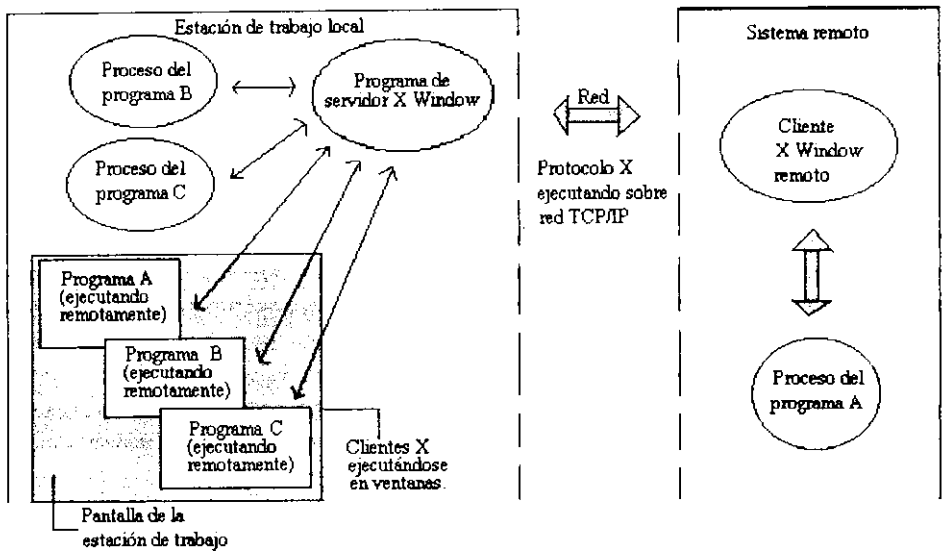


Figura 34. Entorno cliente-servidor en X Window

a) Un programa llamado el Servidor X se ejecuta en la estación de trabajo local y gobierna sus ventanas y programas.

b) Cada ventana de programa se llama un Cliente X e interacciona con el programa del servidor X que se ejecuta en la misma máquina con el uso de una relación cliente-servidor.

c) El servidor X realiza todo el procesamiento del programa para los Clientes X, al interactuar con aquellos clientes con un sistema de mensajería. El Servidor X controla el entorno local entero, así que los programas cooperan cuando acceden a memoria y a otros recursos del sistema.

d) El Servidor X ejecuta el programa Gestor de X Window (X Window Manager), que proporciona interacción con GUI. Actualmente, están disponibles dos gestores de ventana: Motif y Open Look. Ambos son similares funcionalmente y ejecutan los mismos programas.

e) El Servidor X que se ejecuta en la máquina local puede interactuar con programas que se ejecutan en computadoras remotas y muestran la salida de aquellos programa en una ventana local. Esto es una relación cliente-servidor, pero el servidor local posee el control completo, con lo que los procesos remotos se denominan clientes, no servidores, porque están bajo el control del Servidor X local.

Este último punto es extremadamente importante en Internet y en otros entornos de red de área extensa. Los usuarios pueden trabajar con programas que se ejecutan en computadoras remotas. El programa remoto se ejecuta próximo a los recursos a los que necesita acceder frecuentemente, como datos en disco. Sólo la información necesaria par la actualización de la pantalla del usuario local se transmite sobre el enlace remoto con la consiguiente reducción de los cuellos de botella que pudieran producirse si se transmitiera todo el programa y sus datos al sistema local para su procesamiento.

La interfaz entre el Servidor X y los Clientes X remotos es orientada a eventos y se basa en los protocolos X. Este protocolo se ejecuta sobre el Protocolo de Control de Transmisión/Protocolo Internet TCP/IP. En algunos casos, los vendedores han mejorado el entorno X Window mediante la adición de facilidades como las imágenes tridimensionales. Una ventaja del entorno X es que las aplicaciones servidor pueden ejecutarse en cualquier plataforma, mientras la

aplicación puede intercambiar mensajes sobre un protocolo de transporte común con el cliente. Así, los programadores pueden construir aplicaciones compatibles con X Window en varios sistemas y cualquier aplicación que soporte X Window puede acceder a esas aplicaciones.

X Window es la interfaz de usuario par Motif de la Fundación de Software Abierto (OSF, Open System Foundation) y el sistema Open Look. También el sistema operativo Solaris 2 de SunSoft incrementa una prestación de X Window desarrollada por AT&T.

3.2.3.4 PROTOCOLO X.25

El protocolo X.25 es una recomendación del CCITT (ITU) que define las conexiones de terminales y de computadoras a las redes de conmutación de paquetes. Las redes de conmutación de paquetes encaminan los paquetes de datos a través de una red a los nodos destinos. X.25 es un servicio de conmutación de paquetes bien conocido que tradicionalmente use usa para la conexión de terminales remotos a sistemas anfitriones (host). El servicio proporciona conexiones cualquiera a cualquiera para usuarios simultáneos. Como muestra la figura 35, se pueden multiplexar las señales de múltiples usuarios a través de una interfaz X.25 en la red de conmutación de paquetes y distribuirlas a diferentes lugares remotos. Un canal de comunicación llamado *circuito virtual* conecta estaciones finales a

través de la red sobre un trayecto predefinido. La interfaz X.25 soporta velocidades de línea de hasta 64 Kbits/seg., aunque una parte importante del rendimiento es la sobrecarga para la corrección de errores.

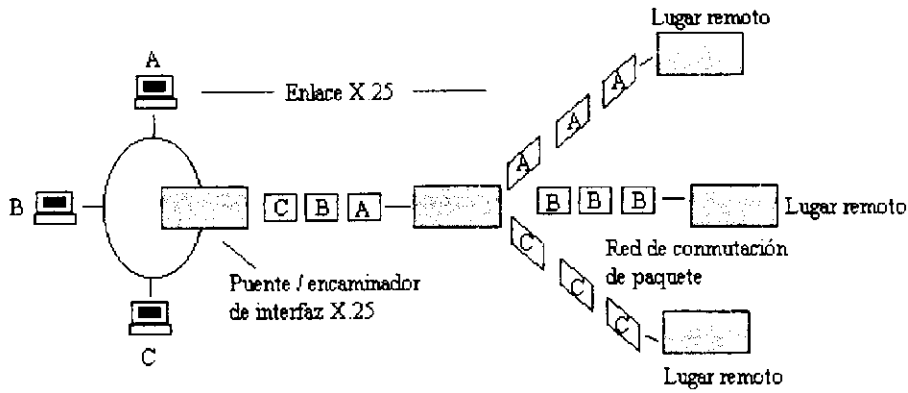


Figura 35. Red de conmutación de paquetes X.25

La arquitectura de conmutación de paquetes de X.25 incluye ventajas y desventajas. Los paquetes de información se encaminan a través de una red de malla, en función de la información que contenga la cabecera del paquete sobre la dirección destino. Los usuarios pueden conectarse con muchos lugares diferentes, a diferencia de las redes orientadas a circuitos donde existe un trayecto dedicado entre sólo dos puntos. Debido a que los paquetes viajan a través de los puertos compartidos de los encaminadores, es posible que se produzcan los retardos en la distribución. Los usuarios experimentan una prestación lenta cuando más y más personas acceden a la red, aunque la mayoría de las redes pueden soportar exceso de tráfico por el encaminamiento alrededor de las áreas congestionadas. Por contraposición, las redes orientadas a circuitos proporcionan un ancho de banda fijo entre dos

puentes que no se acomoda a las ráfagas de tráfico que sobrepasen ese ancho de banda.

La sobrecarga en X.25 es excesiva si se compara con Frame Relay. Por ejemplo, en X.25, cada nodo a lo largo de un trayecto de paquetes, debe recibir completamente un paquete y realizar una verificación de errores en el paquete antes de enviarlo. Los nodos Frame Relay simplemente examinan la información del destino de la cabecera del paquete y lo envían inmediatamente, en algunos casos antes de recibirlo completamente. Frame Relay no necesita las tablas de estado usadas en X.25 en cada nodo intermedio, par ocuparse de la gestión, control de flujo y verificación de errores. Los nodos finales deben detectar tras perdidas y pedir una retransmisión.

X.25 adolece de prestaciones pobres y no es aceptable para la mayoría de las aplicaciones en tiempo real LAN o WAN. Sin embargo X.25 es muy conocido, entendido y aceptado para el acceso a terminales o a computadoras remotas, siempre y cuando el tráfico sea ligero. X.25 puede ser el único camino fiable para establecer enlaces de red internacionales con países con sistemas telefónicos no fiables. Casi todos los países poseen servicios X.25. Por el contrario, la obtención de circuitos dedicados fiables en algunos países es casi imposible.

X.25 precede al modelo del protocolo de Interconexión de sistemas abiertos OSI, lo que explica que la terminología usada para explicar

X.25 sea diferente. La norma define protocolos en tres niveles, que se corresponden exactamente con los tres niveles más bajos de la pila de protocolos de OSI, como se describe a continuación:

a) **Nivel físico.-** Llamado interfaz X.21, define la Interfaz Física/Eléctrica desde la Computadora/Terminal (DTE, Data Terminal Equipmet o Equipo terminal de datos) al nodo de unión de la red de conmutación de paquetes X.25.

b) **Nivel de acceso de enlace.-** Define las transmisiones de datos como una secuencia de tramas. El protocolo usado en el Procedimiento de Acceso a Enlaces Equilibrados (LAP-B, Link Access Procedure-Balanced), que forma parte del protocolo de Control de Enlace de Datos a Alto Nivel (HDCL, High-level Dat Link Control). Se diseña LAP-B para las conexiones punto a punto. Proporciona la estructura de trama, mecanismos de control de errores y flujo para sesiones en modo asíncrono equilibrado. LAP-B proporciona un modo de reconocer que un paquete ha alcanzado cada enlace de la red.

c) **Nivel de paquetes.-** Define los circuitos virtuales fiables a través de la red de conmutación de paquetes. Así, X.25 proporciona la distribución de datos punto a punto, el lugar de la distribución punto a punto multipunto.

El concepto de circuito virtual es importante en X.25. Un circuito virtual establece un canal de comunicaciones lógico temporal o permanente entre dos puntos extremos a través de la red de conmutación de paquetes. El uso de un circuito garantiza que los paquetes lleguen en secuencia, ya que siguen la misma trayectoria. También proporciona transporte fiable de datos a través de la red. hay dos tipos de circuitos virtuales en X.25:

a) **Circuitos virtuales temporales y basados en llamada.-** Se establece y a continuación se desarman cuando la sesión de transferencia de datos se completa.
b) **Circuitos virtuales permanentes.-** Mantienen una conexión constante entre dos nodos finales.

X.25 usa paquetes de establecimiento de llamada para el establecimiento inicial de un canal de comunicaciones entre dos estaciones finales. Una vez que se establece la llamada, los paquetes de datos transfieren información entre las estaciones. Nótese que debido a que X.25 es un servicio orientado a la conexión, los paquetes no necesitan direcciones fuente y destino. Los circuitos virtuales proporcionan un trayecto a los paquetes a través de la red hasta el destino. Sin embargo, se asigna un número a los paquetes que los identifica con el canal que enlaza la fuente y el destino.

Las redes X.25 son fáciles de instalar y mantener. Los costos son en función del número de paquetes enviados y en algunos casos, del tiempo de conexión. Téngase en cuenta que para el tráfico de red de área local de alta velocidad son preferibles otros servicios como Frame Relay o conexiones dedicadas.

La fundación europea X/OPEN Consertium Ltd. se estableció para que proporcione normas para el entorno UNIX. Su objetivo principal es promover los protocolos de sistemas abiertos para lenguajes, interfaces, redes y aplicaciones UNIX. También promueve la portabilidad de las aplicaciones entre diferentes entornos de UNIX y soporta las especificaciones de la Interfaz de Sistema Operativo Portátil para UNIX (POSIX, Portable Operating System Interface for UNIX) del Instituto de Ingenieros Eléctricos y Electrónicos IEEE.

3.2.4 NETWARE DE NOVELL

Novell ofrece una serie de sistemas operativos de red bajo el nombre de Netware, desde el básico y económico NetWare Lite al NetWare 4.x, un sistema operativo diseñado específicamente para redes corporativas. Aquí se describe la línea de productos del sistema operativo y más adelante las características generales de los productos NetWare 3.x y NetWare 4.x.

a) NetWare Lite.- Sistema operativo de red par a par de 2 a 25 usuarios. Se ejecuta sobre el sistema operativos DOS y es compatible con

Windows de Microsoft. Los usuarios con poco conocimiento sobre conexión de redes, pueden establecer una para la compartición de archivos, aplicaciones e impresoras.

b) **NetWare 2.x.-** Diseñado para grupos de trabajo y oficinas de pequeño a medio tamaño dentro de grandes compañías. El sistema operativo se ejecuta tanto en modo dedicado como no dedicado en computadoras basadas en 80286 , 80486 de Intel. Proporciona soporte para la interconexión de red local y remota, tanto como las herramientas para los administradores de red.

c) **NetWare 3.x**.- Sistema operativo diseñado para dar soporte a cientos de usuarios en un único servidor dedicado. Ofrece muchas de las utilidades avanzadas, incluso el diseño modular y la capacidad de integrar distintos sistemas, también minicomputadoras.

d) **NetWare 4.x.-** Sistema operativo corporativo de Novell que hereda todas las capacidades de *NetWare 3.x* y añade nuevas utilidades propias para crear un entorno multiservidor distribuido que ofrece servicios de directorio y da soporte a la red corporativa.

El sistema operativo NetWare reside en un servidor de red que es normalmente una computadora de Intel. Proporciona servicios y conexiones de red a las estaciones de trabajo. Como se muestra en la figura 36 se ilustra la relación entre el servidor y la estación de trabajo. Esta relación ofrece un

sistema de comunicación que distribuye los servicios de red a los usuarios de las estaciones de trabajo. El componente importante en el lado del cliente es el software de redirección, que se carga generalmente cuando se arrancan las computadoras. El redireccionador intercepta las órdenes para los servidores de NetWare y las envía a través de la red. Las órdenes que no vienen de la red se envían al sistema operativo local.

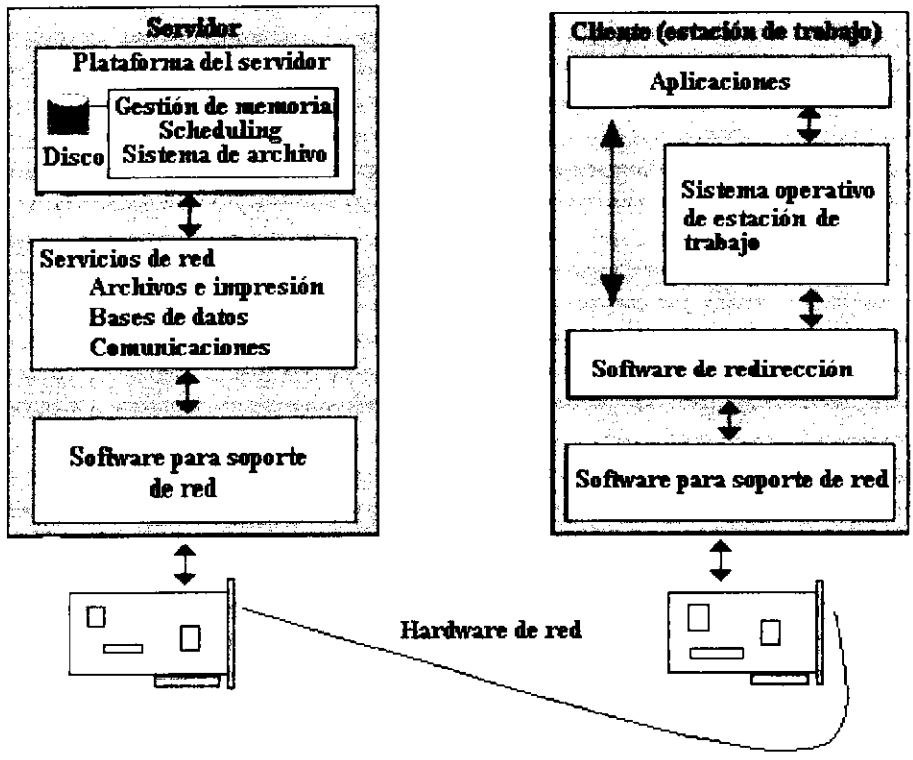


Figura 36. Entorno cliente-servidor en Netware

Las funciones principales proporcionadas por el servidor de NetWare son la gestión del sistema de archivos, la gestión de la memoria y la planificación de las tareas de procesamiento. Obsérvese que la relación entre el servidor y la estación de trabajo se basa en la de cliente-servidor, lo cual significa que las estaciones de trabajo gestionan mucha de la carga de procesamiento, lo que

libera al servidor para que pueda realizar sus propias tareas más eficientemente.

El software que da soporte a la red une el hardware y el sistema de cableado al sistema operativo de la misma. Este software utiliza controladores específicos que proporcionan el soporte para los tipos de tarjetas de red instaladas en el servidor y en las estaciones de trabajo.

3.2.4.1 ARQUITECTURA DE NETWARE

NetWare 3.x y 4.x son sistemas operativos completos de 32 bits que utilizan un único espacio de direcciones sin segmentación (un problema con los sistemas DOS). Esto permite que los programas trabajen de forma más eficiente. El sistema operativo puede gestionar miles de interrupciones y procesos de miles de peticiones de clientes por segundo.

NetWare 3.x y 4.x son modulares y ampliables. Permiten los cambios, actualizaciones y adiciones de la red. Se puede incluir un Módulo Cargable de NetWare (NLM, NetWare Loadable Module) que enlace el servidor al sistema operativo para ofrecer servicios como los siguientes:

a) Soporte que permite el almacenamiento de archivos no DOS.
b) Servicios de comunicación.

c) Servicios de base de datos.

d) Servicios de mensajería.

e) Servicios de archivado y copias de seguridad.

f) Servicios de gestión de red.

Se puede cargar o descargar cualquier módulo de la consola del servidor cuando se quiera sin desconectarlo. Cada módulo utiliza memoria adicional, así que es necesario asegurarse de que el servidor posee suficiente memoria para gestionar los Módulos Cargables de NetWare que se piensen cargar. Debido a que los módulos se localizan en el servidor junto con el sistema operativo, se juntan firmemente con él y poseen acceso a los servicios de forma instantánea.

NetWare es una plataforma ideal para aplicaciones de servidor. Resuelve los problemas de conexión con la gestión concurrente de múltiples protocolos y normas en los niveles intermedios, de transporte, de protocolo de servicio y de sistema de archivos.

Una de las características más importantes de NetWare es su soporte para otros sistemas operativos o *Independencia de protocolos*. Puede unir estaciones de trabajo que ejecuten DOS, Windows, OS/2 y UNIX. Con NetWare se mantiene el soporte para las estaciones de trabajo DOS, Windows y OS/2, al igual que las distintas utilidades de gestión que utilizan la interfaz de Windows. El software para la estación de trabajo OS/2 de NetWare suministrado con NetWare

proporciona el soporte que las estaciones de trabajo OS/2 necesitan para comunicarse con un servidor de NetWare. NetWare permite los atributos extendidos y los nombres de archivos largos de OS/2, y que las aplicaciones del servidor de OS/2 se ejecuten en la red. Se pueden añadir a la red de NetWare como productos opcionales, el soporte para Macintosh de Apple. NFS basado en UNIX, y Acceso y Gestión en la Transferencia de Archivos (FTAM, File Transfer Access and Management) de OSI.

NetWare utiliza una estructura de protocolo independiente conocida como la Interfaz Abierta de Enlace de Datos (ODI, Open Data-link Interface), que proporciona soporte simultáneo para los distintos protocolos en la red. La interfaz ODI ofrece soporte multiprotocolo al servidor. Se permiten diversas tarjetas de interfaces. Los controladores de estas tarjetas se enlazan al nivel de la Interfaz abierta de enlace de datos. Los paquetes se dirigen a la pila de protocolos apropiada por encima del nivel ODI, como los sistemas operativos IPX, TCP/IP o Apple Talk. Los protocolos de servicio próximos a la cima ofrecen soportes de archivos y sistemas para los distintos sistemas operativos que se pueden instalar en un servidor de NetWare.

Se utiliza un esquema parecido en las estaciones de trabajo para permitir a los usuarios conectarse a redes que utilizan diferentes protocolos de comunicación., como TCP/IP. Necesitará productos

WorkPlace para LANs de Novell o parecidos de otros vendedores que proporcionen el soporte TCP/IP para las estaciones de trabajo.

Si se necesita conectar estaciones de trabajo a LANs de NetWare tanto como a otros tipos de redes, como las redes LAN Manager de Microsoft. LAN Server de IBM y 3Com 3+Share, se puede instalar el controlador par Soporte de Red de la Interfaz Abierta de Enlace de Datos (ODINSUP, Open Data-link Interface Network Support) suministrado con el paquete de NetWare. ODINSUP permite que coexistan la interfaz del controlador de red de ODI y la Especificación de la Interfaz del Controlador de Red (NDIS, Network Driver Interface Specification), que es una especificación de Microsoft para el soporte de múltiples controladores.

3.2.4.2 UTILIDADES DE PRESTACIONES

Una de las razones de que NetWare sea popular en el entorno de LAN son sus prestaciones. Novell hace mucho tiempo que se alejó de un sistema operativo de red que se ejecutase en DOS y diseñó NetWare para acceder directamente a las utilidades avanzadas de la CPU del servidor. NetWare 386 fue el primer sistema operativo de red de 32 bits en el mundo de las computadoras para equipos de escritorio. El núcleo del sistema operativo NetWare es tanto multitarea como multihilos, lo cual significa que proporciona capacidades de multiusuario en el servidor y altas prestaciones durante el tiempo en

que hay cargas pesadas en el sistema. Algunas de las características de NetWare se describen a continuación:

a) **Configuración dinámica.-** NetWare se configura dinámicamente para equiparar las condiciones de uso en la red. Las siguientes características se configuran dinámicamente:

- Uso de memoria.
- Caché de directorios.
- Número de entradas al volumen del directorio.
- Tamaño de la tabla de archivos abierta.
- Búferes o memoria intermedia de encaminamiento.
- Indexación de la Turbo FAT.
- Procesos de servicios.
- Transacciones activas del Sistema de Seguimiento de Transacciones (TFS, Transaction Tracking System).

Se pueden alterar los valores límite y máximo de modo que no se fuerza NetWare. También se puede cambiar la rapidez de configuración del sistema operativo y se puede establecer la cantidad máxima de recursos utilizados.

b) **Gestión de memoria.-** NetWare soporta hasta 4 GB de RAM en el servidor. La gestión de memoria en NetWare 4.x se diseñó para incrementar su eficiencia. NetWare V3.11 asigna memoria

para diferentes usos en cinco o más zonas. Esto produce que algunas aplicaciones se queden sin ella debido a que, cuando un proceso utiliza la memoria, las rutinas de gestión no la reasignan para otros usos. NetWare 4.x gestiona la memoria como si se tratase de una única zona y es más efectivo en la asignación de memoria entre operaciones.

c) **El sistema de archivos.-** El sistema universal de archivos en NetWare posee muchas utilidades que mejoran la eficiencia como:

- **Método del ascensor (elevator seeking):** Esta utilidad del sistema de disco da prioridad a las peticiones de lectura que entran, proporcionado su localización actual, y que se basan en cómo la cabeza lectora de la unidad de disco puede mejorar el acceso a ellas. El funcionamiento del método del ascensor es análogo al del ascensor de un edificio. No sube y baja pisos al azar, simplemente se basa en quién solicitó el servicio primero; se para en los pisos intermedios hacia arriba o hacia abajo para recoger pasajeros que necesitan montarse. El método del ascensor minimiza el movimiento de la cabeza del disco, de esta manera mejora el tiempo de acceso y reduce la degradación del hardware.

- **Caché de archivos:** La caché de archivos minimiza el número de veces que se debe acceder al disco. En el búfer de la caché se mantienen los archivos que se leen más menudo, donde si es necesario pueden ser accedidos. Esto elimina la necesidad de ir al disco a por la información. Se da prioridad a los archivos en la caché de tal manera que se saca de ella al menor número de archivos utilizados para dejar espacio a los nuevos.

- **Escrituras en paralelo:** Las escrituras en disco se gestionan independientemente de las lecturas del mismo en NetWare. Esta separación permite que el sistema operativo escriba datos en el disco cuando disminuyen las peticiones de los usuarios al mismo. Las escrituras en paralelo dan mayor prioridad a los usuarios que necesitan leer datos de la unidad, lo cual mejora las prestaciones desde su punto de vista.

- **Búsquedas solapadas:** Esta utilidad de NetWare está disponible si hay dos o más discos rígidos y cada uno se conecta a su propio controlador (canal de disco). NetWare accede a todos los controladores simultáneamente. Si se enlazan dos discos a un controlador, sólo se accede a uno de estos discos en un momento dado.

- **Turbo FAT:** Esta utilidad también se conoce como tabla de asignación de archivos indexada. La turbo FAT indexa esta tabla de archivos sobre 2 MB, así el sistema operativo localiza los segmentos de la FAT de forma inmediata sin necesidad de leerla.

- **Compresión de archivos:** NetWare 4.x puede incrementar el espacio del disco hasta un 63 por ciento con su utilidad de compresión de archivos. NetWare gestiona la compresión en paralelo. Los administradores y usuarios pueden marcar los archivos que serán comprimidos después de utilizarlos.

- **Subasignación de bloques:** Esta utilidad de NetWare 4.x maximiza el espacio del disco. Si hay bloques de disco utilizados parcialmente (por lo general un bloque posee un tamaño de 8K), NetWare los divide en bloques con subasignaciones de 512 bytes para el almacenamiento de los archivos pequeños o de los fragmentos de los archivos.

Se permiten archivos con un tamaño de hasta 4 GB y el sistema de archivos soporta más de 2 millones de directorios y archivos por volumen, y 100.000 archivos abiertos. Los volúmenes se pueden extender sobre múltiples unidades de disco y se puede

incrementar dinámicamente su tamaño si se añaden nuevas unidades.

El sistema de archivos salvables de NetWare permite la recuperación de los archivos borrados. Se puede asignar una mínima cantidad de tiempo durante la cual un archivo borrado se mantiene recuperable, así como marcar los archivos par que se depuren de forma inmediata. También se pueden mantener todos los archivos borrados hasta que el volumen se quede sin espacio de disco; después los archivos borrados hace más tiempo se eliminan para liberar espacio para los nuevos. Los derechos de administrador para los archivos se conservan tras recuperar un archivo y se pueden asignar para controlar quiénes pueden almacenarlos. Los archivos borrado se conservan incluso si se borra un directorio

3.2.4.3 UTILIDADES PARA PROTECCION DE LOS DATOS

El sistema operativo de red NetWare contiene diversas utilidades que garantizan la seguridad y fiabilidad de los datos. Las de seguridad protegen los datos de los usuarios no autorizados y de los ataques de virus. NetWare soporta utilidades de fiabilidad hardware que proporcionan redundancia, la cual asegura que los datos se escriben correctamente y están disponibles si una parte del sistema falla.

a) **Seguridad.-** Las utilidades de seguridad de NetWare son críticas para grandes entornos de red corporativa. Los sistemas de archivos de NetWare y de DOS son bastante diferentes; un usuario no puede acceder al sistema de archivos de NetWare si arranca el servidor con un disco DOS o simplemente si inicializa el disco. Por supuesto, esto no evita que la gente robe o destruya un disco; aún se necesita realizar una copia de seguridad para protegerse contra tales desastres, pero un ladrón no puede acceder a los datos in los derechos de acceso y las palabras clave adecuados.

La seguridad se ofrece a varios niveles:

- **Seguridad de inicio de sesión/palabra clave:** Los usuarios escriben la orden LOGIN para tener acceso al sistema de archivos. Introducen su nombre de usuario y después una palabra clave. No se permite el acceso sin la clave. Después de haber iniciado la sesión, pueden acceder a las computadoras de una inter-red en función de los derechos de acceso que les asignen los administradores de la red.

- **Restricciones de cuenta:** En NetWare, el administrador de la red gestiona la cuenta de cada usuario. Se pueden aplicar restricciones a las cuentas para controlar cuándo

pueden iniciar la sesión los usuarios, las estaciones en las que pueden iniciarla y cuándo finalizan sus cuentas. También es posible forzar a los usuarios a cambiar sus palabras clave regularmente y requerirles una clave única que no se parezca a ninguna de las utilizadas recientemente.

- **Seguridad de archivos y objetos:** En NetWare 4.x el administrador de la red otorga a los usuarios derechos de administrador a objetos tanto como a directorios y archivos. Estos derechos determinan exactamente cómo pueden acceder los usuarios a los recursos del sistema. Normalmente a los gestores se les otorga derechos sobre objetos como pueden ser los servidores y las cuentas de usuarios. A los usuarios se les da derechos a archivos y directorios, así pueden acceder al sistema de clasificación.

- **Seguridad inter-red:** Los Servicios de Directorios en NetWare (NDS, NetWare Directory Services) siguen a todos los objetos en una inter-red, entre los que se cuentan los objetos de usuario y sus derechos de acceso. Los administradores de la red utilizan NDS para la creación y gestión de cuentas de usuarios, seguimiento de los recursos de la red y asignación de acceso a estos recursos para los usuarios. Los usuarios que inician la sesión

poseen acceso a todos los recursos de la red que el sistema NDS les otorga.

Además de la implementación de estas utilidades de seguridad para el usuario, NetWare realiza controles de seguridad entre bastidores. Cifra todas las palabras clave del servidor y las claves de los usuarios en el cable cuando se trasladan al servidor. Esta última utilidad evita que escuchas electrónicas ocultas obtengan una palabra clave si "pinchan" el cable y después accedan al sistema como usuarios normales.

b) **Utilidades de fiabilidad.-** El sistema operativo de red NetWare ofrece varias utilidades importantes que aseguran la supervivencia y la recuperación rápida de los datos en el servidor.

- **Verificación para leer después de escribir:** Esta utilidad lee todas las escrituras del disco al tiempo que se escriben para verificar que son correctos. Si aparece un error, los datos se reescriben mientras permanecen en la caché. Un error puede indicar un sector defectuoso, que la utilidad Hot Fix, que se describe más adelante, puede marcar como inutilizable.

- **Directorios duplicados:** NetWare duplica la estructura del directorio raíz para proporcionar una copia de seguridad en caso de que se corrompa la estructura del directorio principal.

- **FAT duplicada:** Se mantiene un duplicado de la tabla de asignación de archivos como una copia de seguridad. Si el original se puede, el disco permanecerá accesible por medio del duplicado.

- **Hot Fix:** Esta utilidad detecta y corrige defectos del disco cuando se ejecuta el sistema. Los datos en sectores defectuosos se trasladan a otra parte del disco y los sectores se marcan como inutilizables.

- **Tolerancia a Fallos del Sistema (SFT, System Fault Tolerance):** Esta utilidad permite que se proporcione redundancia en el hardware del sistema. Se pueden instalar dos discos y hacer una imagen (mirror) del contenido del disco principal al disco secundario. Si el disco principal falla, el disco secundario le sustituye. También se puede duplicar o duplexar el controlador del disco, para mayor protección ante fallos hardware. SFT Leve III (opcionalmente disponible) lleva a otra etapa de redundancia con la duplicación del servidor entero. Si el

servidor principal se viene abajo, el servidor secundario toma el mando sin interrupción.

- **Sistema de Seguimiento de Transacciones (TTS, Transaction tracking system):** Protege los archivos de datos de escrituras incompletas. Esto se puede producir cuando un usuario edita los registros de una base de datos y el servidor se viene abajo. Cuando el servidor se rearranca, retira las transacciones incompletas de modo que los archivos se encuentren igual que antes de comenzar la transacción. En este sistema se deben completar o abandonar las transacciones totalmente.

- **Supervisión de UPS:** NetWare supervisa el estado de una Fuente de Alimentación Ininterrumpida (UPS, Uninterruptible Power Supply) para determinar si el servidor funciona con una fuente de reserva. Una UPS compatible con NetWare es capaz de proporcionarle esta señal. Si se produce un fallo en la fuente, NetWare avisa a los usuarios (que deben estar fuera del área suprimida o en su propia UPS) y después almacena cualquier información abierta (datos de la caché) antes de cerrar el sistema.

3.3 EVALUACION DE LA CONFIGURACION DE LOS EQUIPOS CLIENTE

3.3.1 MODELO CLIENTE-SERVIDOR

En el modelo cliente-servidor, los usuarios trabajan en computadoras denominadas sistemas frontales (front-end) e interaccionan con sistemas servidores denominados posteriores (back-end), que proporcionan servicios tales como el acceso a una base de datos, la gestión de red y el almacenamiento centralizado de archivos. Una red de computadoras ofrece la plataforma de comunicación en la que numerosos clientes pueden interactuar con uno o más servidores. La interacción entre la aplicación que ejecutan los usuarios en sus sistemas frontales y el programa (generalmente base de datos o un sistema operativo de red) en el servidor posterior se denomina relación Cliente-Servidor. Esto implica que el usuario dispone de una computadora con su propia capacidad de procesamiento, que ejecuta un programa que puede efectuar la interacción con el usuario y la presentación de la información. Así, el modelo cliente – servidor reemplaza al paradigma de informática centralizada como se describe a continuación:

a) En el modelo de informática centralizada, los usuarios situados en terminales no inteligentes se comunican con computadoras anfitrionas (host). Todo el procesamiento tiene lugar en el anfitrión, y los usuarios únicamente escriben órdenes que envían a dicho anfitrión y observan el resultado en su monitor.

b) En el modelo de informática cliente-servidor, el sistema cliente ejecuta una aplicación que interacciona con otro programa que se ejecuta en el servidor.

El modelo cliente-servidor se aplica en sistemas operativos y aplicaciones. Los sistemas operativos de red, tales como NetWare de Novell están orientados a este modelo puesto que los usuarios situados en las estaciones de trabajo realizan peticiones de obtención de los servicios de la red al servidor adecuado, además de enviar las peticiones de servicios locales al sistema operativo local. En los sistemas gestores de bases de datos que siguen el modelo cliente-servidor, los clientes realizan las consultas a través de una aplicación frontal que atienden los servidores. En una relación cliente-servidor el procesamiento se divide entre las dos partes. El sistema cliente ejecuta una aplicación que muestra una interfaz de usuario. Da formato a las peticiones de los servicios de la red y muestra la información o los mensajes enviados por el servidor. El servidor realiza el procesamiento posterior, como por ejemplo la clasificación de datos o la realización de un informe. Debido a que los datos se encuentran perfectamente accesibles, el cliente realiza este proceso de forma eficiente. Después de la clasificación, realización del informe o de cualquier otra tarea solicitada por un usuario, el servidor envía los resultados al cliente. El tráfico en la red se reduce debido a que el cliente únicamente obtiene la información que solicitó, no todo el conjunto de datos para clasificar, según el ejemplo anterior.

Los servidores en un entorno cliente-servidor son a menudo potentes sistemas superservidores, minicomputadoras o computadoras centrales, capaces de gestionar adecuadamente las múltiples y simultáneas peticiones que reciben de los clientes, además de realizar tareas de seguridad y gestión de red. Algunas organizaciones han reemplazado sus computadoras centrales, que proporcionaban cinco Millones de Instrucciones por Segundo (MIPS, million instructions-per-second), por un grupo de servidores capaces de ejecutar 1.000 MIPS. Las diversas estrategias cliente-servidor ofrecen una forma de crear plataformas informáticas relativamente asequibles y fáciles de configurar según las necesidades específicas de las aplicaciones.

El software de un sistema cliente-servidor habitualmente consiste en un Sistema Gestor de Base de Datos (DBMS, database management system) instalado en un servidor posterior, hacia el que los clientes dirigen sus peticiones a través de un Lenguaje de Consulta Estructurado (SQL, Structured Query Language). Es particularmente deseable disponer de un Sistema de Procesamiento de Transacciones Interactivo (OLTP, On-Line Transaction Processing) en el modelo cliente-servidor. Mientras que los servidores de archivo y los servidores de base de datos son más comunes, un servidor posterior también puede proporcionar comunicaciones dedicadas y servicios de impresión.

3.3.2 SOFTWARE DEL CLIENTE

El software del cliente se ejecuta en estaciones de trabajo conectadas a las redes. Algunas veces se conoce con el nombre de *software de shell* o de peticiones. Proporciona una forma de que las aplicaciones en ejecución en las estaciones de trabajo realicen peticiones a los servicios proporcionados por los servidores conectados a la red. El software actúa como redireccionador, mediante el reenvío de las peticiones a los servicios locales hacia el sistema operativo local y de las peticiones de servicios remotos a los servicios de la red.

a) **Software cliente de Netware.-** En el entorno Netware, el software cliente se conoce como software de peticiones. Netware constituye un sistema operativo centrado en el servidor (los clientes realizan peticiones a los sistemas configurados específicamente para proveer dichos servicios). En contraste, el entorno de entidades pares de Windows para trabajo en grupo, Windows NT, LANtastic y otros se ha diseñado para permitir a los usuarios la compartición de recursos sobre sus propios sistemas a voluntad, aunque también puedan existir servidores dedicados en la red.

En el entorno Netware, se dispone de software de peticiones para DOS y OS/2. Los módulos relativos a DOS se instalan mediante un disco de instalación especial en cada máquina. El software de peticiones DOS realiza la carga de numerosos módulos en un directorio especial

reconocido durante el arranque de la computadora. Aquí se incluye una relación de los módulos de Netware 4.x:

- **LSL (Link Support Layer):** Carga el controlador que sirve de soporte para múltiples tarjetas de una interfaz de red y realiza la conmutación de los paquetes entre ellas.
- **Lan Driver:** Carga un controlador específico de cada una de las tarjetas de interfaz de red. los controladores se seleccionan en la fase de configuración.
- **IPXODI:** Carga el controlador IPX (Internetwork Packet Exchange) que sirve de soporte a las comunicaciones entre los servidores sobre la tarjeta de interfaz de red especificada. Existen otros controladores disponibles par Apple Talk y TCP/IP.
- **VLMs (Virtual Loadable Modules):** Se realiza la carga de una variedad de VLMs para servir de soporte de las funciones realizadas en la estación de trabajo, tales como cifrado y autenticación, servicios de directorio, redirección a DOS y otras.

Existe una utilidad llamada WSUPDATE, que realiza la actualización del software cliente desde la estación de trabajo de gestión central. Los sistemas que posean programas, utilidades y aplicaciones fuera de fecha se actualizan automáticamente con esta utilidad.

b) Software del cliente Microsoft.- En los entornos Windows para trabajo en grupo y Windows NT, el software cliente se encuentra incorporado.

Durante la instalación del software, el procedimiento de configuración consulta el tipo de tarjeta de interfaz de red instalada en la estación de trabajo, realizando dicha configuración de acuerdo con ella.

El método principal de comunicación en la red implica a los protocolos NetBIOS y NetBeui, que ya se encuentran instalados por defecto. NetBEUI establece y mantiene las sesiones de comunicación entre las estaciones de trabajo, y NetBIOS proporciona una interfaz de red para las aplicaciones, de modo que puedan realizar peticiones de archivo o de impresión a otras estaciones. Téngase en cuenta que la Especificación de la Interfaz del Controlador de Red (NDIS, Network Device Interface Specification) sirve de soporte a IPX/SPX y TCP/IP.

La utilidad de configuración realiza la carga de varios controladores en el directorio WINDOWS y efectúa las modificaciones en los archivos de inicialización (en Windows para trabajo en grupo). Las opciones de inicialización se especifican en un archivo denominado PROTOCOL.INI del directorio Windows.

El software del cliente permite que las estaciones de trabajo actúen como redireccionadores, receptores y servidores. El protocolo SMB (Server Message Blocks) proporciona una forma de comunicación entre estaciones de trabajo a través de la interfaz NetBIOS.SMB, trabaja en el nivel de aplicación del modelo de Interconexión de Sistemas Abiertos OSI. Dispone de las siguientes características:

- **El redirector:** Traduce las peticiones y las encamina a los servidores de la red.
- **El servicio receptor:** Permite una estación de trabajo que escuche los mensajes SMB procedentes de las estaciones que los dirigen a ella.
- **El servicio servidor:** Permite a cualquier sistema Windows NT o Windows para trabajo en grupo proporciona servicios de archivo e impresoras a las estaciones de la red.

c) Clientes TCP/IP.- El protocolo TCP/IP consiste en un protocolo común de comunicaciones implantado en entornos UNIX y sobre Internet.

La mayoría del software de clientes proporciona soporte de TCP/IP, ya incorporado o bien opcional. TCP/IP puede trabajar junto a las pilas de protocolos IPX o NetBIOS en clientes Netware o Windows NT. Por ejemplo, la interfaz abierta de enlace de datos ODI, en Netware d Novell, proporciona la carga de varias pilas de protocolos de modo tal que las estaciones de trabajo puedan ejecutar aplicaciones para acceder a sistemas multiproveedor. La especificación de la interfaz del controlador de red NDIS de Microsofts proporciona estas mismas funciones y permite a los clientes efectuar la carga de NetBEUI/NetBIOS, SPX/IPX, TCP/IP y otros protocolos de forma simultánea.

3.3.3 CONTROLADORES DE LAN

Un controlador de red de área local es un módulo de software incorporado a la estación de trabajo o al servidor que proporciona una interfaz entre una tarjeta de interfaz de red NIC y el software redirector que se ejecuta en la computadora. El controlador se diseña para una NIC específica y se configura para una estación de trabajo o servidor con el uso de un programa de configuración. Este programa pide al instalador que especifique el tipo de NIC y después que inserte el disco que contiene el módulo controlador para esa NIC. Entonces se integra el controlador dentro de la pila de protocolos en uso en esa red, como por ejemplo el protocolo de Intercambio de paquetes entre redes IPX, el Protocolo de control de transporte/Protocolo Internet TCP/IP. Como se muestra en la figura 37 se indica la localización del controlador de NIC en relación con el modelo de Interconexión de sistemas abiertos OSI.

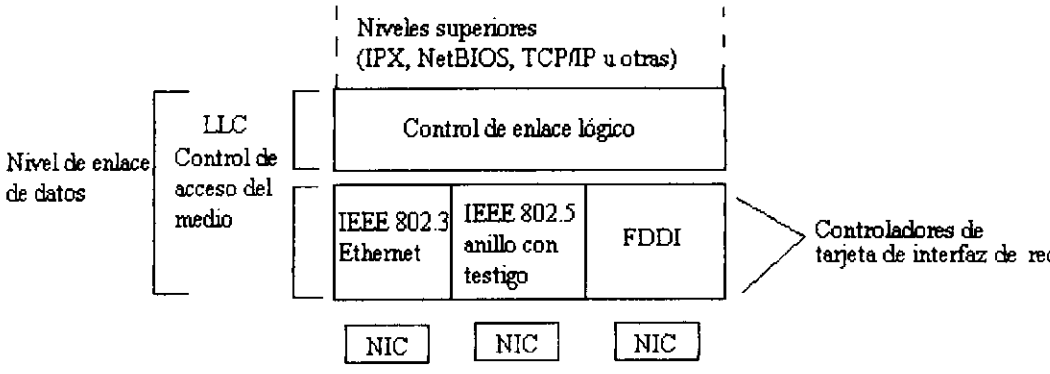


Figura 37. Posición del controlador de LAN en la pila de protocolos

Nótese que los controladores residen en el subnivel más bajo del Control de Acceso al Medio (MAC) del nivel de enlace de datos. La parte superior,

llamada subnivel de Control de Enlace Lógico (LLC), puede realizar la conmutación de datos entre múltiples controladores de tarjetas de red. según se muestra, un servidor podría disponer de tres tarjetas de interfaz de red (Ethernet, anillo con testigo, Interfaz de datos distribuidos por fibra FDDI). Se instala un controlador por cada tarjeta y el subnivel LLC actúa como un puente que conmuta el tráfico entre ellos.

Novell y Microsoft han desarrollado normas especiales de soporte de interfaz que permite a una o más tarjetas de interfaz trabajar con uno o más protocolos de red, según se muestra en la figura 38 la interfaz abierta de enlace de datos ODI de Novell, y la especificación de la interfaz del dispositivo de red NDIS, de Microsoft proporcionan una forma de:

- Transportar IPX, TCP, IP, Apple Talk y otros protocolos sobre una única tarjeta de interfaz de red y un único cable de red.
- Instalar múltiples tarjetas de interfaz de red en una única computadora y trabajar con múltiples pilas de protocolos y operar con dichas tarjetas.

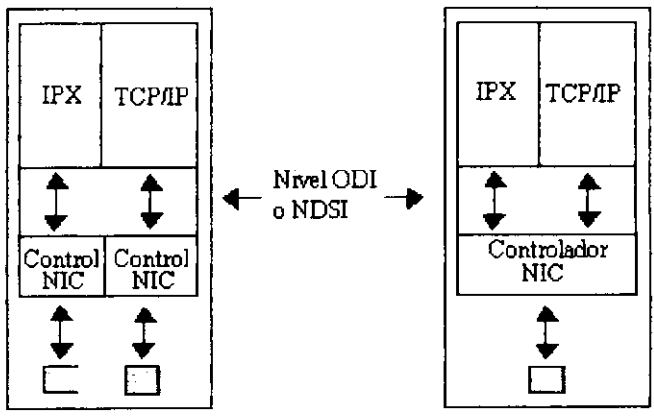


Figura 38. Normas soportadas por el controlador del protocolo de red

3.3.4 PROTOCOLOS DE COMUNICACION

Se definen los protocolos de comunicación dentro del contexto de arquitectura de red en niveles. Cada nivel especifica un protocolo para manejar subsistemas o funciones del proceso de comunicación. Se enumeran las pilas de protocolos de red más comunes para la industria:

a) Modelo de interconexión de sistemas abiertos OSI.

b) Arquitectura de sistemas de red de IBM.

c) DECnet de DEC.

d) Apple Talk de Apple.

e) El grupo Internet, inclusive TCP/IP.

Los protocolos existen en cada nivel para realizar algunas de las tareas que afectan a la comunicación entre los sistemas, mientras los dos sistemas operan con protocolos similares. Aunque típicamente las pilas de protocolo incluye unos siete niveles, es práctico agruparlas dentro de las categorías siguientes:

a) Aplicación.

b) Presentación.

c) Sesión.

d) Transporte.

e) Red.

f) Enlace de datos.

g) Físico.

a) **Protocolo de aplicación.-** Abarcan los niveles de aplicación, presentación y sesión, que son fundamentalmente usuarios de servicios de comunicaciones de red y proporcionan interacción entre aplicaciones e intercambio de datos. Los protocolos de comunicación genéricos incluyen aquellos enumerados aquí, tanto como las Llamadas a Procedimiento Remoto RPCs, (Remote Procedure Calls), los sistemas de procesamiento de transacciones y los sistemas de mensajería. Los protocolos de aplicación establece los siguientes servicios:

- Aplicaciones de IBM y Comunicación Avanzada Programa a Programa APPC, (Advanced Program-to-Program Communication) también llamada LU 6.2.
- Terminal virtual de OSI, Acceso y Gestión en la Transferencia de Archivos FTAM, File Transfer Access y Management), Procesamiento de transacciones de mensajes X.400 y Servicios de directorio X.500.
- Internet, el Sistema de archivos de red de UNIX, el Protocolo Básico de Transferencia de Correo SMTP, (Simple mail Transfer Protocol), el Protocolo de transferencia de archivos FTP, TelNet y el Protocolo Básico de Gestión de Red SNMP (Simple Network Management Protocol).

- Protocolo Principal de Red NCP (Network Core Protocol) de Netware de Novell y shells de los clientes o de los redireccionadores.
- Bloque de mensajes del servidor de Microsoft, NetBIOS y shells de cliente o redireccionadores.
- AppleShare de Apple Talk, Protocolo de Clasificación de Apple Talk AFP (Apple Talk Filing Protocol) y l os protocolos del nivel de sesión como el Protocolo de flujo de datos de Apple Talk ADSP, el Protocolo de sesión de Apple Talk ASP, el Protocolo de acceso a la impresora PAP y el Protocolo de información de zona ZIP.

b) Protocolos de transporte.- Proporcionan servicios de distribución de datos orientados a la conexión a través de redes. Fundamentalmente proporcionan intercambio de datos extremo a extremo en los cuales se mantienen sesiones o conexiones entre sistemas para el intercambio secuencial y fiable de datos. Los protocolos de transporte incluye aquellos aquí enumerados:

- Conexión de Red Avanzada Par a Par APPN (Advanced Peer-to-Peer Networking) de IBM.
- Servicio de Transporte Orientado a la Conexión (COTS, Connection-Orientated Transport Service) y Servicios de Transporte no Orientados a la Conexión CLTs, Connectionless Transport Services) de OSI.

- Parte del Protocolo de control de transmisión TCP del grupo de protocolos de TCP/IP de Internet y UNIX.
- Parte de SPX del grupo de protocolos SPX/IPX de Novell.
- Ingeraces NetBIOS y NetBEUI de Microsoft.
- Protocolo de Mantenimiento de la Tabla de Encaminamiento RTMP (Routing Table Maintenance Protocol) de Apple Talk, Protocolo de Eco de AppleTalk AEP (Apple Talk Echo Protocol), Protocolo de Transacción de Apple Talk ATP (Apple Talk Transaction Protocol), Protocolos de Vinculación de Nombre NBP (Name Binding Protocol).

c) **Protocolos de red.-** Los protocolos del nivel de red proporcionan servicios de enlace para los sistemas de comunicaciones. Manejan la información de direccionamiento y encaminamiento, comprueban los errores y las peticiones de retransmisión. También proporcionan los procedimientos para el acceso a la red, cuando la red usada los especifica en concreto (como Ethernet, anillo con testigo y etc.). entre los protocolos de red se incluyen los siguientes:

- Conexión de red avanzada par a par APPN de IBM.
- Servicio de red orientado a la conexión CONS y Servicio de red no orientado a la conexión CLNS.
- Protocolo Internet del grupo de protocolos TCP/IP de Internet y UNIX.
- La parte del IPX del grupo de protocolos SPX/IPX de Novell.

- Interfaces NetBEUI de Microsoft.
- Protocolo de distribución de datagramas DDP.

Los sistemas de comunicación no necesitan ejecutarse en todos los niveles de los protocolos superiores en un grupo de protocolos particular; sin embargo, los sistemas que no realizan la serie completa de protocolos pueden comunicarse mediante el ascenso al nivel de aplicación.

En el modelo de arquitectura en niveles, cada nivel de la pila de protocolos de una computadora construye una Unidad de Datos del Protocolo (PDU) que envía al nivel par de la computadora con la que se comunica. Realmente el nivel físico transmite PDUs, como bits de datos en forma de tramas al otro sistema, pero los niveles superiores de la pila de protocolos construyen las PDUs, luego las pasas a los niveles inferiores para empaquetarlas de nuevo hasta que alcanzan el nivel físico. El sistema receptor pasa el paquete de información hacia arriba a través de su pila de protocolos, con la extracción de las PDUs de cada nivel de la pila de protocolos. La información extraída de la PDU contiene información de los niveles del protocolo par.

El diálogo entre los niveles del protocolo consta de mensajes y actividades como las enumeradas aquí:

- Hacer peticiones y envío de datos.
- Recibir peticiones e información.
- Rechazar peticiones y datos.
- Reconocimiento de recepción.
- Manejar el búfer de los datos de entrada.
- Pausa y reinicio de las transmisiones.
- Fijar las prioridades de transmisión.
- Manejar la detección, la corrección y la retransmisión de errores.
- Mantener sesiones orientadas a la conexión.
- Numerar y secuenciar paquetes.
- Manejar el direccionamiento y el encaminamiento.

Las entidades de los niveles del protocolo intercambian información de control para efectuar las tareas enumeradas anteriormente. Una vez que se establece una sesión, se intercambian los datos. Durante este intercambio, cada sistema transmite de forma ocasional la información de control que describe el estado de cada sistema al otro. Si se usa, el control de flujo mantiene apartados los datos del exceso de flujo de los búferes del sistema receptor. En los entornos de conexión de red, los niveles del protocolo transmiten los datos en paquetes y luego como flujos de tramas de bits sobre la conexión física. La división de la información de este modo es importante por dos razones. Primera, cualquier error en la red sólo afecta a paquetes individuales, los cuales ser retransmiten más fácilmente que una sesión entera. Segunda, una transmisión grande puede inmovilizar repetidores y conmutadores que

retardan otro tráfico. Los paquetes subdividen la transmisión y permiten que otro tráfico consiga pasar. Una celda, que es una trama de información de tamaño fijo, proporciona mejores prestaciones a este respecto porque la conmutación es constante y predecible.

Una transmisión no orientada a la conexión envía paquetes de una fuente a un destino sin establecer primero un trayecto específico a través de la red. Si hay múltiples trayectos al destino, los paquetes pueden tomar diferentes rutas y llegar fuera de secuencia. Se deben añadir los números de secuencia a los paquetes para que de ese modo la estación receptora pueda ponerlos en orden en caso de que alguno se retarde en la red. también el número de secuencia puede indicar los paquetes perdidos, de ese modo la estación receptora puede solicitar una retransmisión.

a) Protocolo de Control de Transmisión/Protocolo Internet TCP/IP.- Los objetivos de desarrollo para el grupo de protocolos TCP/IP (Transmision Control Protocol/Internet Protocol) fueron el permitir comunicaciones entre varios sistemas independientes y multivendedores. En 1983, los protocolos TCP/IP se convirtieron en el mecanismo de transporte oficial para el Internet del Departamento de defensa, que evolucionó en un sistema de redes interconectadas expandidas pro todo el mundo. Posee fuertes capacidades de interconexión de red listadas a continuación:

- **Protocolo Internet IP:** Es un protocolo de comunicación sin conexión que por sí mismo proporciona un servicio de datagramas. Los datagramas son paquetes independientes de información, que se envían a través de los encaminadores en función de su dirección y a la información de la tabla de encaminamiento contenida en los encaminadores. Los datagramas se pueden direccionar a un único nodo o a múltiples nodos. No hay control de flujo, reconocimiento de recepción, comprobación de error ni secuenciamiento. Los datagramas pueden atravesar trayectos diferentes para llegar al destino y así llegar a fuera de secuencia. La estación receptora es responsable del resecuenciamiento y de determinar si se han perdido los paquetes. IP maneja la congestión simplemente con el descarte de paquetes. Los protocolos de nivel superior cuidan el re-secuenciamiento y le manejo de errores, que no lo debe hacer IP. Por eso, IP es rápido y eficiente, y muy adecuado para las redes y los sistemas de telecomunicaciones modernos, que ya proporcionan un servicio relativamente fiable.

  IP trabaja con diversas redes de área local y extensa. Cuando IP se ejecuta en el entorno LAN de una red Ethernet, por ejemplo, el campo de datos de la trama Ethernet mantiene el paquete IP y un campo específico de la trama que indica la información IP que contiene. IP usa un esquema de direccionamiento que trabaja independientemente del esquema de direcciones de la red. Por

ejemplo cada adaptador Ethernet incluye una dirección hardware asignada en la fábrica. IP no la utiliza pero sí una asignada a cada nodo, como se describe a continuación.

Direccionamiento IP: Cada nodo en una red TCP/IP requiere una dirección numérica de 4 bytes (32 bits) que identifica una red y un anfitrión local o nodo de la red. esta dirección se compone de cuatro números separados por puntos, por ejemplo 191.31.140.115. En la mayoría de los casos, el administrador de la red establece esas direcciones cuando instala nuevas estaciones de trabajo; sin embargo en algunos casos es posible, para una estación de trabajo, consultar un servidor para una asignación dinámica de dirección cuando arranca.

La asignación de direcciones es arbitraria dentro de una compañía y organización, pero si ésta planea conectarse con Internet alguna vez en un futuro cercano, es necesario que obtenga las direcciones registradas por el Centro de información de red NIC de la red de datos de defensa DDN, gobernada por Network Solutions en Chantilly, Virginia. Con el aumento de la popularidad de Internet, se recomienda que todas las organizaciones obtengan sus direcciones registradas para evitar conflictos de direcciones en el futuro.

Hay tres clases de direcciones Internet: A, B, C:

- *Clase A.* Soporta 16 millones de anfitriones (computadoras fijas) pero únicamente se puede asignar 127 números de red.
- *Clase B.* Soporta 65.000 anfitriones y 16.000 redes.
- *Clase C.* Soporta 254 anfitriones y 2 millones de números de red.

Debido a que la dirección Internet es una combinación de números de anfitriones y de red, múltiples anfitriones pueden compartir la parte del número que corresponde con el anfitrión, pero cada anfitrión posee su propio número único. Por ejemplo, en los números de la clase C, el primer conjunto de dígitos representa el número del anfitrión y los últimos tres conjuntos de dígitos el de red.

El direccionamiento IP soporta millones de direcciones, pero recientemente, ha surgido una limitación potencial. Con el aumento de la popularidad de Internet, es inevitable una escasez de las direcciones asignables.

Se hicieron estimaciones que Internet agotaría sus direcciones hasta 1995, por eso se creó un nuevo protocolo llamado Protocolo Básico Internet (SIP), el cual remedió esta situación. SIP utiliza

direcciones de 64 bits en vez del direccionamiento de 32 bits que utiliza IP, lo que dobla el número de direcciones posibles.

- **La estructura de datagramas de IP:** El datagrama de IP contiene direcciones, información de encaminamiento y otra información de cabecera, para la distribución de un paquete de datos de una fuente a un destino. A continuación, se describen los campos de datagrama IP. Nótese que las banderas (flags) y campos de desplazamiento de segmento tienen que ver con la fragmentación de los paquetes en dos o más datagramas para su distribución sobre subredes que son incapaces del manejo de datagramas grandes:

  - *Versión.* Describe la versión del protocolo IP y permite la transición de una versión de protocolo a otra.
  - *Longitud.* Especifica la longitud de la cabecera.
  - *Tipo de Servicio (TOS, Type of Service).* Utilizado para indicar el tipo o calidad del servicio requerido para el datagrama. Los encaminadores que manejan el datagrama leen este campo y proporcionan, si es necesario, prioridad al servicio. En un principio, este campo especificaba la prioridad del paquete para emergencias militares o eventos de crisis. La definición de TOS cambia para indicar una necesidad de minimizar el retardo y el costo, maximizar el rendimiento o la fiabilidad, de acuerdo con una discusión

reciente dentro del Grupo para tareas de ingeniería Internet IETF.

- *Longitud total.* Especifica la longitud total del datagrama, que posee una longitud máxima de 65.536 bytes.
- *Identificación.* Proporciona información para unir los datagramas fragmentados, de ese modo el destino puede reemsamblarlos de forma unívoca en paquetes completos.
- *Banderas (flags).* Hay dos bits de bandera. El primero indica que un paquete no se debería fragmentar y de ese modo se debe enviar a lo largo de una subred que pueda manejar su tamaño actual. El segundo bit de bandera indica que un datagrama es el último de un paquete fragmentado.
- *Desplazamiento de fragmento.* Para datagramas fragmentados, este campo indica la posición de los datos en el paquete y se usa durante el reensamblado.
- *Tiempo de vida.* El tiempo en segundos que un datagrama puede estar en tránsito. Si se excede este tiempo el datagrama se considera perdido o en un bucle y por lo tanto se descarta.
- *Protocolo.* Identifica el tipo de protocolo de datagrama, de ese modo permite protocolos no TCP/IP.
- *Código de paridad de la cabecera.* Proporciona un valor para comprobar los errores y de esta forma asegurar la integridad de un paquete distribuido.

- *Dirección fuente/destino.* Las direcciones de la fuente y del destino del datagrama.
- *Opciones.* Este campo contiene opciones que proporcionan un modo de grabar un trayecto a través de una red o imponer un trayecto (encaminamiento fuente).

b) Protocolo de Control de Transmisión TCP (Transmission Control Protocol).- Proporciona un modo de establecer una conexión entre sistemas finales para la distribución fiable de mensajes y de datos. La conexión TCP posee todas las características orientadas a la conexión discutidas previamente, como control de flujo, reconocimiento, secuenciamiento, código de paridad y retransmisión. Cuando una aplicación usa TCP, hay una fase de establecimiento de conexión, pero una vez que se hace, proporciona distribución fiable y eficiente de los datos entre los sistemas finales. Las sesiones orientadas a la conexión con útiles para los intercambios de datos prolongados o cuando es necesaria una conexión relativamente permanente.

Para establecer una conexión TCP, la estación activa envía un mensaje a otra estación. Esta responde a la estación activa que está preparada para el establecimiento de una sesión de comunicación. Luego, la primera estación responde para conformar la conexión y tiene lugar una transferencia consiguiente. Se describen los campos de los paquetes TCP aquí:

- **Puerto fuente/destino:** Contiene el número del puerto para el proceso de aplicación mediante el uso de servicios TCP.
- **Número de secuencias:** Proporciona la información necesitada por el receptor para ordenar los paquetes y saber si se ha perdido alguno.
- **Número de reconocimiento:** Proporciona una indicación de los bytes devueltos al emisor, de modo que puede retransmitir los paquetes perdidos si es necesario.
- **Longitud de desplazamiento:** Especifica la longitud de la cabecera.
- **Códigos:** Este campo contiene códigos que indican la necesidad urgente de datos o que este paquete es el final de los datos.
- **Ventana corredera:** Proporciona una manera de incrementar el tamaño del paquete, de este modo mejora la eficiencia de la transferencia del os datos.
- **Código de paridad de la cabecera:** Proporciona un valor de comprobación de errores para asegurar la integridad de un paquete distribuido.
- **Punto urgente:** Indica la posición de los datos donde se localizan datos urgentes.
- **Opciones:** Una variable reservada para opciones futuras especiales.

Nótese que se usa IP sin conexión para el transporte de datos entre los nodos en la red, mientras que los niveles TCP que se ejecutan en los

sistemas finales proporcionan las funciones de fiabilidad. El paquete IP contiene la dirección del nodo final, mientras que el paquete TCP contiene el número del puerto de la fuente y el destino. Una analogía sería una conversación que se mantenga con un amigo mientras se le transfiere información sobre otra línea telefónica. La conversación de voz se utiliza para establecer los parámetros de la sesión de comunicación de datos; a continuación comenta cómo progresa el intercambio, a medida que éste tiene lugar y finalmente reconoce la recepción del conjunto del conjunto de datos completo. A continuación se presentan las características del protocolo TCP:

- **Protocolo de aplicación.-** Las aplicaciones siguientes se han construido encima del grupo de protocolos TCP/IP y están disponibles en la mayoría de las instalaciones TCP/IP, inclusive Internet:

  - *Sistema de Archivos de Red (NFS, Network File System).* Un sistema de archivado para anfitriones UNIX que es compatible y distribuido.
  - *Protocolo Básico de Gestión de Red (SNMP, Simple Network Management Protocol).* Un protocolo que recoge la información sobre la red e informa de ello a los administradores.
  - *Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol).* Permite las transferencias de archivos entre

estaciones de trabajo y un anfitrión UNIX o un sistema de archivos en red de NetWare de Novell.

- *Protocolo básico de Transferencia de Correo (SMTP, Simple Mail Transfer Protocol)* Un protocolo que permite mensajería electrónica.
- *Telnet.* Emulación de terminal VT100 y VT330 de DEC.

3.3.5 GRUPOS

Los grupos son colecciones de usuario o de cuentas de usuarios. Se crean para simplificar la tarea de gestión y definición de derechos para un gran número de usuarios. Es más sencillo enviar mensajes a un grupo que a todos los usuarios individuales que pertenecen a él. Los grupos disponen de nombres específicos, y pueden incluir a usuarios que trabajan en proyectos similares, que pertenecen al mismo departamento o incluso a un club dentro de la compañía. Por ejemplo, un usuario podría pertenecer a los grupos gestión, consultoría y golf.

Los derechos de acceso se asignan a los grupos a través de archivos, de la misma forma que se hace con usuarios individuales. Sin embargo, es más simple asignar los derechos a los grupo y añadir usuarios a éstos. El usuario obtiene así todos los derechos y privilegios de ese grupo. Los grupos deberían definirse cuando se planea la estructura de la red y crearse antes de añadir ningún usuario. Así, según se crean nuevas cuentas de usuario se pueden añadir usuarios a los grupos.

A continuación se ofrecen algunos ejemplos de utilización de grupos:

a) Un grupo de tratamiento de textos con derechos de ejecución de un cierto procesador de textos y de almacenamiento de datos en directorios.
b) Grupos de correo electrónico que simplifican el direccionamiento de los mensajes. Por ejemplo, creación de grupos denominados Gestores, Empleados y Temporales.
c) Un grupo de gestión de sistemas de derechos sobre directorios especiales.
d) Un grupo de realización de copias de seguridad con derechos de acceso especiales sobre los directorios donde se almacenan las copias de seguridad.

Otro aspecto interesante de los grupo es que proporcionan una forma conveniente de cambiar o eliminar los derechos de un gran número de usuarios. Se puede borrar un grupo completo, o bien eliminar los usuarios de un grupo. Cuando se eliminan los usuarios de un grupo, mantienen una cuenta en el sistema, pero sin los derechos que tuvieran en el grupo.

A continuación se presentan los diferentes tipos de grupos:

a) **Grupos en Windows NT.-** Windows NT incorpora un conjunto de grupos predefinidos con derechos de acceso también predefinidos, que

dan a sus miembros la capacidad de realizar varias tareas y actividades en el sistema.

Existen dos tipos de grupos: locales y globales. Los grupos locales se componen de uno o más usuarios que acceden directamente a la computadora local. Los grupos globales se componen de los usuarios que acceden a los recursos de la computadora desde otra estación de trabajo de la red. Los miembros de un grupo local sólo disponen de derechos de acceso en la estación de trabajo donde está definido el grupo. Un grupo local típico es el Power User Group, que incluye los miembros con algunos pero no todos los derechos de acceso a un servidor NT desde cualquier computadora de la red.

En la mayoría de los casos, uno de estos grupos debería proporcionar un conjunto de derechos de acceso apropiados para cada tipo de usuario. Si no es así, pueden crearse grupos propios y asignarles derechos de acceso personalizados mediante la utilidad User Manager de Windows NT. Las siguientes cuentas se crean automáticamente en NT:

- **El grupo Administrador:** Este grupo posee el nivel más alto de control y acceso sobre a estación NT. La cuenta Administrator obtiene sus derechos de acceso siendo miembro de este grupo. Inicialmente, el grupo consta de las cuentas Administrator, Initial User y, si la estación NT forma parte de un dominio Windows NT

Advanced Server, del grupo denominado Domain Administrator, que puede ser eliminado fácilmente si es necesario.

El grupo Administrator posee derechos de realización de las siguientes tareas:

- Creación y gestión de cuentas de grupos y usuarios sobre el sistema local.
- Asignación de derechos a usuarios.
- Bloqueo y desbloqueo de la estación de trabajo.
- Formato y gestión de discos duros.
- Creación de grupos genéricos Program Manager.
- Compartición de directorios e impresoras.
- Mantenimiento de perfiles locales.

- **El grupo Users:** Todas las cuentas añadidas tras la instalación inicial se incorporan al grupo Users. Las cuentas Administrator, Guest e Initial User no pertenecen a este grupo, que posee los derechos de conexión local y desconexión del sistema, y capacidad de bloqueo de la estación de trabajo y mantenimiento de un perfil local. Pueden asignarse permisos y directorios al grupo si es necesario.

- **El grupo Guest:** Este grupo proporciona acceso limitado al sistema para usuarios ocasionales. Sus miembros tienen el

derecho de conexión local, aunque pueden asignarse permisos sobre directorios y archivos adicionales si es necesario (pensar en invitados como empleados temporales). Inicialmente, cualquiera que pertenezca a este grupo puede conectarse sin contraseña; sin embargo, el acceso al sistema es extremadamente limitado. Por ejemplo, un miembro del grupo Guest puede almacenar archivos sobre un disco flexible, pero no sobre un disco duro. Podría desearse incrementar los derechos de una cuenta Guest mediante la creación de un directorio especial que permitiera el almacenamiento de archivos de estos usuarios.

- **El grupo Everyone:** Este grupo incluye a todos los usuarios que utilizan una computadora. Cuando se necesita conceder derechos y permisos a todos los usuarios del sistema, hay que efectuar esta concesión sobre este grupo, que incluye además a los usuarios que acceden a la computadora en la red aunque estén incluidos en el grupo Users. Pueden concederse permisos sobre archivos y directorios según sea necesario. Los miembros de este grupo tienen derecho de realización de las siguientes tareas:

  - Conexión local.
  - Acceso remoto a la computadora asignada a la cuenta Power User.
  - Parada del sistema.

- **El grupo Backup Operators:** Este grupo posee permisos de realización de copias de seguridad, lo que requiere la capacidad de leer todos los archivos del sistema. Esto incluye a los archivos de los que su propietario ha denegado el acceso a todos los usuarios, incluyendo a los miembros de este grupo. El derecho de realizar copias de seguridad precede a los permisos de archivos y directorio aplicados por el propietario del mismo. Los operadores de este grupo pueden realizar las siguientes tareas:

  - Conexión local.
  - Parada del sistema.
  - Copia de seguridad de archivos y directorios.
  - Restauración de archivos y directorios.

- **Grupos Network e Interactive:** Consta de todos los usuarios que acceden a la computadora sobre una conexión de red y el grupo Interactive consta de los todos usuarios locales de la computadora. En otras palabras los miembros de estos grupos dependen de quienes acceden normalmente al sistema, localmente o sobre la red.

- **Grupos de trabajo:** Es un grupo de usuarios que están localizados físicamente en el mismo lugar y conectados a la misma red de área local. De manera alternativa, un grupo de trabajo es un agrupación lógica de usuarios que están dispersos en

una organización, pero conectados a la misma red. En ambos casos, los usuarios de los grupos de trabajo comparten documentos, aplicaciones, correo electrónico y recursos del sistema, de un modo prefijado. Un grupo de trabajo podría ser una simple agrupación de usuarios con un nombre como Administradores o Temporales que se usa como dirección de correo electrónico. Por otra parte, el grupo de trabajo puede tener privilegios especiales en la red como el acceso a los servidores de datos o a aplicaciones especiales.

Los grupos de trabajo y el software con el que trabajan, se están haciendo muy comunes. Por ejemplo, la aplicación Schedule+ que se suministra con Microsoft Windows para trabajo en grupo permite que los usuarios colaboren en la planificación y que las reuniones se convoquen de acuerdo con los programas de actividades de los asistentes. La arquitectura de software abierto de Windows de Microsoft WOSA está diseñada para integrar facilidades para grupos de trabajo directamente en el sistema operativo Windows. Con estas facilidades, los programadores y usuarios pueden crear o usar facilidades que estimulan la ejecución de actividades de grupo o de flujo de trabajo en la red. WOSA incluye interfaces para los sistemas habituales de mensajería, servicios de directorio, facilidades de seguridad y acceso a servicios de bases de datos posteriores.

- **Grupos locales:** Se definen en el entorno Windows NT. Todos los sistemas operativos de red proporcionan características de gestión de grupos para la simplificación de la tarea de asignación de derechos y permisos a un número grande de usuarios. Crea una cuenta de usuario y entonces se añade esa cuenta a un grupo. Windows NT incluye un conjunto de grupos predefinidos con derechos de acceso también predefinidos que dan a sus miembros la capacidad de realizar varias tareas y actividades en el sistema.

3.3.6 AUTENTICACION Y AUTORIZACION

En un entorno de informática distribuida, generalmente los usuarios acceden a algunos recursos que no sean los unidos a sus servidores locales. Tradicionalmente, un usuario inicia una sesión para acceder a los recursos locales. Cuando accede a los recursos remotos (que pueden estar en otras ciudades), el usuario debe iniciar de nuevo una sesión. Este método de iniciar una sesión por cada recurso no solo es incómodo, sino también dificulta la gestión. Se debe mantener una cuenta de usuario con la clave actual en cada servidor. Además, la conexión a dispositivos remotos no es fiablemente segura y los intrusos podrían controlar la línea e interceptar la información de inicio de sesión para su propio uso. Claramente, se necesitan métodos mejores. Los métodos de cifrado de clave también fallan si un intruso enmascarado como un usuario legítimo captura la clave cifrada.

UNIX, NetWare 4.x y otros sistemas operativos usan el concepto "anfitrión de confianza", donde un sistema confía en que otro sistema haya verificado correctamente la identidad de un usuario. Se discuten los métodos para realizarlo en el párrafo siguiente, pero una vez que se ha autentificado un usuario, este puede acceder a cualquier recurso al que tenga autorización. La información usada puede verificar el acceso de un usuario a los recursos remotos es diferente cada vez que el usuario inicia la sesión, así si se intercepta esta información, no se puede utilizar una vez que el usuario finaliza la sesión.

Las técnicas de autenticación deben determinar si se origina una petición desde el usuario correcto o la aplicación correcta y que dicha petición no se ha modificado de alguna forma. Una vez que se verifican las peticiones como auténticas, entonces los procedimientos de autorización determinan el tipo de acceso que un usuario tiene a un recurso.

3.3.7 CUENTA DE USUARIO EN RED

Generalmente, los usuarios de computadoras en red poseen cuentas que guardan información como su nombre, clave y restricciones a la red. El administrador de la red controla el acceso del usuario mediante el cambio de unos valores en dichas cuentas. Por ejemplo, se puede inutilizar la cuenta temporalmente si un usuario falla en la introducción de la clave (password) correcta después de tres intentos. La cuenta puede tener también una limitación de tiempo, así a un empleado temporal se le puede conceder acceso

por un periodo de dos semanas. Igualmente, una cuenta puede restringir el inicio de sesión (login) a un usuario sólo durante un periodo de tiempos específico o en una máquina específica. La información de la cuenta puede contener además información general, como la dirección de las estación de trabajo en la red o un número de teléfono de contacto del usuario.

3.3.8 CUENTAS DE INICIO DE SESION

El inicio de sesión (*logon o login*) es un procedimiento que sigue un usuario para obtener el acceso a un sistema privilegiado, tal como un servidor de archivos, una base de datos o la red. Primero, el usuario ejecuta el software que conecta la estación de trabajo a la red y establece un canal de comunicaciones hacia un servidor de la red. Este proceso se ejecuta a menudo automáticamente cuando se enciende la estación de trabajo. Entonces el usuario escribe LOGON o LOGIN. El proceso de inicio de sesión pide el nombre y la clave (password) de la cuenta del usuario. Si el usuario introduce cualquiera de las dos incorrectamente, generalmente el procedimiento de inicio de sesión permite otra oportunidad al usuario que inicia la sesión. Después de un cierto número de fallos repetidos en a escritura de la información pedida, el procedimiento de inicio de sesión asume que el usuario es un intruso y bloquea la estación para evitar más intentos de inicio de sesión. Cuando un usuario inicia la sesión con éxito, llega a ser autentificado en la red y consigue una serie de autorizaciones preasignadas para el uso de los recursos en la red. De esta forma, el usuario sólo necesita iniciar la sesión una vez, no cada vez que accede a un recurso.

Un usuario debe disponer de una cuenta en el sistema en el que inicia la sesión. Esta cuenta consta del nombre de inicio de sesión, de los derechos de acceso del usuario y de un guión de inicio de sesión que puede ejecutar varias ordenes cuando el usuario inicia la sesión. Por ejemplo, el guión de inicio de sesión deberá fijar varias relaciones de trayectos de directorios y mostrar un menú diseñado específicamente por el usuario. Un supervisor puede aplicar restricciones de inicio de sesión a la cuenta de usuario, según se describe a continuación:

a) Puede limitar el tiempo en el que un usuario puede iniciar la sesión, de ese modo se previene que el usuario inicie la sesión fuera de las horas permitidas.
b) Puede especificar las estaciones de trabajo donde un usuario inicia la sesión, lo que evita que el usuario inicie la sesión en estaciones de trabajo no autorizadas.
c) Puede requerir claves únicas, de ese modo se fuerza al usuario a crear una clave distinta de una que usó recientemente.
d) Puede definir una fecha de expiración de la cuenta, que bloquea la cuenta del usuario después de un cierto periodo de tiempo.

3.3.9 DIRECCIONES DE RED

Cada nodo en una red incluye una dirección asignada que otros nodos usan cuando se comunican con él. Para los adaptadores de redes Ethernet y anillo con testigo se asigna una dirección única en la fábrica. Las redes ARCNET

incluye direcciones definibles por el usuario. Por ejemplo, la dirección de un adaptador de red Ethernet y anillo con testigo consta de una dirección de 6 bits, la mitad de los cuales es un número especial que identifica al fabricante de la placa. La última mitad de la dirección es un número único asignado a la placa en la fábrica. Esta estrategia garantiza prácticamente que dos tarjetas de la Interfaz de red de Ethernet o anillo con testigo nunca tendrán la misma dirección y con lo que se evitan posibles conflictos.

Cuando se conectan redes distintas en una inter-red, se requiere un esquema nuevo de direcciones. En redes NetWare interconectadas, cada segmento de red posee su dirección propia, la cual se usa con propósitos de encaminamiento y para la diferenciación de cada segmento de los otros.

En redes TCP/IP como Internet, cada nodo contiene una dirección numérica que identifica a una red y aun anfitrión o nodo local de la red. Esta dirección consta de 4 números separados por puntos, por ejemplo (191.31.140.115). la asignación de la dirección es arbitraria dentro de una compañía u organización, pero si la compañía proyecta conectarse con Internet, debería obtener una dirección registrada, mediante la solicitud a una agencia externa, para adecuarse a las normas internacionales de direccionamiento. También las aplicaciones que se ejecutan en las computadoras contienen direcciones que otras aplicaciones, tanto locales como remotas, usan para comunicarse con la aplicación. En redes TCP/IP, un conector (socket) es una combinación de una dirección Internet más una dirección de aplicación.

3.3.10 DIRECTORIO DE INICIO DE SESION (HOME)

Un directorio de inicio de sesión se asocia a cada cuenta de usuario de la red, con objeto de permitir la creación de subdirectorios, almacenar archivos e instalar aplicaciones personales. Los directorios de inicio de sesión son opcionales, pero proporcionan una ubicación inicial en la conexión al sistema y pueden ser esenciales para los usuarios de estaciones sin disco. Los gestores pueden permitir a los usuarios almacenar los archivos en directorios públicos compartidos, aunque éstos no son lugares idóneos para almacenar archivos personales, o archivos que deben mantenerse seguros respecto a otros usuarios.

Algunos gestores dan a los usuarios derechos completos de archivo y directorio en sus directorios de inicio de sesión, lo que permite a éstos crear directorios nuevos y conceder a otros usuarios derechos sobre estos directorios. De esta forma, los usuarios controlan el nivel de acceso a los directorios y determinan los usuarios de la red que pueden acceder a los archivos del directorio. Los administradores pueden impedir que usuarios determinados tengan la capacidad de crear estructuras de directorio y definir la seguridad en ellas. Sin embargo, la mayoría de los sistemas operativos de red pueden invalidar la seguridad impuesta por los usuarios en sus directorios personales.

Si se decide crear directorios de usuario, hay que crear primero un directorio denominado HOME o USERS y después subdirectorios para cada usuario a

partir de éste. Los sistemas operativos tales como NetWare y Windows NT crearán de forma opcional directorios de usuario cuando se añade una cuenta de usuario. En entornos con muchos usuarios, podría ser necesario dedicar a un servidor para los directorios de usuario.

3.4 ¿COMO SE APLICA EN LA RED DE LA PUCESA?

La aplicación de lo anotado anteriormente tiene su aplicación en la red de la PUCESA en los siguientes puntos:

a) **Servidor central.-** La PUCESA utiliza tres servidores centrales, uno de Windows NT, uno con Novel l y uno con LINUX. El servidor Windows NT utiliza las características mencionadas en este capítulo como son:

- **Soporte para otros entornos:** Es el entorno de DOS a través del cual se pueden ejecutar cualquier cantidad de comandos directamente en una ventana que simula el DOS tradicional.

- **Memoria virtual:** Windows NT nos permite utilizar parte del disco duro para poder simular memoria RAM denominada Memoria Virtual, esto nos permite tener acceso a un recurso muy grande en dependencia del espacio libre en el disco duro.

- **Soporte de archivo de Windows NT:** Es el sistema de localización de archivos de Windoes NT.

- **Protección de archivos del sistema:** Se tiene acceso a la protección de datos y archivos que posee Windows NT, esto hace posible determinar usuarios y niveles de acceso a los archivos que tiene el servidor.

b) Redes .- Windows NT permite que se tenga acceso a redes Novell por lo que este servidor se puede conectar y acceder al servidor Novell existente en el Laboratorio.

c) Jerarquía de usuarios y seguridad.- Se puede crear usuarios y jerarquía de los mismos para protección de los datos, es decir cada usuario puede tener un acceso específico a los diferentes recursos del sistema

d) Impresión .- Se cuenta con todos los recursos y características del Administrador de Impresión de Windows NT para controlar y acceder a todas las impresoras de red compartidas en el sistema.

e) El Servidor LINUX.- Cuenta con todas las bondades que provee UNIX para control de red, se está aprovechando una conexión directa a Internet, es decir se utiliza este servidor como pasarela desde la red interna hacia Internet y de Internet hacia la red interna. Se aprovecha los recursos de creación de usuarios y protección de archivos para evitar el ingreso de personas no autorizadas a la red como se puede ven en la figura 39.

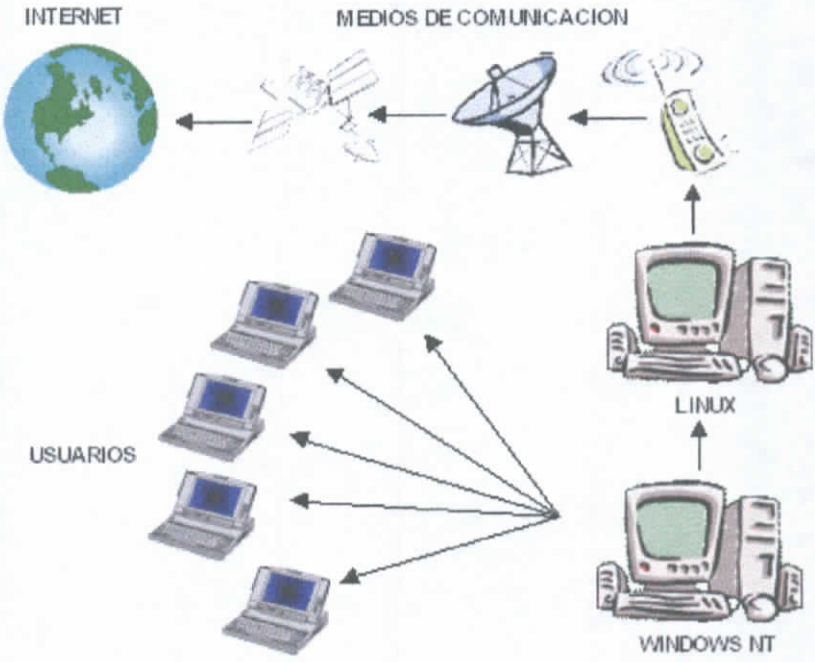


Figura 39. Modelo de conexión a Internet de la PUCESA.

f) **El servidor Novell.-** Utiliza la configuración básica de red que provee este tipo de servidores, básicamente se usa con terminales sin disco duro, estas terminales utilizan los recursos del servidor central. Se aprovecha el soporte de creación de usuarios y control de archivos para evitar el ingreso de personas no autorizadas a los datos que maneje este servidor.

g) **Equipos de cliente:**

- **Modelo Cliente-Servidor:** Se maneja el modelo cliente-servidor en el caso del laboratorio de IBM ya que se utiliza SQL Server para dictar clases de Base de Datos, todos los recursos de la base de datos se

encuentran acumulados o concentrados en el servidor Windows NT y cada uno de los equipos cliente del laboratorio IBM los toman de éste.

- **Software de cliente:** Se cuenta con el soporte de software de cliente en todos y cada uno de los equipos clientes de la red, ya que a través de éstos se tiene acceso a los recursos de la red por parte de dichos equipos.

- **Clientes TCP/IP:** Todos los clientes o máquinas de los laboratorios de IBM y Compaq son clientes TCP/IP ya que estos tienen acceso a INTERNET y mejoran la velocidad de acceso a redes con una topología en estrella que es lo que nos permite poseer los HUB´s.

- **Protocolos de comunicación:** Como protocolos de comunicación se cuenta con tres: TCP/IP, IPX/SPX y NETBEUI, los cuales permiten un acceso libre a los datos y servicios de los servidores y entre equipos clientes. Y cumplen como protocolos de:

  - Aplicación.
  - Transporte.
  - Red.

- **Grupos:** El tipo de servidores con los que se cuenta podrían permitir la definición de grupos de trabajo. Se puede decir que se cuenta con tres

grupos de trabajo definidos como son el Grupo Novell, Grupo IBM y Grupo Compaq.

- **Autenticación y autorización:** Se manejan nombre de usuario y claves de acceso para acceder a todos los recursos de red que proporcionan los servidores, estos sistemas de seguridad se detalla en el capítulo de Administración de Redes Lan y Wan.

- **Direcciones de red:** Cada uno de los equipos de red cuentan con una dirección de red bien definida, estas direcciones se encuentran custodiadas y manejadas por la administración del laboratorio.

PARTE II

ADMINISTRACION DE REDES WAN Y LAN

INTRODUCCION

El creciente número de organizaciones como son escuelas, colegios, universidades, bancos, corporaciones, etc., que poseen redes de computadoras sean éstas de área local o de área extensa, cuentan con un grande número de usuarios, lo cual ha hecho indispensable la organización y administración de estos centros con personal adecuado, por ello se considera necesario que cada uno de dichos centros cuente con un administrador, el cual cree y haga cumplir reglas, procesos y políticas para el uso de los recursos tanto humanos como tecnológicos con los que cuenta el departamento o sección de computadoras.

La creación o redacción de procesos, políticas y reglamentos de trabajo para el eficiente manejo de los equipos, recursos físicos y humanos, representa un punto importante para la correcta administración de un centro de computo, laboratorio de informática, departamento de sistemas o cualquier otra locación en la que se encuentren involucrados el manejo de equipos de computación y su correcta utilización de información o programas de trabajo evitando que se cometan errores y problemas por parte de las personas que comparten dicha área de acción.

En la actualidad, en universidades y escuelas politécnicas existen laboratorios de informática debido al volumen de usuarios que tienen acceso a los mismos y la variedad de datos que manejan, hacen imprescindible el establecer un reglamento de uso, tanto de equipos como de programas, horarios y sanciones, y lo más importante cumplir y hacer cumplir dicho reglamento.

Todos los reglamentos van dirigidos no sólo a proteger el equipo, sino a proteger la información que se almacenan, siendo para las empresas el recurso más preciado, desafortunadamente, al ser la información un elemento intangible, no se le presta mayor importancia hasta el momento en que se pierden, invirtiendo grandes contingentes para recuperarlos.

El presente estudio se realiza una evaluación de las políticas existentes en el laboratorio de informática de la PUCESA y recomienda un modelo de políticas que se podría manejar e implementar en la misma.

Se especifica en la sección de 4.6. "Evaluación de las Nuevas Políticas Sanciones y Horarios", políticas dirigidas a varios tipos de personas o usuarios que pueden tener acceso a la red de la PUCESA, en la redacción de las políticas puede parecer repetitivo el especificar hasta cierto punto las misma obligaciones para los distintos tipos de usuarios, pero no lo es, ya que se debe especificar de forma explícita las obligaciones de cada uno de los tipos de usuario para evitar omisiones en el momento de interpretarlas, debido a que se debe entregar una copia de estas normativas a todos los afectados por estas.

CAPITULO IV

CREACION DE POLITICAS Y PROCEDIMIENTOS PARA REDES LAN Y WAN

4.1 EVALUACION DE POLITICAS EXISTENTES EN EL LABORATORIO

El reglamento existente en el laboratorio de la PUCESA fue entregado por la administración del laboratorio para motivos del presente trabajo como se describen a continuación:

a) **Reglamento de utilización de los equipos del laboratorio.-** Los objetivos que posee el laboratorio son las siguientes:

- Educar y responsabilizar al estudiante sobre el uso y manejo de todos los equipos de computación, demás elementos y suministros, para así garantizar la seguridad y calidad en los servicios que brinda el laboratorio.
- Lograr un ambiente de cordialidad, orden y disciplina dentro de las aulas del laboratorio.

b) **Normas para el uso del laboratorio.-**

- **Del ingreso al laboratorio:**

  - Todo profesor o estudiante de la PUCESA, tiene derecho a ingresar a los laboratorios de computación.
  - El único documento válido para utilizar los laboratorios fuera del horario de clase es el carné actualizado de la universidad.
  - El estudiante deberá firmar el registro a la entrada de los

laboratorios.

- Si un equipo va a ser utilizado por más de un estudiante, la persona que firma el registro de entrega es el responsable de dicho equipo.
- Queda prohibido el ingreso a los laboratorios sin la debida autorización.
- El estudiante que utilice algún equipo sin el correspondiente permiso, será sancionado consistiendo dicha sanción en el impedimento de uso de equipos durante cinco días laborables.
- Toda persona ajena a la institución podrá usar el laboratorio previo pagó del derecho correspondiente, y de la autorización requerida.

- **Tiempo y uso de las máquinas:**

- Durante todo el tiempo de uso hasta la entrega de los equipos, el único responsable del buen estado de los mismos y la totalidad de sus componentes es el estudiante que firmó la entrega.
- Queda terminantemente prohibido prestar a otra persona la máquina asignada.
- Los estudiantes que deseen utilizar equipos para Internet deberán reservar su turno con un día de anticipación como mínimo. Tendrán un tiempo límite de uso que será de dos horas diarias, las mismas que pondrán ser ampliadas dependiendo del número de estudiantes que requieran el servicio.

- El turno será respetado hasta 10 minutos después de la hora reservada, caso contrario se dispondrá del respectivo equipo.
- Durante las clases al laboratorio no es necesario que los estudiantes presenten el carné siempre y cuando el profesor esté presente en el aula; caso contrario el estudiante deberá acercarse a solicitar la máquina de la forma convencional.

- **Manipulación del equipo:**

- No está permitido por ninguna razón cambiar las configuraciones de las máquinas o agregar fondos de pantallas, o borrar programas instalados. Si es detectado se le suspenderá el ingreso al laboratorio durante cinco días laborables.
- Cualquier requerimiento de software y suministros, deberá ser solicitado a la persona encargada del Laboratorio de computación.
- Por ningún concepto podrán los equipos ser cambiados de posición hacia otro lugar.
- Cada grupo de trabajo deberá utilizar una máquina fija.
- Está prohibido realizar trabajos que no estén relacionados con la hora de clase sin autorización del profesor.
- Terminar la práctica cinco minutos antes de la hora indicada, para tener tiempo de llegar a la próxima clase.
- Una vez que finaliza la utilización de los equipos, colocar los cobertores y dejar las sillas en su respectivo lugar.

- **Utilización de los disquetes:**

  - Chequear los disquetes a utilizar con el objeto de verificar que estén libres de virus.
  - Si el disquete tiene virus se procederá a vacunarle o formatearle en caso de que no sea posible limpiar el virus.

- **Cuidado de las aulas:**

  - Está prohibido ingresar a las aulas alimentos y/o bebidas.
  - No fumar en el laboratorio.
  - No ensuciar ni manchar: equipos, mesas y pisos.
  - Utilizar los basureros.

- **De los profesores:**

  - Nuestros profesores tienen derecho a utilizar el laboratorio en el horario establecido para sus clases.
  - Deberán solicitar con anticipación cualquier modificación de horario de clase caso contrario no se le podrá facilitar el uso del laboratorio.
  - Cuando un profesor dicta su clase en las aulas del laboratorios, se le entregará y responsabilizará de todos los equipos del aula, del buen funcionamiento de las máquinas así como de la totalidad de sus componentes, previa verificación de los mismos.

- El personal docente que necesite utilizar las computadoras para investigación y desarrollo de su materia, deberá solicitarlo al encargado del laboratorio, y lo podrá hacer sin límite de tiempo.

c) Políticas y procedimientos generales.-

Normas y obligaciones del uso del Internet: A continuación se presentan las normas que debe cumplir el usuario de la red Internet de la Pontificia Universidad Católica Sede Ambato. Y las penalidades que implican contravenir dichas normas. Al firmar la solicitud de una cuenta de Internet en la red de la PUCESA y aceptar la misma Ud. esta aceptando expresamente estas normas.

Toda cuenta tiene un responsable. Las cuentas asignadas a profesores de la PUCESA son responsabilidad del/la profesor/a titular de la cuenta, quien se hace responsable por todas las actividades (accidentales o no) que ocurran con dicha cuenta.

De igual manera, las cuentas extendidas a estudiantes y empleados son responsabilidad del profesor o departamento que solicita la cuenta para dicha persona. En cuanto a las cuentas departamentales, el responsable es el profesor o el representante del departamento que solicita la cuenta.

Las cuentas son estrictamente personales, e intransferibles. El titular de la cuenta no puede en ningún caso prestar la cuenta a otra(s) persona(s)

mediante la comunicación de su login y password de entrada. También el titular de la cuenta debe tomar las medidas necesarias para que sin su consentimiento otros puedan tener acceso a su cuenta. En tal sentido pueden ser aconsejados por el personal de la red PUCESA. En caso de incumplir esta norma de la red PUCESA tiene el derecho de cerrar en forma definitiva la cuenta y de negarse en el futuro a conceder otra cuenta al infractor.

Igualmente no esta permitido el uso de otras cuentas y archivos no otorgados explícitamente para su uso.

El password utilizado por el usuario para el acceso a su cuenta debe cumplir con las siguientes normas:

- Debe tener entre 6 y 8 caracteres.
- Debe contener al menos un carácter numérico y un carácter especial (,.:; "'&%$#).
- No debe ser una palabra que aparezca en el diccionario, ni en español ni en otro idioma utilizado comúnmente.
- No debe ser el mismo login, o nombre real del usuario o allegados al mismo.

En caso de que se detecte el uso de passwords inadecuados por parte de los usuarios, la red PUCESA puede bloquear la cuenta hasta que el usuario corrija su situación y se ajuste a las normas dictadas en este documento. Puesto que la existencia de cuentas con password fácilmente adivinables

constituyen una amenaza para todos los usuarios de una red, la infracción reiterada de esta norma puede acarrear la cancelación definitiva de la cuenta.

El usuario de la cuenta debe acatar las indicaciones y solicitudes que el personal de la red PUCESA y de administración de las redes le haga con respecto al mantenimiento de las cuentas. El incumplimiento de esta norma puede acarrear la cancelación definitiva de la cuenta y la red PUCESA tiene derecho a negarse en el futuro a conceder otra cuenta al infractor.

El usuario de la cuenta debe velar por que el directorio y subdirectorios asignados tengan los permisos adecuados para impedir el abuso por parte de terceras personas. Tampoco esta permitido cambiar las restricciones de su cuenta.

Cualquier usuario de la red PUCESA que sea descubierto intentando ganar acceso ilícito a otras cuentas, o utilizando herramientas de software para obtener información sobre otras cuentas o sobre el password de las mismas perderá en forma definitiva su cuenta, y no se le permitirá en el futuro realizar una reinscripción.

La red PUCESA se reserva el derecho de impedir su acceso a servicios públicos desde el exterior. Lo mismo es aplicable a usuarios que suministren a personas ajenas a la institución información que pueda ser utilizada para descubrir passwords o atacar al sistema.

El intento a tener acceso a cualquier sistema de computación, incluyendo los no operados por la red PUCESA, esta prohibido. El incumplimiento de la norma acarreara la cancelación de las cuentas otorgadas a Ud. para su uso en la red PUCESA.

Queda expresa y terminantemente prohibido el uso de la cuenta y recursos de red PUCESA para propósitos ilegales.

Si un usuario va a estar temporalmente fuera de Ambato, y desea conectarse a la red PUCESA con el objeto de poder utilizar su cuenta en forma remota debe, notificar al administrador de red desde donde planea conectarse e indicar por cuanto tiempo estará ausente porque como esto no es usual el administrador al detectar un acceso desde el exterior a una cuenta lo considera en principio una ruptura de seguridad del sistema y tomara las previsiones para evitar que esto vuelva a suceder. Estas previsiones suelen comprender el bloqueo de la cuenta.

La red PUCESA se reserva el derecho de limitar el espacio de disco duro, tiempo de CPU, tiempo de conexión y derecho de uso de la impresora asignada al usuario.

No esta permitida la ejecución de programas "demonios" o de servidor sin la autorización explícita de su administrador.

Ningún usuario de la red PUCESA tiene derecho a realizar instalación de

maquinas o equipos conectados a la red PUCESA sin el consentimiento expreso de los administradores de la red. Para esto deben ajustarse a las normas de instalación de maquinas conectadas a la red PUCESA.

No se pueden utilizar los recursos de la red PUCESA con fines comerciales, a menos que en ellos estén involucrados la administración de la red PUCESA, la administración de la universidad, o que la red PUCESA otorgue explícitamente permiso para ello. La red PUCESA se reserva el derecho de eliminar de una cuenta todo el material que considere es empleado para fines comerciales.

La utilización de los servicios y recursos de red PUCESA para tareas no universitarias, las cuales tengan un impacto negativo sobre las actividades universitarias no están permitidas, y serán eliminadas.

Conclusiones.- Las normativas del laboratorio se encuentran bien definidas, pero, en base a nuestra investigación, su redacción actual tiene problemas de forma más no de fondo, ya que con la redacción actual, se puede incurrir en errores de interpretación y exclusión de responsabilidades por parte de las personas sujetas a este reglamento por tal motivo en los siguientes capítulos, se entrega una propuesta de la posible distribución y redacción de políticas y reglamentos que podrían regir en el laboratorio de la PUCESA.

Cabe anotar que es una propuesta, por lo que la administración del laboratorio podría modificarlos si el caso fuera necesario para que se acomode a sus

necesidades y organización.

Se procederá a determinar primero las áreas que se debería cubrir en lo que se refiere a políticas o procedimientos para poder definir un conjunto de políticas y procedimientos dirigidos al laboratorio de la PUCESA.

4.2 CREACION DE POLITICAS PARA EL USO DE LOS EQUIPOS

Las políticas de uso de los equipos cubren muchas áreas las cuales pueden ser:

a) Protección contra robo.
b) Protección contra descargas eléctricas.
c) Protección contra mal uso de los equipos.
d) Protección contra polvo.
e) Protección contra incendios.
f) Protección contra desastres naturales (inundaciones, terremotos, etc.).

a) Protección contra robo.- Los servidores deben protegerse de los robos, no sólo porque el equipo es valioso, sino porque la inactividad mientras se reemplazan los servidores puede costar mucho más que los equipos, ya que en ellos se concentran los datos vitales de la empresa, institución o para el centro de computo. Se deben considerar los siguientes puntos:

- Los tiempos que se requieren para recuperar los datos que mantenía el servidor central.

- Considérese el tiempo que se necesitará para reponer los equipos.
- El número de personas que se necesita para lograr una recuperación pronta que permita a la empresa no paralizarse por mucho tiempo.

Una posible lista de políticas para asegurar los equipos serían:

- Colocar los servidores en jaulas o armarios metálicos atornillados al piso, para que en el caso de un robo, éstos sean difíciles de desensamblar y sustraer.
- Tener copias de seguridad de por lo menos tres días en zonas de seguridad lejos del departamento o laboratorio.
- Tener copia de los instaladores de todos los programas que tiene el equipo instalado como son: sistema operativo, aplicaciones con las que se trabaja, procesadores de texto, bases de datos, etc.

b) **Protección contra incendios.-** La protección de valiosos equipos y datos contra incendios es de interés primordial. Piense en situar los equipos en un sótano o habitación que tenga protección interior y exterior contra incendios. Muchas organizaciones tienen equipos archivadores incombustibles en habitaciones con sistemas de rociado automático o sistemas de gas halan que reducen las pérdidas producidas por el fuego. Se debe determinar sistemas manuales para combatir incendios como son extintores los mismos que pueden ser de espuma, polvo químico o gas, la selección del mejor mecanismo se escoge dependiendo del tipo de equipos y del presupuesto.

c) **Protección contra desastres naturales (inundaciones, terremotos, etc.).-** Protéjase el equipo ante desastres naturales tales como terremotos e inundaciones. Se podría necesitar reforzar o elevar el área del servidor y desarrollar planes, de modo que los usuarios puedan acceder a los datos del servidor en caso de producirse un desastre. Los generadores alimentados por gas pueden suministrar energía a los servidores y estaciones de trabajo cuando se corte el suministro de energía. En la actualidad se crean cuartos de UPS's, las misma que dan un soporte continuo de energía mientras se manejan planes emergentes de recuperación de energía ya sea con generadores propios o de servicio público, las capacidades de estos cuartos es dependiendo del presupuesto de la empresa.

d) **Protección contra polvo.-** Un problema común en centros de computadoras es el polvo que se acumula en los componentes y piezas que integran los equipos, por este motivo, es recomendable que se creen políticas de limpieza y de prevención sobre la acumulación de polvo en las computadoras, es necesario que se practique una limpieza total de los quipos en lapsos de tiempo no mayores a tres meses, usar cobertores cuando no se esté utilizando los equipos y realizar labores de limpieza en el suelo y escritorios del centro o lugar donde se encuentran ubicados los equipos.

e) **Protección contra mal uso de los equipos.-** Es necesario evitar que personas que tienen poco o nada de conocimiento sobre el uso de las computadoras o equipos tengan libre acceso a los mismos, el avance en los sistemas operativos y el desarrollo de aplicaciones gráficas permite que el uso

de los equipos sean más intuitivos, pero a la vez pueden ser un potencial peligro en el caso de que una persona con poca experiencia en el manejo de los equipos puedan producir perdidas importantes de información si se utilizan de forma errónea.

f) **Protección contra descargas eléctricas.-** Es importante asegurarse que las instalaciones eléctricas se encuentran bien diseñadas y en perfecto estado, en nuestro medio es muy común que las instalaciones eléctricas tengan deficiencias en su diseño, sobre todo cuando se las realiza en construcciones no previstas para tener un centro de computadoras y/o sistemas, se debe considerar la distribución de fase y neutro y que la instalación a tierra bien estructurada. El retorno de corriente por tierra es un factor importante para que las computadoras fallen y en el peor de los casos que se quemen.

4.3 CREACION DE POLITICAS PARA EL USO DEL SOFTWARE

A continuación se detallan las políticas para el uso del software:

a) **Gestión centralizada o gestión distribuida.-** Tanto la gestión centralizada como la gestión distribuida ofrecen ventajas. Para centralizar la gestión, se trasladan los recursos de la red (servidores, centros de cableado, concentradores, encaminadores e incluso las impresoras) a emplazamientos centrales donde personal calificado puede gestionar los sistemas en áreas protegidas y de seguridad. Sin embargo, hacerlo así supone el riesgo de catástrofes, tales como terremotos e incendios. Una alternativa es la

distribución de los recursos de la red y la reproducción automática de los datos a lugares remotos regularmente. Estas zonas se conectan con enlaces de datos de alta velocidad, lo que asegura que los datos se sincronizan y actualizan correctamente.

b) **Utilización de técnicas de tolerancia a fallos.-** Los sistemas operativos de red deberían proporcionar técnicas de tolerancia a fallos, como la técnica de duplicación de información en disco (mirroring y duplexing), para recuperarse rápidamente de los fallos del disco. Estas técnicas de duplicación de discos protegen los datos con la escritura de las actualizaciones en múltiples discos al mismo tiempo. El duplicado es una estrategia de duplicación de componentes hardware tanto como de almacenamiento en disco.

c) **Mantenimiento de copias de seguridad adecuadas.-** Asegúrese que se hacen copias de seguridad de los datos. Se debe implementar un proyecto de copias de seguridad que las alterne en almacenamientos externos. Las copias de seguridad se pueden clasificar de las siguientes formas:

- Copias de seguridad para restaurar toda la información de un servidor en el caso de que se produzca un desastre.
- Copias de seguridad para restaurar la información de los bloques de datos corrompidos o alterados accidentalmente. Por ejemplo, podría necesitarse restaurar la información de contabilidad del día anterior y reintroducir los datos a causa de los errores producidos en la entrada

de datos.

- Copias de seguridad que almacenen los datos que no se utilizan en cinta o discos ópticos.
- Copias de seguridad que proporcionen una forma sencilla de recuperar sólo los archivos que los usuarios borran o reescribieron accidentalmente.

d) **Utilización de estaciones de trabajo sin disco.-** Este tipo de estaciones de trabajo carecen de unidades de disco, de esta manera los usuarios no pueden sacar datos valiosos de la compañía, introducir información que podría contener virus o desordenar el disco del servidor. Estas estaciones son también más económicas que los sistemas con discos y posteriormente muchas se pueden ampliar a sistemas completos, que los hacen más prácticos para organizaciones con presupuestos ajustado. Aunque estos sistemas proporcionan seguridad en lugares remotos o no supervisados, incrementan el tráfico en la red debido a que los usuarios deben acceder al disco de red para todos los programas y archivos. Los entornos operativos Windows requieren archivos de intercambio (swap) en disco. Si un disco no está disponible, la información del archivo de intercambio debe almacenarse en el servidor, lo cual acrecienta más adelante el problema del tráfico en la red.

e) **Protecciones contra virus.-** Los virus de las computadoras son comunes y muestran gran potencial para infiltrarse en la red cada vez que un usuario inicia la sesión. Esto es particularmente cierto para los usuarios que trabajan desde el sistema instalado en su casa de forma remota con una red de área

local o para los que trabajan con su computadora portátil desde la carretera. Los tablones de anuncio (Bulletin Boards), los discos de utilidades para dominio público y los discos de demostración pueden contener virus. Estos virus se encuentran a veces en el software que llegan en los paquetes envasados. Todo el software nuevo debería instalarse y actualizarse en un sistema de pruebas y comprobación de virus antes de ser instalado en el servidor de la red. También deberían utilizarse derechos de archivos y directorios adecuados, para asegurarse de que los usuarios no pueden alterar los archivos ejecutables en los directorios de programas. Hay otras medidas que se pueden tomar. Las técnicas de seguridad avanzadas pueden eliminar las amenazas de los virus. Estas técnicas autentican a los usuarios o a cualquier proceso que intente acceder a un sistema y a sus a sus archivos.

f) **Protección contra intrusos.-** Los intrusos pueden utilizar varios métodos para tener acceso a una red. El acceso de intrusos a una LAN local se puede prevenir asegurándose de que estos usuarios finalizan la sesión cuando lo intentan, muchos sistemas operativos de red proporcionan características que restringen la estación a la que los usuarios acceden y la hora de acceso. También se pueden añadir restricciones de tiempo para que no se pueda acceder antes o después de las horas de trabajo normales. Un intruso que consiga acceso al sistema con la palabra clave del nivel supervisor puede crear otras cuentas del mismo nivel y luego borrar los caminos mediante la alternación del sistema de acceso. Los elementos de auditoría pueden acceder a las actividades de los usuarios y revelarle a un auditor independiente las violaciones de seguridad que se hayan producido.

El acceso de usuarios no autorizados a estaciones de trabajo remotas constituye otra amenaza, pero un sistema vuelve a llamar y puede proporcionar un nivel de seguridad contra estos intrusos. Cuando un usuario marca desde una estación remota, el sistema cuelga la llamada y llama al usuario de nuevo para asegurarse de que está en el lugar indicado. No obstante, esta utilidad no puede utilizarse para proteger la LAN remota o un sistema que tenga una conexión permanente. En ese caso, un intruso podría encontrar la forma de establecer una cuenta que parezca legítima del sistema. Tómese medidas para evitar que los intrusos descubran las claves o los métodos de puerta trasera para introducirse en la red.

g) **Administración de los derechos de acceso.-** Los derechos y restricciones de acceso a directorios o archivos son técnicas importantes que los administradores y supervisores utilizan para proteger los datos contra pérdidas maliciosas, accidentales o de corrupción por parte de los usuarios. A los usuarios nunca se les debe dar más derechos de los que necesiten en los directorios de programas y datos. La mayoría de los usuarios no necesitan más que el derecho para leer en un directorio de programas. Cualquier otro derecho más abre los archivos de programas al ataque de virus, corrupción y reescritura. La gestión del acceso a los directorios de datos es un poco más complicada. A los empleados o usuarios temporales se les puede asignar el derecho de leer archivos y bases de datos, pero no el de cambiar sus contenidos. Los derechos de leer, escribir y otros adecuados se les asignan, en función del sistema operativo, a los usuarios autorizados a actualizar archivos. Hay que tener cuidado cuando se otorguen derechos que permitan a

los usuarios borrar archivos, modificar atributos de archivos o modificar los derechos de otros usuarios.

En los sistemas gestores de base de datos, los procedimientos almacenados pueden evitar que los usuarios accedan a los datos que no tienen autorización de ver o usar. En lugar de dar a los usuarios acceso a los datos, se les da acceso a procedimientos que realicen operaciones genéricas en los mismos. Por ejemplo, un procedimiento podría mostrar clientes con balances no pagados sólo por el número de cliente y ocultar la información personal como el nombre, la dirección y el número de teléfono del cliente. Los usuarios que no tienen derechos para visualizar esta información nunca tendrán la oportunidad de verla. Los procedimientos almacenados pueden contener también controles que aseguren que el usuario que ejecuta un procedimiento tiene autorización para hacerlo y proporciona usuarios privilegios con niveles mayores de acceso.

h) **Formación de los usuarios.-** Instrúyase a los usuarios para que inicien y finalicen correctamente sus sesiones en la red y para que protejan sus claves. Si necesitan dejar sus computadoras desatendidas, asegúrese de que finalizan su sesión o saben cómo activar un protector de pantalla protegido por una palabra clave que bloquee la computadora (pero mantenga la sesión) mientras se marcha. Los protectores de pantalla también permiten la ejecución de tareas desatendidas sin posibilidad de interrupción. En la mayoría de los sistemas operativos, pueden asignarse operaciones en las cuentas de usuario que, por ejemplo, fuercen a los usuarios a cambiar sus claves en un intervalo

de tiempo predeterminado, previniendo la reutilización de claves recientes, o el requisito de usar claves que no se hayan utilizado anteriormente.

Una de las pérdidas de datos más comunes en una red es la que producen los usuarios no cualificados, que pueden borrarlos o corromperlos accidentalmente. Se deben usar los derechos de seguridad para evitar que los usuarios utilicen órdenes potencialmente destructivas o debe asegurarse de que están adecuadamente instruidos en la utilización de órdenes que eviten los accidentes. Aunque los usuarios tienen normalmente todos los derechos de acceso en sus propios directorios personales, se debería evitar que los usuarios instalasen cualquier archivo o software en el servidor. Esto no sólo protege contra la infección de virus, además evita que los usuarios llenen un disco con archivos innecesarios.

i) Seguimiento de los usuarios.- No perder la pista de los usuarios. Téngase administradores de departamento que informen de los usuarios que han dejado la compañía o han cambiado sus puestos, de manera que puedan eliminarse o alterarse adecuadamente sus cuentas. Las revisiones de cuentas creadas por un sistema de auditorías pueden ayudar a seguir a los usuarios que alteraron la red tanto accidentalmente como a propósito.

4.4 SANCIONES POR MAL USO DE EQUIPOS Y SOFTWARE

Se debe establecer sanciones que permitan concientizar a los usuarios de los equipos o recursos del centro de computadoras de la importancia de respetar las

políticas y procedimientos, se puede establecer sanciones siguiendo los puntos detallados a continuación:

a) **Sanciones en dependencia de la responsabilidad.-** Se pueden establecer sanciones por daños causados a los equipos o a los datos a las personas o funcionarios en dependencia de su nivel de responsabilidad con los datos o equipos afectados por los daños, por ejemplo si la persona es un digitador y por una falencia del sistema se eliminaron todos los datos de un servidor importante, la sanción debe ir en proporción de responsabilidad a los responsables del sistema y al digitador. Estas proporciones las debe catalogar la administración del departamento de sistemas y/o la gerencia o dirección de la empresa o institución. Además de esto, se bebe establecer un tribunal para establecer el nivel de daño causado para poder aplicar la sanción.

b) **Sanciones en dependencia del daño.-** Este tipo de sanciones es más efectivo que la anterior ya que se cataloga un tipo de sanción para un tipo de daño específico, la sanción se aplica directamente en dependencia del daño por ejemplo si el borrar la información de un servidor califica a una sanción equivalente a la suspención del acceso a los equipos por un tiempo determinado, el administrador del sistema reporta a la persona que cometió el daño y se aplica la sanción sin necesidad de proceder a un tribunal para catalogarlo. De todas maneras, si el daño se produjo por deficiencias o falencias de los sistemas o de las políticas o procedimientos, también se deberían especificar sanciones para las personas responsables de evaluar los mismos.

c) **Sanciones por negligencia.-** La negligencia es una de las razones por las cuales más fallan los procedimientos o políticas e incluso los sistemas informáticos, es común que cuando se crean políticas, procedimientos y sistemas se incurre frecuentemente en:

- Confiar en el desconocimiento de los usuarios sobre los sistemas y la tecnología por lo cual se dejan muchas cosas implícitas en la redacción de las políticas ya que se considera que las personas nunca podrían incurrir en errores comunes.
- Ocultar errores en el momento del desarrollo de los sistemas, ya que si existen errores o frenos al momento de desarrollar el sistema, si existe una forma muy rápida de resolverlo se aplica la solución, caso contrario, se deja este error para ser resuelto cuando existan las herramientas necesarias o para una nueva versión del sistema, desafortunadamente algunos usuarios por su trabajo, actividades o por curiosidad, detonan estos errores los cuales pueden ser fatales para la empresa o institución.
- Dejar pasar errores no relacionados con las actividades propias, ya que las personas suelen medir los errores o peligros en dependencia de sus propias responsabilidades, un ejemplo de esto es que si una persona es responsable de un equipo y por error deja la máquina en una posición en la que se puede producir un daño en el equipo y otra persona produce un daño considerable al equipo por culpa de la otra persona, hay que determinar sanciones para las dos personas.

Este tipo de sanciones es muy difícil de determinar por lo que es en estos casos obligatorio la creación de un tribunal para determinar el nivel de responsabilidad de los involucrados en el problema.

d) **Sanciones por incompetencia.-** Las sanciones por incompetencia son establecidas de acuerdo a las personas que están inmersas en un problema determinado esta tipo de sanciones se determinan por intermedio de un tribunal el cual determina el nivel de incompetencia y sanción, por lo general estos casos se enmarcan dentro de negligencia, si existen casos muy marcados en que la capacidad de la persona para realizar una u otra actividad crean daños irreparables los cuales caen en el nivel de incompetencia.

4.5 CREACION DE HORARIOS PARA EL USO DE LOS EQUIPOS

El determinar horarios para el acceso a los equipos y sistemas de la empresa o institución son determinados por diversos factores que pueden influir en el normal desempeño de las actividades que se desempeñan en la misma, estos factores pueden ser:

- Acceso a la información, se determinan horarios de acceso a la información de la empresa, por ejemplo, un empleado del área de contabilidad debe tener acceso al sistema desde las 7 en la mañana hasta las 12 del medio día, se puede especificar el horario de acceso en éste período de tiempo, transcurrido éste el usuario no podrá ingresar al sistema.
- En instituciones educativas, los horarios de acceso en instituciones

educativas están determinados por el número de usuarios que pueden necesitar los equipos, en este caso se clasifican los horarios por prioridades y por usuarios, las prioridades por lo general están supeditadas por tiempo de uso para cursos o clases normales y por tiempos para practicas estudiantiles.

- Acceso a los equipos, se determinan los horarios en los que las instalaciones estarán abiertas para poder tener un acceso físico a los equipos, lo cual no representa que se tenga acceso a la información que éstos contienen.

4.6 EVALUACION DE NUEVAS POLITICAS, SANCIONES Y HORARIOS

En esta sección se presenta una propuesta de las reglas que podrían regir el laboratorio de informática de la Pontificia Universidad Católica del Ecuador Sede Ambato, como se muestra a continuación:

a) Reglamento de utilización de los equipos del laboratorio de informática.-

Los objetivos que tendría el laboratorio sería los siguientes:

- Especificar normas, políticas y procedimientos que permitan a los usuarios del laboratorio de informática dar un correcto uso a los equipos de computación y recursos que integran el mismo.
- Garantizar la seguridad y calidad de servicios brindados por el laboratorio de informática.
- Dotar a los usuarios de un ambiente de cordial y ordenado en el área en la que está ubicado el laboratorio de informática.

b) Especificaciones generales.- El laboratorio de informática que se hace mención en el presente conjunto de Normas, Políticas y Procedimientos pertenece a la Escuela de Ingeniería en Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ambato y que se encuentra administrado por personal de la misma.

La Administración del laboratorio de informática y de la escuela se reservan todo derecho sobre la aplicación y cumplimiento de las Normas, Políticas y Procedimientos para el uso del laboratorio de informática; su área física y equipos de computación se encuentran bajo su responsabilidad.

El conjunto de Normas, Políticas y Procedimientos se publicarán en un lugar visible para todas las personas interesadas en el uso del laboratorio de informática.

En el Laboratorio se reconocerán los siguientes tipos de usuarios, de acuerdo a la importancia de los mismos:

- Estudiantes de la PUCESA de la Escuela de Ingeniería de Sistemas.
- Estudiantes de la PUCESA de otras Escuelas.
- Profesores de la PUCESA de la Escuela de Ingeniería de Sistemas.
- Profesores de la PUCESA de otras Escuelas.
- Personas Particulares.

Cada uno de los tipos de usuarios tendrán reglas clasificadas por:

- Normas para el uso del laboratorio.
- Políticas y procedimientos generales.

Las normas estarán distribuidas en grupos de acuerdo a su importancia y trascendencia para la correcta aplicación de las mismas, como se indica a continuación:

- Del ingreso al laboratorio.
- Tiempo y uso de las máquinas.
- Manipulación del equipo.
- Utilización de medios de almacenamiento.
- Cuidado de las aulas.
- Castigos y sanciones.

c) Normas para el uso del laboratorio.-

Estudiantes de la PUCESA de la escuela de ingeniería en sistemas:

- **Del ingreso y salida del laboratorio:**

  - Todo estudiante de la Escuela de Ingeniería en Sistemas tiene derecho a ingresar al laboratorio de informática.
  - El único documento que valida al estudiante a utilizar los

laboratorios es el carné de la universidad, especificando la última matrícula del período en curso. Si el ingreso al laboratorio es con el propósito de recibir clases no es necesario que los estudiantes presenten el carné siempre y cuando el profesor esté presente para solicitar el uso del laboratorio.

- El estudiante deberá firmar el registro de entrada a los laboratorios de informática.
- Si el ingreso al laboratorio es para recibir clases, se debe formar grupos para el uso de los equipos en el caso de que los equipos existentes sean insuficientes para la cantidad de alumnos que recibirán clases. Los grupos deben ser integrados por un número igual de estudiantes cada uno. La lista de los grupos se deberán entregar al administrador del laboratorio para asignar un equipo a cada grupo.
- La persona encargada del registro asignará un equipo a las persona o grupo de personas que ingresen al laboratorio.
- Si un equipo es asignado a más de un estudiante, los estudiantes que estén usando el equipo serán responsables por el mismo.
- Queda prohibido el ingreso al laboratorio de informática sin la debida autorización.
- El estudiante que utilice algún equipo sin el correspondiente permiso, será sancionado de acuerdo a lo especificado en la sección de Castigos y Sanciones.
- Al salir del laboratorio de informática, el estudiante debe firmar el registro de salida para descargar su responsabilidad sobre el

equipo, de no hacerlo se aplicará las respectiva sanción de acuerdo a lo especificado en la sección de Castigos y Sanciones.

- **Tiempo y uso de las máquinas:**

  - Durante el período de tiempo comprendido desde la recepción, tiempo de uso y entrega del equipo, es o son responsables del mismo el estudiante o grupo de estudiantes que firmaron la recepción del mismo.
  - Si el equipo es utilizado por otra persona diferente a la persona o personas que firmaron la recepción del equipo se sancionará a los infractores tanto a la persona o personas responsables del equipo como a la persona ajena a la responsabilidad del mismo, de acuerdo a lo especificado en la sección Castigos y Sanciones.
  - Los estudiantes que deseen utilizar equipos para Internet deberán reservar su turno con un día de anticipación como mínimo. Tendrán un tiempo límite de uso que será de dos horas diarias, las mismas que pondrán ser ampliadas dependiendo del número de estudiantes que requieran el servicio.
  - El turno será respetado hasta 10 minutos después de la hora reservada, caso contrario se dispondrá del respectivo equipo.

- **Manipulación del equipo:**

  - No está permitido por ninguna razón cambiar las configuraciones

de las máquinas o agregar fondos de pantallas, borrar programas instalados. Si es detectado se aplicará la sanción respectiva indicada en la sección Castigos y Sanciones.

- Cualquier requerimiento de software y suministros, deberá ser solicitado a la persona encargada del laboratorio de informática.
- Por ningún concepto podrán los equipos ser desplazados hacia otro lugar.
- Cada grupo de trabajo deberá utilizar una máquina fija.
- Está prohibido realizar trabajos que no estén relacionados con la hora de clase sin autorización del profesor.
- Terminar la práctica cinco minutos antes de la hora indicada, para tener tiempo de llegar a la próxima clase.
- Una vez que finaliza la utilización de los equipos, colocar los cobertores y dejar las sillas en su respectivo lugar.

- **Utilización de medios de almacenamiento:**

- Revisar los disquetes a utilizar con el objeto de verificar que estén libres de virus.
- Si el disquete tiene virus se procederá a vacunarle o darles formato en caso de que no sea posible limpiar el virus.
- Revisar que físicamente el disco se encuentre en perfectas condiciones.
- En caso que el equipo se vea afectado por la utilización de disquetes en mal estado, se procederá de acuerdo a las sanciones

especificadas en la sección Castigos y Sanciones

- **Cuidado del laboratorio:**

  - Está prohibido ingresar a las aulas alimentos y/o bebidas.
  - No fumar en el laboratorio.
  - No ensuciar ni manchar: equipos, mesas o pisos.
  - Se ubicarán basureros al alcance y vista de los estudiantes para ayuda a conservar limpio el área física del laboratorio.
  - En caso de incumplimiento se procederá de acuerdo a la sección *Castigos y sanciones.*

- **Castigos y sanciones para estudiantes:** Se aclara que las sanciones con respecto al no permitir la entrada al laboratorio será fuera de las horas de clase.

  - El o los estudiantes responsables de introducir alimentos y/o bebidas o fumar, se suspenderá el ingreso al laboratorio por un período de 3 a 5 días, la sanción será aplicada por el administrador del laboratorio.
  - El o los estudiantes responsables de manchar: equipos, mesas o pisos deberán cancelar los gastos en los que se incurran para la limpieza de los mismos, más la prohibición de ingreso al laboratorio por un período no mayor a 10 días, siendo determinado por el administrador del laboratorio, en el caso de

que el daño sea irreversible, el estudiante deberá cancelar los gastos en los que se incurran más una sanción establecida por el Consejo de escuela.

- En el caso de daños físicos a los equipos por mal uso de los mismos, el estudiante deberá cancelar el costo de reparación del equipo más la prohibición de ingresar al laboratorio por un período no mayor de 15 días, siendo determinado por el administrador del laboratorio,.
- Si el estudiante cambia configuraciones de los programas instalados en el equipos, será sancionado con la prohibición de ingresar al laboratorio por un lapso no mayor de 5 días, siendo determinado por el administrador del laboratorio.
- En el caso de que un estudiante ingrese al laboratorio y/o utilice un equipo sin la debida autorización, se restringirá su ingreso por un período no mayor de 5 días siendo determinado por el administrador del laboratorio.
- El estudiante que permita el uso del equipo a otro estudiante fuera del grupo de trabajo al que pertenece, se castigará tanto al responsable del equipo como a la persona no responsable del mismo, a la imposibilidad de ingresar al laboratorio por un lapso no mayor de 10 días siendo determinado por el administrador del laboratorio.
- Si un estudiante saliera del laboratorio sin firmar el respectivo documento de descargo de responsabilidad del equipo, será sancionado de no ingresar al laboratorio por un lapso no mayor de

10 días siendo determinado por el administrador del laboratorio, además de detectarse cualquier daño ya sea en el equipo, mesas o pisos pertenecientes al que usaba el estudiante se hará responsable al estudiante, haciéndose acreedor a las sanciones estipuladas para dicha falta.

Profesores de la PUCESA de la Escuela de Ingeniería de Sistemas:

- **Del ingreso y salida del laboratorio:**

  - Todo de la Escuela de Ingeniería en Sistemas tiene derecho a ingresar al laboratorio de informática.
  - Deberán solicitar con anticipación cualquier modificación de horario de clase caso contrario no se le podrá facilitar el uso del laboratorio.
  - Cuando un profesor dicta su clase en las aulas del laboratorio, se le entregará y responsabilizará de todos los equipos del aula, del buen funcionamiento de las máquinas así como de la totalidad de sus componentes, previa verificación de los mismos.
  - El personal docente que necesite utilizar las computadoras para investigación y desarrollo de su materia, deberá solicitarlo al encargado del laboratorio, y lo podrá hacer sin límite de tiempo.
  - El profesor deberá firmar el registro de entrada a los laboratorios de informática.
  - Si el ingreso al laboratorio es para dictar clases, se debe formar

grupos para el uso de los equipos en el caso de que los equipos existentes sean insuficientes para la cantidad de alumnos que recibirán clases. Los grupos deben ser integrados por un número igual de estudiantes cada uno. La lista de los grupos se deberán entregar al administrador del laboratorio para poder asignar un equipo a cada grupo.

- La persona encargada del registro asignará un equipo a las persona o grupo de personas que ingresen al laboratorio.
- Queda prohibido el ingreso al laboratorio de informática sin la debida autorización.
- El profesor que utilice algún equipo sin el correspondiente permiso, será sancionado de acuerdo a lo especificado en la sección de Castigos y Sanciones.
- Al salir del laboratorio de informática, el profesor debe firmar el registro de salida para descargar su responsabilidad sobre el equipo, de no hacerlo se aplicará las respectiva sanción de acuerdo a lo especificado en la sección de Castigos y Sanciones.

- **Tiempo y uso de las máquinas:**

  - Durante el período de tiempo comprendido desde la recepción, tiempo de uso y entrega del equipo, es responsables del mismo el profesor que firmó la recepción del mismo.
  - Si el equipo es utilizado por otra persona diferente a la persona que firmo la recepción del equipo se sancionará a los infractores

tanto la persona responsable del equipo como a la persona ajena a la responsabilidad del mismo, de acuerdo a lo especificado en la sección Castigos y Sanciones.

- El profesor que desee utilizar equipos para Internet deberán reservar su turno con un día de anticipación como mínimo. Tendrán un tiempo límite de uso que será de dos horas diarias, las mismas que pondrán ser ampliadas dependiendo del número de personas que requieran el servicio.
- El turno será respetado hasta 10 minutos después de la hora reservada, caso contrario se dispondrá del respectivo equipo.

- **Manipulación del equipo:**

  - No está permitido por ninguna razón cambiar las configuraciones de las máquinas o agregar fondos de pantallas, borrar programas instalados. Si es detectado se aplicará la sanción respectiva indicada en la sección Castigos y Sanciones.
  - Cualquier requerimiento de software y suministros, deberá ser solicitado a la persona encargada del laboratorio de informática.
  - Por ningún concepto podrán los equipos ser desplazados hacia otro lugar.
  - Terminar la práctica cinco minutos antes de la hora indicada, para tener tiempo de llegar a la próxima clase.
  - Una vez que finaliza la utilización de los equipos, se debe revisar si se colocaron los cobertores y dejaron las sillas en su lugar.

- **Utilización de medios de almacenamiento:**

  - Revisar los disquetes a utilizar con el objeto de verificar que estén libres de virus.
  - Si el disquete tiene virus se procederá a vacunarle o darles formato en caso de que no sea posible limpiar el virus.
  - Revisar que físicamente el disco se encuentre en perfectas condiciones.
  - En caso que el equipo se vea afectado por la utilización de disquetes en mal estado, se procederá de acuerdo a las sanciones especificadas en la sección Castigos y Sanciones

- **Cuidado del laboratorio:**

  - Está prohibido ingresar a las aulas alimentos y/o bebidas.
  - No fumar en el laboratorio.
  - No ensuciar ni manchar: equipos, mesas o pisos.
  - Se ubicarán basureros al alcance y vista de las personas para ayuda a conservar limpio el área física del laboratorio.
  - En caso de incumplimiento se procederá de acuerdo a la sección Castigos y Sanciones.

- **Castigos y sanciones para profesores:** Se aclara que las sanciones con respecto al no permitir la entrada al laboratorio será fuera de las horas de clase dictadas por los mismos

  - El profesor responsable de introducir o permitir el ingreso de alimentos y/o bebidas o fumar, se suspenderá el ingreso al laboratorio, por un período de 3 a 5 días, la sanción será aplicada por el administrador del laboratorio.
  - El profesor responsable de manchar o permitir manchar: equipos, mesas o pisos deberán cancelar o asegurarse del cobro del valor por los gastos en los que se incurran para la limpieza de los mismos, más la prohibición de ingreso al Laboratorio por un período no mayor a 3 días, siendo determinado por el administrador del laboratorio, en el caso de que el daño sea irreversible, el profesor deberá cancelar y asegurar el cobro de los gastos en los que se incurran más una sanción establecida por el Consejo de Escuela.
  - En el caso de daños físicos a los equipos por mal uso de los mismos, el profesor deberá cancelar o asegurar el cobro del costo de reparación del equipo más la prohibición de ingresar al laboratorio por un período no mayor de 15 días, siendo determinado por el administrador del laboratorio,.
  - Si el profesor cambia configuraciones de los programas instalados en el equipos, será sancionado con la prohibición de ingresar al laboratorio por un lapso no mayor de 5 días, siendo determinado

por el administrador del laboratorio.

- En el caso de que un profesor ingrese al laboratorio y/o utilice un equipo sin la debida autorización, se restringirá su ingreso por un período no mayor de 5 días siendo determinado por el administrador del laboratorio.
- El profesor que permita el uso del equipo a personas fuera del grupo de trabajo autorizado, se castigará tanto al responsable del equipo como a la persona no responsable del mismo a la imposibilidad de ingresar al laboratorio por un lapso no mayor de 10 días siendo determinado por el administrador del laboratorio.
- Si un profesor saliera del laboratorio sin firmar el respectivo documento de descargo de responsabilidad del equipo, será sancionado de no ingresar al laboratorio por un lapso no mayor de 20 días siendo determinado por el administrador del laboratorio, además de detectarse cualquier daño ya sea en el equipo, mesas o pisos pertenecientes al que usaba el grupo guiado por el profesor se hará responsable al el, haciéndose acreedor a las sanciones estipuladas para dicha falta.

Profesores de la PUCESA de otras escuelas: Regirán las mismas reglas y sanciones estipuladas para los profesores de la escuela de ingeniería de sistemas más las sanciones y garantías estipuladas en convenios entre escuelas o que rijan a nivel de Universidad.

Estudiantes de la PUCESA de otras escuelas: Regirán las mismas reglas y sanciones estipuladas para los estudiantes de la escuela de ingeniería de sistemas más las sanciones y garantías estipuladas en convenios entre escuelas o que rijan a nivel de Universidad.

Personas Particulares:

- **Del ingreso y salida del laboratorio:**

  - Todo persona particular tiene derecho a ingresar al laboratorio de informática, presentando el salvoconducto autorizado por la escuela de ingeniería de sistemas de la PUCESA, este salvoconducto está regido por las reglas de la escuela.
  - El único documento que valida a una persona particular a utilizar los laboratorios es el salvoconducto de la escuela, conteniendo todas las características estipuladas para este documento.
  - Toda persona particular deberá firmar el registro de entrada a los laboratorios de informática.
  - La persona encargada del registro asignará un equipo a las persona o grupo de personas que ingresen al laboratorio.
  - Si un equipo es asignado a más de una persona particular , las personas particulares que estén usando el equipo serán responsables por el mismo.
  - Queda prohibido el ingreso al laboratorio de informática sin la debida autorización.

- La persona particular que utilice algún equipo sin el correspondiente permiso, será sancionado de acuerdo a lo especificado en la sección de Castigos y Sanciones.
- Al salir del laboratorio de informática, la persona particular debe firmar el registro de salida para descargar su responsabilidad sobre el equipo, de no hacerlo se aplicará las respectiva sanción de acuerdo a lo especificado en la sección de Castigos y Sanciones.

- **Tiempo y uso de las máquinas:**

- Durante el período de tiempo comprendido desde la recepción, tiempo de uso y entrega del equipo, es o son responsables del mismo la persona particular o grupo de personas particulares que firmaron la recepción del mismo.
- Si el equipo es utilizado por otra persona diferente a la persona o personas que firmaron la recepción del equipo se sancionará a los infractores tanto la persona o personas responsables del equipo como a la persona ajena a la responsabilidad del mismo de acuerdo a lo especificado en la sección Castigos y Sanciones.
- Las personas particulares que deseen utilizar equipos para Internet deberán reservar su turno con un día de anticipación como mínimo. Tendrán un tiempo límite de uso que será de dos horas diarias, las mismas que pondrán ser ampliadas dependiendo del número de personas que requieran el servicio.

- El turno será respetado hasta 10 minutos después de la hora reservada, caso contrario se dispondrá del respectivo equipo.

- **Manipulación del equipo:**

  - No está permitido por ninguna razón cambiar las configuraciones de las máquinas o agregar fondos de pantallas, borrar programas instalados. Si es detectado se aplicará la sanción respectiva indicada en la sección Castigos y Sanciones.
  - Cualquier requerimiento de software y suministros, deberá ser solicitado a la persona encargada del laboratorio de informática.
  - Por ningún concepto podrán los equipos ser desplazados hacia otro lugar.
  - Cada grupo de trabajo deberá utilizar una máquina fija.
  - Una vez que finaliza la utilización de los equipos, colocar los cobertores y dejar las sillas en su respectivo lugar.

- **Utilización de medios de almacenamiento:**

  - Revisar los disquetes a utilizar con el objeto de verificar que estén libres de virus.
  - Si el disquete tiene virus se procederá a vacunarle o darles formato en caso de que no sea posible limpiar el virus.
  - Revisar que físicamente el disco se encuentre en perfectas condiciones.

- En caso que el equipo se vea afectado por la utilización de disquetes en mal estado, se procederá de acuerdo a las sanciones especificadas en la sección Castigos y Sanciones

- **Cuidado del laboratorio:**

  - Está prohibido ingresar al laboratorio alimentos y/o bebidas.
  - No fumar en el Laboratorio.
  - No ensuciar ni manchar: Equipos, mesas o pisos.
  - Se ubicarán basureros al alcance y vista de todas las personas para ayuda a conservar limpio el área física del laboratorio.
  - En caso de incumplimiento se procederá de acuerdo a la sección Castigos y Sanciones.

- **Castigos y sanciones para personas particulares:**

  - El o las personas particulares responsables de introducir alimentos y/o bebidas o fumar, se suspenderá el ingreso al laboratorio por un período de 5 a 8 días, la sanción será aplicada por el administrador del laboratorio.
  - El o las personas particulares responsables de manchar: equipos, mesas o pisos deberán cancelar los gastos en los que se incurran para la limpieza de los mismos, más la prohibición de ingreso al Laboratorio por un período no mayor a 10 días, siendo determinado por el administrador del laboratorio, en el caso de

que el daño sea irreversible, la persona particular cancelar los gastos en los que se incurran más la prohibición de ingresar al laboratorio por un tiempo estipulado por el Consejo de Escuela.

- En el caso de daños físicos a los equipos por mal uso de los mismos, la persona particular deberá cancelar el costo de reparación del equipo más la prohibición de ingresar al laboratorio por un tiempo indefinido, siendo determinado por el administrador del laboratorio,.
- Si la persona particular cambia configuraciones de los programas instalados en el equipos, será sancionado con la prohibición de ingresar al laboratorio por un lapso no mayor de 5 días, siendo determinado por el administrador del laboratorio y cancelará los costos de reparación de acuerdo a las tarifas especificadas por el consejo de escuela.
- En el caso de que una persona particular ingrese al laboratorio y/o utilice un equipo sin la debida autorización, se restringirá su ingreso por un período no mayor de 5 días siendo determinado por el administrador del laboratorio y deberá cancelar de acuerdo a los costos estipulados por el Consejo de Escuela.
- La persona particular que permita el uso del equipo a otra persona, se castigará tanto al responsable del equipo como a la persona no responsable del mismo a la imposibilidad de ingresar al laboratorio por un lapso no mayor de 10 días siendo determinado por el administrador del laboratorio.
- Si una persona particular saliera del laboratorio sin firmar el

respectivo documento de descargo de responsabilidad del equipo, será sancionado de no ingresar al laboratorio por un lapso no mayor de 20 días siendo determinado por el administrador del laboratorio, además de detectarse cualquier daño ya sea en el equipo, mesas o pisos pertenecientes al que usaba la persona particular se hará responsable a la misma, haciéndose acreedor a las sanciones estipuladas para dicha falta.

d) Normas y obligaciones del uso del Internet.-

A continuación se presentan las normas que debe cumplir el usuario de la red Internet de la Pontificia Universidad Católica sede Ambato. Y las penalidades que implican contravenir dichas normas. Al firmar la solicitud de una cuenta de Internet en la red de la PUCESA y aceptar la misma Ud. esta aceptando expresamente estas normas.

Toda cuenta tiene un responsable. Las cuentas asignadas a profesores de la PUCESA son responsabilidad del/la profesor/a titular de la cuenta, quien se hace responsable por todas las actividades (accidentales o no) que ocurran con dicha cuenta.

De igual manera, las cuentas extendidas a estudiantes y empleados son responsabilidad del profesor o departamento que solicita la cuenta para dicha persona. En cuanto a las cuentas departamentales, el responsable es el profesor o el representante del departamento que solicita la cuenta.

Las cuentas son estrictamente personales, e intransferibles. El titular de la cuenta no puede en ningún caso prestar la cuenta a otra(s) persona(s) mediante la comunicación de su *login* y *password* de entrada. También el titular de la cuenta debe tomar las medidas necesarias para que sin su consentimiento otros puedan tener acceso a su cuenta. En tal sentido pueden ser aconsejados por el personal de la red PUCESA. En caso de incumplir esta norma de la red PUCESA tiene el derecho de cerrar en forma definitiva la cuenta y de negarse en el futuro a conceder otra cuenta al infractor.

Igualmente no esta permitido el uso de otras cuentas y archivos no otorgados explícitamente para su uso.

El password utilizado por el usuario para el acceso a su cuenta debe cumplir con las siguientes normas:

- Debe tener entre 6 y 8 caracteres.
- Debe contener al menos un carácter numérico y un carácter especial (,.:; "'&%$#).
- No debe ser una palabra que aparezca en el diccionario, ni en español ni en otro idioma utilizado comúnmente.
- No debe ser el mismo login, o nombre real del usuario o allegados al mismo.

En caso de que se detecte el uso de passwords inadecuados por parte de los usuarios, la red PUCESA puede bloquear la cuenta hasta que el usuario

corrija su situación y se ajuste a las normas dictadas en este documento. Puesto que la existencia de cuentas con password fácilmente adivinables constituyen una amenaza para todos los usuarios de una red, la infracción reiterada de esta norma puede acarrear la cancelación definitiva de la cuenta.

El usuario de la cuenta debe acatar las indicaciones y solicitudes que el personal de la red PUCESA y de administración de las redes le haga con respecto al mantenimiento de las cuentas. El incumplimiento de esta norma puede acarrear la cancelación definitiva de la cuenta y la red PUCESA tiene derecho a negarse en el futuro a conceder otra cuenta al infractor.

El usuario de la cuenta debe velar por que el directorio y subdirectorios asignados tengan los permisos adecuados para impedir el abuso por parte de terceras personas. Tampoco esta permitido cambiar las restricciones de su cuenta.

Cualquier usuario de la red PUCESA que sea descubierto intentando ganar acceso ilícito a otras cuentas, o utilizando herramientas de software para obtener información sobre otras cuentas o sobre el password de las mismas perderá en forma definitiva su cuenta, y no se le permitirá en el futuro realizar una reinscripción.

La red PUCESA se reserva el derecho de impedir su acceso a servicios públicos desde el exterior. Lo mismo es aplicable a usuarios que suministren a personas ajenas a la institución información que pueda ser utilizada para

descubrir passwords o atacar al sistema.

El intento a tener acceso a cualquier sistema de computación, incluyendo los no operados por la red PUCESA, esta prohibido. El incumplimiento de la norma acarreará la cancelación de las cuentas otorgadas a Ud. para su uso en la red PUCESA.

Queda expresa y terminantemente prohibido el uso de la cuenta y recursos de red PUCESA para propósitos ilegales.

Si un usuario va a estar temporalmente fuera de Ambato, y desea conectarse a la red PUCESA con el objeto de poder utilizar su cuenta en forma remota debe, notificar al administrador de red desde donde planea conectarse e indicar por cuanto tiempo estará ausente porque como esto no es usual el administrador al detectar un acceso desde el exterior a una cuenta lo considera en principio una ruptura de seguridad del sistema y tomara las previsiones para evitar que esto vuelva a suceder. Estas previsiones suelen comprender el bloqueo de la cuenta.

La red PUCESA se reserva el derecho de limitar el espacio de disco duro, tiempo de CPU, tiempo de conexión y derecho de uso de la impresora asignada al usuario.

No esta permitida la ejecución de programas "demonios" o de servidor sin la autorización explícita de su administrador.

Ningún usuario de la red PUCESA tiene derecho a realizar instalación de maquinas o equipos conectados a la red PUCESA sin el consentimiento expreso de los administradores de la red. Para esto deben ajustarse a las normas de instalación de maquinas conectadas a la red PUCESA.

No se pueden utilizar los recursos de la red PUCESA con fines comerciales, a menos que en ellos estén involucrados la administración de la red PUCESA, la administración de la universidad, o que la red PUCESA otorgue explícitamente permiso para ello. La red PUCESA se reserva el derecho de eliminar de una cuenta todo el material que considere es empleado para fines comerciales.

La utilización de los servicios y recursos de red PUCESA para tareas no universitarias, las cuales tengan un impacto negativo sobre las actividades universitarias no están permitidas, y serán eliminadas.

CONCLUSIONES

Como conclusiones del trabajo de investigación y por experiencia obtenida en esta materia, hemos clasificado las conclusiones en dos grupos:

a) Conclusiones sobre la red de la PUCESA:

- Al evaluar y diagnosticar la red existente en la PUCESA, se encontró un nivel de organización eficiente para la misma, en un proceso de implantación por parte de la administración del laboratorio, el cual permitirá a la universidad contar con un laboratorio de informática moderno y estructurado.

- Se ha visto conveniente que, para profundizar los conocimientos sobre redes se deben entender primero algunos conceptos básicos que permita tener una idea clara de las ventajas de establecer una red de computadoras así como los amplios servicios que brinda una red mundial como lo es Internet o una red limitada como lo es una Intranet.

- Al conocer el funcionamiento de las diversas clases de redes que existen en la actualidad, como redes de área local o redes de área extensa permite a la PUCESA establecer un punto de partida para aprovechar los avances tecnológicos referentes a la informática como es el compartir recursos existentes dentro de las áreas de la universidad, explotando al máximo su información, logrando elevar su productividad.

- La red de la PUCESA, su configuración física, entornos, componentes, topologías de red, servicios de cable estructurado, métodos de conexiones, concentradores, hubs y sus normativas establecen una configuración óptima para armar redes LAN o WAN obteniéndose una conexión natural a Internet o Intranet en las distintas áreas del laboratorio informático, obteniéndose un beneficio de seguridad y aprovechamiento eficiente de los recursos existentes.

- Basándose en el Modelo de Interconexión de Sistemas abiertos se ha logrado la correcta integración de los componentes físicos, utilizados en la estructura de la red PUCESA, siendo necesario que las aplicaciones de interfaz entre los usuarios y los equipos, sean las que ofrezcan el mejor servicio y, estén en constante desarrollo, como son los programas de Windows NT, LINUX y Novell que brindan seguridad y confianza al compartir los recursos de una forma eficaz. Así también, la configuración de los equipos cliente ofrecen a los usuarios la autorización apropiada para utilizar dichos recursos para sus labores cotidianas.

- Es importante la implantación de políticas y procedimientos para el uso de los equipos y del software, el mismo que se debe tener en cuenta para su buen funcionamiento. Con la evaluación de las nuevas políticas, sanciones y horarios se establece los parámetros y características necesarias para dar una idea clara del funcionamiento del laboratorio de la PUCESA.

- El sitio WEB creado a partir del material producto de la tesis permite explorar y consultar toda la información referente a redes por las personas que deseen

involucrarse en esta materia o simplemente deseen conocer la estructura de la red de la PUCESA. En el momento que se tiene una herramienta tan versátil como ésta, ofrece una interfaz gráfica interactiva como son gráficos, texto y video, entre el computador y el lector, manteniendo un mayor interés sobre la información, que si se tratara de un libro normal.

b) Conclusiones generales:

- El desconocimiento sobre el trabajo que se debe realizar en una red es uno de los principales problemas que tienen las empresas en nuestro medio provocando de esta forma desperdicios de recursos importantes para las mismas.

- La falta de entendimiento sobre los elementos que componen una red y los alcances que se pueden conseguir con una correcta integración de los mismos, provocan problemas operativos en los sistemas y recursos convirtiéndose en factores que retrasan el desempeño normal de los recursos que componen la empresa.

- La falta de criterio técnico con los que se arman las redes provoca deficiencias a largo plazo de los sistemas.

- La falta de conocimiento de la forma en la que se debe armar y trabajar una red provocan decepciones por parte de los empresarios el momento de trabajar con estos recursos.

- La deficiencia de una cultura informática por parte de las personas son la fuente de problemas por parte de la empresa para los técnicos o profesionales que están armando los sistemas de redes.

- La existencia de personas que no tienen los conocimientos apropiados sobre la materia generan desconfianza en los empresarios ya que el trabajo que estas realizan es deficiente y lleno de errores por lo que no se toman en cuenta criterios técnicos básicos en el momento de armar las redes.

- Las deficiencias educacionales en los centros de enseñanza son también un freno fundamental para el desarrollo en las empresas.

RECOMENDACIONES

Las recomendaciones están divididas en dos grupos:

a) Recomendaciones para la PUCESA:

- Crear o fortalecer la materia en la cual se estudien los tópicos más importantes para el entendimiento y conocimiento de la forma en la que trabajan las redes y como están constituidas, en especial la red de la PUCESA.

- Crear una política de actualización constante de la tecnología de redes para la PUCESA permitiendo avanzar a la par con la tecnología de punta, ofreciendo un mejor nivel académico a los alumnos que ingresen a la universidad.

- Hacer conocer y respetar las políticas y procedimientos que posee el laboratorio de informática a todos los usuarios, evitando así la mala utilización de los equipos y el software correspondiente.

- El personal encargado del laboratorio de informática debe ir actualizando sus conocimientos sobre la materia para la correcta administración de la misma.

- Incluir en Internet o en una aula virtual, la página Web conteniendo el presente trabajo de investigación, ya que sería una herramienta de consulta a los estudiantes y profesores para conocer cómo y porqué se diseñó la red de la universidad de una forma rápida y eficaz..

- Integrar a todas las escuelas y secciones de la PUCESA en una sola red de computadoras para aprovechar al máximo los recursos que posee la universidad y así agilizar los trámites cotidianos entre las mismas ahorrando tiempo y dinero, convirtiendo a esta entidad en una de las mejores en su tipo.

b) Recomendaciones generales:

- Crear organismos que permitan regular y controlar los trabajos de ingeniería que se realicen en la empresas, como son colegios de ingenieros u otros organismos de control.

- Dirigir seminarios de actualización de redes para las personas inmersas en la materia para conocer las nuevas tecnologías que permiten mejorar la estructura y servicios de dichas redes.

BIBLIOGRAFIA

- Sheldon Tom, ENCICLOPEDIA DE REDES, Editorial Osborne – McGraw-Hill, España 1994.
- Bardinas Felipe, METODOLOGIA DE LA INVESTIGACION, Editorial Siglo Veintiuno, Mexico 1978.
- Kris Jamsa, 1001 TRUCOS PARA DOS Y PC Y 114 TRUCOS MÁS DE DOS 6, Editorial Osborne – McGraw-Hill, 1994.
- Joe Campbell, GUIDE TO SERIAL COMMUNICATIONS, Editorial Sams, Indiana España 1994
- Microsoft Corp, MANUALES DE INSTALACION Y CONFIGURACION DE WINDOWS NT, 1994 – 1999
- PC MAGAZINE, Volumenes 9, 10, Editorial Televisa, 1999
- PC WORD, Editorial Ediworld, 1999
- www.pucesa.edu.ec
- www.panduit.com
- www.microsoft.com
- www.imprice.com
- neutron.ing.ucv.ve/comunicaciones

ANEXO I

LISTA DE EQUIPOS DEL LABORATORIO DE INFORMÁTICA DE LA PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE AMBATO – UNIDAD DE INGENIERIA DE SISTEMAS

En ésta sección se presentan los equipos existentes en los laboratorios de informática con sus características físicas en forma detallada dando al lector una idea de los elementos necesarios para instalar una red dirigida a Internet o Intranet.

LABORATORIO NOVELL

MAQUINA 1

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	Beltron	300135190	DM14V	
Teclado	BTC	235060301		
Tarjeta Madre	Genérica	AA0909399		386S
Controladora	Winbond	ID2W83757S		
T. De Video	Cirruslogic	JAX8223A10378132		
Tarjeta de Red	Netware	668893268		
Drive 3 1/2				
Drive 5 1/4	Toshiba	0805A140481A37		
Fuente de Poder	Morex	9323741		
Memoria				4 M

MAQUINA 2

Monitor	Beltron	300136081	DM14V	
Teclado	Best Keyboard	9407500443		
Tarjeta Madre	Genérica			486 S
Controladora	Winbond	9501882		
T. De Video	HMC	3121538		
Tarjeta de Red	Netware	495903000		
Drive 3 1/2	Epson	F400749471	SMD300	
Drive 5 1/4				
Fuente de Poder	Intek	92517988		
Memoria				2 M

MAQUINA 3

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	Hiunday	MAGHA306620305	DM14V	
Teclado	Genérica	312025946		
Tarjeta Madre	Genérica	3241144206		386S
Controladora	Eastern	3008641		
T. De Video	HMC	305449		
Tarjeta de Red	UMC	RRS86524		
Drive 3 1/2	Shinon	17260644	SMD300	
Drive 5 1/4	Toshiba	0805A140486A37		
Fuente de Poder	Morex	9623534		
Memoria				4 M

MAQUINA 4

Monitor	Hiunday	MAGHA302603676	HMM413	
Teclado	Best Keyboard	9407500448		
Tarjeta Madre	Genérica	9439A3A		386S
Controladora	Goldstar	GPGIOPT606B		
T. De Video	Realtek	950401F		
Tarjeta de Red	UMC	768516		
Drive 3 1/2				
Drive 5 1/4	Toshiba	0805A140483A37		
Fuente de Poder	Chieve	840428		
Memoria				4 M

MAQUINA 6

Monitor	Beltron	303135651	DM14V	
Teclado	BTC	235060304		
Tarjeta Madre	Genérica	3241247731		386S
Controladora	Holtek	147260		
T. De Video	Realtek	950401F		
Tarjeta de Red				
Drive 3 ½	Chinon	17260642	SMD300	
Drive 5 ¼				
Fuente de Poder	Intek	92528943		
Memoria				4 M

MAQUINA 7

Monitor	Beltron	300136091	DM14V	
Teclado	Best Keyboard	9407500445		
Tarjeta Madre	Amibios	AA0780329		386
Controladora	Goldstar	JPJ10PT606V		

T. De Video	Cirruslogic	JAX8223A10377717		
Tarjeta de Red	UMC	9600900494		
Drive 3 ½	Sony	11835865		
Drive 5 ¼	Morex	9323751		
Fuente de Poder	Toshiba	080SA132394A37		
Memoria				2 MI

MAQUINA 9

UNIDAD	MARCA	SERIE	MODELO	CAPACI
Monitor	EDI	9473261	VM14AF	
Teclado	BTC	K403182316		
Tarjeta Madre	Genérica	A9441		386D
Controladora	Goldstar	JPJI0PT606V		
T. De Video	Realtek	950401F		
Tarjeta de Red	UMC	9611900509		
Drive 3 ½	NEC	168316761		
Drive 5 ¼				
Fuente de Poder	Chieve	840428		
Memoria				4 MI

MAQUINA 10

Monitor	EDI	9676247	VM14AF	
Teclado	BTC	K404103848		
Tarjeta Madre	Genérica	AA0780332		386S
Controladora	Goldstar	JN6GW2760PX		
T. De Video	Realtek	950401		
Tarjeta de Red	UNC	9611900491		
Drive 3 1/2	Chinon	17260643		
Drive 5 1/4				
Fuente de Poder	Morex	9323749		
Memoria				4 M

MAQUINA 11

Monitor	EDI	94733346	VM14AF	
Teclado	BTC	FT7000		
Tarjeta Madre	Genérica	3241144209		386S
Controladora	Inbond	W83757S		
T. De Video	Beltron	17KV291005		
Tarjeta de Red	Netware	495902983		
Drive 3 1/2	Chinon	17260649		
Drive 5 1/4				
Fuente de Poder	Intek	92528406		
Memoria				2 M

LABORATORIO IBM

MAQUINA 1

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	IBM	23BXDH0	654000E	
Teclado	IBM	22128		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746675		
CD ROM	Cyber Drive	79010998		32 X
Tarjeta de Red	Genérica	808010067		
Tarjeta Madre	IBM			PII Celer
Disco Duro	Quantum	332817173104		
Drive 3 1/2	Sony	247488		
Fuente de Poder	Astek	J14X24377Z2		
Memoria				32 M
Ratón	IBM	23-114490		

MAQUINA 2

Monitor	IBM	32BWLC7	654000E	
Teclado	IBM	29669		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746674		
CDROM				32 X
Tarjeta de Red	Tricom	6M61270392		
Tarjeta Madre	IBM	11S0K428621N08J49624		PII Celer
Disco Duro	Quantum	332817675096		
Drive 3 1/2		368167		
Fuente de Poder	IBM	J14NV468PIW		
Memoria				32 M
Ratón	IBM	23047350		

MAQUINA 3

Monitor	IBM	23BXDH3	654000E	
Teclado	IBM	29633		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746118		
CDROM				32
Tarjeta de Red	IBM	01300D3		
Tarjeta Madre	IBM	11S01K428621Z1N08JJ030		PII Celer
Disco Duro	Quantum	632817825854		
Drive 3 1/2	Sony	406130		
Fuente de Poder	Ciber Drive	79010995		
Memoria				32 M
Ratón	IBM	23047309		

MAQUINA 4

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	IBM	23BNZF5		
Teclado	IBM	21604		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746244		
CDROM	Actima	436J280025945		32 X
Tarjeta de Red	Tricom	6MC127005B		
Tarjeta Madre	IBM	1100K4282ZIN0815030		PII Celer
Disco Duro	Quantum	332816772761		
Drive 3 1/2	Sony	1247554		
Fuente de Poder	IBM	J14NV467TV0		
Memoria				32 M
Ratón	IBM	28047307		

MAQUINA 5

Monitor	IBM	23BNXK9		
Teclado	IBM	29606		
T. De Sonido	Genérica			16 B
Parlantes	Genérica			
CDROM	Ciber Drive	79010994		32 X
Tarjeta de Red	Tricom	6MC127049F		
Tarjeta Madre	IBM	11S01K4286Z1N08J521		PII Celer
Disco Duro	Quantum	332817674072		
Drive 3 1/2	Sony	1526423		
Fuente de Poder	IBM	J14NV467NV5		
Memoria				32 M
Ratón	IBM	23047355		

MAQUINA 6

Monitor	IBM	23BRFH3		
Teclado	IBM	29728		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746117		
CDROM	Ciber Drive	79010996		32 X
Tarjeta de Red	Tricom	6MC12704A0		
Tarjeta Madre	IBM	11S01K42862N08J5031		PII Celer
Disco Duro	Quantum	3328176774923		
Drive 3 1/2	Sony	367988		
Fuente de Poder	IBM	J14NV468P2C		
Memoria				32 M
Ratón	IBM	23047328		

MAQUINA 7

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	IBM	23BWLD1		
Teclado	IBM	35100		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746676		
CDROM	Ciber Drive	79010999		32 X
Tarjeta de Red	Genérica			
Tarjeta Madre	IBM	1101K4L86Z1N08J52178		PII Celer
Disco Duro	Quantum	332817672135		
Drive 3 1/2		1526506		
Fuente de Poder	IBM	J14NV468P9G		
Memoria				32 M
Ratón	IBM	23023180		

MAQUINA 8

Monitor	IBM	23BWLD1		
Teclado	IBM	47332		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746115		
CDROM	Ciber Drive	79010991		32 X
Tarjeta de Red	IBM			
Tarjeta Madre	IBM	11S01K4286ZIN08JJ0517		PII Celer
Disco Duro	Quantum	332817671759		
Drive 3 1/2	IBM	J128T023664		
Fuente de Poder	IBM	J14NV474X3J		
Memoria				32 M
Ratón	IBM	23293179		

MAQUINA 9

Monitor	IBM	23BWWP0		
Teclado	IBM	44777		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	744263		
CDROM	Ciber Drive	79010832		32
Tarjeta de Red	Tricom	6MC1270200		
Tarjeta Madre	IBM	1101K4286Z1N08J5050		PII Celer
Disco Duro	Quantum	332817673461		
Drive 3 1/2	IBM			
Fuente de Poder	IBM	J14NV9967TUV		
Memoria				32 M
Ratón	IBM	23022946		

MAQUINA 10

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	IBM	23BTDG8		
Teclado	IBM	22037		
T. De Sonido	Genérica			16 B
Parlantes	Genérica	746116		
CDROM				
Tarjeta de Red	Genérica	808010048		
Tarjeta Madre	IBM	11S01K4286Z1N08J5130		PII Celer
Disco Duro	Quantum	632817824329		
Drive 3 1/2	IBM	75H9550		
Fuente de Poder	IBM	J14NV474VVK		
Memoria				32 M
Ratón	IBM	23117912		
HUB	**ACCOM**	**EH2041S**	**S9552200**	

LABORATORIO COMPAQ

MAQUINA 1

Monitor	Compaq	626AG23G0028	
Teclado	Compaq	B03C80C39EM86M	
Tarjeta de Red	Tricom	6CD1678C3A	
Drive 3 1/2	Mitshu	M014923	
CDROM			22
Fuente de Poder	Genérica		
Tarjeta Madre	Compaq	238481001	
Disco Duro	Quantum	242993001	
Memoria			32 M
Ratón	Compaq	DZL210472	

MAQUINA 2

Monitor	Compaq	724AG26GG392	
Teclado	Compaq	B03C80A39E125033	
Tarjeta de Red	Tricom	6FW16071A8	
Drive 3 1/2	Mitshu	356764A69	
CDROM			22
Fuente de Poder	Genérica		
Tarjeta Madre	Compaq	238481001	
Disco Duro	Quantum	238500003	
Memoria			32 M
Ratón	Compaq	DZL210472	

MAQUINA 3

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	Compaq	724AG26GG373		
Teclado	Compaq	B04200A39E3051		
Tarjeta de Red	Genérica	9611900496		
Drive 3 1/2	Mitshu	269913A69		
CDROM	NO			
Fuente de Poder				
Tarjeta Madre	Compaq	238481001		
Disco Duro	Quantum	BF25A011		
Memoria				32 M
Ratón	Compaq	DZL210472		

MAQUINA 4

Monitor	Compaq	603AA11AC928		
Teclado	Compaq	11742388		
Tarjeta de Red	Tricom	6CD1C78C16		
Drive 3 1/2	Teak	8709507		
CDROM		177072001		22
Fuente de Poder	Genérica			
Tarjeta Madre	Compaq	P05620P4LDYGTC		
Disco Duro	Samsung	59SA52058086		
Memoria				16 M
Ratón	Genérica	505037490		

MAQUINA 5

Monitor	Compaq	611AA11AC735		
Teclado	Compaq	20639D002519		
Sonido	Genérica	970603		
Tarjeta de Red	Genérica	VV3803007627		
Drive 3 1/2	Teck	8633223		
CDROM	Sony	3062791		22
Fuente de Poder	Compaq	D0624109470		
Tarjeta Madre	Compaq	P05620P4LDY1MK		
Disco Duro	Samsung	59SAJ2056572		
Memoria				16 M
Ratón	Genérica	003M1		

MAQUINA 6

Monitor	Compaq			
Teclado	IBM	27266		
Tarjeta de Red	Genérica	RR586511		
Drive 3 1/2	NO			
CDROM	NO			
Fuente de Poder				

Tarjeta Madre	Compaq	210262001	
Disco Duro			
Memoria			16 M
Ratón	Genérica	505036541	

MAQUINA 8

UNIDAD	MARCA	SERIE	MODELO	CAPAC
Monitor	Goldstar	259R68032411		
Teclado	BTC	ESXSRSBTCFT7000		
Sonido	Genérica	9706030		
Tarjeta de Red	Tricom	6CD1C78C41		
Drive 3 1/2	No			
CDROM	No			22 X
Fuente de Poder	Chieve			
Tarjeta Madre	Genérica	L5050176		
Disco Duro	Cgate	ST51080A		
Memoria				16 M
Ratón	Genérica	505036559		
Video	Genérica	66829		

MAQUINA 10

Monitor	Compaq		
Teclado	Compaq	A1940623	
Tarjeta de Red	Tricom	6CD1C7C2D2	
Drive 3 1/2	Compaq		
CDROM			
Fuente de Poder			
Tarjeta Madre	Compaq	210262001	
Disco Duro			
Memoria			
Ratón	Genérica		

HUB	TRICOM	16 Puertos	7XPV00A680
HUB Novell 16 Puertos		ENCORE	7J79239
HUB TRICOM	12 Puertos	7JVV219327	

ROUTER RAD	8107260
MODEM RAD	2812168

SERVIDOR INTERNET COMPAQ SCOSI PROSIGNE 500 LINUX RELAY 50 486

SERVIDOR NT CLON /1.9 /PENT./ Un. 3 1/2 / CD / 64 R IMPRESORA