Escuela Superior
Politécnica del Litoral

Facultad de Ingeniería en Electricidad
y Computación

Optimización de la Red de INTERNET TELCONET Guayaquil

Topico de Graduación

Previo a la obtención del Título de:

Ingeniero en Electricidad
ESPECIALIZACION ELECTRONICA

Presentado por :

Carlos Aveiga Painii
Segundo Contreras Puco
Carlos Silva Gavidia

Guayaquil - Ecuador
1998

DEDICATORIA

A nuestros padres
A nuestros hermanos
A todas las personas que colaboraron con nosotros en la realización de este proyecto.

DECLARACION EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestos en este proyecto final del Tópico de Graduación, nos corresponden exclusivamente; y el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".

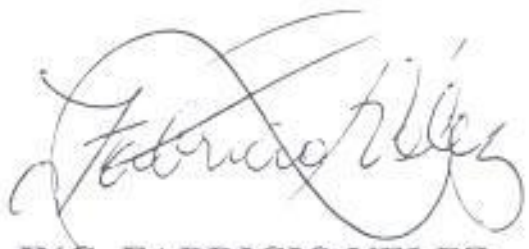
Carlos Aveiga Painii

Segundo Contreras Puco

Carlos Silva Gavidia

TRIBUNAL DE GRADO

ING. JOSE ESCALANTE
PROFESOR



ING. FABRICIO VELEZ
MIEMBRO PRINCIPAL

ING. WASHINGTON MEDINA
MIEMBRO PRINCIPAL

RESUMEN.-

Nuestro proyecto está basado en la necesidad de optimizar una red de datos que cubra los requerimientos tales como: Mejorar los tiempos de respuestas en servidores locales y remotos, facilidad de conexión del cliente y descongestión de tráfico de paquetes en la red y servidores.

En el Capítulo 1 se realiza una breve descripción de Internet, su historia, principales aplicaciones y requerimientos para la conexión a la red.

En el Capítulo 2 se da a conocer los fundamentos teóricos utilizados en la red, protocolos, medios de comunicación.

En el capítulo 3 se hace un análisis y diagnóstico de la red original, describiendo sus medios de comunicación, velocidad, capacidad, características de equipos utilizados, enlaces redundantes y monitoreo, con una previa descripción del software utilizado. Además se enfocan las necesidades de la red.

El Capítulo 4 se plantean las soluciones de las necesidades mediatas e inmediatas de la red. Se describen medios de comunicación y equipos a utilizar.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCION

La red de Telconet es muy interesante por el número de enlaces que posee, sus caracteristicas y la forma de solucionar problemas de pérdida temporal de señales, es decir enlaces de respaldo. El tema es de real actualidad, INTERNET. En este momento, las redes locales que brindan dicho servicio tienen muchos problemas con relación al tema de telecomunicaciones. Asi que, en vista del estudio de mercado, la experiencia alcanzada, atendiendo a la queja de muchos clientes, sean estos locales y extranjeros, se ha considerado importante realizar este proyecto, cuyo objetivo primordial es brindar un gran desarrollo tecnológico al pais. La empresa actualmente está brindando servicio a cerca de 1500 clientes, el cual comprende personas independientes y empresas privadas, que posee 60 empleados, incluyendo departamento técnico, departamento de ventas y administrativo.

Entre las principales quejas de los clientes se tiene: la pérdida de paquetes importantes para ellos, enviados tanto local como internacionalmente, o la dificil tarea que se vuelve cuando intentan conectarse durante muchas horas del dia, a pesar que de poseer un módem de alta velocidad. Sin embargo, también admitian que los clientes una vez conectados, navegaban fácilmente y a gran velocidad.

El proyecto está exclusivamente orientado al área de Telecomunicaciones. Se empieza con un detallado estudio del protocolo diseñado para Internet, TCP/IP. Luego se explica las especificaciones de la red original y de los equipos usados, además de datos importantes como el monitoreo de la red, con datos exactos y reales que ayuda en los cambios a realizar, se analiza las ventajas y desventajas, para finalmente concluir con los cambios que deben realizarse ahora y los que se pueden a futuro.

A pesar de contar con un protocolo de comunicaciones que tiene muy pocos errores en cuanto a pérdidas de paquetes y que tiene un mínimo porcentaje de fallas, se tiene actualmente estos problemas.

Otra idea es mejorar el monitoreo y velocidad de transmisión y comunicación con otros lugares, inclusive nacionalmente, que aunque parezca increible, cuando un cliente desea conexión con algún servidor de comunicaciones del país, es decir, con web que pertenecen otras empresas locales, el tiempo de respuesta es mayor al de comunicación con el extranjero. Algo que debe ser solucionado, debido a que otros paiseś, sin ser potencias mundiales, ya han mejorado este inconveniente, como por ejemplo Perú.

Como se menciona anteriormente, el objetivo es progresar tecnológicamente, y una parte importante de este desarrollo es Internet, que va a ser una de las pocas armas conque se cuente para sacar adelante al país.

1.1. ¿QUE ES INTERNET?

A medida que el hombre ha evolucionado, se ha visto en la necesidad de encontrar medios de comunicación cada vez más eficientes que permitan movilizar grandes cantidades de información (textos, gráficos, etc.) a través de grandes distancias.

Las empresas empezaron a organizar redes independientes en cada departamento, surgieron las primeras LAN (Local Area Networks). La tecnología LAN es especial para cada una, sus especificaciones, sus protocolos, etc. Como consecuencia la información de una red no podia pasarse con solo conectar un cable a otra red.

Luego aparecieron las WAN (Wide Area Networks) o Redes de Area Amplia. Estas utilizaban una computadora de enlace, por donde pasaba toda la información que iba dirigida a otra computadora de la red ubicada en un lugar remoto. Esto implicaba obtener lineas dedicadas y módems.

Internet es la red de computadoras más grande, de la que forman parte miles de redes distribuidas por todo el mundo. Tienen como finalidad principal la de poner información al servicio de los usuarios.

Para poder receptar o emitir información las computadoras deben ser capaces de comunicarse entre sí, para lo cual utilizan protocolos que son reglas o acuerdos sobre como poder comunicarse. El protocolo de Internet es TCP/IP.

Internet es una gigantesca base de datos distribuida en todo el mundo, en la que se puede encontrar información y servicios de todo tipo, y que para poder ser accesada requiere de herramientas que permitan buscar rápidamente la información que se necesita a través de máquinas localizadas en cualquier parte.

Existen herramientas que permiten saber alguien que se fue a estudiar a otro pais esta en sesión en ese momento, mandar y recibir correo electrónico, recibir noticias y correo acerca de temas de interés personal, buscar por el nombre de un archivo, consultar catálogos en linea, periódicos, revistas, etc., y bases de datos de bibliotecas en todo el mundo, buscar información de una persona con acceso a la red, "platicar" con una o varias personas en linea (IRC), observar el desarrollo de una partida de ajedrez, transferir archivos, comprar cosas en linea o simplemente "mirar y brincar" de una máquina a otra sólo por curiosidad.

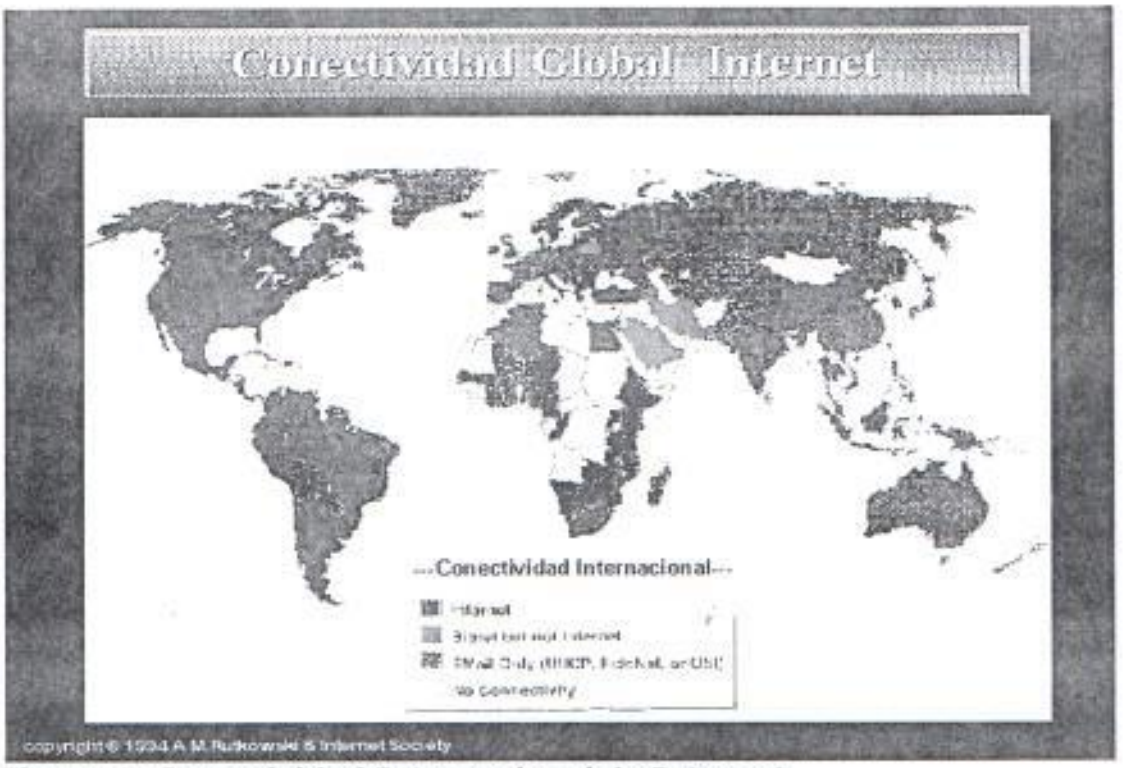


Figura 1: Conectividad Internacional de Internet

No existe una definición precisa que pueda englobar a todo lo que compone a Internet, puede ser definida con relación a sus protocolos comunes, como una colección física de ruteadores y circuitos, como un conjunto de recursos compartidos, y hasta como una actitud acerca de interconexión e intercomunicación.

Figura 2: Comunicación en Internet

1.2. HISTORIA DE INTERNET

Una de las primeras redes de conmutación de paquetes de área amplia, ARPANET, fue construida por ARPA (Advanced Research Projects Agency), su arquitectura y protocolos tomaron su forma actual entre 1977 y 1979. ARPANET sirvió como campo de prueba para muchas de las investigaciones sobre conmutación de paquetes.

ARPANET utilizaba interconexión convencional de linea rentada punto a punto, pero ARPA también ofreció fondos para la exploración de conmutación de paquetes a través de redes de radio y mediante canales de comunicación por satélite.

Además de utilizarla como una red de investigación, los investigadores en varias universidades, bases militares y laboratorios gubernamentales, utilizaban con regularidad ARPANET para intercambiar archivos y correo electrónico y para proporcionar conexión remota entre estos sitios.

En 1983 el Departamento de Defensa dividió ARPANET en dos redes conectadas, dejando ARPANET para investigaciones experimentales y formando la MILNET para usos militares.

La Internet global se inició alrededor de 1980 cuando ARPA comenzó a convertir las máquinas conectadas a sus redes de investigación en máquinas con el nuevo protocolo TCP/IP. ARPANET, una vez en su lugar se convirtió rápidamente en la columna vertebral del nuevo Internet y fue utilizada para realizar muchos de los primeros experimentos con el TCP/IP.

La transición hacia la tecnología Internet se completó en Enero de 1983 cuando la Oficina del Secretario de Defensa ordenó que todas las computadoras conectadas a redes de largo alcance utilizaran el TCP/IP.

Internet

1960's

1969 ARPANET (Advanced Research ProjectsAgency Network)

1970's

1972 Centro Nacional de Aplicaciones para Supercomputadoras
1973 FTP (Protocolo de Transferencia de Archivos)

1980's

1982 Berkeley UNIX
1982 Protocolos de red TCP/IP

1982 Fundación de Ciencias de los EEUU
1987 NSFNET
1987 Primer nodo UUCP en Uruguay
1987 Se disuelve ARPANET

1990's

1991 Es desarrollado el Gopher en la Universidad de Minnesota
1993 World Wide Web
1994 Los navegadores (browsers) gráficos
1995 VBNS (very high speed backbone network system)

El concepto general de conectar diferentes tipos de computadoras a una red surgió de la Investigación realizada por la agencia de proyectos DARPA de la defensa de los E.U.A. formando un pequeño grupo de investigadores que exploraran las comunicaciones entre redes de computadoras.

Dentro del trabajo de investigador, DARPA desarrolló la serie de protocolos TCP/IP (Transmisión Control Protocol/ Internet Protocol) para establecer comunicación entre redes, e implantar el concepto de Inter-red "Internetwork" llamado ARPAnet, que más tarde se convertiría Internet.

En este proyecto participaron investigadores de diferentes Universidades como el Instituto de Investigaciones de Standford (SRI), la Universidad de California de los Angeles (UCLA), la Universidad de California y Santa Bárbara (UCSB), y la Universidad de Utah.

En la década de los 70's DARPA se encargó de formar un comité que coordinó y guió el diseño de los protocolos y arquitectura de Internet.

Para 1980, ARPANET se convirtió en la 'espina dorsal' de Internet, siendo utilizada por la mayoría de los experimentos con TCP/IP. En 1983 la Secretaría de Defensa de los Estados Unidos mandó que todas las computadoras conectadas utilizaran TCP/IP.

En el mismo año, y debido al crecimiento en el número de computadoras conectadas, la Agencia de Comunicaciones de la Defensa dividió ARPANET en dos redes independientes, una para la investigación (ARPANET) y otra para la milicia (MILNET).

A partir de entonces se produjo un crecimiento casi desmedido en el número de maquinas conectadas a la red, debido en gran parte a la estandarización de los protocolos de comunicación. Actualmente existen 107 países que tienen algún acceso a Internet, aproximadamente 3 millones de computadoras conectadas y más de 15 millones de usuarios que se conectan alrededor del mundo.

Una Red de computadoras es una colección de nodos conectados físicamente entre si. Su finalidad es proporcionar comunicación entre diversos nodos para compartir los recursos y distribuir el procesamiento de datos. Un Nodo puede ser una minicomputadora, un mainframe, una PC, una Impresora, etc.

En toda red de computadoras existe una colección de computadoras destinadas para correr programas de usuario (aplicaciones), llamados hosts. Cada máquina en una red es un host. Existe un host específico dentro de la red denominada *Servidor* que proporciona ciertos servicios especiales en la red requeridos por otros host conocidos como clientes.

La adopción de los protocolos TCP/IP y el crecimiento de Internet no se ha limitado a proyectos con fondos del gobierno. Grandes corporaciones computacionales se conectaron a Internet, así como muchas otras grandes corporaciones, incluyendo: compañías petroleras, automovilísticas empresas electrónicas, compañías farmacéuticas y de telecomunicaciones.

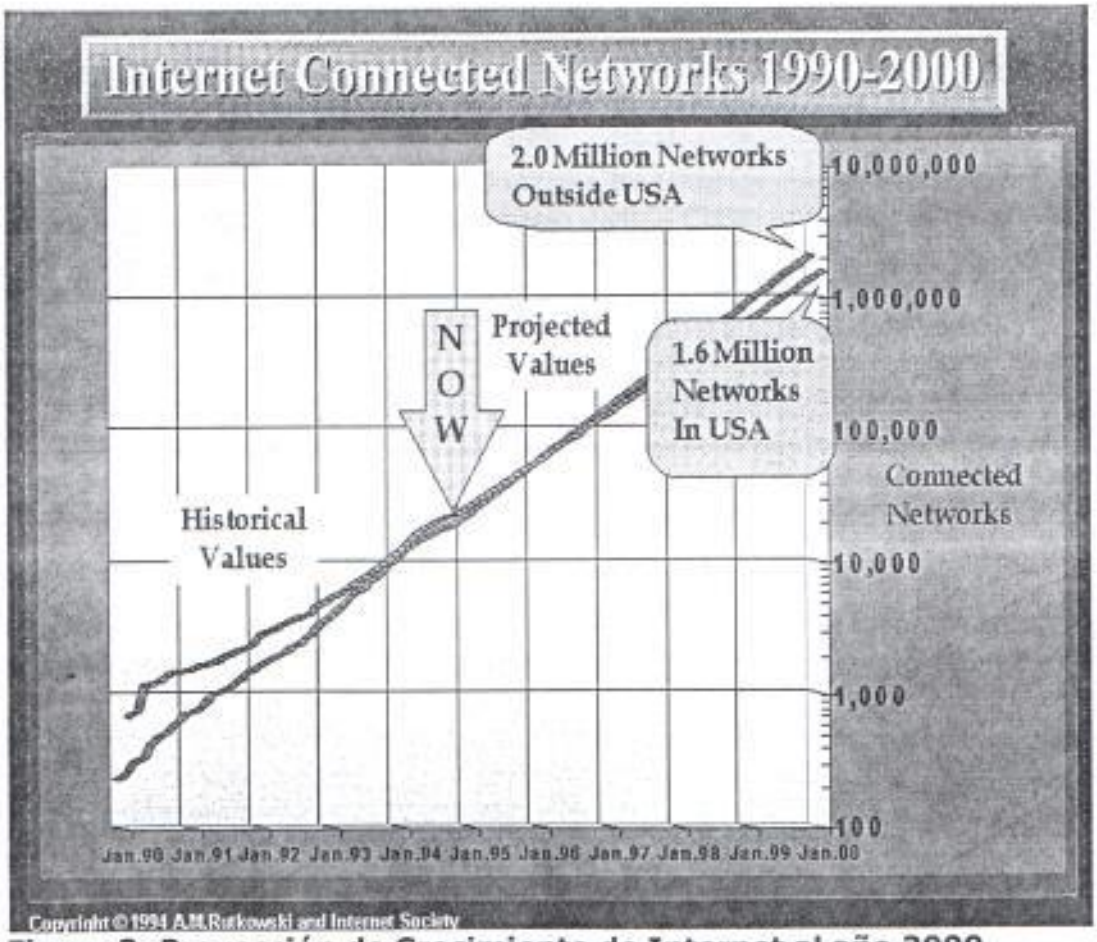


Figura 3: Proyección de Crecimiento de Internet al año 2000

1.3. SERVICIOS DE INTERNET.

➢ Servicios de Internet al nivel de Aplicación

Desde el punto de vista de un usuario, una red TCP/IP aparece como un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación. La mayoría de los usuarios que accesan a Internet lo hacen al correr programas de aplicación sin entender la tecnología TCP/IP, la estructura de las redes subyacentes o incluso sin entender el camino que siguen los datos hacia su destino.

Los servicios de aplicación de Internet más populares y difundidos incluyen:

- Correo Electrónico. El correo electrónico permite que un usuario componga memorándums y los envíe a individuos o grupos. Otra parte de la aplicación de correo permite que un usuario lea los memorándums que ha recibido. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su máquina local, se habrá recibido exitosamente.

- Transferencia de archivos. Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, que permite que los usuarios envíen o reciban archivos arbitrariamente grandes de programas o datos. Como el correo, la transferencia de archivos a través de una red TCP/IP es confiable debido a que las dos máquinas comprendidas se comunican de manera directa, sin tener que confiar en máquinas intermedias para hacer copias del archivo a lo largo del camino.

- Acceso remoto. El acceso remoto permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva.

➢ Servicios de Internet al nivel de Red

En el nivel de red proporciona dos grandes tipos de servicios que todos los programas de aplicación utilizan:

- **Servicio sin conexión de entrega de paquetes.** Significa que una red TCP/IP rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden.

- **Servicio de transporte de flujo confiable.** La mayor parte de la aplicaciones necesitan mucho más que solo la entrega de paquetes, debido a que requieren que

el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable permite que una aplicación en una computadora establezca una "conexión" con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si esta fuera permanente y directa del hardware. Por su parte los protocolos de comunicación dividen el flujo de datos en pequeños mensajes y los envían uno tras u otro.

Los servicios o herramientas de acceso a la información disponible son los siguientes:

- FTP (File Transfer Protocol) permite transferir archivos desde una computadora remota a la nuestra, o viceversa

- Telnet. Permite conectar una computadora remota como si la computadora fuera una terminal de la misma. Esto hace posible que tengamos acceso a todo el software y recursos de la máquina a la que se conecten e incluso que se ejecute programas en ella.

- Gopher. Permite acceder al sistema de información que algunas universidades y organismos ponen a disposición de los usuarios en sus servidores Gopher.

Los servicios o herramientas de búsqueda disponibles son los siguientes:

- Archie. Permite localizar el nombre de directorios o archivos contenidos en los servidores FTP a los que tenemos acceso. Archie proporciona la dirección (el host y la ruta de acceso) en la podemos encontrar el archivo que estamos buscando.

- Verónica. Permite realizar búsqueda en los Gopher existentes en el mundo.

- Wais (wide area information server). Permite buscar cualquier palabra o texto contenido en los documentos (base de datos, libros, catálogos, etc.) que circulan por Internet.

- WWW (word wide web). Es un sistema hipertexto que permite buscar y consultar documentos, base de datos o cualquier información de una forma fácil y atractiva proporcionada por los sistemas multimedia.

- Páginas Blancas (white pages). Directorios en Internet que permiten buscar direcciones de correo electrónico

1.4. TIPOS DE CONEXIÓN A INTERNET

Para usar las aplicaciones y los recursos que ofrece, debemos tener conexión. El tipo de conexión determina los servicios que se pueden utilizar y el grado de comodidad.

Todas las conexiones se realizan a través de un host que tiene asignada su propia dirección IP, es decir que está conectado directamente a Internet.

Este host puede proporcionar servicio a los usuarios conectados a él, a las computadoras que forman parte de una red en la que es el servidor, o a los usuarios que pueden conectarse con sus computadoras a través de la línea telefónica (con un módem) como si fueran terminales.

Los cuatro tipos de conexiones posibles, que ofrecen distintos niveles de servicio son los siguientes: permanente, directa, como un terminal y mail.

1.4.1. CONEXIÓN PERMANENTE

Un usuario dispondrá de conexión permanente siempre que trabaje con el host que está conectado a Internet, o con cualquier computadora de una Red de Area Local que tenga como servidor a ese host.

Esta es la mejor conexión posible, pero el costo que supone su configuración, alquiler de líneas telefónicas dedicadas y mantenimiento es muy elevado. Normalmente, la conexión permanente es utilizada por las universidades, organismos oficiales, bibliotecas o grandes empresas, que necesitan proporcionar el servicio a todos sus miembros.

La conexión permanente da acceso a todos los servicios de Internet: correo electrónico, FTP, Telnet, Gopher, WWW, boletín de noticias, etc.

1.4.2. CONEXIÓN DIRECTA

La conexión se la realiza con los nodos de Internet a través de la línea telefónica haciendo uso de un módem. Para la conexión la computadora del proveedor y la del usuario deben ejecutar el protocolo SLIP o PPP. La conexión directa también da acceso a todos los servicios de Internet, pero no de una forma tan rápida y eficaz como proporciona la conexión permanente.

La Figura 4 ilustra de forma esquemática los tipos de conexión con el host.

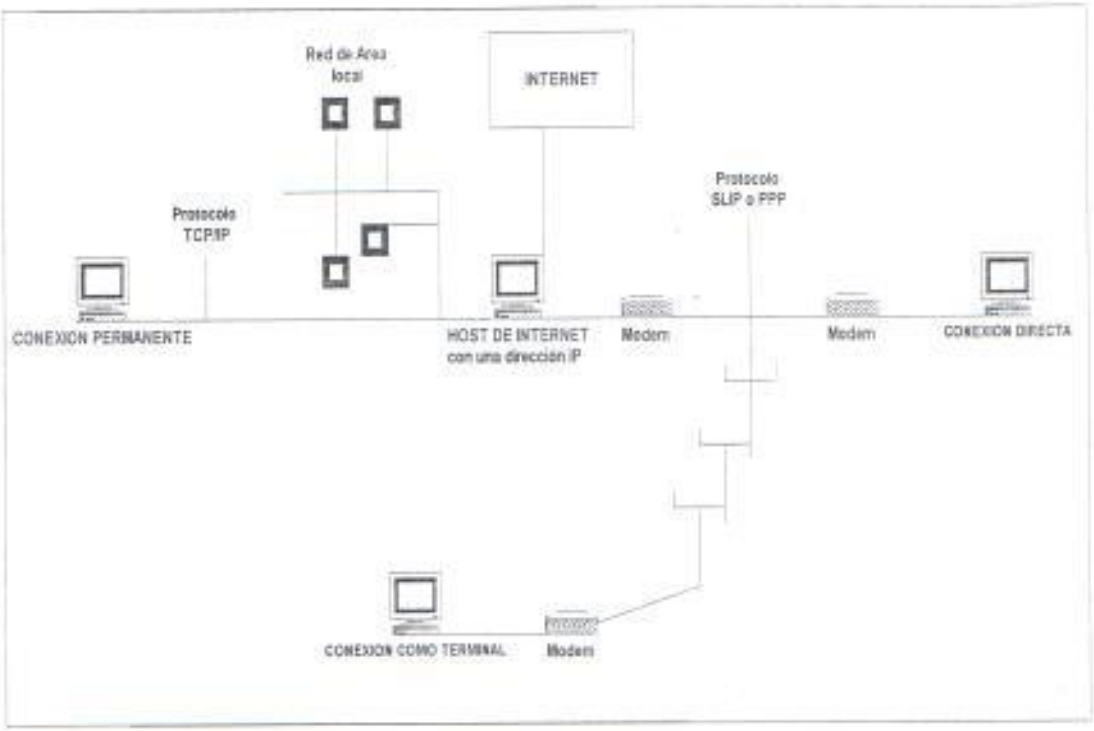


Figura 4: Tipos de conexiones con un host de Internet.

1.4.3. CONEXIÓN COMO EMULACION DE TERMINAL

Este tipo de conexión se establece a través de la linea telefónica haciendo uso de un módem. La computadora permanece en el modo de emulación de terminal, una vez que se establece la conexión con el host que proporciona el servicio de Internet.

Esto puede limitar el uşo de los recursos de Internet, ya que si, por ejemplo, copiamos un archivo se almacenará en el host del proveedor y no en la computadora. Para transferirlo a la computadora tendremos que utilizar un programa de comunicaciones. Además, si se utiliza un protocolo de comunicaciones serie, tal como Kermit o Xmodem, las limitaciones todavia pueden ser mayores.

En una conexión como emulación de terminal, el acceso a los servidores de Internet está limitado a los servicios que el proveedor pueda ofrecer o a los servicios que hayan contratado. El costo del servicio será el de la llamada telefónica, más las cuotas que cobra el proveedor por hora de uso de recursos Internet.

1.4.4. CONEXIÓN MAIL

Esta es la forma más sencilla de conexión en la que los usuarios sólo pueden enviar y recibir correo electrónico.

Los factores que determinan el tipo de conexión posible dependen de la clase de redes disponibles en el entorno; de las posibilidades de contratación de servicio con los proveedores o instituciones, tales como universidades u organismos públicos que disponen de una red con acceso a Internet; y de la cantidad de dinero que estemos dispuestos a invertir.

La única alternativa para la mayoría de los particulares a pequeñas empresas que desean conectarse a Internet es contratar los servicios de una empresa o proveedor de servicios Internet.

1.5. ¿QUE SE NECESITA PARA LA CONEXIÓN CON INTERNET?

Los elementos hardware y software necesarios para conectarse a Internet dependerán del tipo de conexión. Sin embargo, en general, para conectarse a Internet necesitará, además de tener acceso a la línea telefónica, los siguientes elementos:

- Un proveedor de servicio que le proporcione una cuenta de Internet.
- Una computadora.
- Un módem.
- Un software de comunicaciones e información sobre los parámetros de comunicación.
- Un nombre de identificación.
- Una contraseña.

2. FUNDAMENTOS TEÓRICOS DE LA RED ORIGINAL

La red a analizar y optimizar es muy interesante. Una real actualidad, INTERNET. En este momento, las redes locales que brindan dicho servicio tienen muchos problemas con relación al de telecomunicaciones.

Un tipico prototipo de una red local de Internet que actualmente está brindando el servicio a casi 1500 clientes, que posee 60 empleados, incluyendo departamento técnico, departamento de ventas y administrativo.

Entre las principales molestias que muchos clientes manifestaron tenemos: la pérdida de paquetes importantes para ellos, enviados tanto local como internacionalmente, o la difícil tarea que se vuelve cuando intentan conectarse durante muchas horas al dia, a pesar de tener un módem de alta velocidad. Sin embargo, también admitian que los clientes una vez conectados, navegaban fácilmente y a gran velocidad.

Orientado exclusivamente al área de Telecomunicaciones, se realiza un detallado estudio del protocolo diseñado para Internet, TCP/IP. Especificaciones de la red original y de los equipos usados, inclusive se tuvo la oportunidad de realizar un monitoreo de la red, con datos exactos y reales que dan la certeza de los cambios a ejecutar, a las ventajas y desventajas, y finalmente los cambios que deben hacerse ahora y los que se pueden a futuro.

A pesar de contar con un protocolo de comunicaciones que tiene muy pocos errores en cuanto a pérdidas de paquetes y que tiene un mínimo porcentaje de fallas, sin embargo actualmente existen problemas.

También mejorar el monitoreo y velocidad de transmisión y comunicación con otros lugares, inclusive nacionalmente, cuando una conexión con algún servidor de comunicaciones del pais, es decir, con web que pertenecen otras empresas locales, el tiempo de respuesta es mayor al de comunicación con el extranjero. Algo que debe ser solucionado, debido a que otros paises, sin ser potencias mundiales, ya han mejorado este inconveniente, como por ejemplo Perú.

2.1. ARQUITECTURA DE NIVELES

A continuación se muestra un gráfico comparativo entre las capas del modelo OSI Y la estructura TCP/IP.

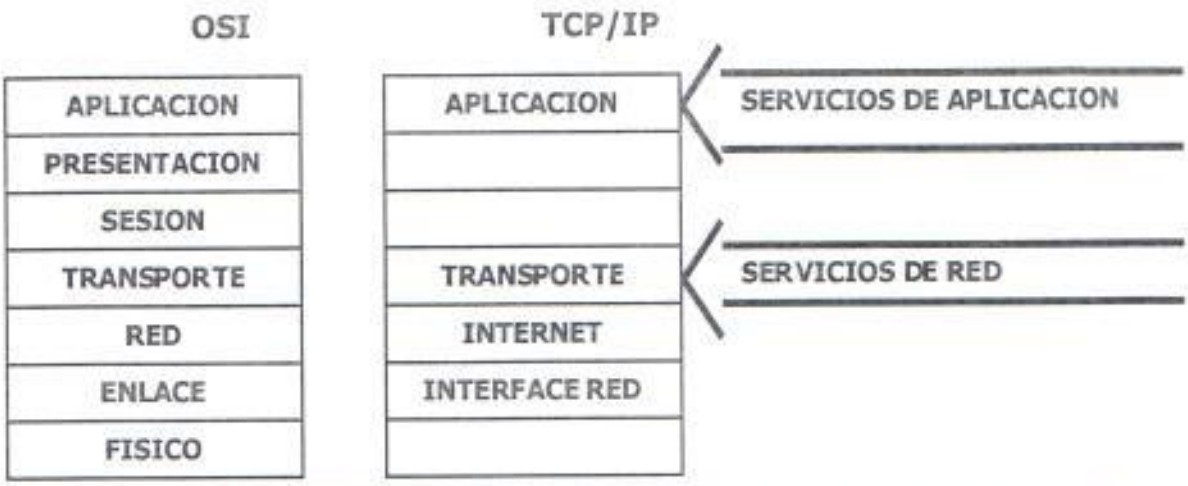


Figura 5: Comparación entre las capas del modelo OSI y la estructura TCP/IP

2.1.1. EL MODELO OSI:

El modelo OSI (Open Systems Interconection) fue inicialmente publicado por la ISO en 1.978 como un Standard para permitir la interconexión de Sistemas Abiertos. La Organización de Estándares Internacional (ISO) es responsable por el desarrollo de los estándares, por acuerdo internacional sobre un amplio rango de áreas técnicas y ha adoptado el titulo de OSI por el conjunto de estándares concernientes con la comunicación de computadores.

El modelo de 7 capas del estándar ISO/OSI es usado como referencia usualmente y concibe un sistema abierto como aquel que desarrolla protocolos de comunicación a 7 niveles.

Pueden aparecer sistemas incompatibles que actúan como: Gateways, Routers, Bridges, Repetidores u otras redes. Es característica de estos modelos multiestratos, que cada capa sólo pueda comunicarse con las capas inmediatamente adyacentes, que las funciones de ellos están muy bien definidas y que se minimice el flujo de información entre capas. Una de las finalidades de los sistemas abiertos de interconexión OSI, es la de proveer servicios de usuario basados en comunicación que operan entre sistemas de computación que pueden estar localizados entre países diferentes y provistos por fabricantes diferentes.

Debemos recordar que el estándar ISO/OSI es usado como modelo y no tiene implementaciones prácticas significativas.

CAPA	DESCRIPCION	UNIDAD DE INTERCAMBIO	COMPONENTE EN LAN
Capa de Aplicación	Usualmente presenta los recursos de la red en forma transparente a los programas de aplicación. Provee de servicios al usuario final como e-mail, emulación de terminal, acceso a base de datos remotas y demás programas usuales..	Mensaje	Programa de aplicación
Capa de Presentación	Transformación de datos y funciones recurrentes.	Mensaje	Funciones de DOS y de la Red.
Capa de Sesión	Interface de usuario a la red.	Mensaje	Interface NetBIOS
Capa de Transporte	Enlace virtual punto a punto sin error. Lo hace punto a punto sin importar que estos no sean nodos adyacentes	Mensaje	Protocolos específicos a la red, TCP, UDP, SPX.
Capa de Red	Paquetización de mensajes y enrutamiento de ellos hacia destino. Controla la congestión de los paquetes.	Packet	Protocolos específicos a la red, IPX, IP, ICMP
Capa de Enlace	División y secuencialización en Frames. Provee de comunicación confiable entre nodos adyacentes.	Frame	Manejadores de tarjeta de red
Capa Física	Requerimientos eléctricos y mecánicos del medio físico de enlace	Bit	Cables y conectores

Tabla 1: Capas del modelo OSI

2.1.1.1. FUNCIONES DE LOS NIVELES OSI

- **Capa Física**

Establece los requerimientos sean eléctricos o mecánicos necesarios para la transmisión y recepción de unidades básicas de información sobre canales de transmisión. Una serie de bits, la misma que es entregada a la capa 2.

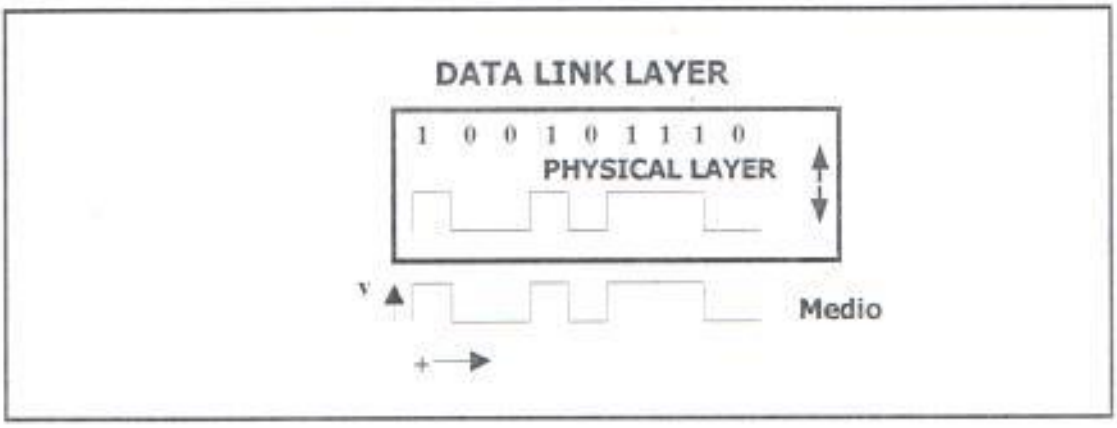


Figura 6: Paquete en la Capa física

- **Capa de Enlace**

División y secuencialización en Frames. Provee transferencia de información sobre canales ruidosos y/o compartidos entre nodos adyacentes. Recibe los datos de la capa III los separa en frames predefinidos de datos y los entrega secuencialmente a la capa I. Es responsabilidad de esta capa el identificar el comienzo y el final de un frame, puesto que la capa I no puede hacer esto. Detección y corrección de errores pueden ser realizadas en este estrato.

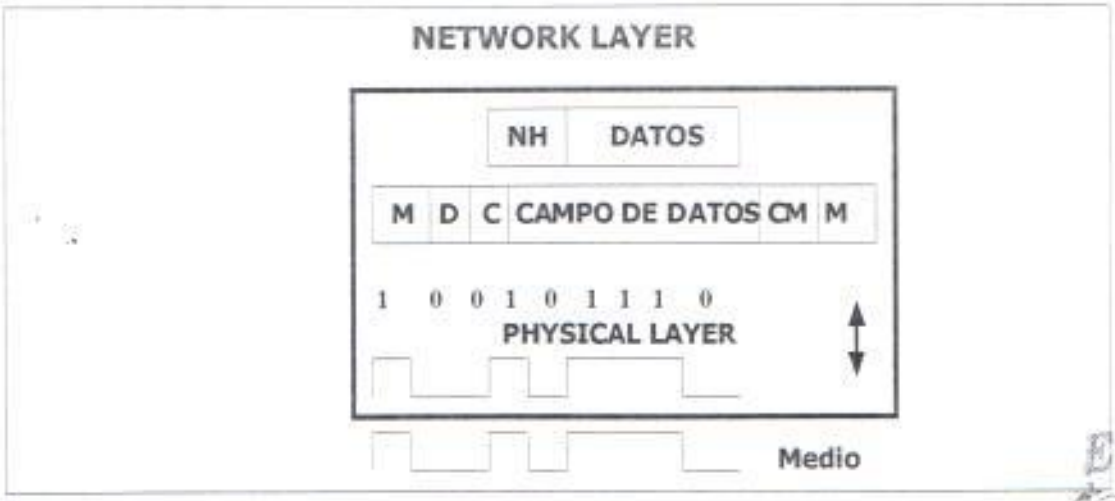


Figura 7: Paquete en la capa de enlace

M: Bits para indicar comienzo de "frame"
D: Bits de dirección
C: Bits para Control
CM: Chequeo secuencia de "frame"
M: Bits para indicar fin de "frame"

- **Capa de Red**

El estrato de red hace uso de los servicios de enlace de datos inferior para proveer servicios de transmisión de datos a través de subnetworks, es decir conecta sistemas no enlazados directamente. Tiene mucho que ver con enrutamiento, esto es establecimiento de una ruta entre los dos sistemas de computación. Además del uso de sistema de computación intermedios para proveer un flujo de datos de una subred a otra.

Los servicios ofrecidos por el estrato de red es la de coger los números y tipos de subred que pueden ser involucrados en la comunicación: paquetiza los mensajes y los enruta adecuadamente. En muchas ocasiones se encarga de llevar la "contabilidad" de los paquetes, esto es cuántos y de quién han pasado por esta capa.

- **Capa de Transporte**

Su función es la operar entre dos sistemas de computación finales estableciendo un canal punto a punto virtual esto es sin involucramiento explícito en cualquier sistema de computación intermedio que puede ser usado para relaciones entre subnetworks.

- **Capa de Sesión**

El estrato de sesión ocupa el área entre los estratos superiores orientados a aplicación y el ambiente de comunicación de datos en tiempo real. Provee servicios para el manejo y control de flujo de datos entre 2 sistemas de computación. Aparte de la capa de presentación (que sólo hace transformaciones de datos) esta capa es la interface del usuario de red.

Una conexión entre 2 usuarios, (técnicamente entre 2 capas de presentación) se llama usualmente una sesión. Esta capa es la responsable de manejar la sesión, de recuperarse transparentemente en caso de pérdida de conexión. Es importante por ejemplo para sistemas de bases de datos, donde un conjunto de actualizaciones no puede interrumpirse ya que se corromperán los datos, en este caso, la capa de sesión provee la capacidad de enviar un conjunto de mensajes a la capa de presentación destino y no entregárselos hasta que todos los mensajes del conjunto hayan llegado completos.

La sesión permite la inserción de puntos de sincronización en el flujo de información de aplicación, permitiendo identificar puntos específicos en el flujo de información y que en el caso de ser interrumpidos puedan ser retomados.

Los servicios de manejo de actividad del estrato de sesión permiten que estas abandonen bajo la instrucción (indirecta) de la capa de aplicación. El uso de estos servicios permite que una aplicación ordene y maneje su trabajo. El estrato de sesión provee comunicación dúplex y fullduplex entre los estratos superiores e inferiores.

- **Capa de Presentación**

La función de este estrato es la de proveer una representación común de la información de una aplicación mientras que está en tránsito entre 2 sistemas de computación cooperantes.

Como un ejemplo de las diferencias que deben ser absorbidas está la representación de carácter. Por ejemplo, si tenemos 2 sistemas en los cuales uno utiliza codificación ASCII y el otro codificación EBCDIC, entonces el estrato de presentación debe asegurarse que las transformaciones necesarias sean hechas sobre la información. Para hacer esto, se establece mediante negociación de los 2 sistemas de computación, una forma representacional común. La conversión de formato de línea de DOS a UNIX (CR-LF a LF), la compresión de datos, eliminación de caracteres repetidos, etc. son ejemplos de estas funciones también.

- **Capa de Aplicación**

La finalidad de OSI está realizada en el estrato de aplicación debido a que este estrato provee los servicios basados en comunicación a los usuarios finales. Los estratos subordinados del modelo existen para soportar y hacer posible, las actividades que toman lugar en el estrato de aplicación.

Aquí existe lo que se llama un agente de aplicación. Un agente de aplicación puede operar puramente como una provisión de servicio para el acceso de un usuario remoto para los recursos de sistema de computación locales. El estrato de aplicación se preocupa de proveer servicios, cubriendo un rango de aplicaciones a un usuario final.

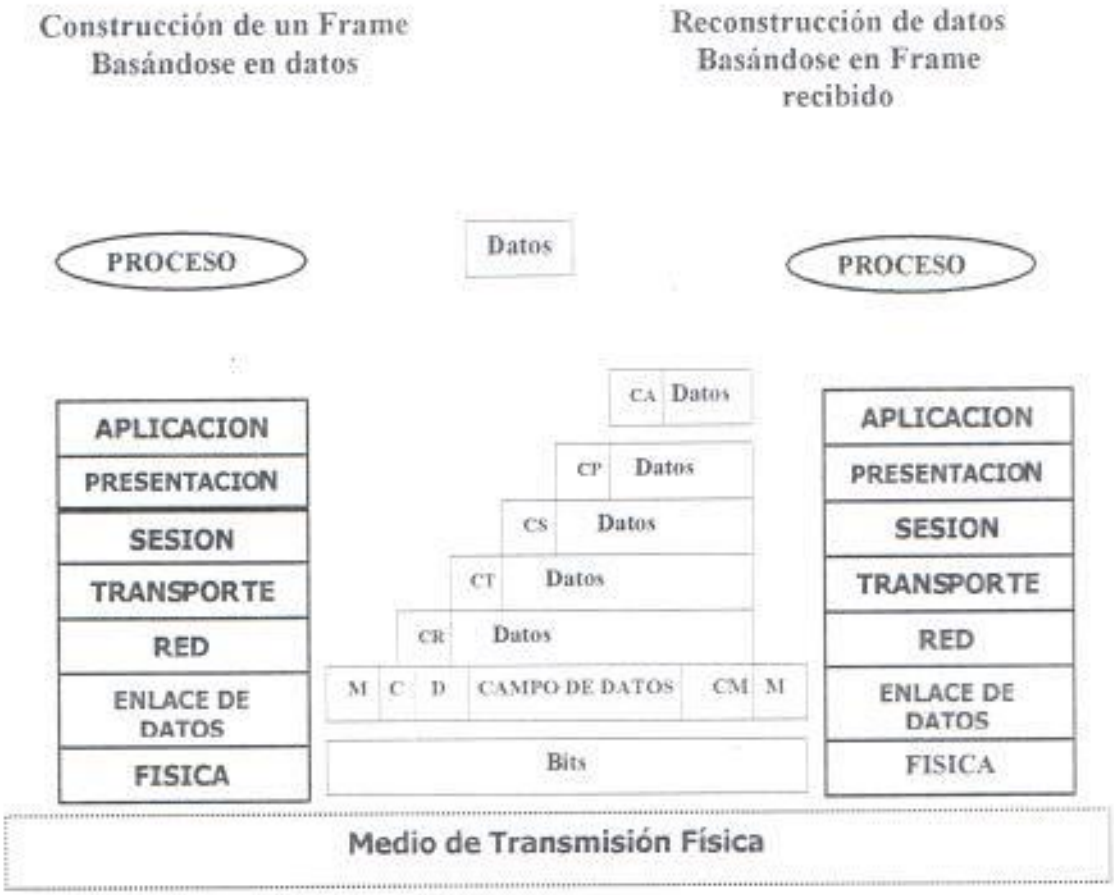


Figura 8: Forma de los paquetes en la capa de Aplicación

Donde:

CA	: Cabecera de capa de Aplicación
CP	: Cabecera de capa de Presentación
CS	: Cabecera de capa de Sesión
CT	: Cabecera de capa de Transporte
CR	: Cabecera de capa de Red
M	: Conjunto de bits para indicar inicio/fin de marco
D	: Dirección Destino y Origen
C	: Bits de Control
CSM	: Bits de control y Secuencia de Marco

2.1.2. EL MODELO TCP/IP: CAPAS DE TCP/IP

El intento fue facilitar la comunicación de ideas e información entre estas organizaciones. En las posibilidades de redes múltiples, tipos de redes posibles y los diversos equipos, el usuario es capaz de ver a la red como si fuera una simple LAN. De este surgió la fundación del protocolo el cual se llama TCP/IP.

TCP/IP usa un sistema análogo al del modelo OSI.

Figura 9: Capas de la estructura TCP/IP

- **Capa de Interface de Red**

Administra el cambio de datos entre un dispositivo y la red a la que está adjunta. Corresponde a la capa física y a la capa de enlace del modelo OSI. Normalmente incluye la Tarjeta de Interface de Red (NIC) y el correspondiente dispositivo que maneja los detalles de la interface de la red. Cada computadora necesita una tarjeta para que transmita y reciba las señales que se ejecutan a lo largo del cable de red (medios). El NIC sólo tiene la responsabilidad de controlar el acceso a los medios (Control de Acceso a los Medios (MAC)). Las técnicas incluyen Topología de Anillo, Sensor de Acarreo de Acceso Múltiple con detección de colisiones, (CSMA/CD).

Las *Técnicas de Control de acceso a los medios* asignan formatos a computadoras individuales que rigen la transmisión de información.

Los *NICS* se diseñan para operar sobre una dirección MAC. En las MAC (DIRECCIONES FISICAS), para cada tarjeta de red (NIC) se tiene una dirección física única. La dirección física es asignada por el fabricante de la NIC. La dirección física tiene 48 bit de dirección. Los primeros 24 bits son reservados para distinguir entre diferente fabricantes (NIC). Los segundos 24 bits para distinguir entre tarjetas por cada fabricante.

➢ **Capa de Internet**

En Ethernet y Token Ring los datos se envian en un formato en una manera muy especifica para que las diferentes estaciones en una red puedan usar direcciones fisicas para transmitir información a computadoras sobre la misma red.

La capa de Internet es un sistema que se diseña para permitir a las estaciones transmitir información a otras computadoras que están sobre redes diferentes.

Asi como la capa de red del modelo OSI, la capa de Internet introduce el concepto de dirección de red. El Ruteo de paquetes toma lugar en esta capa.

En términos IEEE, la capa de Internet provee una conectividad.

- **IP**= es el Protocolo de Internet que define el método para transmitir datos a esta capa
- **ICMP**= es el Protocolo de Internet para Mensajes de Control que es responsable de informar al cliente la condición en que llegaron los datos.

➢ **Capa de Transporte**

Provee conectividad punto a punto entre la fuente y el destino. Corresponde a la capa de transporte del modelo OSI. La capa de transporte es también responsable de dar formato a los datos en uno muy especifico. Se constituye de dos protocolos diferentes: TCP y UDP.

- TCP es para el Protocolo de Control de Transmisión. TCP se ocupa de dividir los datos a transmitir desde el terminal, en el tamaño apropiado para la capa de red. Provee un flujo de datos confiable entre el host y el usuario (Capa de Aplicación).

- UDP es el Protocolo para la corrección de errores en los datos.

➢ **Capa de Aplicación**

La última capa en el modelo TCP es la de aplicación.

Administra las funciones (transferencia de archivos) requeridas por los programas del usuario. Maneja los detalles de la aplicación.

Muchos protocolos diferentes de aplicación existen para numerosas aplicaciones TCP. Algunas de las aplicaciones son: FTP, Telnet, NFS y DNS.

2.2. INTERFACES FISICAS

La interface de comunicación V.35 es la utilizada en la red original, entre los ruteadores y los 2 enlaces Satelitales y el Microondas, es decir con los puertos de comunicación de los módem satelital y sincrónico digital respectivamente, que son los que realizan la respectiva modulación-demodulación. La interface de comunicación V.35 es balanceada por lo que puede trabajar a distancias superiores a 50 metros. El estándar de comunicación de la CCITT para una interface V.35 permite la interconexión de equipos de diferentes modelos.

La interface V.35 tiene 2 tipos de conectores: whinchester y el DB 25, que son los que se indican en la tabla, el tipo de conector depende del fabricante, pero como hay un estándar establecido internacionalmente el conector puede ser de los tipos. En esta red se utiliza el conector D-25.

D-25	V.35	SEÑAL DEL V.35	DESCRIPCION DEL V.35
4	F	RLSD	Receive Line Signal Detect
6	H	DTR	Data Terminal Ready
7	B	SG	Signal Ground
8	C	RTS	Request to Send
9	R	RD A	Receive Data A
10	T	RD B	Receive Data B
11	S	SD B	Send Data B
12	P	SD A	Send Data A
16	AA	SCT B	Serial Clock Transmit B
18	W	SCTE B	Serial Clock Transmit External B
19	U	SCTE A	Serial Clock Transmit External A
20	E	DSR	Data Set Ready
21	X	SCR B	Serial Clock Receive B
22	V	SCR A	Serial Clock Receive A
23	Y	SCT A	Serial Clock Transmit A
25	D	CTS	Clear to Send

Tabla 2: Interface de cable V.35 entre dos DCEs

2.3. MEDIOS DE COMUNICACION

➢ Medios de Transmisión Guiados

Tres tipos de medios guiados son usados principalmente en redes de transmisión de datos:

- **Par trenzado**, el cual puede ser blindado (STP) o no blindado (UTP).
- **Cable coaxial**, el cual puede ser grueso o delgado.
- **Fibra óptica**, la cual puede ser en modo simple, multimodo o multimodo de grado indexado.

Cables coaxiales, par trenzado transmiten electricidad. Los cables de fibra óptica en cambio transmiten señales de luz. Cada uno de estos tipos de cables esta dividido en categorias más especializadas, que tienen sus propios diseños y especificaciones, estándares, ventajas y desventajas. Estos cables difieren en precio, velocidad de transmisión y distancias de transmisión recomendadas. Por ejemplo, el cableado con par trenzado es actualmente el más barato. El cable de fibra óptica es más caro pero mucho más rápido y resistente. El cable coaxial descansa entre estos dos tipos en caracteristicas de precio y funcionamiento.

Los diferentes tipos de cables mencionados, tienen en común los siguientes componentes:

- Un conductor que provee el medio para la señal. El conductor podria ser un alambre de cobre o un tubo de vidrio.

- Un aislante de algún tipo alrededor del conductor para ayudar a tener la señal dentro del conductor y alejado de las interferencias.

- Una envoltura exterior para recubrir a los elementos del cable. La envoltura mantiene a los componentes del cable juntos, y además sirve para proteger a los componentes del cable de agua, presión o algún otro tipo de daño.

Cada tipo particular de cable tiene otros componentes, asi el cable coaxial tiene uno o más tipos de blindaje en particular entre el aislador y la envoltura. El par trenzado tiene dos alambres conductores enlazados uno alrededor del otro. La fibra óptica puede incluir algún material para ayudar a proteger la fibra de la presión.

La capa de aislamiento mantiene a la señal dentro del medio de transmisión y además ayuda a proteger la señal de interferencias externas. Para el cable de fibra óptica es hecho de un material con un menor indice de refracción que el del núcleo. El indice de refracción es una medida que indica la manera en la cual un material reflejará los rayos de luz. Un indice de refracción menor asegura que la luz no se salga del núcleo.

La envoltura plenum o envoltura de cable provee una capa que mantiene a los elementos del cable juntos. Existen dos clases de envoltura: plenum o no plenum. Para ciertos ambientes, el cable plenum es requerido por la ley.

Este debe ser usado cuando el cable trabaja sin estar puesto en un conductor dentro de las paredes y deberia ser usado cuando sea posible, tienen menor pérdida de señal que los cables no plenum.

Los factores que afectan el funcionamiento del cable

- **Atenuación**

La atenuación es el decrecimiento de la fuerza de la señal medida en decibelios (dB) por 100 pies o por kilómetro. Tales pérdidas ocurren cuando la señal viaja a través del alambre. La Atenuación ocurre más rápidamente a frecuencias más elevadas y cuando la resistencia del cable es más alta.

- **Diafonía**

La diafonía es una interferencia en forma de una señal que viene del cable o circuito vecino, por ejemplo, señales en diferentes pares de cable par trenzado pueden interferir unos con otros. Una medida común usada para esta interferencia en cables de par trenzados es la diafonía de cercano término, la cual es representada en decibelios (dB). Un valor más alto en decibelio indica menor diafonía.

- **Impedancia**

La impedancia es una medida de la resistencia eléctrica, ésta no es directamente un factor del funcionamiento del cable. Sin embargo, la impedancia puede hacerse un factor si ésta tiene diferentes niveles en diferentes localizaciones de la red. Una impedancia más alta indica una resistencia más alta. Por lo tanto se hace más grande la atenuación a frecuencias más elevadas.

2.3.1. PAR TRENZADO

El cable es ampliamente usado, barato y fácil de instalar. Este puede transmitir datos a una aceptable tasa de velocidad (hasta 100Mbps en algunos tipos de arquitectura de red).

El más conocido ejemplo de cableado con par trenzado es probablemente el telefónico, el cual es no blindado y usado normalmente para la transmisión de datos que requieren de mayor calidad.

En la siguiente tabla se observa la clasificación del cable de par trenzado, las características principales de cada uno de ellos y sus principales usos. El trenzado dentro de un par minimiza la diafonía entre pares. Además ayuda a tratar con la interferencia electromagnética y la interferencia de radio frecuencia, así como también la pérdida de la señal debido a la capacitancia.

Propiedades del Par Trenzado Blindado (STP) Incluye blindaje alrededor de los pares trenzados. Impedancia de 150 ohmios. Sujeto a la diafonía. Sujeto a la interferencia electromagnética. Generalmente usa conectores RJ-
Usos del par trenzado blindado Redes IBM Token-Ring. Redes Ethernet.
Propiedades del Par trenzado No Blindado. (UTP) No existe blindaje alrededor de los pares trenzados. Impedancia de 100 ohmios. Sujeto a diafonía. Sujeto a interferencias electromagnéticas. Generalmente usa conectores RJ-
Usos del Par Trenzado No Blindado. Redes Ethernet 10 base T. En ciertas secciones de las redes IBM Token-Ring. Líneas telefónicas (grado de voz).

Tabla 3: Propiedades de cables STP y UTP

Alambres conductores.- Los alambres de señal para este cable vienen en pares que están enlazados uno con otro. Los alambres conductores son generalmente hechos de cobre. Ellos pueden ser sólidos o trenzados.
Capa de Blindaje.- El par trenzado blindado (STP) incluye una delgada capa blindada alrededor de cada par de conductores.
Envoltura.- El paquete de alambres es recubierto en una envoltura hecha de polivinil clorhídrico (PVC) o cables que están llenos de Teflón.

El cable par trenzado se clasifica en:

- Par trenzado blindado (STP)
- Par trenzado no blindado (UTP).

a) Cable Par Trenzado Blindado (STP)

El cable STP tiene pares de alambres enlazados unos con otros. Cada par es cubierto con una delgada pantalla protectora para reducir interferencia y minimizar la diafonía entre pares de alambres. STP puede manejar transmisiones de alta velocidad, pero el cable es relativamente caro, puede ser un poco grande, pesado, difícil.

b) Cable Par Trenzado No Blindado (UTP).

El cable UTP no incluye pantallas protectoras extras alrededor de los pares de alambres. Este tipo de cable trabaja a velocidades bajas. UTP además puede ser usado en arquitectura Ethernet y Token-Ring. UTP no es la primera alternativa para cualquier arquitectura de red, pero la IEEE ha aprobado un estándar la red Ethernet 10BaseT que usa cableado UTP a 10 Mbps. UTP no es tan bueno para evitar ruido e interferencia como el STP o cable coaxial. Consecuentemente, los segmentos del cable UTP deben ser más cortos que cuando se usan otro tipo de cables. Para el estándar UTP, la longitud de un segmento no debería exceder nunca a 100 metros. Por otro lado, es bastante económico, muy fácil de instalar y trabajar con él.

La mayoría de los cables telefónicos son UTP y algunos cables telefónicos tienen alambres extras ya que los cables vienen con 4 pares y la compañía de teléfonos necesita únicamente dos de estos pares para la conexión telefónica. Si existen pares no usados, uno puede usar éstos para un cableado de red. El cable telefónico es de baja calidad, usado principalmente para la transmisión de datos a menos que uno quiera transmitir sobre cortas distancias.

Las cualidades que caracterizan a los cables STP y UTP incluyen lo siguiente:

- **Atenuación**

Este valor indica cuanta potencia ha perdido la señal y es independiente de la frecuencia de transmisión.

- **Capacitancia**

Este valor indica el rango al cual el cable guarda carga. Bajos valores en (pF) indican un mejor funcionamiento. Típicos valores están entre 15 y 25 pF/ft.

- **Impedancia**

Todos los cables UTP deberían tener una impedancia de 100 +/- 15 ohmios.

- **Diafonía**
  - Esta característica indica el grado de interferencia de los pares de alambres vecinos.

Esto es además medido en decibelios por unidad de distancia, pero un valor más alto es mejor para esta característica. Diafonía depende de la frecuencia de la señal y de la categoría del cable. El funcionamiento es mejor a frecuencias más bajas y en las categorías de cables más altas.

A continuación se describirán las ventajas y desventajas del cable par trenzado.

Ventajas:

- Es fácil de conectar a los diferentes dispositivos. Si existe un sistema de cables instalado, tal como el cable telefónico, existen cables extras no usados que pueden ser incluidos para uso personal. Por ejemplo, para usar el sistema de cables telefónicos, uno necesita un cable telefónico que tenga 4 pares de alambres, así no se necesitan segundas líneas de dos pares para la conexión telefónica.
- STP hace un trabajo en el bloqueo de la interferencia.
- UTP es económico.
- UTP es fácil de instalar.
- UTP puede ya estar instalado pero hay que asegurarse de que el cableado instalado funcione adecuadamente y que tenga las especificaciones de funcionamiento que una red cualquiera necesite).

Desventajas:

- STP es pesado y es difícil trabajar con él.
- UTP es más susceptible al ruido o interferencia que el cable coaxial o que el cable de fibra óptica.
- Las señales que viajan a través de cables UTP no pueden ir muy lejos antes de que necesiten regeneración a amplificación.
- Un efecto de piel puede incrementar la atenuación. Esto ocurre cuando los datos se transmiten a tasas rápidas sobre alambre de par trenzado. Bajo estas condiciones la corriente tiende a fluir mayormente en la superficie exterior del alambre. Esto disminuye la sección transversal del alambre que es por donde fluye los electrones y por lo tanto aumenta la resistencia. Esto a su vez, incrementa la atenuación de la señal o pérdida.

2.3.2. CABLE COAXIAL

Consiste de un conductor cilindrico externo que encierra un alambre conductor central. El conductor externo puede ser sólido o en forma de malla, entre los dos conductores existe un material dieléctrico que los separa. El principio del cable coaxial es el de la Jaula de Faraday, si la superficie está conectada al terminal de tierra, entonces será imposible que algún campo eléctrico o magnético pueda penetrar e influir sobre la carga. Este principio es ventajoso ya que permite que este cable pueda trabajar en lugares con alta intensidad electromagnética, sin que se degenere la señal que conduce.

Funcionalmente los cables coaxiales se dividen: baseband y broadband. El cable baseband tiene un canal sobre el cual un solo mensaje puede ser enviado a velocidades de hasta 80 Mbps. Dicha señal no está modulada. Su impedancia caracteristica, es decir la impedancia que deben tener los equipos a los cuales se va a conectar el cable para proporcionar la máxima transferencia de potencia, varia según la aplicación pero su valor más usual es de 50Ω. Puede trabajar con señales analógicas o digitales.

La siguiente designación es muy usada para los cables coaxiales. Estos son unos pocos de todos los cables disponibles:

- **RG-6** Usado como cable para bajar la transmisión de CATV. Tiene una impedancia de 75 Ω y es un cable broadband.
- **RG-8** Usado para Ethernet grueso. Tiene una impedancia de 50 Ω. Este cable también es conocido como cable Ethernet serie N.
- **RG-11** Usado principalmente para troncales de CAT. Tiene 75 Ω de impedancia y es un cable broadband.
- **RG-58** Se usa en redes Ethernet. Tiene 50 Ω de impedancia y usa conector BNC.
- **RG-59** Usado para ARCnet. Tiene 75 Ω, usa conector BNC. Este tipo de cable se le usa para conexiones broadband y por compañias de TV cable para conectar a los clientes en forma individual.
- **RG-62** Usado para ARCnet. Tiene 93 Ω de impedancia y usa conectores BNC. También se usa este cable para conexión del terminal al controlador de terminal en el sistema de configuración IBM 3270.

2.3.3: FIBRAS OPTICAS

Uno de los más significativos avances de la tecnología en transmisión de datos es el desarrollo práctico de los sistemas de comunicación por fibras ópticas. Las siguientes caracteristicas distinguen a las fibras ópticas del par trenzado y del cable coaxial:

- Una baja atenuación por Km. cuando se transmite por las llamadas ventanas de transmisión que están ubicadas en torno a los valores siguientes de longitud de

onda: 0.8 mm, 1.3 mm y 1.55mm. Esta última ventana es la que presenta menor atenuación.

- Total inmunidad al ruido y a las interferencias electromagnéticas, lo que constituye un medio especialmente útil en ambientes con alto ruido. Además no irradia energía, razón por la cual no causa interferencia a otros equipos cercanos.
- Uso de potencias del orden de los mW, en comparación con otros medios de comunicaciones que requieren potencias mayores.
- Su pequeño tamaño y poco peso, hace de ellos, medios de comunicaciones fáciles de instalar.
- Ancho de banda mucho mayor. El potencial ancho de banda y velocidades de datos de un medio aumentan con la frecuencia. A las muy altas frecuencias de la luz usada por las fibras ópticas, velocidades de 2 Gbps. Sobre unas decenas de Kms son posibles. Comparando esto con unos cientos de Mbps sobre 1 Km por el cable coaxial o unos pocos Mbps a 1 Km del par trenzado.
- Mayor espacio entre repetidoras. Pocas repetidoras significan menores costos y menores fuentes de error.

Entre las aplicaciones más importantes tenemos:

- Cables troncales de larga distancia.
- Cables troncales Metropolitanos.
- Troncales de intercambio rural.
- Lazos locales.

Características de transmisión

Las fibras ópticas transmiten la información por medio de un rayo de luz el cual se traslada por reflexión interna. La reflexión interna total se da sobre un medio transparente que tiene un indice de refracción mayor que el medio que lo rodea. La luz se compone de ondas electromagnéticas que se propaga en el vacio a una velocidad del orden de 300.000 Km./Seg.

Para el caso de los medios guiados, el medio por si mismo es más importante para determinar las limitaciones de transmisión. En la tabla se observan algunas caracteristicas tipicas de los medios de transmisión guiados, que incluyen la tasa de transmisión que el medio puede soportar, el ancho de banda que puede transmitir y el espacio requerido para un repetidor en transmisiones digitales.

Las fibras ópticas son inadecuadas en su estado bruto después de su fabricación para su tendido por las canalizaciones de la compañia telefónica, así que deben tener propiedades mecánicas similares a las de los cables de cobre. Para alcanzar este objetivo tendria que aumentarse por una parte la resistencia a la tracción de las fibras, y por otra parte impulsarse su facilidad de cableado.

La resistencia a la tracción de la fibra óptica decrece debido a las microfisuras y a la influencia de la humedad, por esto se deposita sobre la cubierta de la fibra una capa protectora de resina orgánica de 4 o 5μm de espesor.

Un problema de la fibra constituye las microcurvaturas. Debido a estas la luz se trasmite de modos de mayor orden superior muy atenuados, o incluso es radiada por la fibra. Desviaciones de solamente 1 um que se repiten continuamente a tramos de 1mm son suficientes para aumentar la atenuación a 20 dB/Km. Para evitar estas perdidas el cable tiene que fabricarse de modo que las fibras ópticas no sean afectadas por irregularidades pequeñas de la estructura del cable, condicionadas por el material o la geometría. Por lo tanto cada fibra se introduce de forma suelta en un hilo o conductor de plástico de aproximadamente 1mm de diámetro. Simultáneamente se aumentan la resistencia al impacto y al aplastamiento.

Solamente con las fibras ópticas no se puede establecer ninguna ruta de transmisión, hay que añadir los empalmes, las conexiones entre fibras y los conectores a la entrada y a la salida de la ruta. Una conexión óptica apropiada para aplicaciones sobre el terreno tiene que cumplir una serie de requisitos entre los cuales se pueden mencionar montaje sencillo, conectado repetible, construcción estable, atenuación de paso mínima, protección de las superficies terminales de la guía de onda contra destrucción y suciedad.

En los conectores ópticos y en los empalmes se presentan atenuaciones para las que a mayoría de las veces hay que considerar tres causas:

- Características diferentes de las fibras ópticas a conectar.
- Defectos mecánicos del conector o del empalme.
- Reflexión y diseminaciones en el punto de conexión.

La causa principal de atenuaciones elevadas en conectores y empalmes son los defectos mecánicos. Para la minimización de las pérdidas tienen que mantener estrictas tolerancias mecánicas, en lo que se requiere al ajuste lineal, es decir a la dislocación axial que sólo se presenta en conectores, así como al ajuste del ángulo β de las superficies frontales de las fibras ópticas entrantes y salientes. En la práctica se presentan las tres causas de atenuación, calculándose la atenuación total a partir de la suma de las atenuaciones individuales. Las pérdidas por reflexión y de diseminación adicionales existentes pueden así mismo ser pequeñas por medio de una cuidadosa construcción de montaje de los conectores.

Los impulsos de información atenuados, ensanchados y desincronizados por la ruta de transmisión son amplificados en el repetidor, recortados y llevados nuevamente a su posición correcta de fase. La regeneración de impulsos es necesaria en cualquier repetidor y en el receptor y en el receptor al final de la ruta de transmisión, haciendo posible la supresión de ruido inherente al proceso de modulación por impulsos codificados.

Las características que en este caso tienen importancia son en el emisor la posibilidad de modulación del componente y la potencia óptica emitida, en la fibra óptica el ensanchamiento del impulso debido a la dispersión y a la atenuación, en la conexión del emisor y fibra óptica las pédidas de acoplamiento y finalmente en el fotodiodo la sensibilidad para una anchura de banda predeterminada. En el gráfico, la longitud de la fibra se determina mediante la potencia óptica del emisor, las pérdidas de acoplamiento y finalmente en el fotodiodo la sensibilidad para una anchura de banda predeterminada.

En la siguiente tabla se muestra un resumen de las principales caracteristicas de medios guiados a transmisión punto a punto.

MEDIO DE TRANSMISION	TASA DE TRANSMISION	ANCHO DE BANDA	ESPACIO DE REPETIDORA
PAR TRENZADO	4 Mbps.	250 KHz.	2 – 10 Km
CABLE COAXIAL	500 Mbps.	350 MHz.	1 – 10 Km
FIBRA OPTICA	2 Gbps.	2 GHz.	10 – 100 Km

Tabla 4: Características de Medios Guiados

En medios no guiados, el espectro o banda de frecuencia de la señal producida por la antena transmisora es más importante que el medio en determinadas caracteristicas de transmisión. Así mientras más alto sea el centro de frecuencia de una señal más grande será el potencial del ancho de banda y por lo tanto la tasa de velocidad de transmisión. Otra propiedad de las señales de transmitidas por las antenas es la direccionalidad. En general, las señales de más bajas frecuencias son omnidireccionales, esto es, la señal se propaga en todas las direcciones de las antenas. En frecuencias mas altas, es posible enfocar la señal como un rayo direccional.

- **Medios de transmisión no guiados**

2.3.4. RADIO

El medio usado para transmisión electromagnética puede ser dividido en dos categorías básicas guiadas y no guiadas. Los diferentes medios de transmisión que se

explicaron anteriormente caen en el rango de guiados y es obvio que se puede ejercer mayor control sobre este tipo de medio comparado con los sistemas no guiados correspondientes a los sistemas de radio, estos últimos son convenientes para comunicaciones sobre barreras tales como aguas, terrenos montañosos, o bosques espesos, donde medios guiados serán difíciles de emplear. Con sistemas de transmisión basados en radio, la potencia de la señal recibida, es función de la potencia transmitida, patrones de la antena, obstrucciones físicas, etc. Cabe anotar que las ondas de radio son afectadas bastante por los factores meteorológicos e inclusive fenómenos extraterrestres.

Los sistemas de Radio se clasifican en:

- **Radio VHF (Onda Corta).**

  Banda Regulada de 136 – 174 MHz.
  Sólo para transmisión de voz.

- **Radio UHF (Onda muy corta)**

  - **Banda Regulada de 350 - 900 MHz.**
    Permite transmisiones de Voz y Datos.
  - **Banda Regulada de 928 – 953 MHz.**
    Uso exclusivo de Datos.
    Banda canalizada de 25 KHz.
    Velocidad de 19.2 Kbps. con equipos analógicos. Usa modulación FM, PM.
    Velocidad de 64 Kbps. con equipos digitales . Usa modulación PSK.
  - **Banda no regulada de 902 – 928 MHz.**

- **Microondas**

  Bandas no reguladas:
  2400 – 2484 MHz., 5725 – 5825. MHz.
  Bandas con 15 canales de 5.1 MHz c/u.
  Uso de técnicas de transmisión tipo Spread Spectrum.
  Permite grandes distancias: 20 – 60 Kms. dependiendo de las condiciones topográficas.
  - Altas tasas de transmisión: de 8-10 Mbps. Con DSSS.
    Hasta 2 Mbps con FH.

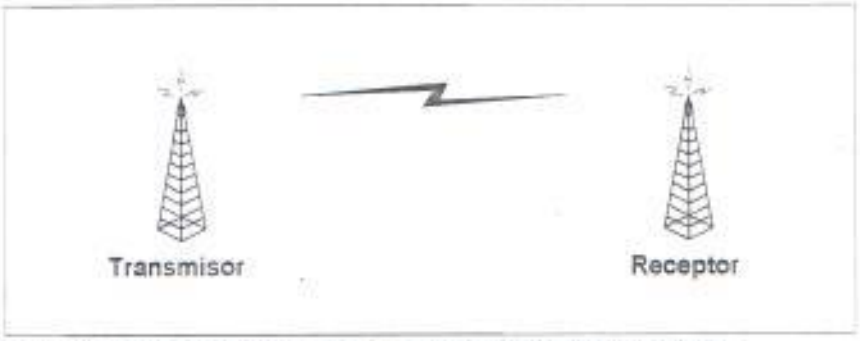


Figura 10: Comunicación para microondas terrestres

Bandas de frecuencia de transmisión.		
Bandas	**Gama de frecuencias**	**Longitud de Onda (cm.)**
HF	3 – 30 MHz.	10000 - 1000
VHF	30 – 300 MHz.	1000 - 100
UHF	300 – 1000 MHz.	100 - 30
L	1 – 2 GHz.	30 – 15
S	2 – 4 GHz.	15 – 7.5
C	4 – 8 GHz.	7..50 – 3075
X	8 – 12 GHz.	3.75 – 2.50
Ku	12 – 18 GHz.	2.50 – 1.67
K	18 – 27 GHz.	1.67 – 1.11
Ka	27 – 40 GHz.	1.11 – 0.75
Milímetro	40 – 300 GHz.	0.75 – 0.10
Microondas Digital		
Banda (GHz)	**Ancho de Banda (MHz)**	**Velocidad de datos (Mbps).**
2	**7**	**12**
6	**30**	**90**
11	**40**	**90**
18	**220**	**274**

Tabla 5: Bandas de frecuencia de transmisión

Las señales de radio aproximadamente arriba de 30 a 50 KHz, tienden a pasar a través de la Ionósfera en lugar de reflejarse o refractarse lo suficiente para su uso más allá del horizonte visual. Estas frecuencias tan altas son útiles para comunicación en línea de vista, por distribución troposférica, difracción o con satélite como repetidor.
La comunicación terrestre vía microondas utiliza sistemas de transmisión y recepción con antenas que deben ser enfocadas o direccionadas con mucha precisión hacia otra antena de recepción.

Estas antenas generalmente se colocan en torres de transmisión a una altura considerable sobre el nivel del suelo para evitar posibles problemas con obstáculos que podrían impedir una excelente transmisión.

Las microondas por línea de vista (radio enlaces) en las bandas de 150 MHz, 450 MHz, 900 MHz, proporcionan la capacidad de transmisión multicanal de 12 a 120 canales nominales de 4 KHz, sobre trayectorias en línea de vista. Arriba de los 2 GHz, los sistemas en línea de vista transmiten hasta 1800 canales y, en algunos casos hasta 2700 canales telefónicos sobre portadora de radio frecuencia.
En los sistemas de línea de vista las ondas de radio viajan en línea recta y se limitan en el horizonte a causa de la curvatura de la tierra. Generalmente las ondas de radio que se propagan en línea recta se curvan o difractan más allá del horizonte óptico.

En trayectoria de radio con varios Km. De largo, las microondas pueden sufrir desvanecimiento, y entre más larga es la trayectoria hay posibilidades de que suceda. El desvanecimiento es la variación del nivel de una señal de radio con el tiempo.

En los sistemas de línea de vist alos desvanecimientos son provocados por los cambios atmosféricos, las reflexiones en la tierra y el agua en la trayectoria de propagación.

Los radioenlaces tienen puntos terminales y puntos de repetición, en los puntos terminales se demodulan todas las portadoras de RF a la banda base; la banda resultante se demultiplexa a la frecuencia de los canales individuales. Los puntos de repetición sirven para fortalecer la señal o amplificarla dependiendo si es una señal digital o analógica.

2.3.5. ENLACE SATELITAL

Los enlaces con microondas satelitales poseen el mismo principio que los enlaces terrestres de microondas. Existe una estación transmisora la cual envía la señal al satélite el que a su vez recibe la transmisión procesa la información y la transmite a una o varias estaciones terrenas.

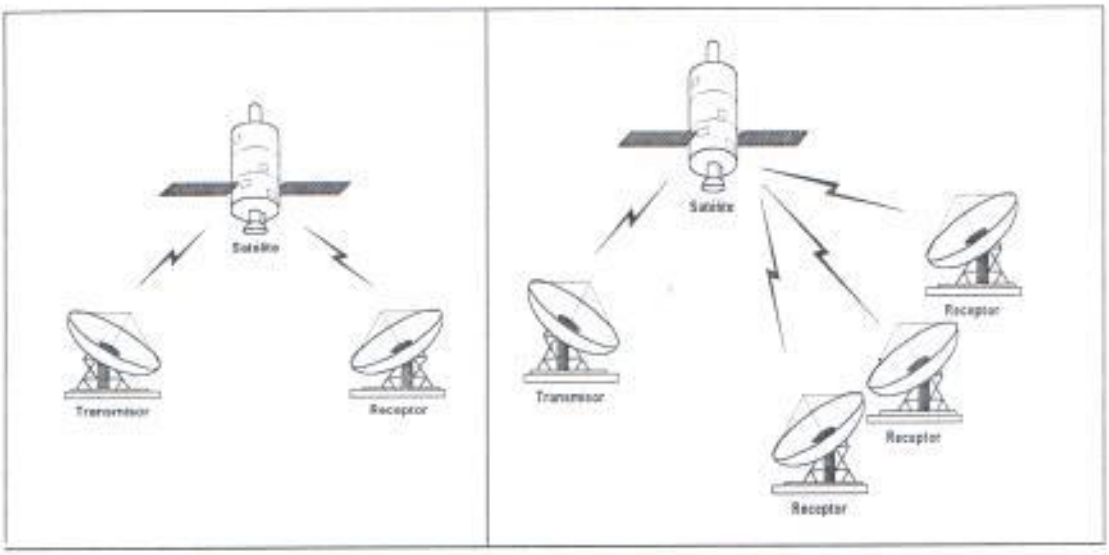


Figura 11: Tipos de Conexión para enlaces satelitales

En las figura 11 se puede apreciar dos aspectos diferentes de enlaces satelitales: enlace punto a punto y enlace punto multipunto.

El satélite recibe la transmisión (Uplink) a una determinada frecuencia, amplifica la señal en caso de ser analógica o la reconstruye en caso de ser digital. Luego esta información es retransmitida a tierra nuevamente (Downlink) a una frecuencia diferente de la que fue recibida por el satélite.

Las Bandas asignadas para este tipo de enlace son:

- **Banda C:**

Ofrece la mayor eficiencia
Alta direccionabilidad
Baja atenuación
Esta banda está completamente saturada.

- **Banda Ku:**

No tiene mayor interferencia con microondas terrestre.
El haz de radiación es más concentrado, lo cual permite antenas más pequeñas.
Ideal para sistemas VSAT.
Sufre de mucha atenuación con la lluvia y otros fenómenos atmosféricos.

Los componentes del enlace satelital son:

- Antena Parabólica.
- Amplificador de bajo ruido
- Receptor satelital.

- **Antena parabólica**

Las antenas parabólicas que se utilizan para la transmisión y la recepción son básicamente reflectores que convierten la potencia de salida de un transmisor en ondas electromagnéticas (para el caso de antenas transmisoras) las que son transportadas a través del espacio libre para que puedan ser recibidas por otra antena de similares caracteristicas en el satélite. El satélite recibe una pequeña porción de la potencia, procesa la información, refortaleciéndola para poder ser retransmitida por otra antena del satélite hacia alguna estación terrena. La señal que se recibe del satélite es muy débil y además las señales pertenecen a las bandas de microondas. Esto exige para la mejor recepción, el empleo de una antena dotada de un reflector parabólico. Dichos reflectores tienen la particularidad de concentrar toda la energia electromagnética que reciben en un punto denominado foco. Precisamente en el punto focal está situado el dipolo o antena propiamente dicha. La antena no es visible pero lo que si se puede ubicar en el punto focal es la ventana de entrada al LNA o LNB.

Entre más grande es el diámetro del plano reflector, mayor será la energia que será posible concentrar en la antena. Para evaluar el diámetro del reflector es necesario disponer de una serie de datos.

En todos los casos el plato parabólico estará montado de manera tal que se lo pueda orientar adecuadamente, para cumplir con los requerimientos que en cada localidad plantea la necesidad de apuntar hacia el satélite.

Los movimientos del plato deben ser dos. Uno de ellos permitirá modificar el ángulo de elevación, equivalente a decir que el plato puede quedar, desde casi horizontal, hasta casi vertical. Lo primero se aplicaria en instalaciones en localidades cercanas a la linea ecuatorial y lo segundo a instalaciones muy al sur o muy al norte de esta linea.

El segundo ajuste tiene que ver con el ángulo de acimut y para cumplir con el mismo debe de ser girada la plataforma que soporta la antena o bien, especialmente en el caso de reflectores grandes, podrá haber un mecanismo que haga girar al plato. Se entenderá que las facilidades para estos ajustes dependen fundamentalmente del precio del conjunto que constituye la antena más su montaje.

La banda de frecuencia utilizada para las transmisiones via satélite son la banda C de 4 a 8 GHz y la banda Ku de 12 a 18 GHz. Entre más fuerte es la potencia con la que transmite el satélite, más pequeña puede ser la dimensión de la antena, por ejemplo en el sistema VSAT la antena tiene un diámetro de 1m aproximadamente, y en los sistemas USAT, las antenas pueden llegar a medir hasta 60 cm. de diámetro, siendo estas ultimas utilizadas con fines para la recepción de canales de televisión via satélite.

- **Amplificador de bajo ruido**

El componente de tecnología más avanzada de la estación receptora es el LNA y se caracteriza por el bajo ruido en su circuito de entrada, condición fundamental para lograr la recepción con relación señal/ruido de buenas características. Se debe tener en cuenta que si una señal débil llega a un circuito de entrada caracterizado por una importante presencia de ruido, la degradación que experimenta ya no puede ser mejorada en el resto del receptor. Si bien es cierto que todas las etapas del receptor generan ruido, a partir de la primera etapa amplificadora, las señales ya tienen mayor nivel y por ello el ruido las afecta menos. Además de su óptimo comportamiento frente al ruido, el LNA debe proporcionar elevada ganancia a la frecuencia de las señales captadas por la antena y teniendo en cuenta que se tratan de microondas, se termina convenciendo de la muy refinada tecnología que se utiliza en este componente.

El LNA está montado, prácticamente en el foco de la parábola, lo que en otras palabras quiere decir que debe de soportar las inclemencias atmosféricas. Su encapsulado debe tener en consecuencia, condiciones adecuadas soportadas. En estas instalaciones se debe incluir una etapa conversora de frecuencia, capaz de reducir la frecuencia de las señales, facilitando así su transmisión hasta el receptor satelital. Esto puede hacerse en forma independiente, utilizando una disposición que se denomina Convertidor descendente. Pero en la actualidad tiende a ser lo más común incluir el conversor junto con el amplificador pasando entonces a llamarse LNB (bloque de bajo ruido).

- **Receptor satelital**

Se trata de otro de los componentes electrónicos que integra el sistema de antena pero que puede ser instalado en interiores. Es un decodificador que descomprime la señal digital receptada y la convierte en una señal de video junto con canales de audio y un canal de datos. Estas características pueden variar según el equipo que se utilice. Este sistema de transmisión de datos satelital utiliza compresión de datos y transmisión digital para transmitir la señal a través de un solo transpondedor en el satélite. Para el enlace ascendente (Uplink), este aparato encodifica, digitaliza, y comprime la señal de video. Multiplexa todas las señales digitales en un canal de datos compuesto, el cual puede operar a 2.9, 3.3 o 6.6 Mbps, luego se formatea los datos en un frame de comunicaciones. A estos frames se les aplica una corrección de errores FEC (Forward Error Correction) luego de lo cual son conducidos a través de un puerto de datos RS-422 para ser modulados en QPSK (Quadrature Phase Shift Keying)

El modulador QPSK recibe el flujo de datos multiplexado desde el encodificador y modula digitalmente una portadora a una frecuencia intermedia (IF) la cual esta a 70 MHz. Luego esta frecuencia intermedia es convertida a una frecuencia más alta (Up convert) para que pueda ser recibida por el transpondedor a una banda determinada. El enlace descendente (Downlink) se descomprime el flujo de bits digitales y son

convertidos a una señal de video NTSC (National Television System Committee) dos canales de audio, y un canal de datos simplex. Para lograr esto, el sitio de recepción utiliza un plato de antena convencional con su correspondiente LNB el que amplifica y baja la frecuencia a la banda L (950-1450 MHZ.)

2.3.6. RED TELEFONICA ANALOGICA.

Es un medio público de transmisión de datos. Básicamente una linea telefónica (que utiliza el cable UTP) es capaz de transmitir señales que tienen energia confinada a la banda de frecuencia de 300 Hz. hasta 3000 Hz. La red brinda los siguientes servicios:

- **Línea dial – up**

Denominadas también líneas de conmutación (ya que son obtenidas por marcación). Consiste en los pares de 2 hilos de la red telefónica pública con conmutación suministrada por las empresas de telecomunicaciones. Es una conexión telefónica normal que puede ser establecida marcando el número, o código asociado con el destino. Estas lineas generalmente soportan velocidades desde 2400 hasta 9600 bps. La conexión se crea en el tiempo de marcar el número, y es destruida cuando la llamada se termina, en contraste con las dedicadas en las cuales la conexión especifica entre dos puntos siempre está disponible. Tiene la ventaja de poder conectarse con cualquier parte de la red telefónica mundial. Los costos se limitan a las tasas correspondientes: presentan un alto nivel de ruido, limitan el rendimiento del sistema debido al tiempo necesario que se utiliza para la conexión, desconexión y los cambios de sentido.

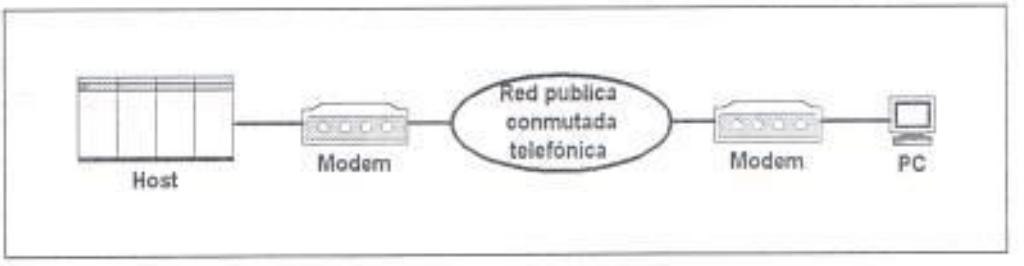


Figura 12: Ilustración de la conexión a través de una línea Dial-Up.

- **Línea dedicada**

Líneas de 2 ó 4 hilos que conectan dos puntos o múltiples puntos permanentemente. Aqui la conexión está siempre disponible ya que están exentas de señales de ocupado, posee tarifas mensuales fijas, brindan un mejor acondicionamiento para una mejor calidad de transmisión, posee velocidades de transmisión superiores y un mayor rendimiento. La transmisión y recepción pueden ser simultáneas eliminando el

cambio de sentido. En cambio, como desventaja se observa el mayor costo que tiene el uso de lineas dedicadas como alternativa para la transmisión de datos.

La calidad de las lineas telefónicas es dificil de predecir, especialmente si atraviesa paises. En el país es mucho más visible esto, ya que ni las lineas dedicadas y peor las dial-up constituyen una alternativa muy confiable (además de su baja velocidad por su naturaleza analógica). Este servicio es solo utilizada solo para aplicaciones criticas de tipo ocasional, y en ningún caso critica. Las empresas recurren a otros medios como son los enlaces de radio y satelitales y dejan a las lineas de Pacifictel para propósitos de Backup.

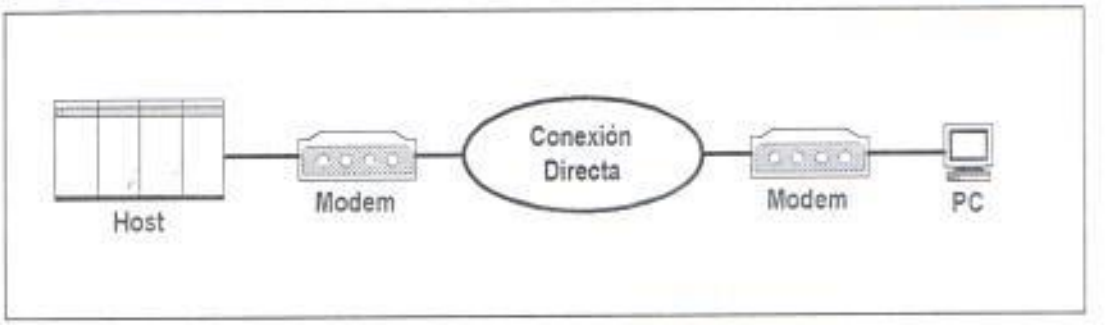


Figura 13: Ilustración de la conexión mediante línea dedicada

2.4. PROTOCOLOS UTILIZADOS EN LA RED

Protocolo es un conjunto de reglas que gobiernan el intercambio de datos entre dos entidades, donde una entidad se refiere a cualquier cosa capaz de enviar o recibir información.

Los protocolos se clasifican de acuerdo a la capa en que son utilizados:

- Protocolos utilizados en la Capa de Interface de Red.
    - Protocolo CSMA/CD
    - SLIP (Serial Line Internet Protocol)
    - PPP (Protocolo Punto a Punto)
    - Protocolo de Control de Enlace
    - Protocolo de Control y Red

- Protocolos utilizados en la Capa de Transporte
    - Protocolo de Datagrama de Ususario (UDP)
    - Protocolo de Control de Transmisión (TCP)
- Protocolos utilizados en la Capa de Aplicación
    - Protocolo de Transferencia de Archivos (FTP)

2.4.1. PROTOCOLO CSMA/CD

- Estaciones detectan la "portadora" antes de transmitir.
    - Estación detecta el estado del canal: libre u ocupado.
    - Si cree que está libre, entonces transmite.
    - Si detectan actividad, entonces esperan para iniciar la transmisión.
- Nodo transmisor tiene que asegurarse que el mensaje llegue a su destino sin interrupciones.
    - Debe permanecer escuchando durante un cierto tiempo. Si luego de ese tiempo no escucha nada entonces comienza a transmitir.
    - Opcionalmente LLC puede enviar confirmaciones (ACKs).
- CSMA se preocupa si el bus está desocupado para que un terminal pueda transmitir.
- CD detecta si hubo una colisión.

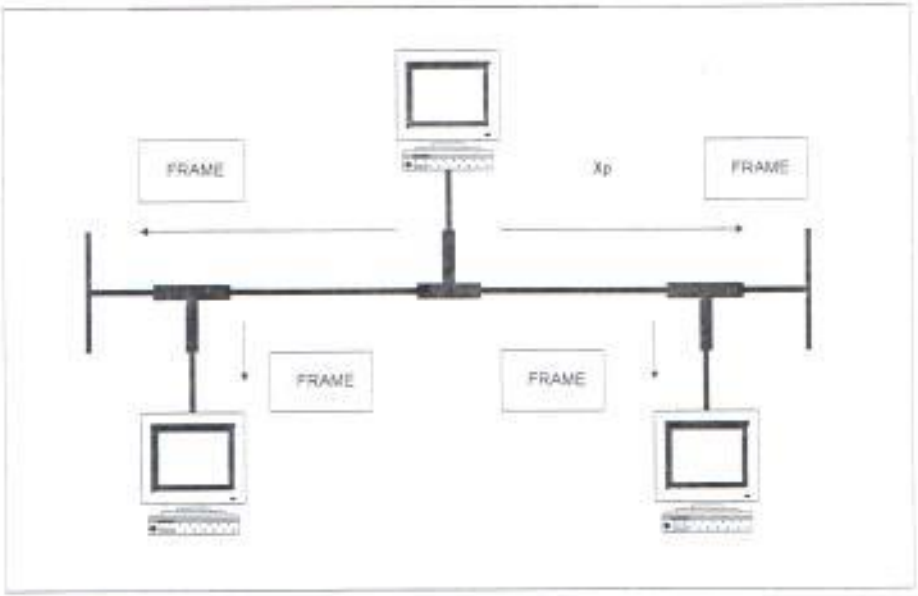


Figura 14: Frame de datos se transmite sin problemas

Transcurridos 2 Xp, CSMA/CD asume que la Tx (Transmisión) fue correcta.
Xp es la duración de propagación en función de la velocidad y distancia.

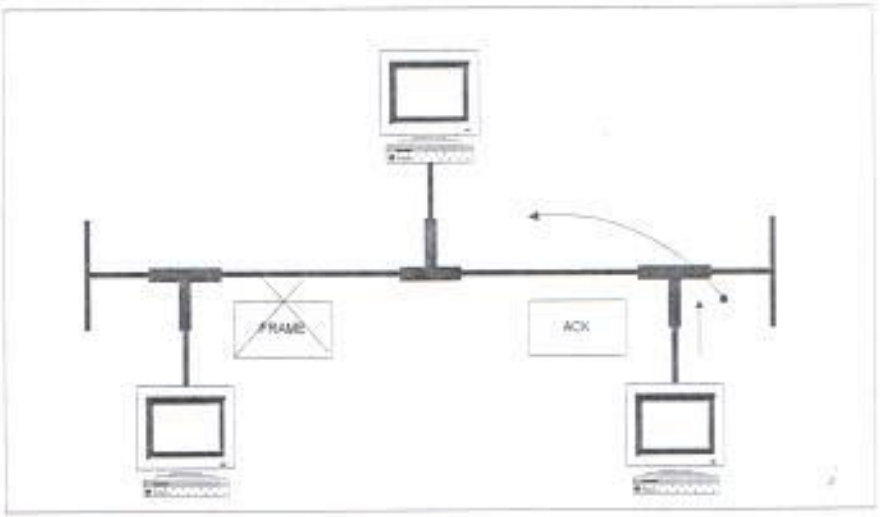


Figura 15: Generación del Ack

Si el frame no es para la estación, lo descarta.
La generación del ACK en realidad no es parte del protocolo 802.3 sino del LLC2 (IEEE 802.2)

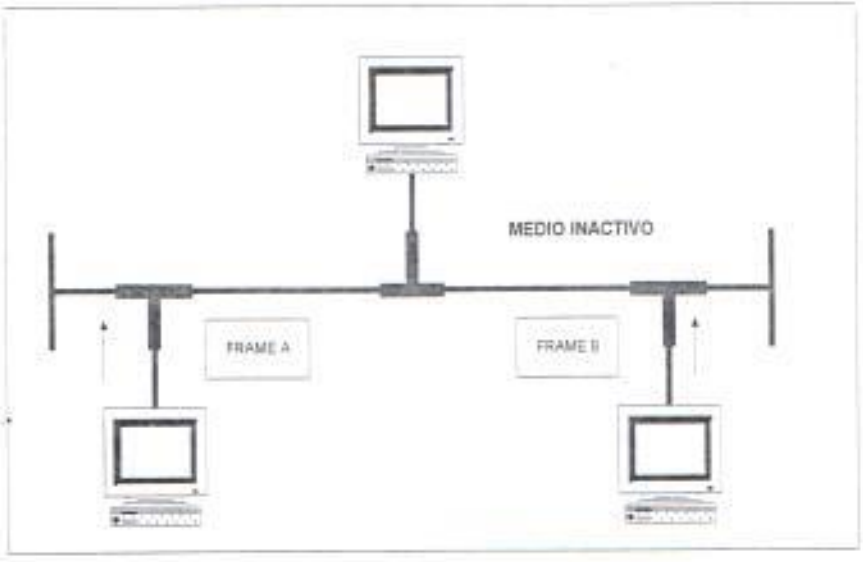


Figura 16: Dos frames a la vez

Ambas estaciones creen que el medio está inactivo, entonces ambas transmiten. Esto produce una colisión con los frames de datos. El frame accidentado sigue su curso hasta llegar a sus respectivos orígenes, lo cual les sirve para detectar la colisión. Ambas estaciones detectan la colisión, entonces ambas deben retransmitir.

2.4.2. SLIP (SERIAL LINE INTERNET PROTOCOL)

Fue el primer protocolo para enlaces seriales definido para TCP/IP
Los frames son muy simples:

0xC0	Datos	0xC0

Figura 17: Frame del protocolo Slip

- Si 0xC0 ocurre en la parte de datos es reemplazado por la secuencia 0xDB-0xDC
- Provee funcionalidad mínima

Ventajas:
- Simple en su diseño e implementación
- Muy eficiente bajo líneas en excelentes condiciones
- Ampliamente difundido

Desventajas:
- Solo sirve para llevar paquetes IP
- No provee detección de errores
- No tiene mecanismo de autenticación a nivel de enlace
- No provee mecanismos de negociación de parámetros

2.4.3. PPP (PROTOCOLO PUNTO A PUNTO)

Es un protocolo completo de capa de enlace y ofrece servicios de:
- Encapsulamiento
- Control del protocolo de enlace (LCP)
- Control de Protocolos de red (NCP)

El esquema es similar al usado por HDLC

Flag	Addr.	Cont.	Protocol	Data	FCS	Flag	Interfr. Fill
Ox7E	OxFF	OxO3	16 bits	variable	16/32 bits	Ox7E	1'S

Figura 18: Frame de datos del protocolo PPP

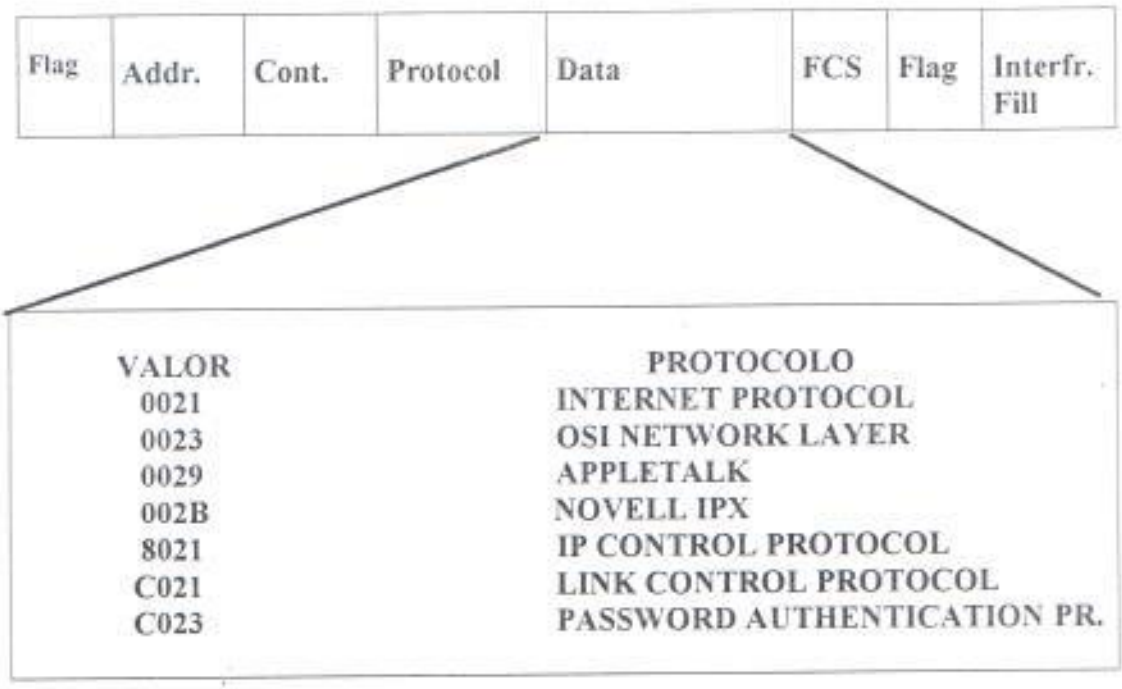


Figura 19: Soporte a Múltiples Protocolos de Red

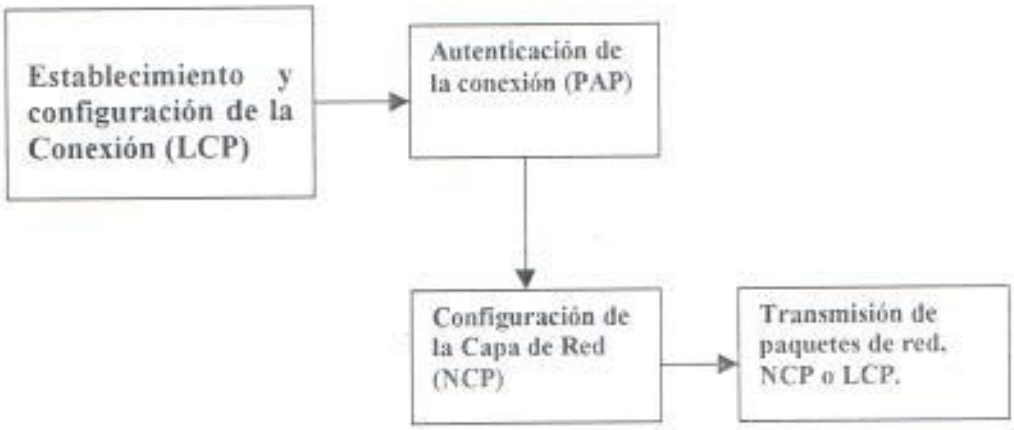


Figura 20: Establecimiento del enlace a través de PPP

2.4.4. PROTOCOLO DE CONTROL DE ENLACE

- Negocia el establecimiento, configuración, mantenimiento y cierre de la conexión.

- Negocia parámetros como la autenticación, el tamaño máximo de los frames, etc.

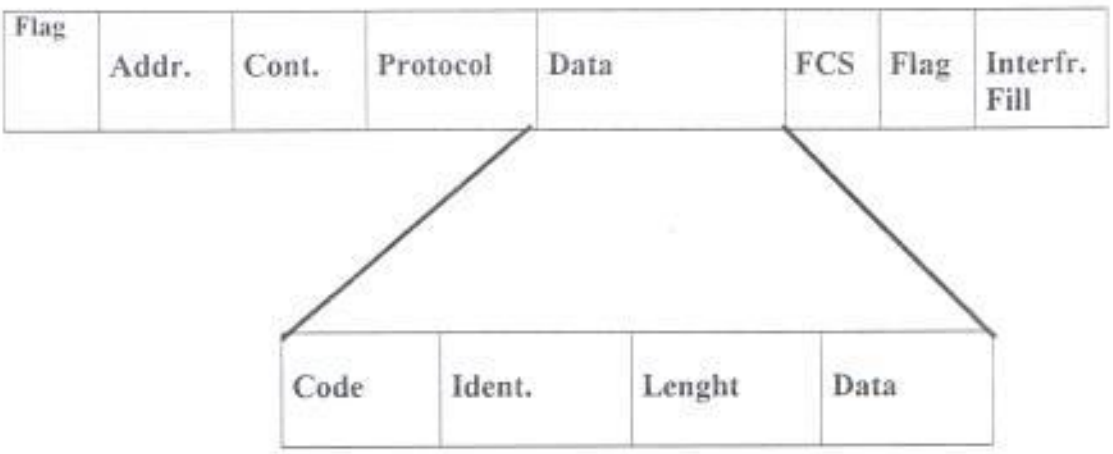


Figura 21: Frame de Control de Enlace

- Utilizados para autenticar la conexión mediante un identificador y un password.
- Estos protocolos esta principalmente orientados a conexiones dial-up.

2.4.5. PROTOCOLOS DE CONTROL DE RED

- Es una familia de protocolos: uno para cada tipo diferente de protocolo de red al que PPP dará servicio.
- Negocia parámetros para la capa de red. En TCP/IP el protocolo se llama IPCP.
- IPCP permite negociar dos cosas:
    - La dirección IP de uno o ambos puntos del enlace.
    - La utilización de compresión para los paquetes IP.

Ventajas:

- Servicio multiprotocolo.
- Detección y corrección de errores.
- Configuración del enlace y de la capa de red.
- Estándar reconocido.

Desventajas:

- Pequeño overhead en procesamiento y tamaño del paquete.
- Más difícil de implementar.

Protocolos utilizados en la capa de transporte

2.4.6. PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)

UDP se usa para aplicaciones que no requieren mucha confiabilidad en el medio de transmisión, y poder beneficiarse de un menor "overhead" que TCP permite. Las aplicaciones que usan UDP para el transporte incluyen NFS, DNS, y otros.

- UDP provee el mecanismo para una aplicación de enviar y recibir datagramas
- Está provisto para múltiples programas de aplicación concurrentes sobre una máquina única. Lo hace mediante el uso de puertos protocolares.

Con UDP, cada operación de salida de datos en un proceso produce exactamente un datagrama UDP, que ocasiona exactamente un datagrama IP para ser enviado.

UDP incluye dos importantes adiciones al servicio proveído por IP:

- El primero, UDP agrega un suma de verificación que permite al destino comparar los datos que se recibió con los que se transmitió, para averiguar su exactitud. La *suma de verificación* del IP sólo se encuentra en la cabecera; no se encuentra en el área de datos del datagrama IP.
- Si se ha estropeado el datagrama al ser recibido, la aplicación puede pedir la misma información nuevamente.
- El segundo, UDP introduce puertos protocolares.

Los puertos protocolares son un sistema abstracto que usan UDP y TCP. la transmisión de datos multiplexados. Los protocolos de la capa de transporte necesitan ser capaces de distinguir entre muchas aplicaciones diferentes para trasmitir datos. El puerto protocolar es diseñado para determinar que aplicación debe procesar los datos entrantes.

2.4.6.1. PUERTOS PROTOCOLARES PARA UDP

- La necesidad de contactar el terminal destino no basado en la funcionalidad del nombre del programa.
- El puerto protocolar, identificado por un número positivo, es el destino abstracto
- El sistema operativo controla el acceso de las aplicaciones a los puertos.
- El remitente necesita conocer la dirección IP y el número del puerto protocolar del destino de la máquina

Los servidores esperan mensajes que llegarán a puertos que se dedican a una aplicación particular. Por ejemplo, el puerto 161 UDP es " el puerto muy conocido" de SNMP.
UDP envía datos como una unidad simple:

- Cuando una aplicación envía datos usando salidas UDP, llegará al terminal remoto como un bloque único.
- UDP nunca destruirá un mensaje o unirá dos.

2.4.6.2. CABECERAS DE UDP

- *Puertos Fuente/Destino de UDP* - contiene el número de puertos protocolares de 16 bits usados para demultiplexar datagramas entre los procesos que los esperan recibir. El puerto fuente es optativo.
- *Longitud* - Conteo de los octetos en el datagrama UDP incluye la cabecera y datos del usuario.

Suma de verificación UDP - es un campo optativo (0 dice que es inutilizado), no requerido para el uso de LANs altamente confiables - reduce "overhead"

Puerto Fuente UDP	Puerto Destino UDP

Longitud de Mensaje UDP	Suma de Verificación

Figura 22: Frame de la Cabecera de UDP

2.4.6.3. ENCAPSULAMIENTO DE UDP

El datagrama se encapsula en una trama cada vez que viaja a través de una red. La Fragmentación IP en una transferencia UDP es: 1500 bytes (DIX) – 20 bytes (IP Hdr) – 8 bytes (UDP Hdr) = 1472 bytes por Datagrama IP de longitud.

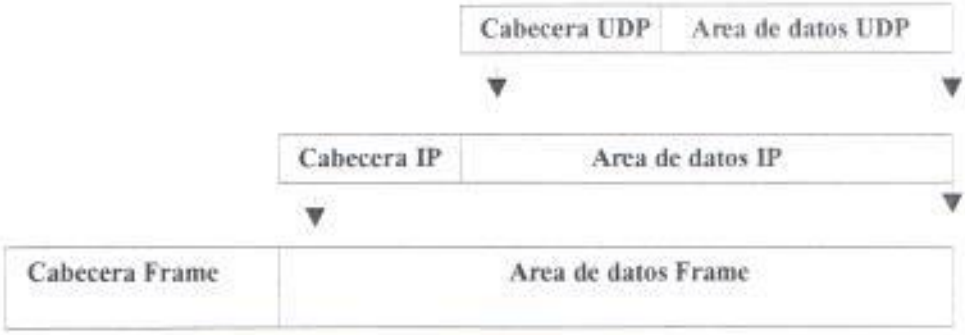


Figura 23: Ilustración del Datagrama UDP encapsulado en un datagrama IP para su transmisión a través de una red.

- **DIX (DIGITAL INTEL XEROX)**

Es una Arquitectura Ethernet, es la más antigua y tiene la base instalada más grande

PREAMBLE	Dest Addr	Src Addr	Ethertype	Data Padding	CRC
7	2/6	2/6	2	46 – 1500	4

Figura 24: Frame DIX

- **PREAMBLE.-** 56 bits de alternativamente 0s y 1s usados para sincronización.
- **DEST ADDR (DIRECCIÓN DE DESTINO).-** La dirección física de la máquina destino (NIC).
- **SRC ADDR (DIRECCIÓN ORIGEN).-** La dirección física de la máquina origen (NIC)
- **ETHERTYPE.-** Usado para identificar la próxima capa del protocolo más alta para la cual este frame de datos es destinado.
- **DATA.-** El frame de datos desde las capas más altas; si está debajo del mínimo (46 bytes) el relleno es añadido.

IP Hdr	UDP Hdr	Datos UDP – 1473 bytes

Datagrama IP

IP Hdr bytes	UDP Hdr	Datos – 1472	IP Hdr	Datos – 1 byte

← Paquete → | ← Paquete →

Figura 25: Frame de la fragmentación IP

La fragmentación requiere que la porción de datos de los fragmentos generados, debe ser un múltiple de 8 bytes para todos los fragmentos pero al final queda uno.

El máximo tamaño del datagrama IP es de 65.535 bytes, (20 bytes para la cabecera IP, 8 octetos para la cabecera UDP) y el remanente para 65.507 bytes se dejan para la porción de datos.

2.4.6.4. DEMULTIPLEXACIÓN DE DATAGRAMAS UDP

UDP se responsabiliza por separar los datos y pasar a la aplicación destino apropiada.

Figura 26: Ilustración de la demultiplexación de los datagramas UDP

2.4.7. PROTOCOLO DE CONTROL DE TRANSMISION (TCP)

- TCP es el protocolo mayormente usado en el Internet; las aplicaciones importantes como Telnet y el Protocolo de Transferencia de Archivos (FTP) usan como el mecanismo de transporte.
- Provee para el traslado confiable de flujo.
- Envía un flujo de bytes, sin marcadores de registro, al destino; llamado un servicio de flujo de datos.
- No es afectado con el tipo de datos transmitidos.
- Los datos pueden ser binarios, ASCII o EBCDIC - TCP no es afectado con el tipo de datos, esto es hasta que la aplicación receptora descifre los datos.
- Provee operación full duplex.
- Los datos pueden enviarse desde el transmisor al receptor así como del receptor al transmisor, simultáneamente.
- Sobre ambos terminales mantiene los números de secuencia para los datos que fluyen en ambas direcciones.

Nota: El número Ack se refiere a los datos recibidos.

- Si la aplicación remitente envía 1 – 1024 bytes, el número ACk reflejará 1025 si el dato es sucesivamente recibido.
- La semejanza con UDP, es que TCP hace uso de puertos protocolares.
- Estos permiten al protocolo clasificar la entrada de datagramas y conducirlos a lo largo de la aplicación apropiada.

- El número de puerto singularmente identifica a la aplicación, la dirección IP singularmente identifica al host.
- A continuación la dirección IP y el número de puerto son definidos por el conector del terminal.
- Cuando una conexión TCP se abre, el cliente y el servidor establecen un "circuito virtual".
- Este proceso se refiere a tan la ligadura dinámica.
- Este circuito virtual es una manera muy especifica de iniciar y concluir una transmisión de datos.
- La semejanza con UDP, es que TCP también usa IP para los datagramas de transmisión

2.4.7.1. REDES EN TCP/IP

TCP/IP es un protocolo independiente que puede implementarse sobre una variedad de sistemas operativos. Es capaz de usar diversos medios de transmisión y técnicas de transmisión (MAC). Los servicios TCP/IP marchan bien dentro de la estructura OSI.

Los aspectos principales de TCP/IP son:

- TCP/IP es una norma (estándar) independiente, de naturaleza no propietaria, significa que diferentes vendedores pueden incluir el departamento protocolar en su software de sistemas operativo para proveer funcionalidad de la red.
- Permite computadoras de fabricantes diferentes, correr diversos sistemas operativos para comunicarse.
- Es un sistema abierto, como es la meta del modelo OSI, desde el departamento protocolar y muchas de sus implementaciones son disponibles al público a un mínimo o ninguno costo.
- Forma la base del Internet a través del mundo Puede usar los diversos medios de transmisión disponible en el mercado. Puede usar las diversas técnicas de transmisión, más comúnmente en uso.

2.4.7.2. PUERTOS PROTOCOLARES PARA TCP

- Son objetos lógicos que identifican el destino definitivo dentro de la máquina.
- Cada aplicación está asignada a un número de puerto para ser identificado.
  - Permite aplicaciones múltiples sobre una máquina única.
- El número del puerto destino es incluido en la cabecera TCP, así como también la dirección IP.
  - Se debe saber los puertos asignados.
  - Ligados dinámicamente.

Los Puertos Protocolares se refieren a los objetos lógicos que identifican el destino definitivo dentro de la máquina.

- Usando la aplicación Telnet como un ejemplo.
  - Al servidor Telnet normalmente se asignará al bien conocido puerto 23.
  - El cliente normalmente se asignará un puerto transitorio; esta es una asignación aleatoria hecha por el cliente TCP.
- Múltiples clientes pueden usar el mismo servidor Telnet, simultáneamente.
  - El número de puerto y la dirección IP de cada cliente Telnet singularmente los identifica al servidor.

Los números de puerto, (fuente y destino) son los campos de la cabecera del TCP.

Entre las características principales se tiene:

- Permite al emisor generar un flujo de bytes
- Divide el flujo en pequeños segmentos para la transmisión
- Envía cada segmento en datagramas IP
- El receptor TCP, devuelve el reconocimiento acerca del recibo exitoso de datos
- El emisor comienza a contar el tiempo después de que el segmento ha sido enviado y retransmite a menos que un reconocimiento positivo llegue.

A diferencia de UDP, donde la aplicación genera una parte de los datos que es encapsulada en un datagrama UDP, TCP no retendrá necesariamente los mismos destinos arbitrarios entre "escritura" durante una transferencia.

Por ejemplo mientras una aplicación podría transmitir datos bajo TCP en cinco "escrituras" separadas al puerto TCP, el TCP en el destino puede realizar hasta 10 "lecturas" para conseguir todos los datos, o podría realizar sólo una "lectura".

TCP enviará los paquetes de datos a transmitir de acuerdo a sus prioridades - generalmente de acuerdo a la eficiencia de transmisión. Permite el traslado confiable de datos para permitir que el destino reconozca la recepción de datos de paquetes individuales. Si el programa fuente no recibe un reconocimiento para los paquetes enviados, este lo envía nuevamente. Mientras este sistema de reconocimiento es necesario para una transmisión confiable, entonces aumenta considerablemente el "overhead" asociado con la transmisión de datos

Cuando es llamado para transmitir datos:

- TCP "divide" los datos en partes menores, (determina los mejores tamaños), llamados **segmentos** para enviar al otro terminal de la conexión TCP.
  - UDP genera un datagrama IP para el tamaño total de la escritura hecha por la aplicación
- Entonces "espera" para un ACK desde el otro terminal

  - Si ACK no es recibido, TCP reenvia el segmento de datos, suponiendo que el otro lado ha perdido los datos
  - Los datos y ACKS se transfieren en ambas direcciones
- Provee un *suma de verificación* en la cabecera y en la porción de datos de la transmisión TCP.
- Puede reordenar los datagramas IP antes de pasar los datos de la pila a la aplicación
- Puede determinar también los paquetes duplicados y desechar la transmisión original que fue enviada.
- Provee para el control del flujo de datos sobre la conexión
- Sólo permitirá al otro terminal enviar los datos si tiene un adecuado espacio en los bancos de memoria. Ambos terminales de la conexión mantienen sus bancos de memoria para recibir los datos en el enlace full-duplex.
- El mecanismo se llama *MSS* (o el *Tamaño Máximo de Segmento*) que especifica el segmento máximo que se desea recibir.

2.4.7.3. FORMAS DE INICIAR UNA COMUNICACIÓN EN TCP

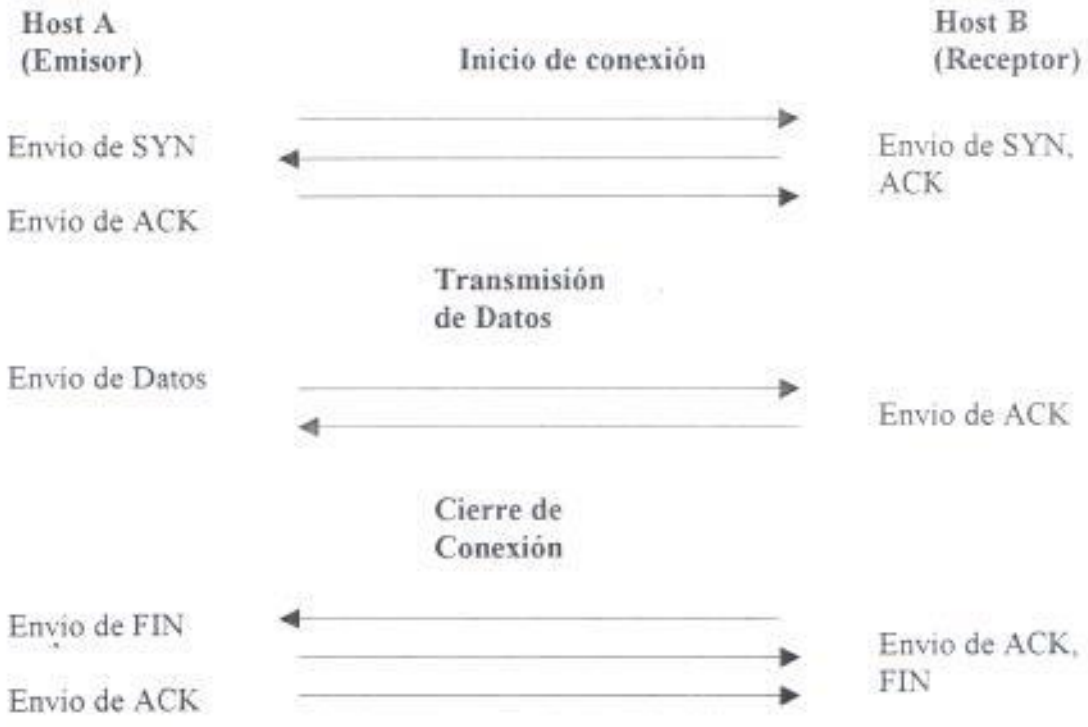


Figura 27: Formas de comunicación en TCP

Estas 3 maneras son usadas por TCP para iniciar un circuito virtual.
El establecimiento de este circuito virtual sirve para dos funciones importantes.

- El primero, garantiza que ambos lados están listos para comenzar la transmisión de datos.
- Adicionalmente, permite que ambos los terminales fuente y destino sincronicen una sucesión de números.
- Esta sucesión de números se usa para reensamblar los datos adecuadamente. Una vez que la conexión se establece adecuadamente, los datos pueden transferirse.
- Cuando se completa la transmisión de los datos, la conexión sigue un procedimiento definido para concluir una "normal transmisión", como muestra el gráfico arriba.

2.4.7.4. LA MEDIDA DEL MÁXIMO SEGMENTO (MMS)

El MSS, especifica el segmento máximo que el emisor puede recibir, se especifica una vez, por cada fin de la conexión, en el primer segmento intercambiado.

- Este es el segmento que contiene el SYN.
- MSS entonces llega a ser el más grande "paquete" de datos que TCP enviará al otro lado.

2.4.7.5. VENTANA DESLIZANTE DEL TCP

La figura 28 muestra una ventana deslizable transfiriendo 6 paquetes

- Las ventanas se desliza hacia el paquete 7 y puede ser enviado cuando un ACK se ha recibido por el paquete 1.
-

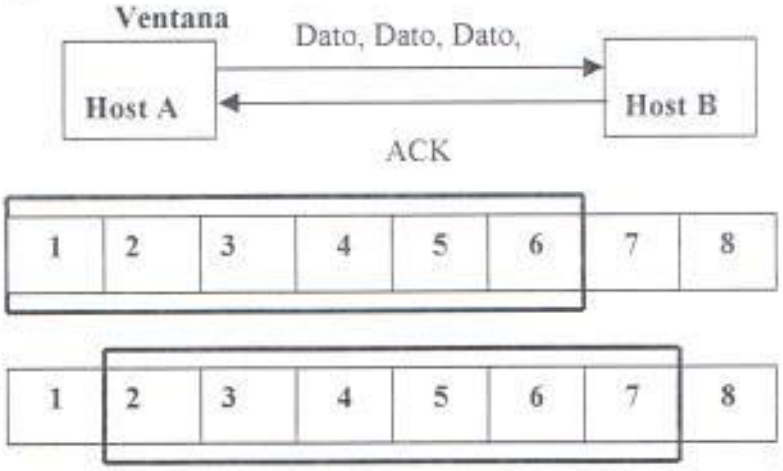


Figura 28: Funcionamiento de la ventana deslizante de TCP

En la figura 29 se muestran ejemplos de la ventana deslizante.

- Los paquetes pueden contener segmentos de datos: 1 - 1024, 1025 - 2048, 2049 - 3072, 3073 - 4096, etc.

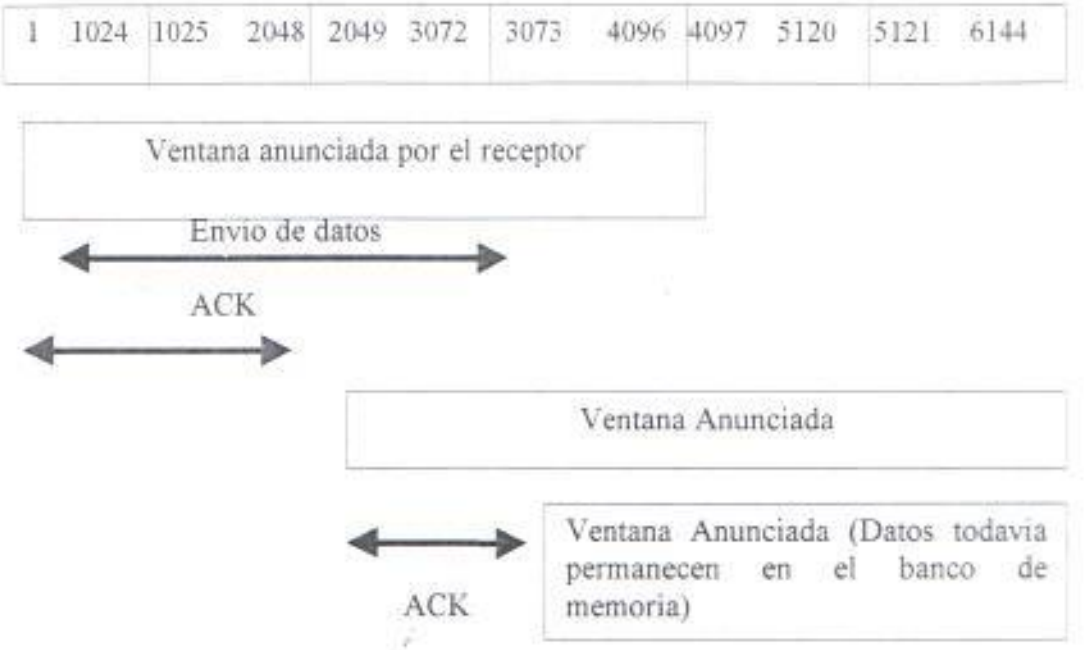


Figura 29: Uso de la ventana deslizante de TCP

Las reglas para la ventana deslizante son:

- El remitente no tiene que transmitir un relleno en la ventana de datos
- Una vez que el emisor recibe un segmento ACK, las Ventanas desliza a la derecha
- El tamaño de la Ventana puede disminuir pero el borde derecho no puede moverse a la izquierda.

2.4.7.6. FORMATO DE CABECERA DE TCP

- **Puerto Fuente** = número usado para identificar la aplicación remitente

- **Puerto Destino** = número usado para identificar la aplicación receptora

NOTA: es el puerto fuente y dirección IP fuente y el puerto destino y la dirección IP destino pares que singularmente identifican una conexión TCP; la combinación del puerto y la dirección IP se refieren frecuentemente como un enchufe.

- **Sucesión Numérica** = identifica el byte en el campo de datos desde el origen al destino TCP que el PRIMER byte en este segmento representa.

- **El Número de Reconocimiento** = contiene la PROXIMA secuencia numérica que el remitente del reconocimiento espera para recibir (esta es la sucesión numérica adicional del anterior byte de datos recibidos) el campo sólo es válido si la bandera ACK está ACTIVO.

- **La Longitud de la Cabecera** - la longitud de la cabecera es de 32 – bits o palabras

- **El bit de Bandera** - uno o más de los 6 bits pueden encenderse en el mismo tiempo.
  - **URG**= el indicador "urgente" está encendido - el remitente usa esto para indicar que los "datos urgentes" de alguna manera se han puesto en el flujo de datos - es hasta la otra aplicación decide qué hacer.
  - **ACK**= el número de Reconocimiento es válido
  - **PSH**= el receptor debería pasar estos datos a la aplicación lo antes posible
    RST= la conexión es reiniciada.
  - **SYN**= la sucesión numérica es sincronizada para iniciar la conexión
  - **FIN** = remitente indica que se termina los datos remitentes
- **El Tamaño de Ventana** = es el número de bytes, comenzando con el uno identificado por el campo numérico ACK, indica que el receptor es dispuesto a aceptarlo - (16 bits limitan el tamaño de la ventana a 65.535 bytes)

- **El Indicador Urgente** = cuando se activa el bit URG, el indicador urgente especifica la posición dentro del segmento en la que terminan los datos urgentes.

- **Opciones** = el software TCP utiliza el campo opciones para negociar con el software TCP en el otro extremo de la conexión; una de las opciones permite que el software TCP especifique el tamaño máximo de segmento (MSS) que está dispuesto a recibir.
  En la figura 30 se muestra el formato de la cabecera TCP

<table>
<tr><td colspan="5">Puerto Fuente</td><td colspan="4">Puerto Destino</td></tr>
<tr><td colspan="9">Sucesión Numérica</td></tr>
<tr><td colspan="9">Número de Reconocimiento</td></tr>
<tr><td>Hdr Lngth(4)</td><td>Reservado (6)</td><td>urg</td><td>ack</td><td>psh</td><td>rst</td><td>syn</td><td>fin</td><td>Ventana</td></tr>
<tr><td colspan="7">Suma de Verificación</td><td colspan="2">Indicador Urgente</td></tr>
<tr><td colspan="9">Opciones (Variable)</td></tr>
<tr><td colspan="9">Datos (Variable)</td></tr>
</table>

Figura 30: Formato de la cabecera de TCP

En la figura 31 se muestra la forma como se realiza el encapsulamiento de TCP

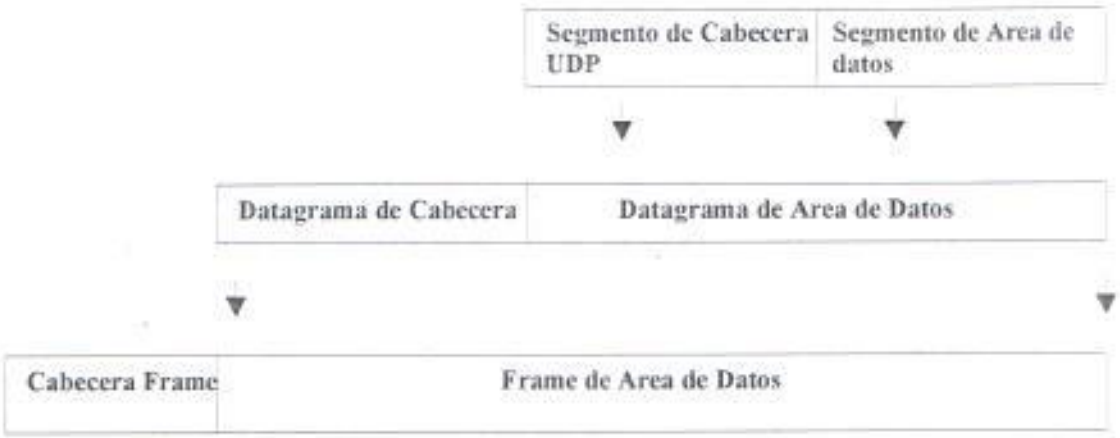


Figura 31: Encapsulamiento de TCP

Protocolos utilizados en la capa de aplicación

2.4.8. PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP)

Dado un protocolo de transporte confiable de extremo a extremo como el TCP, la transferencia de archivos podria parecer trivial. Además, el FTP ofrece muchas facilidades que van más allá de la función de transferencia misma.

- **Acceso Interactivo.-** aunque el FTP está diseñado para usarse mediante programas, la mayor parte de las implantaciones proporciona una interface interactiva que permite a las personas interactuar fácilmente con los servidores remotos. Por ejemplo, un usuario puede pedir una lista de todos los archivos de un directorio en una máquina remota.
- **Especificación de formato (Representación).-** El FTP permite el cliente especificar el tipo y formato de datos almacenados. Por ejemplo, el usuario puede especificar si un archivo contiene enteros de texto o binarios, asi como, si los archivos de texto utilizan los conjuntos de caracteres ASCII o EBCDIC.
- **Control de Autenticación.-** El FTP requiere que los clientes se autoricen asi mismos con el envio de un nombre de conexión y una clave de acceso al servidor antes de pedir la transferencia de archivos. El servidor rechaza el acceso a clientes que no puedan abastecer una conexión o clave de acceso válido.

Como en otros servidores, la mayor parte de las implantaciones FTP de servidores permiten el acceso concurrente de varios clientes. Los clientes se valen del TCP para conectarse a un servidor.

Por lo general, el cliente y el servidor crean un proceso separado para manejar la transferencia de datos. Si bien los detalles precisos acerca de la arquitectura de procesos dependen de los sistemas operativos utilizados.

Como se muestra en la figura 32, el proceso de control de clientes se conecta al proceso de control de servidor mediante una conexión TCP, mientras que los procesos de transferencia de datos asociados utilizan su propia conexión TCP. En general, los procesos de conexión y la conexión de control permanecen activos mientras el usuario continua en la sección FTP. Sin embargo, el FTP establece una nueva conexión de transferencia de datos para cada transferencia de archivos. De hecho, muchas de las aplicaciones crean un nuevo par de procesos de transferencia de datos, asi como también una nueva conexión TCP desde donde quiera que el servidor necesite enviar información al cliente.

Las conexiones de transferencia de datos y los procesos de transferencia de datos que los emplean pueden crearse de manera dinámica cuando se necesitan, pero la conexión de control continúa a través de una sesión. Una vez que la conexión de control desaparece, la sesión se termina y el software en ambos extremos termina todos los procesos de transferencia de datos. Además de enviar comandos del usuario al servidor, el FTP utiliza la conexión de control para permitir los procesos de control cliente y servidor, y asi, coordinar el uso de los puertos de protocolo de TCP asignados dinámicamente y la creación de procesos de transferencia de datos que utilicen tales puertos.

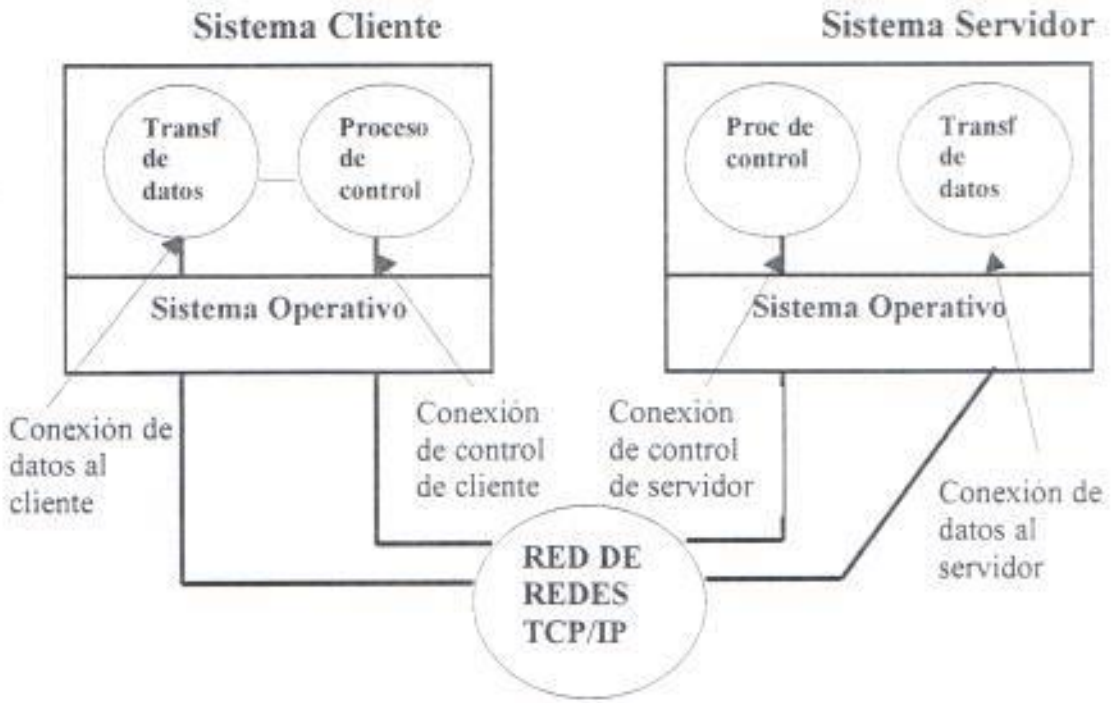


Figura 32: Diagrama del Proceso FTP

2.4.9. SISTEMAS DE ARCHIVOS DE RED (NFS)

Muchas de las localidades TCP/IP utilizan el NFS para interconectar los archivos de sus computadoras. Desde la perspectiva del usuario, el NFS es casi invisible. Un usuario puede ejecutar un programa de aplicación arbitrario y valerse de archivos arbitrarios de entrada y salida.

En la figura 33 se ilustra cómo es que el NFS está inmerso en un sistema operativo. Cuando se ejecuta un programa de aplicación, se llama al sistema operativo para que abra un archivo o para que almacene y recupere datos en archivo.

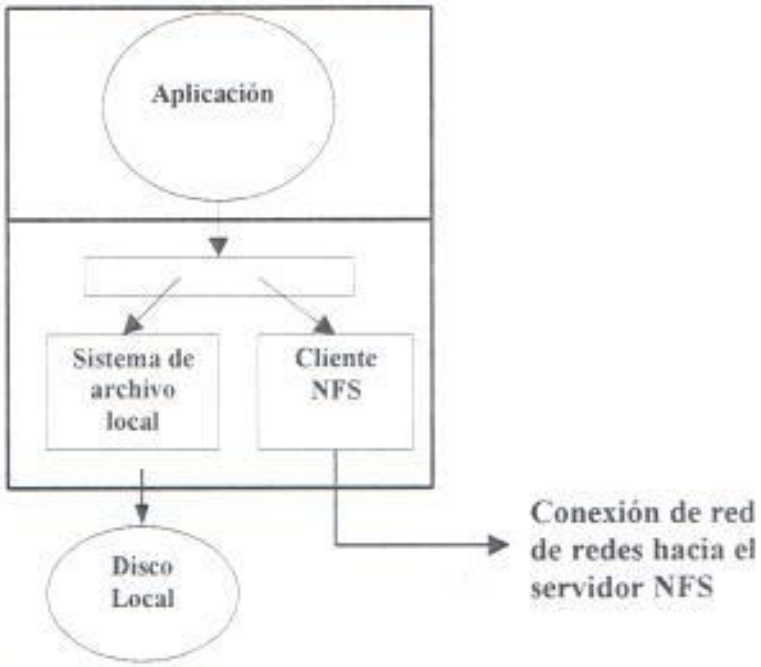


Figura 33: Utilidad del NFS dentro del sistema operativo

El mecanismo de acceso de archivos acepta la petición y la transmite de manera automática al software de sistema de archivo local o al cliente NFS, dependiendo de si el archivo está en el disco local o en una máquina remota. Cuando recibe una petición, el software de cliente utiliza el protocolo NFS para ponerse en contacto con el servidor apropiado en una máquina remota y ejecutar la operación requerida.

2.4.10. SESIÓN DE TELNET SOBRE ETHERNET

El programa *Telnet* (Red de Telecomunicaciones) pretende proporcionar conexión remota o capacidad de terminal virtual a través de una red. En otras palabras, un usuario de la máquina A debería ser capaz de registrarse en la máquina B desde cualquier parte de la red, y por lo que respecta al usuario, aparecer como si estuviera

sentado frente a la máquina B. El servicio Telnet se proporciona a través del puerto N° 23 de TCP.

Cuando dos máquinas se comunican mediante Telnet, durante la fase de conexión Telnet mismo determina y establece los parámetros de comunicación y de terminal para la sesión, e incluye capacidad de no aceptar un servicio que uno de los extremos de la conexión no pueda administrar. Cuando se establece una conexión mediante Telnet, ambos extremos acuerdan un método para el intercambio de información entre las 2 máquinas, descargando la CPU del servidor de un porcentaje considerable de este trabajo.

El protocolo Telnet trata ambos extremos de la conexión como si fueran terminales virtuales de la red. Los dos programas en cada extremo administran la conversión de la terminal virtual a los dispositivos físicos reales. El concepto de terminales virtuales permite a Telnet interconectarse con cualquier tipo de dispositivo, siempre y cuando haya mapeo disponible de los códigos virtuales al dispositivo físico. Una ventaja de este enfoque es que algunos dispositivos físicos no pueden aceptar todas las operaciones, por lo que el terminal virtual no tendrá dichos códigos.

El gráfico muestra el sistema de TCP/IP presente en ambos: en el cliente y en los sistemas de servidores. Cada uno debe tener una tarjeta NIC y el software apropiado también.

El *Cliente/servidor* un sistema en que el procesamiento puede distribuirse entre computadoras personales (clientes) sobre la red que piden servicios desde uno o más sistemas de servidores que radican sobre la red. Los servidores pueden proveer servicios tales como: impresión, manejo de archivos, etc. Seguro las intensas tareas (como E-mail), puede radicar también sobre un servidor que puede ser accesado por las diversas computadoras personales (clientes) sobre la red.

En el diagrama de arriba, cada capa tiene uno o más protocolos en la misma capa los cuales se usan para comunicarse con las mismas capas en otro sistema.

La implemetación de este protocolo provee a la aplicación siguiente la capacidad de conectarse como un terminal de la máquina donde corre el servidor. Telnet define un estándar de terminal virtual (NVT) y la capacidad de negociar opciones o usar datos estándares. Para poder ser utilizado, la máquina donde corre el servidor debe tener la capacidad de definir pseudoterminales. Puede utilizarse para probar otras aplicaciones servidoras que provea una interface tipo texo.

Tiene igual propósito de POP3

- Puede manejar el Mail offline y online.
- En modo Online permite manipular remotamente el mailbox del servidor:
  - Mensajes se recuperan de manera selectiva.

- Evita la innecesaria eliminación de mensajes en el servidor
- También permite la sincronización bidireccional de los mensajes bajados con los del servidor.
- Puede manejar múltiples servidores y Mailboxes en una sola computadora.
- Se puede hacer uploads de los folders al servidor

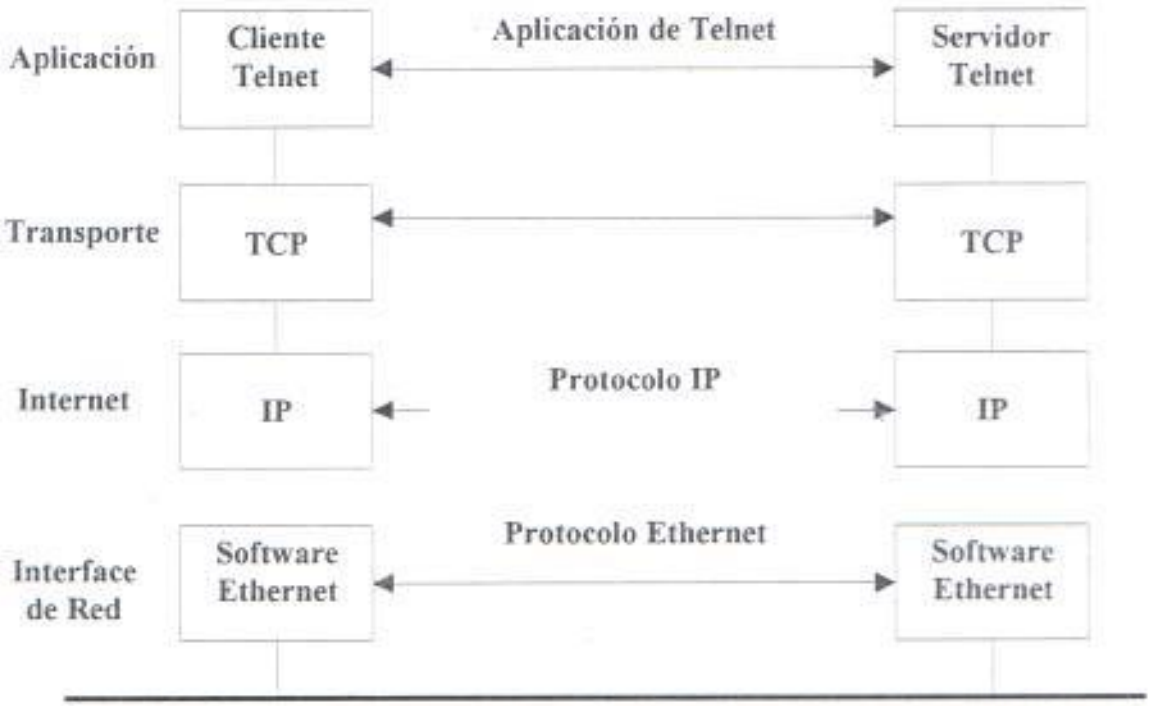


Figura 34: TCP/IP en cliente y servidor

2.4.11. PROTOCOLO DE INTERNET IP

- IP provee un servicio de entrega de datagramas no confiable.
- No garantiza que los datos lleguen a su destino final.
- Además no mantiene ninguna información acerca de la conexión.
- IP fue diseñado para el enrutamiento de datos entre diferentes redes.
- El datagrama es la unidad básica de transmisión. Consiste de una cabecera y una porción de datos.

Con IP no existe la garantía de que los datos lleguen a su destino. Los protocolos orientados a conexión proveen este servicio, IP confía en la aplicación para que provea este servicio. IP no mantiene ninguna información sobre el estado sucesivo de los datagramas, la transferencia de datos puede requerir mas de un datagrama para completarse, por ejemplo en el transporte de un archivo largo.
Cada datagrama se maneja independientemente.

Ninguna conexión se establece entre el remitente y el receptor en la capa Internet antes de que los datos se pongan sobre el cable de red.

Donde Ethernet y Token Ring definieron formatos para el traslado de datos sobre una red única, IP define un mecanismo para el traslado de datos a través de redes
En los datagramas IP, la área de datos y cabecera, puede ser 65,535 bytes de longitud. Esta es una restricción impuesta por los 16 bits destinados al campo de "longitud" en la cabecera del datagrama.

IP formula datagramas desde datos desde la capa lógica de enlace, y los pasa a la capa de transporte.

Paquete es el término usado para el traslado de datos entre IP y la Tarjeta de Interface de Red.
Ethernet / Token Ring - define diferentes formatos de frame para la transmisión de datos en la red. Los datos pueden enviarse sobre la red en un frame (Ethernet, Token Ring).

2.4.11.1. DIRECCIONES INTERNET

Cada host en una red TCP/IP tiene asignada una dirección de número entero de 32 bits que se utiliza en todas las comunicaciones con dicho host. Cada dirección es un par (netid, hostid), en donde "netid" identifica una red y "hostid" a un host dentro de la red.
Una dirección IP puede tener una de las siguientes formas:

Figura 35: Formas de una dirección IP

Se puede determinar el tipo de dirección IP de acuerdo a los tres primeros bits:

Tipo	Bits de identificación	Bits campo de red	Bits campo host
A	0	7	24
B	1 0	14	16
C	1 1 0	21	8

Tabla 6: Tipos de dirección IP

Cuando computadores convencionales tienen dos o más conexiones físicas se los llaman host Multi-homed. Los host multi-homed y los ruteadores requieren de muchas direcciones IP. Cada dirección corresponde a una de las conexiones de red de la máquina.

Debido a que las direcciones IP codifican tanto una red y un host en dicha red, no identifican una computadora individual, sino una conexión a la red.

2.4.11.2 NOTACIÓN DECIMAL DE UNA DIRECCIÓN IP

La mayor parte del software TCP/IP que muestra una dirección IP o que requiere que una persona lo introduzca, utiliza notación decimal. Las direcciones IP se escriben con cuatro enteros decimales separados por puntos, en donde cada entero proporciona el valor de un byte de la dirección IP. Ejemplo:

10000000 00001010 00000010 00011110

se escribe

128.10.2.30

A continuación se muestra un ejemplo de direccionamiento Internet

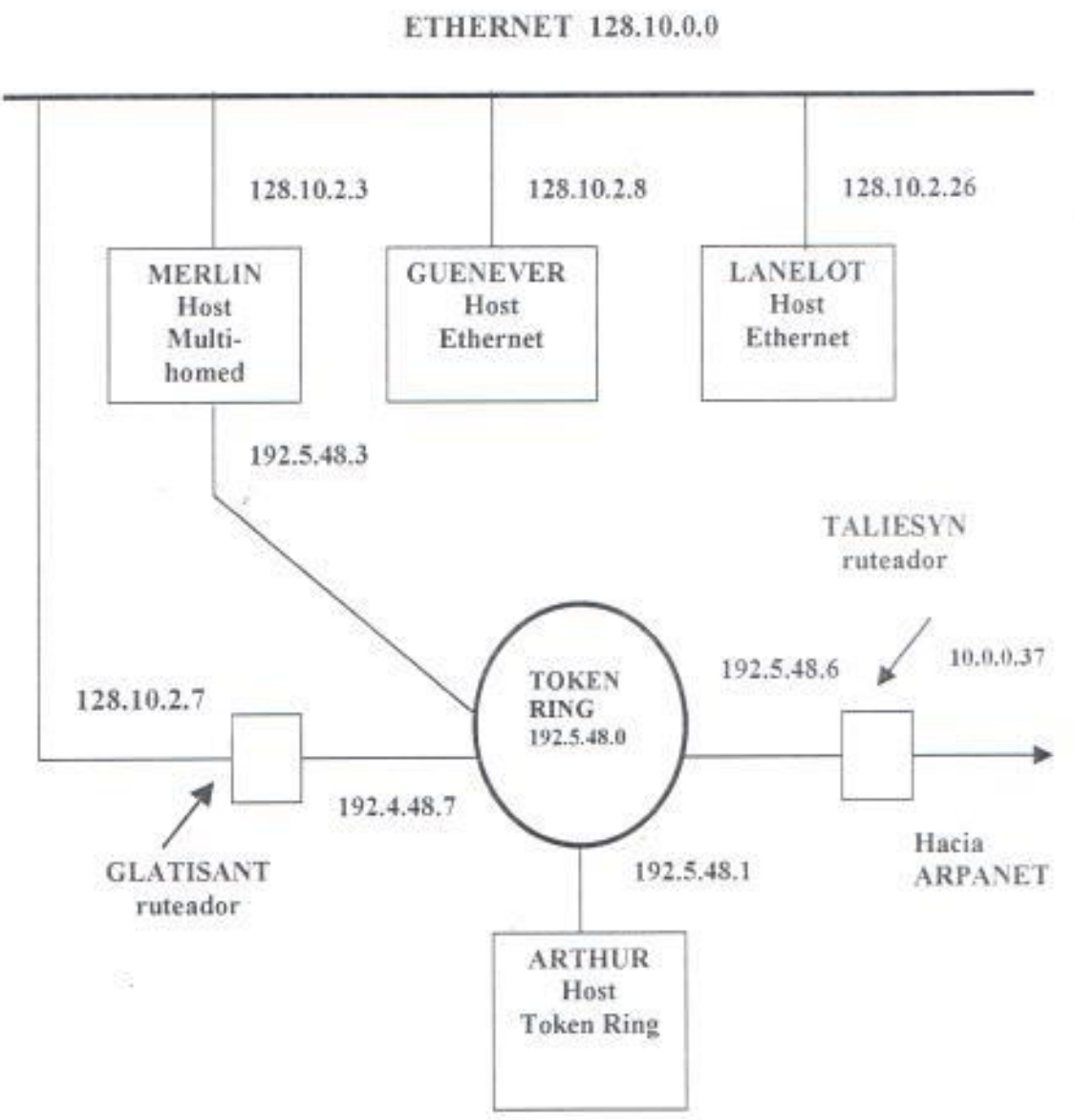


Figura 36: Direccionamiento Internet

La figura muestra tres redes con hosts conectados y direcciones de Internet asignadas a cada conexión de red, además de ruteadores que conectan las diversas redes.

2.4.11.3 AUTORIDAD DE DIRECCIONAMIENTO INTERNET.

Existe una autoridad para asignar las direcciones de Internet a fin de garantizar que esta sea única. La Autoridad Internet de Números asignados (IANA) establece los procedimientos y tiene el control sobre los números asignados. Sin embargo, cuando una organización se une a Internet, puede obtener direcciones de red desde el centro de Información de la Red Internet (INTERNIC).
La autoridad Internet asigna el campo de red de una dirección; una vez que una organización obtiene su prefijo de red, puede asignar un sufijo único a cada host de su red sin tener que contactar a la autoridad.
Una organización individual puede asignar direcciones únicas dentro de su red TCP/IP siempre que su red no se conecte con el mundo exterior. Sin embargo, si una red privada utiliza las mismas direcciones que la red global Internet, tendrá problemas de interoperabilidad cuando trate de intercambiar software con otras redes.

2.4.11.4 DEBILIDADES DEL DIRECCIONAMIENTO INTERNET.

La codificación de información de red en una dirección IP tiene algunas desventajas:

- Las direcciones se refieren a la conexión de red, no al host. Si un host se mueve de una red a otra, su dirección IP debe cambiar.
- Las computadoras personales no pueden tener asignada una dirección IP permanente ya que esta identifica la red a la que esta conectada la computadora.
- Otra debilidad del esquema de direccionamiento de una red TCP/IP es que cuando una red de tipo C crece hasta tener más de 255 host, tiene que cambiar su dirección a una de tipo B. Esto obliga a cambiar las direcciones de todas las máquinas y reiniciar la comunicación utilizando la nueva dirección de red.
- Como el ruteo utiliza la parte de red de la dirección IP, el camino tomado por los paquetes que viajan hacia un anfitrión con muchas direcciones IP depende de la dirección utilizada. Por lo tanto no es suficiente conocer una dirección IP para el destino; puede ser imposible llegar utilizando esa dirección.

2.4.11.5 DIRECCIONES DE SUBRED.

Una de las técnicas que permite que una sola dirección de red abarque muchas redes físicas se conoce como direccionamiento de subred, ruteo de subred o utilización de subredes.

El direccionamiento de subred divide la dirección en una porción de red y una porción local, en donde la porción de red identifica una localidad, posiblemente con muchas redes físicas, y la porción local identifica una red física y un host en dicha localidad.

En la gráfica se muestra primero una interpretación conceptual de una dirección IP de 32 bits siguiendo el esquema original, luego una interpretación conceptual de direcciones que utiliza el esquema de subred.

Figura 37: Esquema de la dirección IP y de la subred

El resultado es una forma de direccionamiento jerárquico, que lleva al correspondiente ruteo jerárquico. El nivel superior utiliza los primeros dos octetos cuando rutea y el siguiente nivel utiliza un octeto adicional. Finalmente, el nivel más bajo utiliza toda la dirección.

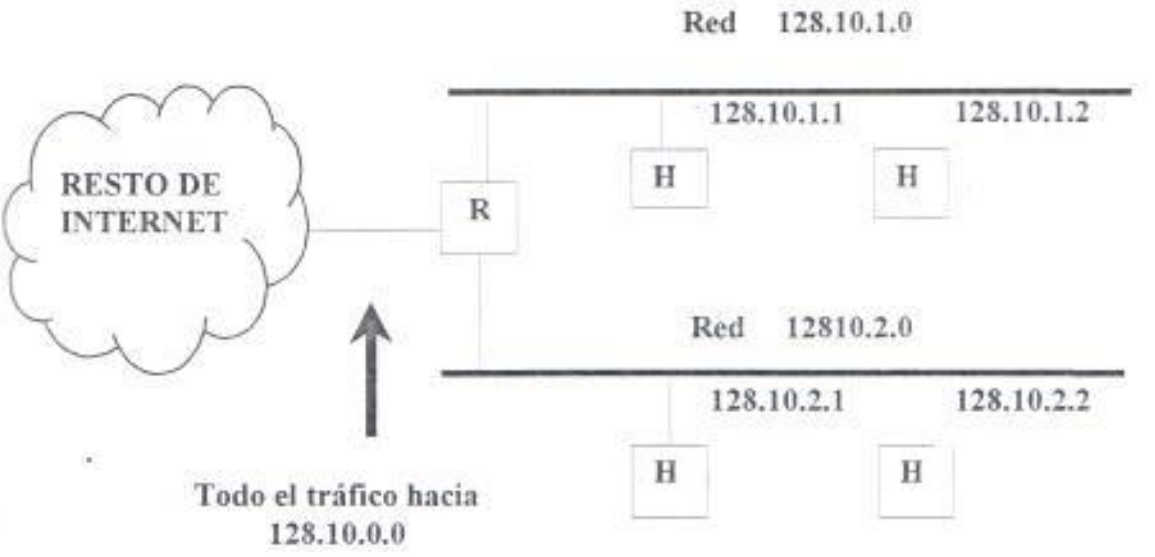


Figura 38: Conexión a través de las direcciones IP y de subred

Localidad con dos redes físicas que utilizan el direccionamiento de subred para etiquetarlas como una sola dirección de red tipo B. El ruteador R acepta todo el tráfico para la red 128.10.0.0 y elige una red física, basándose en el tercer octeto de la dirección.

La ventaja de utilizar el direccionamiento jerárquico es que puede incorporar un gran crecimiento, ya que significa que una ruta no necesita saber muchos detalles sobre destinos distantes, ni destinos locales. Una desventaja es la dificultad de cambiar una estructura jerárquica ya establecida.

2.4.11.6 ENTREGA DE DATAGRAMAS

La transmisión de un datagrama IP puede efectuarse de dos manera: entrega directa y entrega indirecta. La entrega directa, es la transmisión de un datagrama IP entre dos máquinas dentro de una sola red física lo cual no involucra ruteadores. El transmisor encapsula el datagrama dentro de una trama física, transforma la dirección IP de destino en una dirección física de hardware y envía la trama resultante directamente a su destino.

La entrega indirecta es más compleja. Cuando un host quiere enviar un datagrama a otro, lo encapsula y lo envía al ruteador más cercano. Una vez que la trama llega al ruteador, el software extrae el datagrama encapsulado, y el software IP selecciona el siguiente ruteador a lo largo del camino hacia el destino. De nuevo, se coloca el datagrama en una trama y se envía a través de la siguiente red física hacia el segundo ruteador, y así sucesivamente, hasta que se pueda entregar en forma directa.

2.4.11.7 RUTEO IP CONTROLADO POR TABLA

El algoritmo usual de ruteo IP emplea una tabla de ruteo Internet en cada máquina que almacena información sobre posibles destinos y sobre cómo alcanzarlos. Debido a que tanto los ruteadores como los hosts rutean datagramas, ambos tienen tablas de ruteo IP. Siempre que el software de ruteo IP en un host necesita transmitir un datagrama, consulta la tabla de ruteo para decidir a donde enviarlo.

Una tabla de ruteo contiene pares (N, R), donde N es la dirección IP de una red de destino y R la dirección IP del siguiente ruteador en el camino hacia la red N.

Para ocultar información, mantener reducidas las tablas de ruteo y tomar las decisiones de ruteo, de manera eficiente, el software de ruteo IP solo puede guardar información sobre las direcciones de las redes de destino, no sobre las direcciones de hosts individuales.

En la figura, se muestra una red de redes formada por 4 redes interconectadas por tres ruteadores.

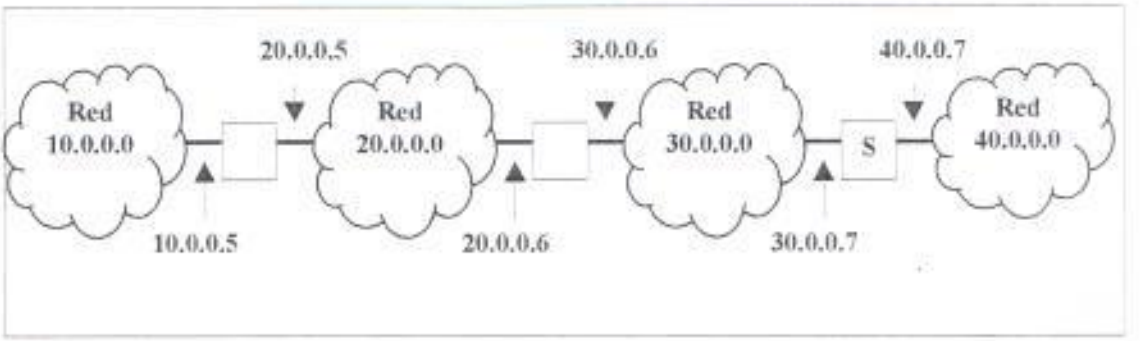


Figura 39: 4 redes y 3 ruteadores

PARA ALCANZAR LOS HOST EN LA RED	RUTEAR A ESTA DIRECCION
20.0.0.0	Entregar directamente
30.0.0.0	entregar directamente
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Tabla 7: Tabla de ruteo

2.4.11.8 DNS (EL SERVIDOR DE NOMBRE DE DOMINIO)

El servidor de nombre de dominio de la red habilita un dispositivo con un nombre común para que sea convertido a una dirección especial de la red. Por ejemplo, no se puede tener acceso a un sistema llamado joes workstation desde una red del otro lado del país, a menos que esté disponible algún método de verificación de los nombres de las máquinas locales. DNS proporciona la conversión del nombre común local a la dirección física única de la conexión de red del dispositivo.

- La necesidad de combinar nombres fáciles para uso del usuario.
- Los sistemas pequeños pueden usar un archivo "host".
- El Servidor de Nombre de Dominio es una base de datos distribuida que transforma nombres a direcciones.
- Los nombres toman la forma: vex.ftp.com

La estructura del nombre del dominio es una estructura jerárquica donde la autoridad para el plan de nombramiento se delegan y particionan.

- En Internet TCP/IP, los nombres jerárquicos de máquina se asignan según la estructura de organizaciones que obtienen la autoridad para partes de los espacios de los nombres, no necesariamente según la estructura de las interconexiones físicas de red.

En vista de la dificultad que representa recordar direcciones IP, se creó un protocolo que permita el manejo de nombres asociados a ellas. Es así como por ejemplo en Internet (la red TCP7IP mas grande), la dirección 192.188.59.2 equivale al nombre ESPOL.edu.ec. Los nombres como el mencionado anteriormente se hallan organizados bajo dominios de manera jerárquica.

En el nombre Espol.edu.ec cada una de las partes separadas por puntos representa una cosa.

Ec: Representa el dominio principal (Ecuador)
Edu. Indica el subdominio (Educación Superior)
Espol Identifica a la institución, en este caso el host.

El nombramiento de las participaciones toma la forma de: local.grupo.lugar como en vex.ftp.com
Donde, vex, ftp, y com son etiquetas.
Y, vex.ftp.com, ftp.com y com son todas los dominios

EL NOMBRE DE DOMINIO	SIGNIFICADO
COM	**Organizaciones comerciales**
EDU	**Instituciones educativas**
GOV	**Instituciones gubernamentales**
MIL	**Grupos militares**
NET	**Centros mayores de soporte de red**
ORG	**Organizaciones diferentes a las anteriores**
ARPA	**Dominio temporal de ARPANET (obsoleto)**
INT	**Organizaciones Internacionales**

Tabla 8: Nombre del dominio y significado

Dominios Geográficos	Paises
Uk	United Kingdom
Au	Australia
Co	Colombia
Ec	Ecuador

Tabla 9: Código de País y País en particular (según esquema geográfico)

En Intenet existe una organización encargada de administrar y distribuir la autoridad de los dominios a otras instituciones: la NIC. En el Ecuador el dominio ec es administrado por Ecuanet.

Si no se quiere acceso a Internet, se tiene completo control para definir y utilizar nombres y dominios. Si el control se desea acceso a Internet, se debe solicitar a la institución a cargo del dominio apropiado:

- El control de su subdominio
- la inclusión de los nombres de sus host en la base de datos del dominio.
- Un dominio no está limitado a una red IP de hecho un dominio abarca varias redes de diferentes clases

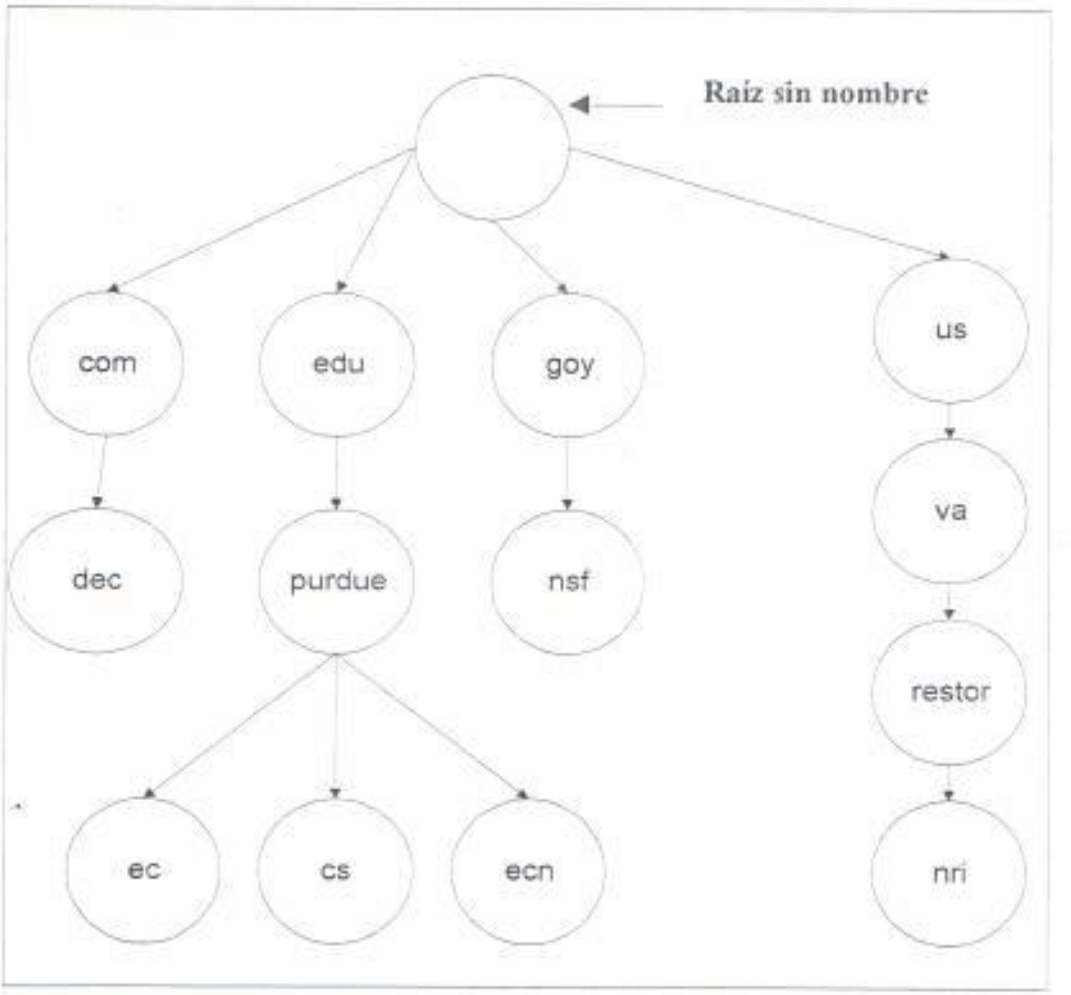


Figura 40: Jerarquía de dominios en Internet

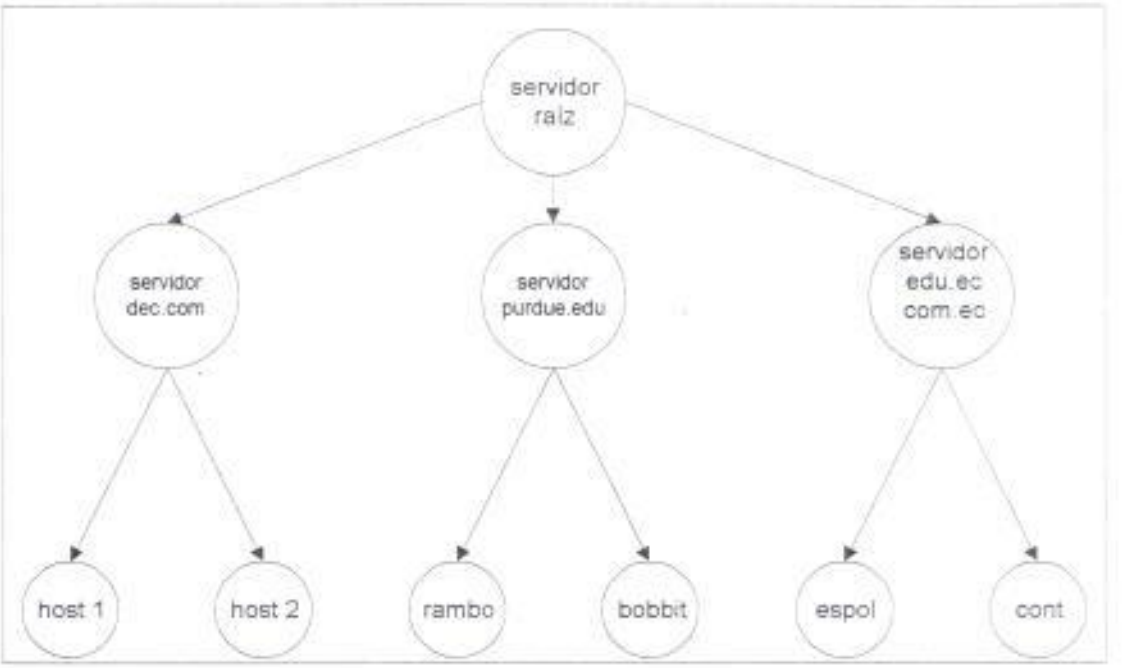


Figura 41: La base de datos más distribuida del mundo

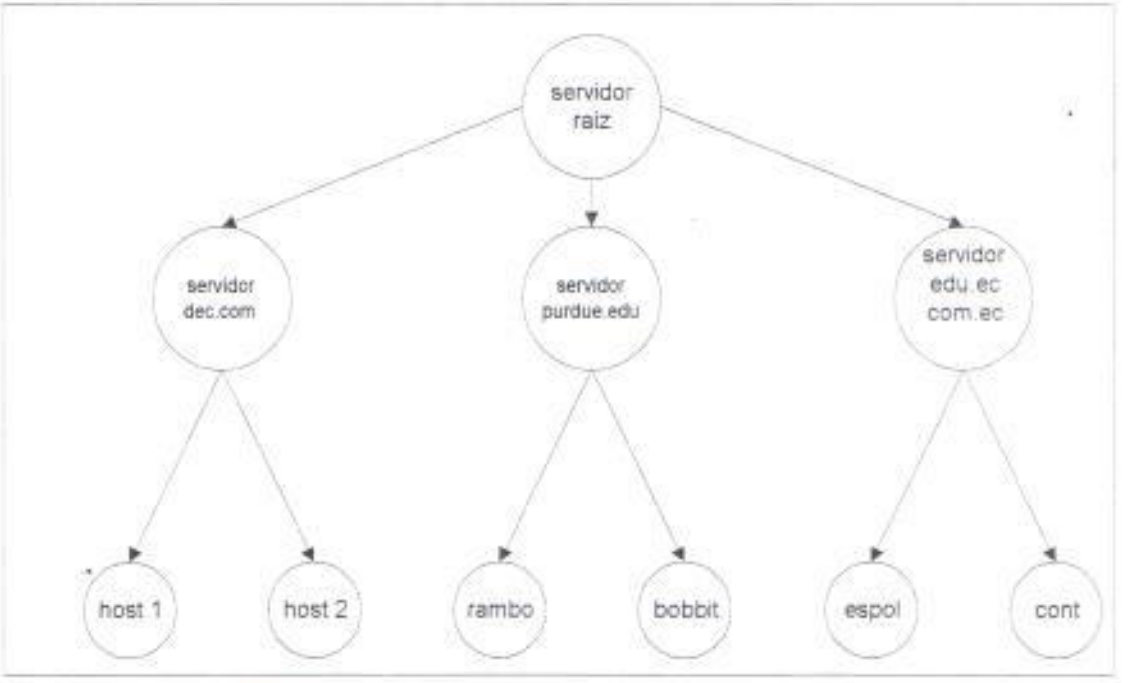


Figura 42: DNS como un Requerimiento Local

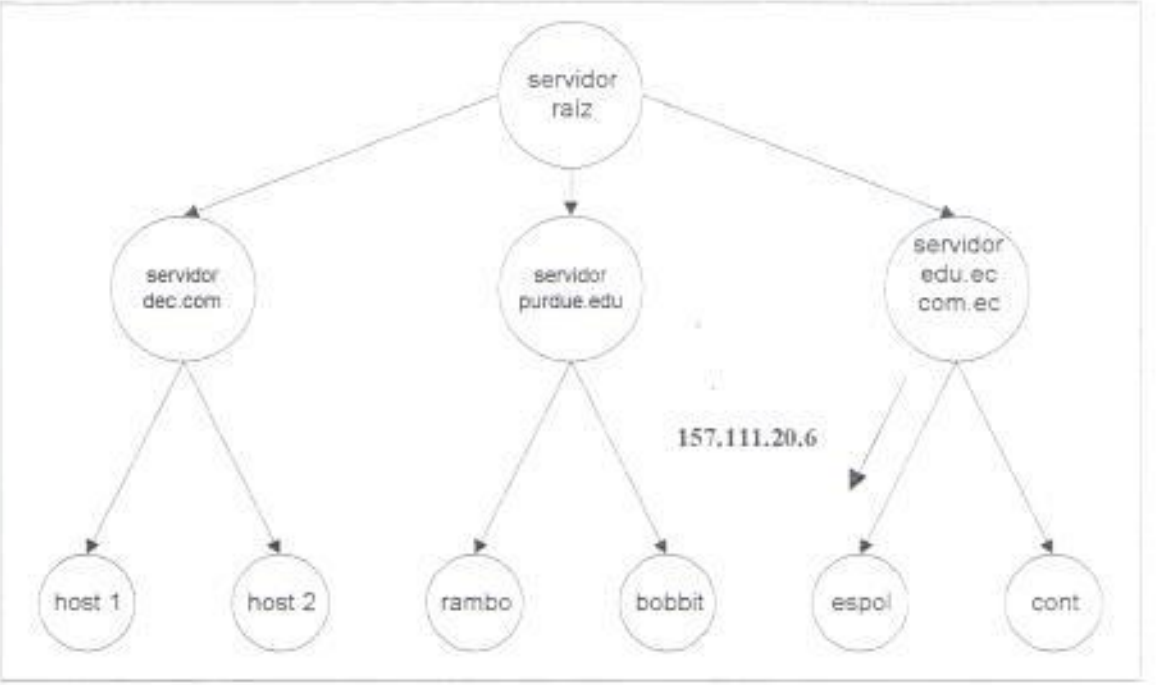


Figura 43: DNS como respuesta Local

2.4.11.8.1 SERVIDORES Y CLIENTES

Cada dominio o subdominio debe tener un servidor primario y otro secundario en redes fisicamente separadas. Los serviodres mantienen información sobre el host en su dominio y sobre servidores de subdominios bajo su control. Todos los servidores mantienen punteros a los servidores raiz. Los clientes mantienen punteros al servidor de su sominio.

Todas las aplicaciónes que realizan una conexión con otra máquina especificando el nombre. Servidores y clientes mantienen una tabla en memoria caché que contienen los resultados de requerimientos recientes. Los servidores también manejan requeriminetos de nombres en base de direcciones.

Un Servidor de Sistema de Nombre de Dominio (DNS) puede combinar también direcciones IP de los hostnames. El DNS frecuentemente distribuye información a los Host a través de aplicaciones de red, como programas de correo electrónico o programas FTP, sobre Host remotos. Los servidores de nombre de dominio guardan la información de sus dominios en el host y comparte con otros servidores de nombre de dominio sobre una red o sobre otras redes. El DNS frecuentemente hace la tarea de distribución de información sobre una red más rápida y más fácil, pero el trabajo de administrar un servidor de DNS es más complejo que mantener una tabla de archivos.

Si se solicita al Centro de Información de Red de Internet (InterNIC) por un número de red, se deberia obtener también una forma de aplicación de nombre de dominio desde el InterNIC, y volver a la forma completa del InterNIC para su aprobación. Un " nombre de dominio" es un nombre único de red que se asocia con ésta. (Por ejemplo, Software de FTP, el nombre de dominio es ftp.com.) Si el InterNIC aprueba su aplicación de nombre de dominio, el InterNIC asigna a su red un dominio único que se asocia con su número de red, y que ninguna otra red puede usar.

Una vez que se obtiene un número de red y un nombre de dominio, puede asignar direcciones IP dentro de la gama de números asignados a la red y nombres de subdominios que se necesite para esta red.

2.4.11.8.2 CORREO ELECTRÓNICO

Existen varios protocolos relacionados con correo electrónico en TCP/IP: 822,SMTP, Popmail,IMAP4,. El correo electrónico ha sido por muchos años la aplicación más utilizada en Internet, al contrario de otras aplicaciones TCP/IP, no es necesario que un mensaje sea enviado a través de una conexión interactiva ni instantáneamente. Las aplicaciones de correo proveen un mecanismo para enviar información de manera eficiente y rápida pero "no en linea"

	teléfono	E-mail	Correo
Sincronizado	si	No	No
Procesable	no	si	Poco
Precisión	verbal	escrita	Escrita
Constancia	baja	media	Alta
Velocidad	alta	media	Baja
Conferencia	pocos	Uno a muchos	Uno a uno
Intrusivo	si	no	no

Tabla 10: Comparación de servicios

- **E-mail – Caracterización funcional**
  - Mensajeria interpersonal
  - No necesita ser interactivo
  - Conexión extremo a extremo o via nodos intermedios
  - Usa protocolo SMTP.
  - Servicio normalizado en el puerto 25

Para manejar la entrega postergada de mensajes, los sistemas de Mail usan una técnica llamada Spooling. Cuando un MTA recibe un mensaje, este pasa a un Spoolde salida para que un proceso cliente se encargue de la conexión y el envio al siguiente MTA.

Cuando el usuario recibe algún mensaje a través de un UA, este es depositado en un spool de entrada. Se utiliza una aplicación "cartero" para chequear los mensajes pendientes.

- **DEL MTU AL UA**

Dos procesos de la misma máquina
Ejemplo: Al recibir un mensaje un usuario del UNIX

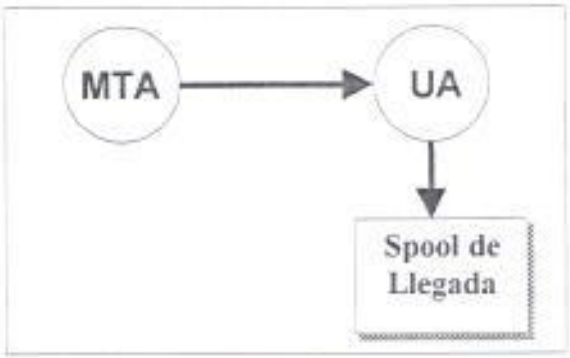


Figura 44: Usuario de Unix recibiendo un mensaje

- **LEYENDO EL E-MAIL**

Ejemplo: al revisar los mensajes usando el programa Mail en un servidor Unix

Figura 45: Usuario revisando los mensajes usando el programa Mail en un servidor Unix

- **RFC 822**

Especifica el formato de los mensajes de Mail.
Especifica el formato de las direcciones de correo electrónico.

- **POPMAIL**

  - Versión Actual: POP3
  - Diseñado para permitir recuperar, leer mensajes alojados en un servidor multiusuario desde un PC.
  - Orientado a streams (opera en el puerto TCP 110).
  - Utiliza autenticación para user y password.
  - Recupera todos los mensajes del Spool en una sola transacción y no se puede recuperar mensajes selectivamente.

- **IMAP-4**

Puede utilizar opciones de búsqueda sin necesidad de bajar los mensajes.

2.4.11.8.3 ARQUITECTURA DEL ENVÍO DE MENSAJES

SMTA es el protocolo utilizado para la transmisión de mensajes entre MTAs y de UAs a MTAs. El UA que envía actúa como cliente, los MTAs actúan como clientes y como servidores.

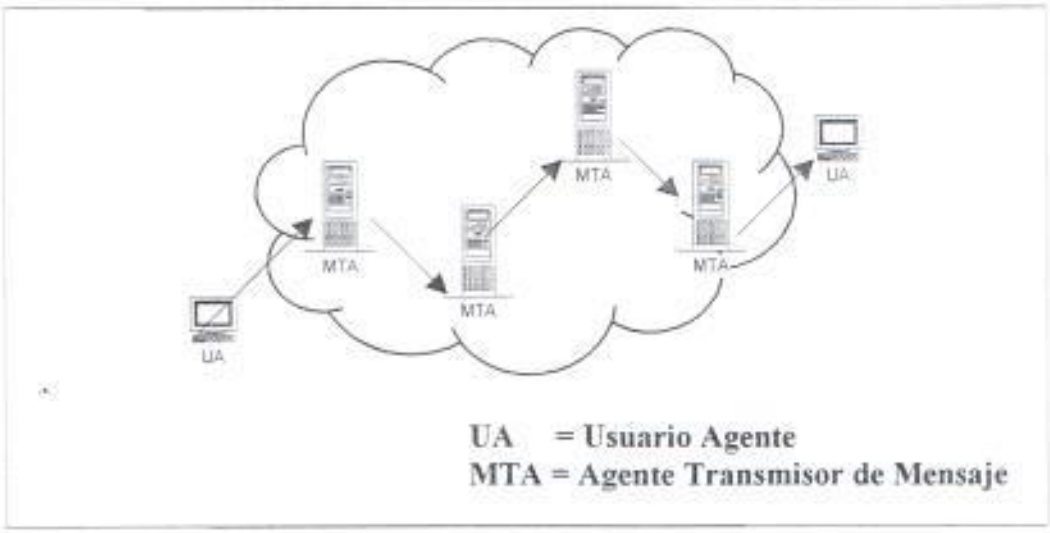


Figura 46: Arquitectura del envío de mensajes

Se realizan sesiones TCP independientes entre cada trama de la conexiónn, si falla luego de algunos intentos, el MTA correspondiente envia un mensaje de error de regreso.

En el gráfico se muestra UA hacia MTA a través de la red, desde una PC hasta un servidor Mail Unix.

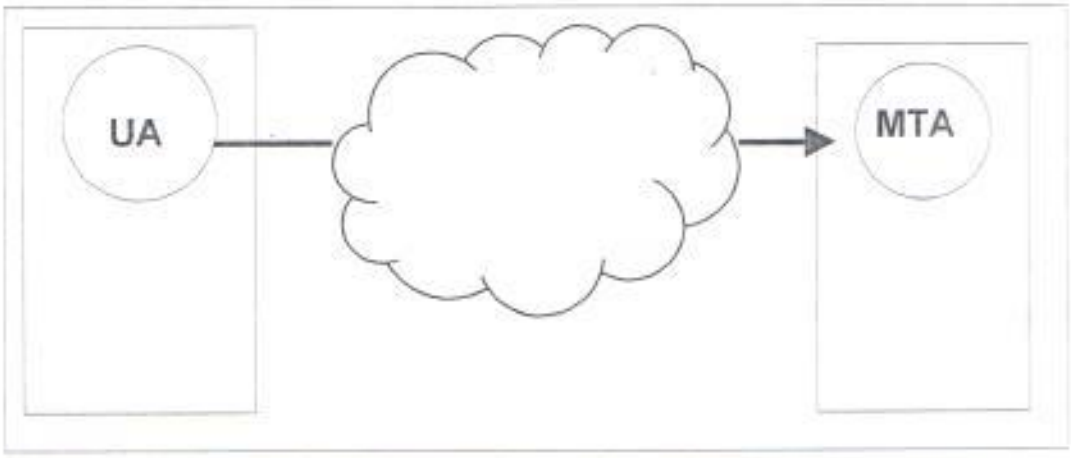


Figura 47: Conexión desde una PC hasta un servidor Mail Unix

2.4.11.9 DATAGRAMA IP

- Es la unidad básica de transferencia para el Internet.
- Parecido al paquete de la red fisica
- Se constituye de dos partes:
  - Datagrama de cabecera
  - Los Datos

El datagrama IP es la unidad básica de transferencia para el Internet. Los datagramas IP se componen de dos partes; una cabecera y una porción de los datos.

- El datagrama IP está parecido al paquete de red, el cual se compone de unos números de campos individuales los cuales representan las diversas acciones o importantes valores para las funciones de IP.

Así como con los paquetes en hardware, un punto emisor y un punto de destino deben identificarse; con IP, existen las direcciones IP del emisor y la dirección IP del destino.

- La analogía de correo permanece intacta; en vez de direcciones físicas a la "carta", las direcciones IP estarian presentes.
- Los datos están contenidos también dentro de la envoltura la cual es la estructura del datagrama IP de la cabecera y la porción de datos.

2.4.11.10 LA FORMA GENERAL DE UN DATAGRAMA IP

Cuando IP contiene datos para enviarlos desde un nivel de protocolo más alto, un datagrama IP se crea. IP determina en qué interfase local el datagrama IP va a ser enviado, (ruteando) e indagando el interface para determinar su MTU.

Cabecera del Datagrama	Area de Datos del Datagrama

Figura 48: Forma del frame de un datagrama IP

- IP compara el MTU (del interface) con el tamaño del datagrama para determinar si la fragmentación es necesaria.
- La fragmentación es el proceso de dividir el datagrama IP en múltiples datagramas si el MTU es menor que el tamaño del datagrama original.
    - La fragmentación puede tomar lugar en el host de origen o ruteador intermedio.
- Cuando un datagrama IP se fragmenta, no es reensamblado hasta que alcance su destino final.
    - La capa de IP en el destino maneja el proceso de reensamblaje.
    - La idea está en hacer esta fragmentación invisible a los protocolos de las capas superiores.
- Si un datagrama IP es fragmentado por el host de origen, el fragmento puede ser posteriormente fragmentado por un ruteador intermedio si la comunicación del router es menor que el fragmento original del host de origen.

Cuando un datagrama IP se fragmenta, cada fragmento llega a ser un paquete propio, (con una cabecera y la porción de datos), y se encamina independientemente de otros paquetes desde el mismo, mensaje original.

2.4.11.11 FORMATO DE LA CABECERA DEL DATAGRAMA IP

Versión	Longitud Hdr	Tipo de Srvc	Longitud Total	
Identificación			Banderas 3)	Compensación de Fragmento (13)
Tiempo de vida		Protocolo	Cabecera de Suma de Verificación	
Dirección de la Fuente				
Dirección del Destino				
Opciones IP (+ relleno)				
Datos (Longitud Variable)				

Figura 49: Formato de la cabecera del datagrama IP

Los campos importantes en el datagrama IP incluyen:

- **El Tipo de Servicio** = El protocolo de la capa superior decide cómo el Protocolo de Internet maneje este datagrama. El campo del bit 8 la separa en 3 subzonas:
  - Bit 0-2 = Precedencia - formalmente usado para indicar la importancia de este diagrama - no usado para ninguno otro.
  - Bit 3-6 = especifica el tipo de transporte que el datagrama requiere
    - Bit 3 – bit D – requiere bajo retardo. Solicita procesamiento con retardos cortos.
    - Bit 4 – bit T - Solicita alto rendimiento.
    - Bit 5 – bit R - Solicita alta confiabilidad
    - Bit 6 = bit C - requiere minimizar costo monetario
      NOTA: este son mutuamente privativos - es decir uno únicos sobre a la vez - todo 0 dice servicio normal
  - Bit 7 = Inutilizado
- **Longitud Total** = Longitud total del datagrama IP.

- **Identificación** = únicamente identifica cada datagrama - el número se copia en cada fragmento

- **Banderas** = Usa dos bits de orden menor del campo de 3 bits *Bandera* que controlan la fragmentación. Por lo general, el software de aplicación que utiliza TCP/IP no se ocupa de la fragmentación debido a que tanto la fragmentación como el reensamblado son procedimientos automáticos que se dan a bajo nivel en el sistema operativo, invisible para el usuario final. Sin embargo, para probar el software de red de redes o depurar problemas operacionales, podría ser importante probar el tamaño de los datagramas en los que se presenta la fragmentación.

  - *Bit 1* - bit D – El primer bit de control ayuda en la prueba de fragmentación, especificando en qué momento se debe fragmentar un datagrama. Se le conoce como Bit de *no fragmentación* porque cuando está puesto a 1 especifica que el datagrama no debe fragmentarse. Una aplicación podría seleccionar no permitir la fragmentación cuando sólo el datagrama completo es útil. Por ejemplo, se considera la secuencia de iniciación de una computadora, en la que una máquina comienza a ejecutar un pequeño programa en ROM y utiliza la red de redes para solicitar una primera iniciación, y otra máquina envía de regreso una imagen de memoria. Si el software ha sido diseñado así, necesitará la imagen completa, pues de otra forma no le será útil; por ello, el datagrama debe tener activado el bit de *no fragmentación*. Cada vez que un ruteador necesita fragmentar un datagrama que tiene activado el bit de *no fragmentación*, el ruteador descartará el datagrama y devolverá un mensaje de error a la fuente.

  - *Bit 2* – bit M – El bit de orden inferio en el campo *Banderas* que especifica si el fragmento contiene datos intermedios del datagrama original o de la parte final. Este bit es conocido como *"más fragmentos"*. Para entender por qué este bit es necesario, se considera el software IP en el destino final cuando trata de reensamblar un datagrama. Este recibirá los fragmentos (es posible que en desorden) y necesitará saber cuándo ha recibido todos los fragmentos del datagrama. Cuando un fragmento llega, el campo *Longitud Total* en el encabezado consulta el tamaño del fragmento y no el tamaño del datagrama original; de esta manera el destino no puede utilizar el campo *Longitud Total* para determinar si ha reunido todos los fragmentos. De los campos *Compensación de fragmentos y Longitud Total* se puede calcular la longitud del datagrama original. Examinando *Compensación de fragmentos* y *Longitud Total* en el caso de todos los fragmentos entrantes, un receptor puede establecer en qué momento los fragmentos que ha reunido contienen toda la información necesaria para reensamblar el datagrama original completo.

- **Compensación del fragmento** = contiene la compensación de este fragmento desde el principio del datagrama.

- **Tiempo de Vida** = El campo *Tiempo de Vida* especifica la duración, en segundos, del tiempo que el datagrama tiene permitido permanecer en el sistema de red de redes. La idea es sencilla e importante: cada vez que una máquina introduce un datagrama dentro de la red de redes, se establece un tiempo máximo durante el cual el datagrama puede permanecer ahí. Los ruteadores y los anfitriones que procesan los datagramas deben decrementar el campo *Tiempo de Vida* cada vez que pasa un datagrama y eliminarlo de la red de redes cuando su tiempo ha concluido.

Una estimación exacta de este tiempo es difícil dado que los ruteadores por lo general no conocen el tiempo de tránsito por las redes físicas. Unas pocas reglas simplifican el procedimiento y hacen fácil el manejo de datagramas sin relojes sincronizados. En primer lugar, cada ruteador, a lo largo de un trayecto, desde una fuente hasta un destino, es configurado para decrementar por 1 el campo *Tiempo de Vida* cuando se procesa el encabezado del datagrama. Sin embargo, para manejar casos de ruteadores sobrecargados que introducen largos retardos, cada ruteador registra el tiempo local cuando llega un datagrama, y decrementa el *Tiempo de Vida* por el número de segundos que el datagrama permanece dentro del ruteador esperando que se le despache.

Cada vez que un campo *Tiempo de Vida* llega a cero, el ruteador descarta el datagrama y envía un mensaje de error a la fuente. La idea de establecer un temporizador para los datagramas es interesante ya que garantiza que los datagramas no viajarán a través de la red de redes indefinidamente, aún cuando si una tabla de ruteo se corrompa y los ruteadores direccionen datagramas en un ciclo.

- **Protocolo** = Es análogo al campo tipo en una trama de red. El valor en el campo *Protocolo* especifica qué protocolo de alto nivel se utilizó para crear el mensaje que se está transportando en el área de *Datos* de un datagrama. En esencia, el valor de *Protocolo* especifica el formato del área de Datos. La transformación entre un protocolo de alto nivel y el valor entero utilizado en el campo *Protocolo* debe administrarlo por una autoridad central para garantizar el acuerdo entre los enteros utilizados en Internet.

- **Direcciones Fuente y Destino IP** = Contienen direcciones IP de 32 bits de los datagramas del emisor y del receptor involucrado. Aún cuando los datagramas sean dirigidos a través de muchos ruteadores inmediatos, los campos de fuente y destino nunca cambian; éstos especifican la dirección IP de la fuente original y del destino final.
- **Opciones** = El campo *Opciones* del IP tiene una longitud variable. El campo señalado como *Relleno* depende de las opciones seleccionadas. Este representa un grupo de bits puestos en cero que podrían ser necesarios para asegurar que la

extensión del encabezado sea un múltiplo exacto de 32 bits (recordar que el campo de longitud del encabezado se especifica en unidades formadas por palabras de 32 bits).

El campo *Opciones* del IP aparece a continuación de la dirección de destino y no se requiere en todos los datagramas; las opciones se incluyen en principio para pruebas de red o depuración. Sin embargo, el procesamiento de las opciones es parte integral del protocolo IP, por lo tanto, todos los estándares de implementaciones se deben incluir.

La longitud del campo *Opciones* de IP varía dependiendo de qué opción sea seleccionada. Algunas opciones tienen una longitud de un octeto; éstas consisten en un solo octeto de *código de opción*. Otras tienen longitudes variables. Cuando las opciones están presentes en un datagrama, aparecen contiguas, sin separadores especiales entre ellas. Cada opción consiste en un solo octeto de código de opción que debe llevar a continuación un solo octeto y un conjunto de octetos de datos para cada opción. El octeto de código de opción se divide en tres campo que se muestran en el siguiente gráfico:

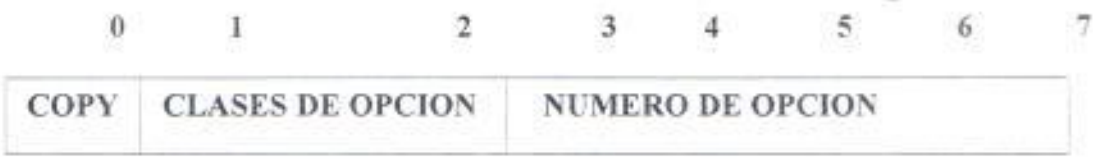


Figura 50: División del octeto de código de opción en tres campos de 1, 2 y 5 bits.

El campo consiste en una bandera de 1 bit, llamada *Copiar*, un segmento de 2 bits, *Clases de Opciones*, y un segmento de 5 bits, *Número de Opción*. La bandera *Copiar* controla la forma en que los ruteadores tratan las opciones durante la fragmentación. Cuando el bit *Copiar* está puesto a 1, especifica que la opción se debe copiar en todos los fragmentos. Cuando está puesto en cero el bit *Copiar* significa que la opción sólo se debe copiar dentro del primer fragmento y no en todos los fragmentos.

Los bits Clases de Opciones y Número de Opción especifican la clase general de opción y establecen una opción específica en esta clase. La tabla que a continuación se detalla la muestra de cómo se asignan las clases.

CLASES DE OPCIONES	SIGNIFICADO
0	Control de red o datagrama
1	Reservado para uso futuro
2	Depuración y medición
3	Reservado para uso futuro

Tabla 11: Bits de clases de opciones y su significado

Clases de opciones IP, como se codifican en los bits de Clases de Opciones en un octeto de código de opción

La siguiente tabla muestra la lista de las opciones posibles que pueden acompañar a un datagrama IP y muestra los valores para *Clases de Opción y Número de Opción*. Como se muestra en la lista, la mayor parte de las opciones se utilizan con propósito de control.

CLASES DE OPCIONES	NUMERO DE OPCIONES	LONGITUD	DESCRIPCION
0	0	-	Finalidad o fin de la lista de opciones. Se utiliza si las opciones no terminan al final del encabezado (ver también campo de relleno de encabezado).
0	1	-	No operación (se utiliza para alinear octetos en una lista de opciones)
0	2	11	Seguridad y restricciones de manejo (para aplicaciones militares).
0	3	Var	Ruteo no estricto de fuente. Se utiliza para registrar el trayecto de una ruta especifica.
0	7	Var	Registro de ruta. Se utiliza para registrar el trayecto de una ruta.
0	8	4	Identificador de flujo. Se utiliza para transportar un identificador de flujo SATNET (Obsoleto).
0	9	Var	Ruteo estricto de fuente. Se utiliza para establecer la ruta de un datagrama en un trayecto especifico.
2	4	Var	Sello de tiempo Internet. Se usa para registrar sellos de hora a lo largo de una ruta.

Tabla 12: Lista de las opciones posibles que pueden acompañar a un datagrama IP y valores para Clases de Opción y Número de Opción

2.4.11.12 ENCAPSULAMIENTO DEL DATAGRAMA IP

- El Datagrama debe ser transportado por la red física.
- El datagrama completo es el frame de datos
- El software de red realiza la encapsulación antes de que el datagrama se transmita.
- **Encapsulación**: El completo datagrama IP está incluido dentro del área de datos de un frame. Una cabecera de frame está adjunta a estos "datos", y esta cabecera provee la información necesaria para viajar a lo largo de diversas redes locales diferentes.

Este procedimiento de capas es el que hace a TCP/IP tan flexible.

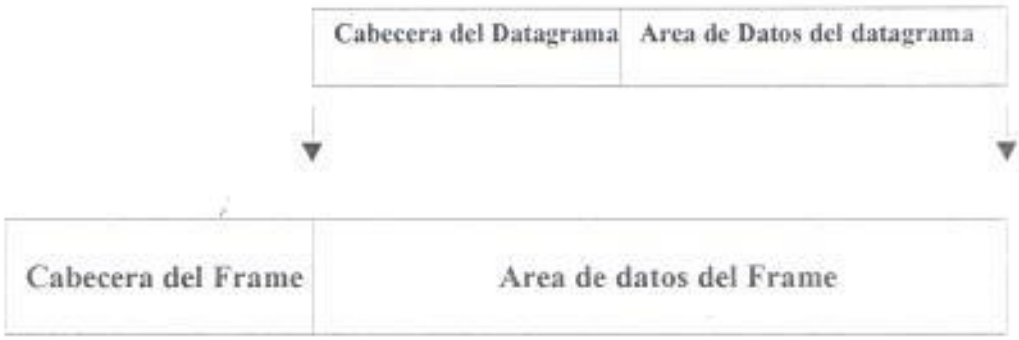


Figura 51: Encapsulamiento de un datagrama IP

2.4.11.13 INTERNET CONTROLA PROTOCOLO DE MENSAJE (ICMP)

ICMP es una parte integral del IP. Permite al gateway, tal como un router, enviar diversa información de control o de error al host de origen, o a otro gateway.

- ICMP provee comunicación entre el software de IP ejecutándose entre la máquina de la fuente y el destino.

Los mensajes ICMP viajan a través del Internet en la porción de datos del datagrama IP.

ICMP sólo reporta errores al origen que deben, a la vez, notificar la aplicación que va a tomar lugar para corregir el problema.

ICMP incluye formatos de mensajes que:

- Retrase la velocidad de transmisión.
- Pida un cambio al host en las tablas de ruteo.
- Permita a un host probar si un destino se puede contactar.

2.4.11.13.1 FUNCIONES DEL ICMP

Anteriormente se muestra como el Software del Protocolo Internet proporciona un servicio de entrega de datagramas, no confiable y sin conexión, al hacer que cada ruteador direccione datagramas. Un datagrama viaja de ruteador en ruteador hasta que llega a uno que lo puede entregar directamente a su destino final. Si un ruteador no puede rutear o entregar un datagrama, o si el ruteador detecta una condición anormal que afecta su capacidad para direccionarlo (por ejemplo, congestionamiento de red), necesita informar a la fuente original para que evite o corrija el problema. Las funciones principales que utilizan los ruteadores y los host de red de redes es comunicar la información de control o de error.

Técnicamente, el ICMP es un mecanismo de reporte de errores. Proporciona una forma para que los ruteadores que encuentren un error lo reporten a la fuente original. Aunque la especificación del protocolo subraya los usos deseables del ICMP y sugiere acciones posibles para responder a los reportes de error, el ICMP no especifica del todo la acción que debe tomarse para cada posible error.

Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

La mayor parte de los errores provienen de la fuente original, pero otros no. Sin embargo, debido a que el ICMP reporta los problemas a la fuente original, no se puede utilizar para informar los problemas a los ruteadores intermedios. Por ejemplo, suponga que un datagrama sigue un camino a través de una secuencia de ruteadores, R_1, R_2,....., R_k. Si R_k tiene información de ruteo incorrecta y, por error, rutea el datagrama hacia el ruteador R_E, éste no podrá utilizar el ICMP para reportar el error a R_k; el ICMP sólo puede enviar un reporte a la fuente original. Por desgracia, la fuente original no tiene ninguna responsabilidad sobre el problema ni sobre el control del ruteador que se equivocó. De hecho, quizá la fuente no sea capaz de determinar qué ruteador causó el problema. Y esto se debe a que un datagrama sólo contiene campos que especifican la fuente original y el último destino.

2.4.11.13.2 ENTREGA DE MENSAJES ICMP

Los mensajes ICMP requieren dos niveles de encapsulación, como se muestra en la figura. Cada mensaje ICMP viaja a través de la red de redes en la porción de datos de un datagrama IP, el cual viaja a través de la red de redes en la porción de datos de una trama. Los datagramas que llevan mensajes ICMP se rutean exactamente como los que llevan información de usuario; no existe ni una confiabilidad ni una prioridad adicionales. Por lo tanto, los mensajes de error se pueden perder o descartar. Además, en una red congestionada, el mensaje de error puede causar

congestionamiento adicional. Hay una excepción en los procedimientos de manejo de errores si un datagrama IP que lleva un mensaje ICMP causa un error. Esta excepción, diseñada para evitar el problema de tener mensajes de error sobre mensajes de error, especifica que los mensajes ICMP no se generan por errores resultantes de datagramas que llevan mensajes de error ICMP.

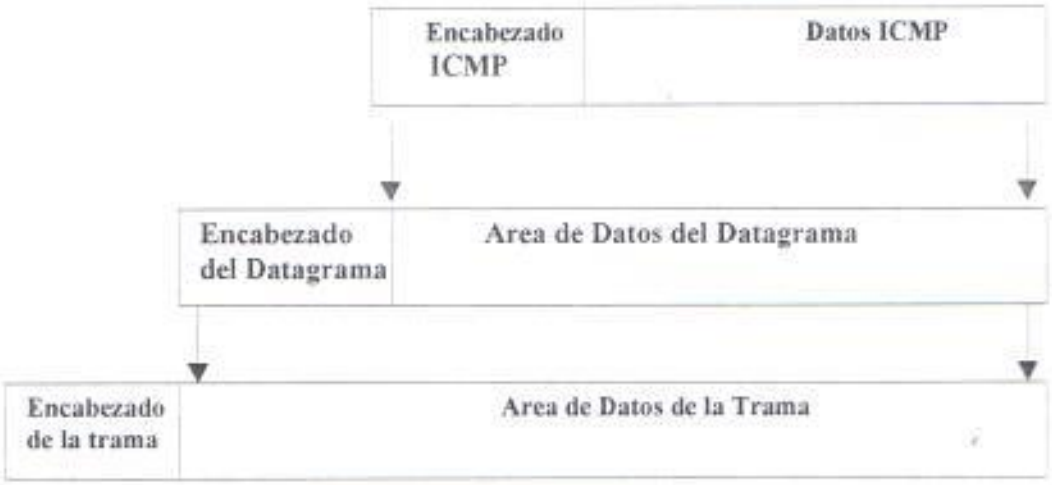


Figura 52: Formato de mensajes ICMP

Dos niveles de la encapsulación ICMP. El mensaje ICMP se encapsula en un datagrama IP que, a su vez, se encapsula en una trama para su transmisión. Para identificar el ICMP, el campo de protocolo del datagrama contiene el valor 1.

Es importante tener en cuenta que aunque los mensajes ICMP se encapsulan y envían mediante el IP, el ICMP no se considera como un protocolo de nivel más alto sino como una parte obligatoria del IP. La razón de utilizar el IP para entregar mensajes ICMP es que quizá necesiten viajar a través de muchas redes físicas para alcanzar su destino final. Por lo tanto, no se pueden entregar sólo por medio de transporte físico.

2.4.11.13.3 FORMATO DE LOS MENSAJES ICMP

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo *Tipo* de mensaje, de 8 bits y números enteros, que identifica el mensaje; un campo *Código*, de 8 bits, que proporciona más información sobre el tipo de mensaje, y un campo *Suma de Verificación*, de 16 bits (el ICMP utiliza el mismo algoritmo aditivo de suma de verificación que el IP, pero la suma de verificación del ICMP sólo abarca el mensaje ICMP). Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 56 bits de datos del datagrama que causó el problema.

La razón de regresar más que el encabezado del datagrama es únicamente para permitir que el receptor determine de manera más precisa qué protocolo(s) y qué programa de aplicación son responsables del datagrama. Los protocolos de más alto nivel del grupo TCP/IP están diseñados para codificar información crucial en los primeros 64 bits.

El campo *Tipo* del ICMP define el significado del mensaje así como su formato. Los tipos incluyen:

Campo de tipo	Tipo de Mensaje ICMP
0	Respuesta de Eco
3	Destino inaccesible
4	Disminución de origen
5	Redireccionar (cambiar una ruta)
8	Solicitud de Eco
11	Tiempo excedido para un datagrama
12	Problema de parámetros en un datagrama
13	Solicitud de timestamp
14	Respuesta de timestamp
15	Solicitud de información (obsoleto)
16	Respuesta de información (obsoleto)
17	Solicitud de máscara de dirección
18	Respuesta de máscara de dirección

Tabla 13: Campos de tipo y tipo de mensaje ICMP

2.4.11.14 PRUEBA DE ACCESABILIDAD Y ESTADO DE UN DESTINO (PING)

Los protocolos TCP/IP proporcionan funciones para ayudar a los gerentes o usuarios de redes a identificar los problemas que ocurran en la red. Una de las herramientas de depuración más utilizadas incluye los mensajes ICMP de *solicitud de eco* y *respuesta de eco*. Un host o un ruteador envía un mensaje ICMP de solicitud de eco hacia un destino específico. Cualquier máquina que recibe una solicitud de eco, formula una respuesta y la regresa al transmisor original. La solicitud contiene un área opcional de datos; la respuesta contiene una copia de los datos enviados en la solicitud. La solicitud de eco y su respuesta asociada se pueden utilizar para comprobar si un destino es alcanzable y si responde. Debido a que tanto la solicitud como la respuesta viajan en datagramas IP, la recepción exitosa de una respuesta verifica que las piezas principales del sistema de transporte están funcionando bien. Primero, el software IP en la computadora de origen debe rutear el datagrama. Segundo, los ruteadores intermedio entre el origen y el destino deben funcionar bien y rutear correctamente el

datagrama. Tercero, la máquina de destino debe estar funcionando (al menos debe responder a las interrupciones), y tanto el software ICMP como el IP deben estar funcionando. Por último, todos los ruteadores a lo largo del camino de regreso deben tener rutas correctas.

En muchos sistemas, el comando que llama el usuario para enviar solicitudes de eco ICMP se conoce como *ping*. Las versiones más sofisticadas de ping envían una serie de solicitudes de eco ICMP, capturan las respuestas y proporcionan estadísticas sobre la pérdida de datagramas. Permiten que el usuario especifique la longitud de los datos que se envían, así como el intervalo entre solicitudes. Las versiones menos sofisticadas sólo envían una solicitud de eco ICMP y esperan la respuesta.

2.4.11.15. FORMATO DE LOS MENSAJES DE SOLICITUD DE ECO Y DE RESPUESTA

En la figura se muestra el formato de los mensajes de solicitud de eco y de respuesta.

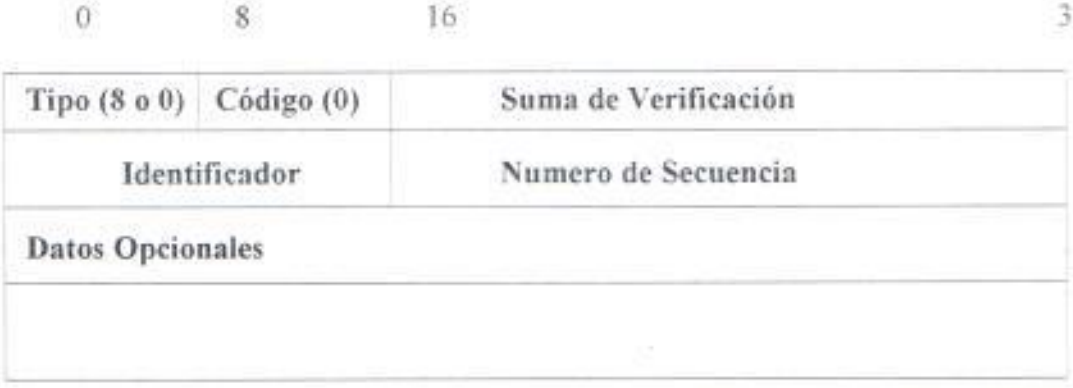


Figura 53: Formato del mensaje ICMP de solicitud de eco o de respuesta

El campo indicado como *Datos Opcionales* en un campo de longitud variable que contiene los datos que se regresarán al transmisor. Una respuesta de eco siempre regresa exactamente los mismos datos que se recibieron en la solicitud. Los campos *Identificador* y *Número de Secuencia* los utiliza el transmisor para responder las solicitudes. El valor del campo *Tipo* especifica si el mensaje es una solicitud (8) o una respuesta (0).

2.4.11.16. REPORTE DE DESTINOS NO ACCESIBLES

Cuando un ruteador no puede direccionar o entregar un datagrama IP, envia un mensaje de *destino no accesible* a la fuente original, utilizando el formato que se muestra

0	8	16	31
Tipo (3)	**Código (0-12)**	**Suma de Verificación**	
No utilizado (debe ser cero)			
Encabezado de red de redes + Primeros 64 bits del datagrama			
.....			

Figura 54: Formato del mensaje ICMP de destino inaccesible.

En la siguiente figura el campo *Código* de un mensaje de destino no accesible contiene un número entero que describe con más detalle el problema. Los valores posibles son:

Valor de Código	Significado
0	Red inaccesible
1	Host inaccesible
2	Protocolo inaccesible
3	Puerto inaccesible
4	Se necesita fragmentación y configuración DF
5	Falla en la ruta de origen
6	Red de destino desconocida
7	Host de destino desconocido
8	Host de origen aislado
9	Comunicación con la red de destino administrativamente prohibida
10	Comunicación con el host de destino administrativamente prohibida
11	Red inaccesible por el tipo de servicio
12	Host inaccesible por el tipo de servicio

Tabla 14: Valores de Código y significado

Aunque el IP es un mecanismo de entrega con el mejor esfuerzo, el descarte de datagramas no se debe tomar a la ligera. Siempre que un error evite que un ruteador direccione o entregue un datagrama, el ruteador envía al origen un mensaje de destino no accesible y luego suelta (por ejemplo, descarta) el datagrama. Los errores de red no accesible por lo general implican fallas en el ruteo. Debido a que los mensajes de error ICMP contienen un prefijo del datagrama que causó el problema, la fuente sabrá exactamente qué dirección no es accesible.

Los destinos pueden no ser accesibles ya sea porque el hardware esté temporalmente fuera de servicio, porque el transmisor haya especificado una dirección de destino no existente o (en circunstancias poco comunes) porque el ruteador no tenga una ruta para la red de destino. Nótese que aunque los ruteadores reportan las fallas que encuentran, quizá no tengan conocimiento de todas las fallas de entrega. Por lo tanto, un ruteador puede seguir enviando paquetes hacia un destino cuando éste se encuentre apagado, sin recibir ninguna indicación de que los paquetes no se están entregando. Aunque un ruteador envía un mensaje de destino no accesible cuando encuentra un datagrama que no se puede direccionar o entregar, no puede detectar la totalidad de dichos errores.

El significado de los mensajes de protocolo y puerto no accesibles se refiere a que los protocolos de un nivel más alto utilizan puntos abstractos de destino llamados puertos. La mayor parte de los mensajes restantes se explican por sí mismos. Si el datagrama contiene una opción de ruta de origen con una ruta incorrecta, activará un mensaje de falla en la ruta de origen. Si un ruteador necesita fragmentar un datagrama pero está activado el bit de "no fragmentar", el ruteador enviará un mensaje de necesidad de fragmentación hacia la fuente.

2.4.11.17. CONTROL DE CONGESTIONAMIENTOS Y DE FLUJO DE DATAGRAMAS

Debido a que el IP funciona sin conexión, un ruteador no puede reservar memoria o recursos de comunicación antes de recibir datagramas. Como resultado, los ruteadores se pueden saturar con el tráfico, condición conocida como *congestionamiento*. Es importante entender que el congestionamiento puede surgir por dos razones totalmente diferentes. Primero, una computadora de alta velocidad puede ser capaz de generar tráfico de forma más rápida de lo que una red lo puede transferir. Por ejemplo, imaginémonos una supercomputadora que genera tráfico para la red de redes. Los datagramas pueden necesitar pasar a través de una red de área amplia (WAN) más lenta, aunque la supercomputadora se conecte a una red de área local de alta velocidad. El congestionamiento ocurrirá en el ruteador que conecta la LAN con la WAN, ya que los datagramas llegan más rápido de lo que se pueden enviar. Segundo, si muchas computadoras necesitan enviar datagramas al mismo tiempo a través de un solo ruteador.

Cuando los datagramas llegan demasiado rápido para que un host o un ruteador los procesen, éstos los ponen temporalmente en una cola de espera en memoria. Si los datagramas son parte de una racha pequeña, este procedimiento de memorización temporal soluciona el problema. Si el tráfico continúa, llega un momento en el que se le acaba la memoria al host o al ruteador, y deben descartar los demás datagramas que lleguen. Una máquina utiliza mensajes ICMP de *Disminución de tasa al origen* para reportar el congestionamiento a la fuente original. Un mensaje de disminución de tasa al origen es una solicitud para que la fuente reduzca la velocidad de transmisión de datagramas. Por lo general, los ruteadores congestionados envían un mensaje de disminución de tasa al origen por cada datagrama que descartan. Los ruteadores también pueden utilizar técnicas más sofisticadas para el control de congestionamientos. Algunos, monitorean el tráfico entrante y reducen las fuentes que tienen las velocidad más altas de transmisión de datagramas. Otros, intentan evitar los congestionamientos al enviar solicitudes de disminución cuando sus colas de espera crecen, pero antes de que se saturen. No existe ningún mensaje ICMP para revertir el efecto de una disminución de tasa al origen. En vez de eso, un Host que reciba mensajes de disminución para un destino D, baja la velocidad de envío de datagramas hacia D, hasta que deja de recibir los mensajes de disminución de tasa al origen: luego, aumenta de manera gradual la velocidad en tanto más solicitudes de disminución de tasa al origen.

2.4.11.18. FORMATO DE DISMINUCIÓN DE TASA AL ORIGEN

Además de los campos normales, ICMP como *Tipo*, *Código*, *Suma de Verificación*, y un campo no utilizado de 32 bits, los mensajes de disminución de tasa al origen tienen un campo que contiene un prefijo de datagrama. En la figura se ilustra el formato. Como sucede en la mayor parte de los mensajes ICMP que reportan un error, el campo antes mencionado contiene un prefijo del datagrama que activó la solicitud de disminución de origen.

0 8 16 31

Tipo (4)	Código (0)	Suma de Verificación
No utilizado (debe ser cero)		
Encabezado de red de redes		

Figura 55: Formato del mensaje ICMP de disminución de origen. Un ruteador congestionado envía un mensaje de disminución de origen cada vez que descarta un datagrama; el prefijo de datagrama identifica el datagrama que se descartó

2.4.11.19 SOLICITUDES PARA CAMBIO DE RUTA DESDE LOS RUTEADORES

Por lo general, las tablas de ruteo de una red de redes se mantienen sin cambios por grandes periodos de tiempo. Los host las inician desde un archivo de configuración en el arranque del sistema y los administradores de sistema muy esporádicamente hacen cambios de ruteo o en un host pueden volverse incorrectas. Un cambio puede ser temporal (por ejemplo, cuando se necesita reparar el hardware) o permanente (cuando se agrega una nueva red a la red de redes). Los ruteadores intercambian en forma periódica información de ruteo para incorporar los cambios en la red y para mantener actualizadas sus rutas. Por lo tanto, como regla general, se asume que los ruteadores conocen rutas correctas; los host comienzan con información mínima de ruteo y aprenden nuevas rutas de los ruteadores.

Para ayudar a que sigan esta ruta y para evitar la duplicación de información de ruteo en el archivo de configuración de cada host, esta configuración especifica la menor información posible de ruteo necesaria para comunicarse (por ejemplo, la dirección de un solo ruteador). Por lo tanto, el host arranca con información mínima y confía en los ruteadores para actualizar su tabla de ruteo. En un caso especial, cuando un ruteador detecta un host que utiliza una ruta no óptima, le envía al host un mensaje ICMP, llamado *redireccionar*, solicitándole que cambie sus rutas. El rutedor también direcciona al datagrama original hacia su destino.

La ventaja del esquema de redireccionamiento ICMP es la simplicidad: permite que un host inicie conociendo solamente un ruteador en la red local. El ruteador inicial genera mensajes de redireccionamiento siempre que un host envía un datagrama para el que existe una ruta mejor. La tabla de ruteo del Host permanece reducida y contiene rutas óptimas para todos los destinos en uso.

Sin embargo, redireccionar mensajes no soluciona el problema de propagar rutas de manera general, ya que están limitados a la interacción entre un ruteador y un Host en una red conectada directamente. En la figura a continuación se ilustra esta limitación. Aquí se asume que la fuente S le envía un datagrama al destino D. También asuma que el ruteador R_1 rutea de manera incorrecta el datagrama a través del ruteador R_2, en vez de hacerlo a través del ruteador R_4 (por ejemplo, R_1 selecciona de manera incorrecta un camino más largo). Cuando el ruteador R_5 recibe el datagrama no puede enviar un mensaje ICMP de redireccionamiento a R_1, ya que no conoce su dirección.

Los mensajes ICMP de redireccionamiento no proporcionan ruteo entre ruteadores. En este ejemplo, el ruteador R_5 no puede redireccionar hacia R_3 no puede redireccionarlo hacia R_1.

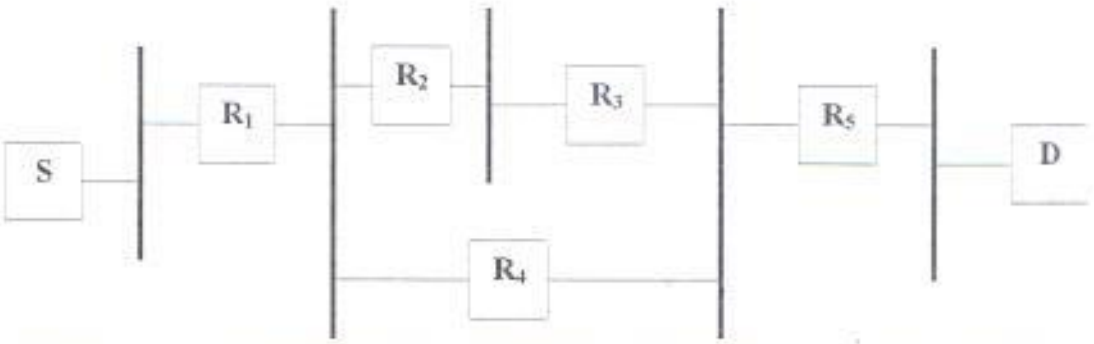


Figura 56: Ilustración de solicitudes de cambio de ruta desde los ruteadores

Además de los campos obligatorios de Tipo, Código y Suma de Verificación, cada mensaje de redireccionamiento contiene un campo de 32 bits, (llamado Dirección de red de redes del ruteador), y un campo Encabezado como se muestra en la figura.

0	8	16	31
Tipo (5)	Código (0-3)	Suma de Verificación	
Dirección de red de redes del ruteador			
Encabezado de red de redes + primeros 64 bits del datagrama			
.....			

Figura 57: Formato del mensaje ICMP de redireccionamiento

El campo *Dirección de los ruteadores en Internet* contiene la dirección de un ruteador que el host utilizará para alcanzar el destino mencionado en el encabezado del datagrama. El campo *Cabecera Internet* contiene el encabezado IP, más los siguientes 64 bits del datagrama que activó el mensaje. Por lo tanto, un host que recibe un redireccionamiento ICMP examina el prefijo del datagrama para determinar la dirección de destino. El campo *Code* de un mensaje ICMP de redireccionamiento especifica con mayor detalle cómo interpretar la dirección de destino, basándose, como se muestra a continuación, en los valores asignados.

Como regla general, los ruteadores envían solicitudes ICMP de redireccionamiento sólo a los host y no a otros ruteadores.

Valor de Código	Significado
0	Redireccionar datagramas para la red (ahora obsoleto)
1	Redireccionar datagramas para la Host
2	Redireccionar datagramas para el tipo de servicio y la red
3	Redireccionar datagramas para el tipo de servicio y el host

Tabla 15: Valor de código y su significado

2.4.11.20 DETECCIÓN DE RUTAS CIRCULARES O EXCESIVAMENTE LARGAS

Debido a que los ruteadores en una red de redes computan un salto al siguiente ruteador, utilizando tablas locales, los errores en dichas tablas pueden producir un ciclo de ruteo para algún destino, D. Un ciclo de ruteo puede consistir en dos ruteadores, cada uno ruteando al otro un datagrama para el destino D, o puede consistir en muchos ruteadores haciendo lo mismo. Cuando muchos ruteadores forman un ciclo, cada uno rutea un datagrama para el destino D y hacia el siguiente ruteador dentro del ciclo. Si un datagrama entra en un ciclo de ruteo, recorrerá indefinidamente y de manera circular todos los ruteadores. Como se mencionó con anterioridad, para evitar que los datagramas circulen indefinidamente en una red de redes TCP/IP, cada datagrama IP contiene un contador de tiempo de vida, conocido como *conteo de saltos*. Un ruteador disminuye el contador de tiempo de vida siempre que se procese el datagrama y lo descarta cuando el conteo llega a cero.

Siempre que un ruteador descarta un datagrama ya sea porque su conteo de saltos llega a cero o porque ocurre una terminación de tiempo mientras espera fragmentos de un datagrama, envía un mensaje ICMP de tiempo excedido a la fuente del datagrama, utilizando el formato que se muestra a continuación:

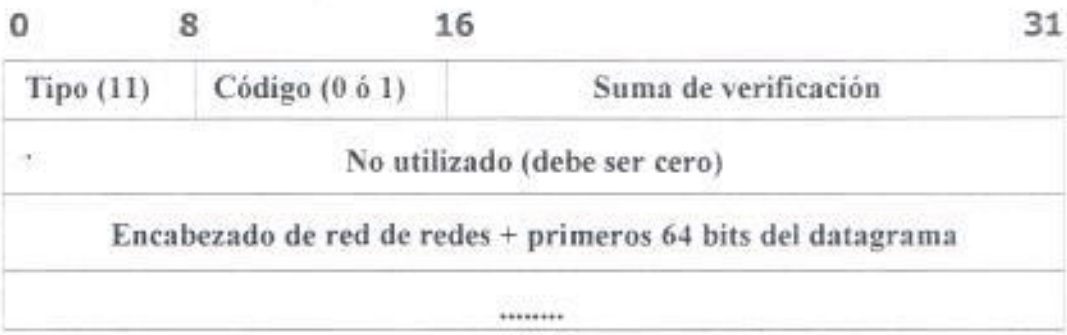


Figura 58: Formato del mensaje ICMP de tiempo excedido.

Un ruteador envia este mensaje siempre que se descarte un datagrama cuando el campo de tiempo de vida en el encabezado del datagrama llega a cero o cuando su temporizador de reensamblado expira mientras éste espera fragmentos.

En el campo *Código* se explica la naturaleza de la terminación de tiempo:

Valor de Código	Significado
0	Conteo de tiempo de vida excedido
1	Tiempo para el reensamblado de fragmentos excedido

Tabla 16: Valor de Código y su Significado

El reensamblado de fragmentos se refiere a la tarea de recolectar todos los fragmentos de un datagrama. Cuando llega el primer fragmento de un datagrama, el host que lo recibe arranca un temporizador y considera como error que dicho temporizador expire antes de que lleguen todas las piezas del datagrama. El valor 1 para el campo *Código* se utiliza para informar dichos errores al transmisor; se envía un mensaje por cada error.

2.4.11.21 REPORTE DE OTROS PROBLEMAS

Cuando un ruteador o un host encuentran problemas que no se han cubierto con los mensajes ICMP de error anteriores (por ejemplo, un datagrama con encabezado incorrecto), envían un mensaje de *problema de parámetros* a la fuente original. Una causa posible de dichos problemas ocurre cuando los argumentos para una opción son incorrectos. El mensaje, formateado como se muestra en la figura, sólo se envía cuando el problema es tan severo que se tiene que descartar el datagrama.

0	8	16	31
Tipo (12)	**Código (0 ó 1)**	**Suma de verificación**	
Indicador	**No utilizado (debe ser cero)**		
Encabezado de red de redes + primeros 64 bits del datagrama			
.....			

Figura 59: Formato del mensaje ICMP de problema de parámetros.

Los mensajes sólo se envían cuando el problema origina que se descarte el datagrama.

Para lograr que el mensaje no sea ambiguo, el transmisor utiliza el campo *Puntero* en el encabezado del mensaje para identificar el octeto del datagrama que causó el problema. El código 1 se utiliza para informar que falta la opción requerida (por ejemplo, una opción de seguridad en la comunidad militar), el campo *Puntero* no se utiliza para el código 1.

2.4.11.22 SINCRONIZACIÓN DE RELOJES Y ESTIMACIÓN DEL TIEMPO DE TRANSITO

Aunque las máquinas en una red de redes se pueden comunicar, por lo general operan de forma independiente, con cada máquina, manteniendo su propia noción de la hora actual. Los relojes que varían demasiado pueden confundir a los usuarios de software de sistemas distribuidos. El grupo de protocolos TCP/IP incluye muchos protocolos que se pueden utilizar para sincronizar los relojes. Una de las técnicas más sencillas se vale de un mensaje ICMP para obtener la hora de otra máquina. Una máquina solicitante envía un mensaje ICMP de *solicitud de timestamp* (marca de hora) a otra, solicitándole que informe su valor actual para la hora del día. La máquina receptora envía una respuesta de *timestamp (marca de hora)* a quien la solicitó. En la figura se muestra el formato de los mensajes de solicitud y respuesta de timestamp (marca de hora).

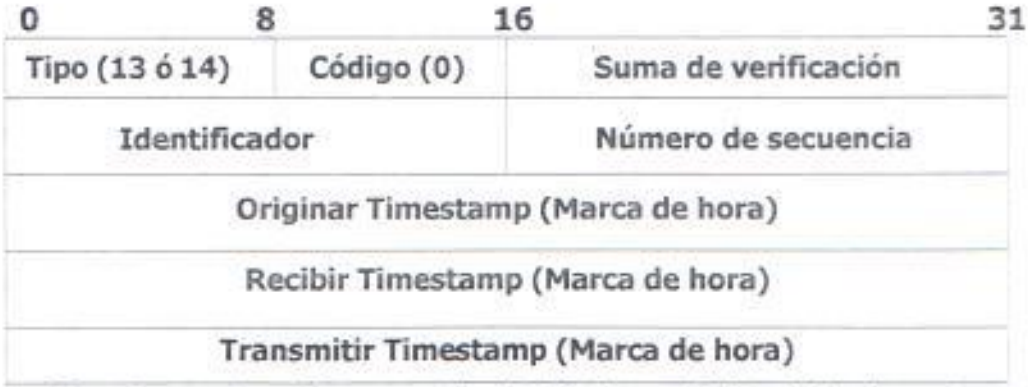


Figura 60: Formato del mensaje ICMP de solicitud de timestamp (marca de hora) o de respuesta de timestamp (marca de hora).

El campo *Tipo* indentifica el mensaje como solicitud (13) o como respuesta (14); los campos Identificador y Número de secuencia los utiliza la fuente para asociar las solicitudes con las respuestas. Los campos restantes especifican la hora, en milisegundos desde la media noche, en Tiempo Universal. El campo Originar

Timestamp *(Marca de Hora)* es llenado por la fuente original justo antes de transmitir el paquete, el campo Recibir Timestamp *(Marca de Hora)* se llena inmediatamente al recibir una solicitud y el campo Transmitir Timestamp *(Marca de Hora)* se llena justo antes de transmitir la respuesta.

Los host utilizan estos tres campos para computar estimaciones del tiempo de retraso entre ellos y para sincronizar sus relojes. Debido a que la respuesta incluye el campo *Originar Timestamp (Marca de Hora)*, un host puede computar el tiempo total requerido para que una solicitud viaje hasta un destino, se transforme en una respuesta y regrese. Debido a que la respuesta lleva tanto la hora en la que la solicitud ingresó a la máquina remota como la hora en la que se transmitió, el host puede computar el tiempo de tránsito de la red, y con ese valor, estimar las diferencias entre el reloj local y los remotos.

En la práctica, el cálculo preciso del retraso en los viajes redondos puede ser difícil y substancialmente restringe la utilidad de los mensajes ICMP timestamp (marca de hora). Para obtener un cálculo preciso del retraso en viajes redondos, se deben tomar medidas y promediarlas. Sin embargo, el retraso del viaje redondo entre 2 máquinas que se conectan a una gran red de redes puede varias de forma dramática, inclusive entre cortos periodos de tiempo. Además, recuerde que debido a que el IP es una tecnología de mejor esfuerzo, los datagramas se pueden perder, retrasar o entregarse en desorden. Por lo tanto, aún tomando muchas medidas no se garantiza la cosistencia; quizá se necesite un análisis estadístico sofisticado para obtener cálculos precisos.

2.4.11.23 OBTENCIÓN DE UNA MASCARA DE SUBRED

Cuando los anfitriones utilizan el direccionamiento de subred, algunos bits en la porción hostid de su dirección IP identifican una red física. Para participar en el direccionamiento de subred, un host necesita saber qué bits de la dirección de redes de 32 bits corresponden a la red física, así como qué bits corresponden a los identificadores del anfitrión. La información necesaria para interpretar la dirección se representa en una cantidad de 32 bits llamada *máscara de subred*.

Para aprender la máscara de subred utilizada para la red local, una máquina puede enviar un mensaje de *solicitud de máscara de subred* a un ruteador y recibir una *respuesta de subred*. La máquina que hace la solicitud puede enviar directamente el mensaje, si conoce la dirección del ruteador, o transmitir el mensaje por difusión. En la figura a continuación se muestra el formato de un mensaje de máscara de subred.

0	8	16	31
Tipo (17 ó 18)	Código (0)	Suma de verificación	
Identificador		Número de Secuencia	
Máscara de dirección			

Figura 61: Formato del mensaje ICMP de solicitud de máscara de red o de respuesta de máscara de red. Por lo general, los anfitriones transmiten por difusión una solicitud sin saber qué ruteador específico responderá.

El campo *Tipo* en un mensaje de máscara de dirección especifica si el mensaje es una solicitud (17) o una respuesta (18). Una respuesta contiene la máscara de dirección de subred en el campo Máscara de dirección. Como es usual, los campos Identificador y Número de Secuencia permiten que una máquina asocie las solicitudes con las respuestas.

2.4.11.24 ARP (ADDRESS RESOLUTION PROTOCOL)

Dos hots en una LAN no se pueden comunicar si no conocen su dirección física, usando ARP se pueden comunicar dos máquinas en una misma LAN si sólo conocen su dirección IP.

En las redes ethernet, la tarjeta de interfaz tiene una dirección fija, única y universal de 48 bits asignada por el fabricante. Para la obtención de la dirección física de otra máquina a partir de su dirección IP:

- Enviar un mensaje broadcast ARP preguntando la dirección física que corresponde a cada maquina.
- Esperar por la respuesta de alguna máquina en la LAN.

Figura 62: Ilustración del requerimiento ARP

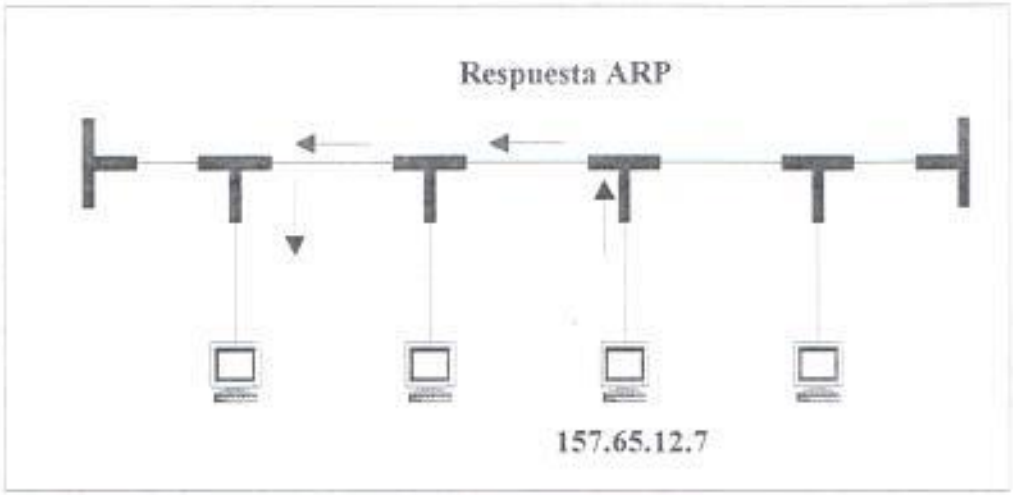


Figura 63: Ilustración de respuesta de ARP

- Las máquinas que usan ARP mantienen una caché con las equivalentes entre las direcciones físicas y lógicas.

Otros refinamientos:

- Una máquina A incluiye su propia dirección física cuando hace un requerimiento ARP para determinar la dirección física de una máquina B.
- Cuando A hace un requerimiento ARP todas las máquinas de la LAN aprovechan para conocer la dirección física de A.
- Al añadir un a nueva computadora a la red se puede enviar un requerimiento ARP para actualizar las tablas del resto de computadoras.

2.4.11.25 RARP (REVERSE ADDRESS RESOLUTION PROTOCOL)

- Utilizado por máquinas que no conocen su propia dirección IP.
- Utiliza el esquema cliente servidor: existe un servidor RARP que corresponde los requerimientos Determina la dirección lógica a partir de la dirección física.
- de las máquinas clientes.
- Las máquinas clientes hacen un requerimiento broadcast así que no necesitan conocer la dirección del servidor.

Ventajas

- Permite tener una administración centralizada de la LAN en lo que se refiere a direcciones IP.
- Facilita la configuraión del software.
- Permite controlar las direcciones de la red en base de las tarjetas de red y no en base a las máquinas.

Desventajas

Es muy simple: básicamente un servidor RARP solo puede proporcionar la direccion IP y no datos adicionales.

2.5 ESTANDARES DE REDES DE AREA LOCAL IEE 802

Este proyecto implementa estándares en lo que corresponde las capas I y II del modelo ISO/OSI. De esta manera, el estrato de enlace está dividido en dos subestratos: un subestrato LLC (control lógico de enlace) similar a HDLC y un medium access control MAC igual que el CSMA/CD usado en Ethernet.

IEEE 802.2 Control lógico de enlace.
IEEE 802.3 CSMA/CD.
IEEE 802.5 Token Ring.

Los estándares consisten en una porción común del subestrato LLC junto con tres opciones mayores que tienen que ver con el subestrato MAC y el estrato físico.

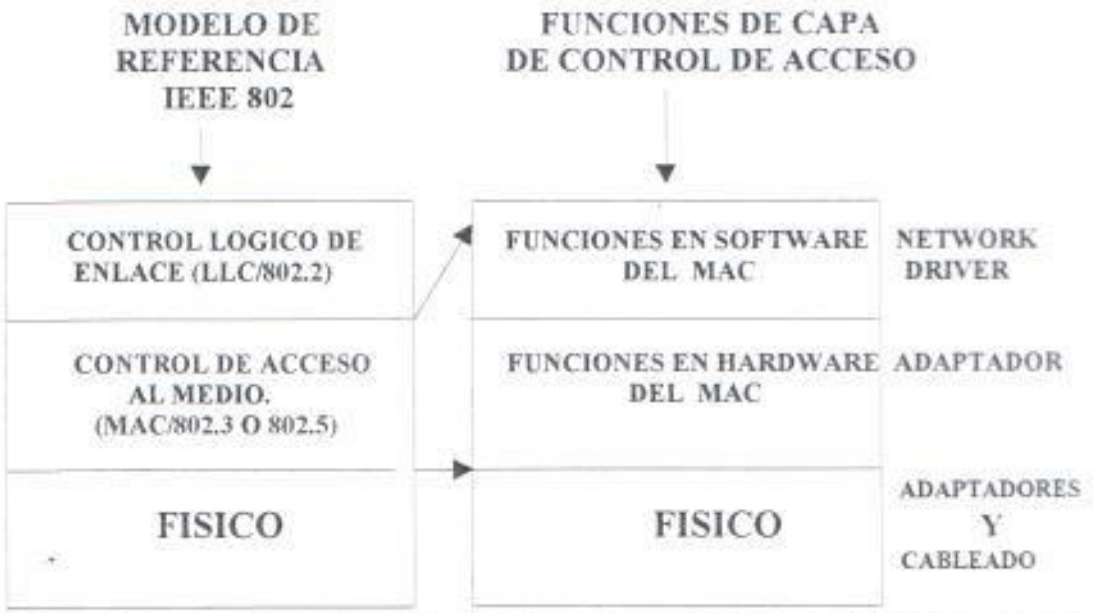


Figura 64: Comparación del modelo de referencia IEEE 802 con las funciones de capa del control de acceso

2.5.1 CONTROL DE ACCESO AL MEDIO (MAC)

- Contiene los algoritmos y procedimientos (protocolos) requeridos para controlar el Acceso al Medio Compartido.
- No se puede definir un solo estándar, por lo que se definieron varios:
  - 802.3: CSMA/CD (empleado por Ethernet)
  - 802.5: Token Ring.
  - Otros procolos reciben un número distinto.
- Entre otras funciones, define el formato de las direcciones fisicas de los nodos.
  - Dirección viene predeterminada en el NIC.
  - Toda dirección fisica de LAN requiere de 6 bytes. Los tres primeros bytes indentifican al proveedor.
- La dirección fisica direcciona a las capas fisica y MAC.
  - Más conocida como dirección MAC.
  - Dirección fisica y dirección MAC, son dos conceptos totalmente equivalentes.

2.5.2 CONTROL LOGICO DEL ENLACE (LLC)

- Resuelto el problema del Acceso al Medio Compartido, el Enlace se comporta como un "Enlace Dedicado".
- Aunque fisicamente sigue compartido. El enlace fisico une a todas las estaciones.
- Como en cualquier "Enlace Dedicado", se requiere un protocolo de control (LLC).
- En el enlace lógico es exclusivo entre solo 2 estaciones. Se produce un enlace dedicado por LLC.
- LLC hace "confiable" al enlace lógico establecido por la capa MAC.

2.6 REDES DE AREA LOCAL

- No es el único tipo de Redes que existe.
  - Aunque si el más común ya que se las encuentra en toda oficina moderna.
- En la mayoria de casos, una LAN constituye sólo la parte terminal de una gran Red de Computadoras.

Clasificación de las redes:

- Según la estructura de sus Enlaces:
  - De enlaces dedicados solamente.
  - De enlaces compartidos.
  - Redes mixtas, que es lo más común.

- Según la técnica de Transmisión:

  - Transmisión/Acceso Múltiple.
  - Conmutadas.
- Según el alcance.
  - De Area Extendida (MAN, WAN).
  - De Area Local (LAN).
- Comunicación de igual a igual entre nodos.
  - Permite esquemas de Procesamiento Centralizado o Procesamiento Distribuido.

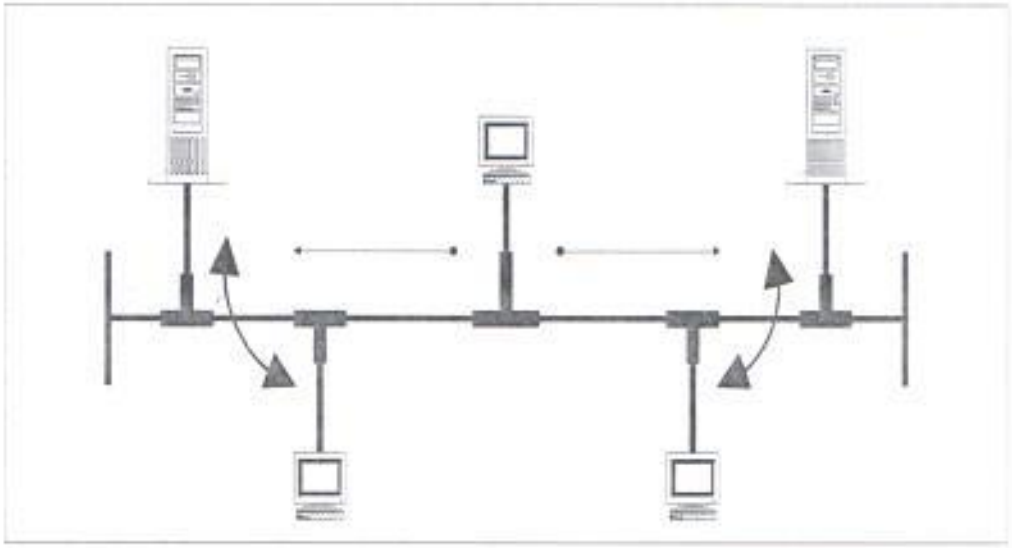


Figura 65: Ilustración de una red de procesamiento distribuido

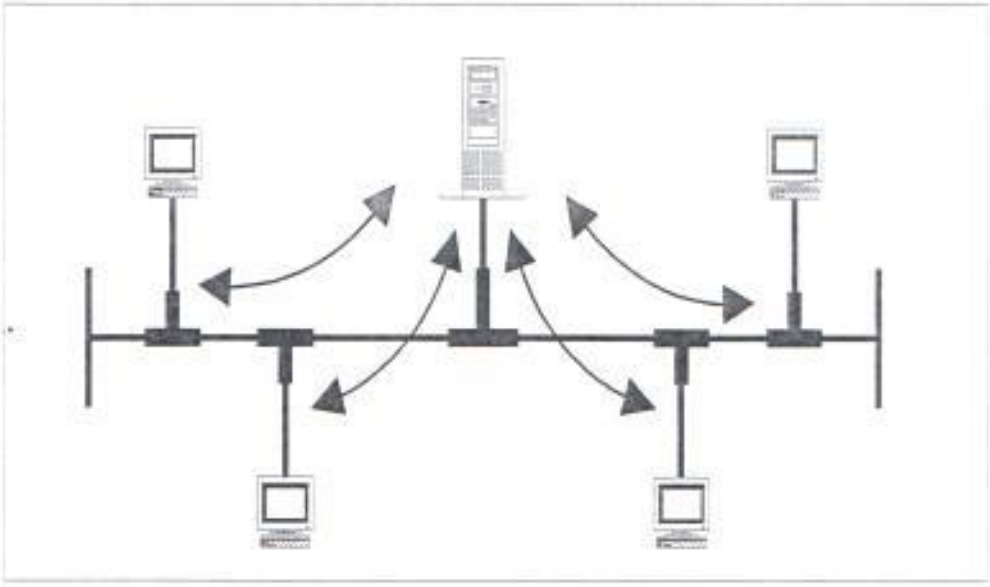


Figura 66: Ilustración de una red de procesamiento centralizado

2.6.1 TIPOS DE LANs

- LANs sobre medio compartido.
  - La forma más tradicional de LANs.
  - Implica la transmisión de Broadcast.

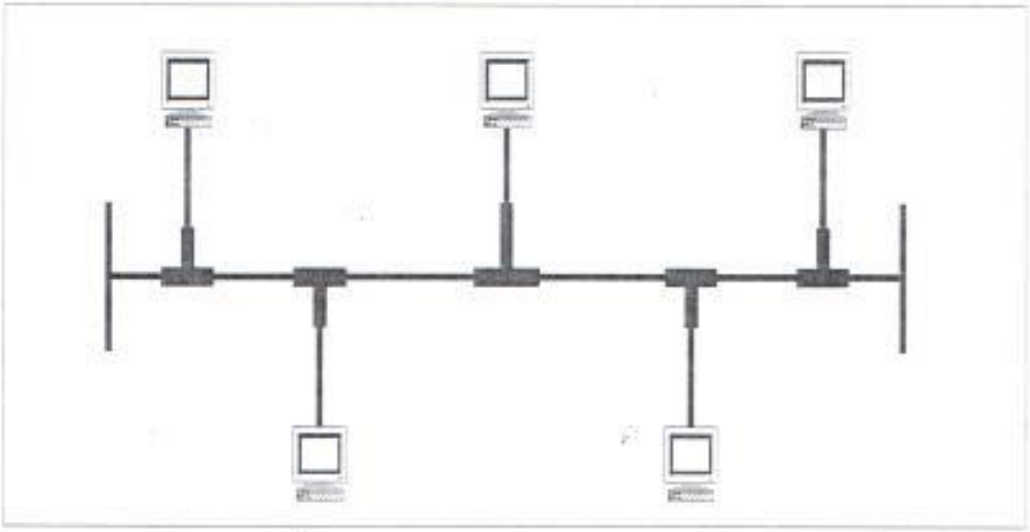


Figura 67: Ilustración de una LAN sobre medio compartido

- LANs Conmutadas.
  - Enlace dedicado entre 2 Nodos, temporalmente establecidos a través de "Switches".

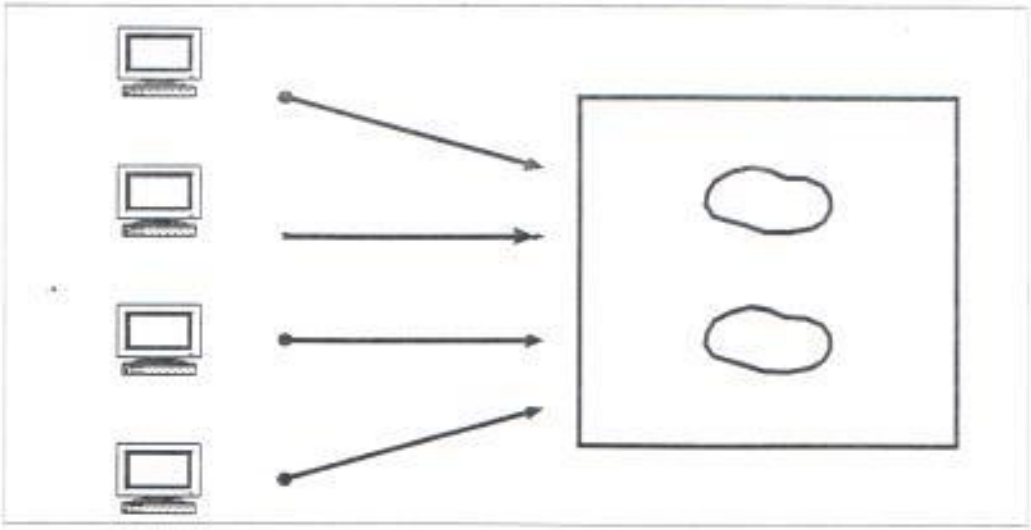


Figura 68: Ilustración de una LAN conmutada

- En la práctica ambas modalidades de LANs deben ser combinadas para obtener el mejor rendimiento: Buen tiempo de Respuesta y buena Relación Costo/Beneficio.

2.6.2 COMPONENTES BASICOS DE LANs

- Medios de transmisión.
  - Guiados.
  - No Guiados.

- Conectores y acopladores.
  - Cable de cobre: RJ45, Conectores de Datos.
  - Cable coaxial: BNC.
  - Fibra óptica.

- Concentradores y Dispositivos de Extensión.
  - Facilitan la distribución fisica de los Medios de Transmisión empleados en una LAN.
  - Ejemplos: Hubs, MAUs, Repetidores.

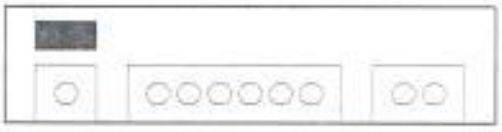


Figura 69: Hub

- Tarjeta de Red.
  - Tarjeta de Interface de Red (NIC).
  - Pueden ser independientes a integradas a la tarjeta principal del computador.
  - Dependiendo del tipo de tecnologia empleada.
    Eternet, FDDI, etc.

- Servidores.
  - Controladores para el Sistema Operativo, el mismo que incluye el Software de Red (TCP/IP, IPX/SPX, etc).
    - WinNT, OS/2, Unix, NetWare.

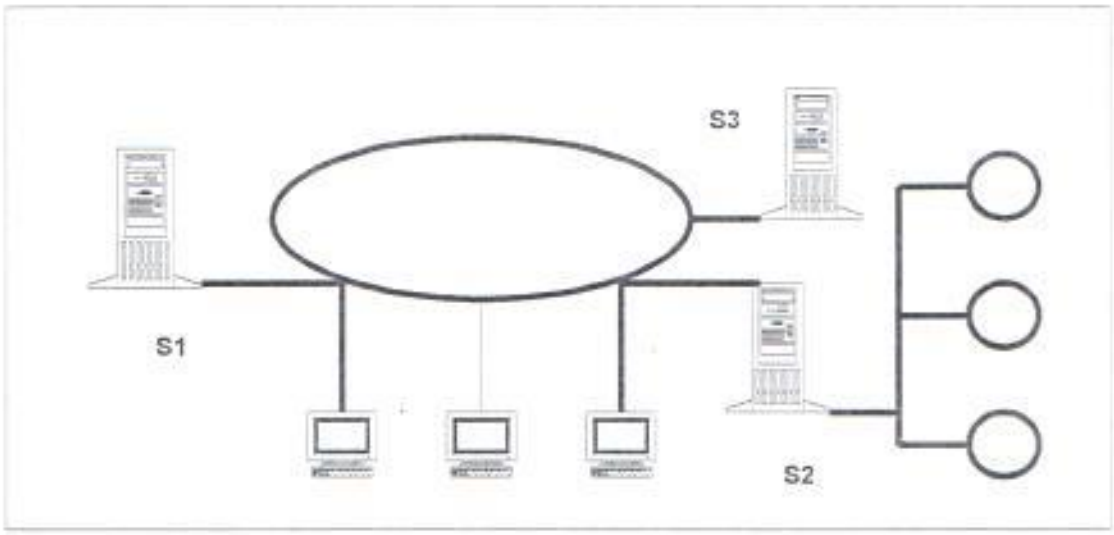


Figura 70: Red con servidores

S1: servidor de comunicaciones(Fax, Acceso Remoto, etc.)
S2: servidor de archivos.
S3: servidor de impresión.

- No siempre es necesario que exista un Servidor en forma explicita, pero si en forma conceptual.
  - Se puede establecer un grupo de trabajo a través de OS/2 o Win95, donde cada nodo podria ser un Servidor.
  - En redes que demandan gran Seguridad e integridad de la información, se requiere un Servidor de mayor poder.

Figura 71: Ilustración de nodos utilizados como servidores

➢ Dispositivos de Interconexión de LANs.

- Bridges

Toman la decisión de Repetir basados en el contenido del paquete.

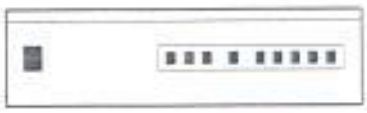


Figura 72: Bridge

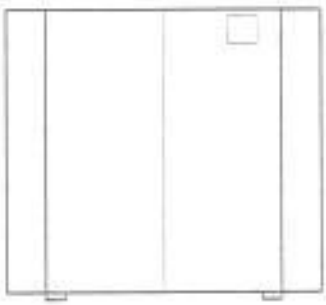


Figura 73: Switching Hub

- Switching Hubs.
  - Equivalentes a los Bridges, pero más rápidos.
- Ruteadores.
  - Consideran la Dirección Lógica.

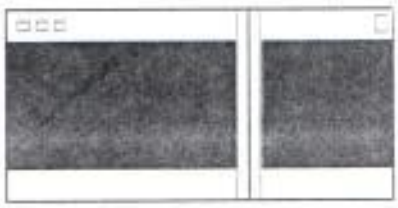


Figura 74: Ruteador

2.6.3 VENTAJAS DE ETHERNET

- Arquitectura Abierta. Los costos son bajos.
  - Interoperabilidad a nivel múltiples vendedores.
  - Tarjetas de Red baratas: $50 - $100.
- Tecnología madura y bien probada.

  - Aunque hay variantes más recientes que aún no han sido bien probadas. (Gigabit Ethernet).
- Fáciles de administrar.
  - Fallas en la red son fácilmente detectables.
  - A veces dependen de la disposición física de la Red.

2.6.4 DESVENTAJAS DE ETHERNET

- Tiempo de respuesta NO ES PREDECIBLE.
  - Sólo en la modalidad de Medio Compartido.
  - No hay problemas con Switched Ethernet (Port Switched y Full Duplex): siempre está disponible.

2.7 RENDIMIENTO DE REDES DE AREA LOCAL (LAN)

Las características principales de la LAN que estructuran la manera en que su rendimiento es analizado es que hay un acceso al medio compartido, requiriendo un protocolo de acceso al medio y que se usa conmutación de paquetes.

Tres medidas de rendimiento de LAN son usadas comúnmente:
D: el retardo que ocurre entre el tiempo en que un paquete o frame está listo para la transmisión en un nodo, y la completa transmisión exitosa.
S: el throughput de la red local; la tasa total de datos que es transmitido entre los nodos (carga transportada).
Q: la utilización del medio de la red local; la fracción de la capacidad total a ser usada.

El parámetro *S* a menudo es normalizado y expresado como una fracción de capacidad. Por ejemplo, si sobre un periodo de 1 segundo, la suma de los datos exitosamente transferidos entre nodos es 1 Mbyte en un canal de 10 Mbps, entonces S=0.1. Luego S también puede ser interpretado como la utilización. El análisis es comúnmente hecho del número total de bits transferidos, incluyendo bits de "overhead" (cabecera, trailers); los cálculos son un poco más fáciles, y este aprovechamiento aisla los efectos del rendimiento debido a la red local por si misma. Uno debe trabajar hacia atrás a partir de esto para determinar el Troughput efectivo.

Los resultados para S y D son generalmente graficados como una función de la carga ofrecida G, la cual es la carga actual o demanda de tráfico presentada para la red local. Note que S y G difieren. S es la tasa normalizada de paquetes de datos transmitidos exitosamente; G es el número total de paquetes ofrecidos a la red; incluye paquetes de control, tales como "Tokens", y colisiones, los cuales son paquetes destruidos que deben ser retransmitidos. G, también es a menudo expresado como una fracción de capacidad. Intuitivamente, se esperaría que D se incrementara

con G: entre más tráfico compitiendo por el tiempo de transmisión, más largo el retardo para cualquier transmisión individual. S debería también incrementarse con G. Si se está más cerca de algún punto de saturación, más allá de que cualquier red no pueda manejar más carga.

La figura a continuación muestra la situación ideal: la utilización del canal se incrementa para acomodar la carga a una carga ofrecida igual a la capacidad total del sistema; entonces la utilización permanece en un 100%. Seguro que cualquier "overhead" o ineficiencia ocasionará que el rendimiento se caiga muy cerca del valor esperado. La representación de S vs G es un ejemplo del punto de vista de la red por sí misma. Muestra el comportamiento del sistema basado en su carga actual. Pero desde el punto de vista del usuario o del dispositivo conectado, puede parecer extraño. ¿Por qué? Porque la carga ofrecida no incluye sólo las transmisiones originales y reconocimientos, y en el caso de errores o colisiones, retransmisiones. El usuario puede querer conocer el throughput y las características del retardo como una función de los datos generados por el dispositivo a ser colocados en el sistema – la carga de entrada. O si la red es el foco, el analista puede querer conocer cuál es la carga ofrecida, dando la carga de entrada.

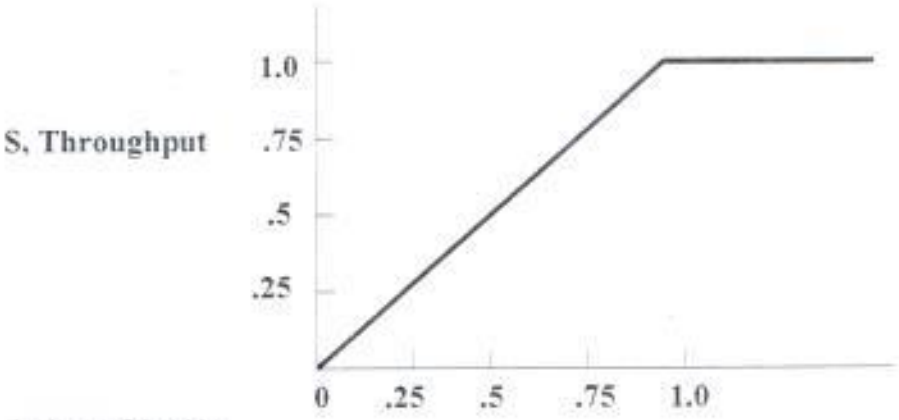


Figura 75: Utilización ideal del canal

Se puede preguntar si la importancia de U, D y S son de real interés, pero la eficiencia o la utilización del canal pueden parecer de menor importancia. Después de todo, se dice que las redes locales tienen un muy elevado ancho de banda y bajo costo comparado a las redes de gran alcance. Aunque es verdad que la utilización es de menor importancia para las redes locales comparadas con las de largo alcance, aún es importante considerarla. La capacidad de la red local no está libre, y la demanda tiene una tendencia a expandirse hasta llenar la capacidad disponible.

1. **G:** la carga ofrecida a la red local; la tasa total de datos presentada a la red para la transmisión.
2. **I:** la carga de entrada; la tasa de datos generada por las estaciones conectadas a la red local.

La tabla que a continuación se detalla un ejemplo muy simplificado que muestra la relación entre estos parámetros. Aquí se asume una red con capacidad de C=1000 frames/seg. Por simplicidad, I,S y G son expresados en frames/seg. Se asume que un porcentaje de todos los frames transmitidos se pierden y deben ser repetidos. Además a una entrada de I=100 frames/seg, como promedio 1 frame/seg será repetido. Con S=100 y G=101. Asuma que la carga de entrada llega en lotes, una vez por segundo. De aquí en adelante, en promedio, con I=100, D=0.0505 seg. La utilización se define como S/C=0.1

I	S	G	D	U
100	100	101	0.0505	0.1
500	500	505	0.2525	0.5
990	990	1000	0.5	0.99
2000	990	-	-	0.99

Tabla 17: Ejemplo de valores de parámetros para el análisis del rendimiento de la red

Capacidad: 1000 frames/s
I: carga de entrada (frames por segundo); **S**: Throughput (frames por segundo); **D**: Retardo (segundos); **U**: utilización (fracción de capacidad)

Se ve claramente que las siguientes 2 entradas son correctas. Note que para I=990, está siendo usada la capacidad total del sistema (G=1000). Si I se incrementa más allá de este punto, el sistema no lo soporta. Sólo 1000 frames/seg serán transmitidos. Así S permanece en 990 y U en 0.99. Pero G y D crecen sin límite tanto como se acumule el "backlog", no hay un valor de estabilización.

2.7.1 EL EFECTO DEL RETARDO DE PROPAGACIÓN Y LA TASA DE TRANSMISIÓN

Las redes LAN se diferencian de las WAN y los sistemas multiprocesadores de los demás, por la tasa de datos ® y la distancia (d) de la trayectoria de comunicaciones. De hecho es el producto de estos 2 términos, Rxd que pueden ser usados para caracterizar redes locales. Más aún, como se observa, éste término o primos de él, es el parámetro más importante para determinar el rendimiento de una red local. Se observa que el rendimiento de una red será el mismo, por ejemplo, para ambos 100 Mbps con 1 Km de bus y 10 Mbps con 10 Km de bus.

Una buena manera de visualizar el significado de Rxd es dividirlo para la velocidad de propagación del medio, que es cercanamente constante entre la media de interés. Una buena aproximación para la velocidad de propagación es cerca de 2/3 de la velocidad de la luz, o $2x10^8$ m/seg.

Un análisis dimensional de la fórmula:

$$Rd/V$$

muestra que esto es igual a la longitud del medio de transmisión en bits, que es, el número de bits que pueden estar en tránsito entre 2 nodos en cualquier momento.

Se puede ver que esto en efecto distingue las redes locales de los multiprocesadores y de las redes de largo alcance. Dentro de un sistema multiprocesador, hay generalmente sólo unos pocos bits en tránsito. Por ejemplo, el canal de E/S de IBM opera hasta unos 24 Mbps sobre una distancia de hasta 120 m., el cual rinde en la mayoría 15 bits. La comunicación procesador a procesador dentro de una sola computadora normalmente involucrará menos bits que esos en tránsito. Por otro lado, la longitud de bit de la red de largo alcance puede ser cientos de miles de bits. Algunos ejemplos: un sistema Ethernet de 500 m. (10 Mbps) tiene una longitud de bits de 25; una tipica LAN-broadband de 5 Km (5Mbps) tiene una longitud de 250 bits.

Una manera útil de aprovechar esto es considerar la longitud del medio comparado al frame tipico transmitido. Los sistemas multiprocesador tienen longitud de bits muy cortas comparadas a la longitud del frame; las redes de largo alcance las tienen largas. Las redes locales generalmente son más cortas que un frame o hasta cercanos del mismo orden de su magnitud.

Intuitivamente, uno puede ver que esto hará una diferencia. Compare las redes locales a computadores multiprocesador. Relativamente hablando, las cosas suceden casi simultáneamente en un sistema multiprocesador; cuando un componente empieza a transmitir, los otros lo saben inmediatamente. Para redes locales, el espacio del tiempo relativo deja a toda clase de complicaciones a los protocolos de control de acceso al medio, como ya se ha visto. Compare las redes de largo alcance a las locales. Para tener alguna esperanza de eficiencia, el enlace de largo alcance deben permitir que transiten simultáneamente frames múltiples. Esto da lugar a que existan requerimientos especificos en el protocolo de la capa de enlace, el cual debe soportar que una secuencia de frames pendientes estén esperando a ser reconocidos. El protqcolo LAN generalmente permite que un frame esté en tránsito a la vez, o al menos unos cuantos para la mayoria de los protocolos de anillo. Otra vez, esto afecta el protocolo de acceso.

La longitud del medio, expresada en bits, comparada con la longitud del frame tipico se denota con a:

a= longitud de la trayectoria de datos (bits) / longitud del frame.

Después de manipular la fórmula

a= Rd/VL

Donde L es la longitud del frame. Pero d/V es el tiempo de propagación del medio (peor de los casos), y L/V es el tiempo que toma a un transmisor enviar al medio el frame completo. Así

a= tiempo de propagación/tiempo de transmisión

Los valores típicos de a están en un rango de 0.01 a 0.1 para LANs. La tabla que a continuación se detalla da algunos ejemplos de valores para topología bus.

Tasa de Datos (Mbps)	Medida de paquetes (bits)	Longitud del cable (Km)	A
1	100	1	0.05
1	1000	10	0.05
1	100	10	0.5
10	100	1	0.5
10	1000	1	0.05
10	1000	10	0.5
10	10000	10	0.05
50	10000	1	0.025
50	100	1	2.5

Tabla 18: Valores para topología tipo bus

Al computar *a*, se tiene en mente que el máximo tiempo de propagación en una red "broadband" es el doble de longitud que la más larga trayectoria desde el "headend", más su retardo en el "headend" si hubiere. Para bus "baseband" y redes anillo, los retardos de la repetidora deben ser incluidos en el tiempo de propagación.

El parámetro *a* determina un límite superior en la utilización de la red local. Considere un mecanismo de acceso eficiente que permite sólo una transmisión a la vez. Tan pronto como una transmisión se termina, otro nodo empieza a transmitir. Más aún, la transmisión es sólo de datos, sin overhead. ¿Cuál es la máxima utilización posible de la red? Puede ser expresada como el radio de el "throughput" del sistema para la capacidad del ancho de banda.

$$U = \text{throughput}/R = \frac{L/(\text{propagación} + \text{tiempo de transmisión})}{R}$$

$$= \frac{L(d/V + L/R)}{R} = 1/(1+a)$$

Entonces la utilización es inversa a *a*. Esto puede ser comprendido estudiando la figura a continuación. Esta figura muestra un bus baseband con dos estaciones lo más

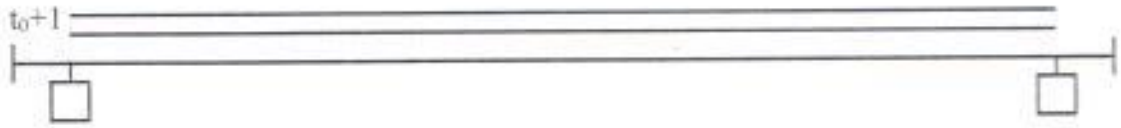
alejadas posible (peor de los casos) que toman turnos para enviar los frames. Si se normaliza el tiempo de tal manera que el tiempo de transmisión del frame sea igual a 1, luego a=tiempo de propagación. La secuencia de eventos puede ser expresada de la siguiente manera:

1. Una estación comienza la transmisión en t_0.
2. La recepción comienza en t_0+a
3. La transmisión se completa en t_0+1
4. La recepción termina en t_0+1+a
5. La otra estación comienza a transmitir.

Tiempo de Propagación = a<1 **Tiempo de transmisión = 1**

Inicio de la Transmisión

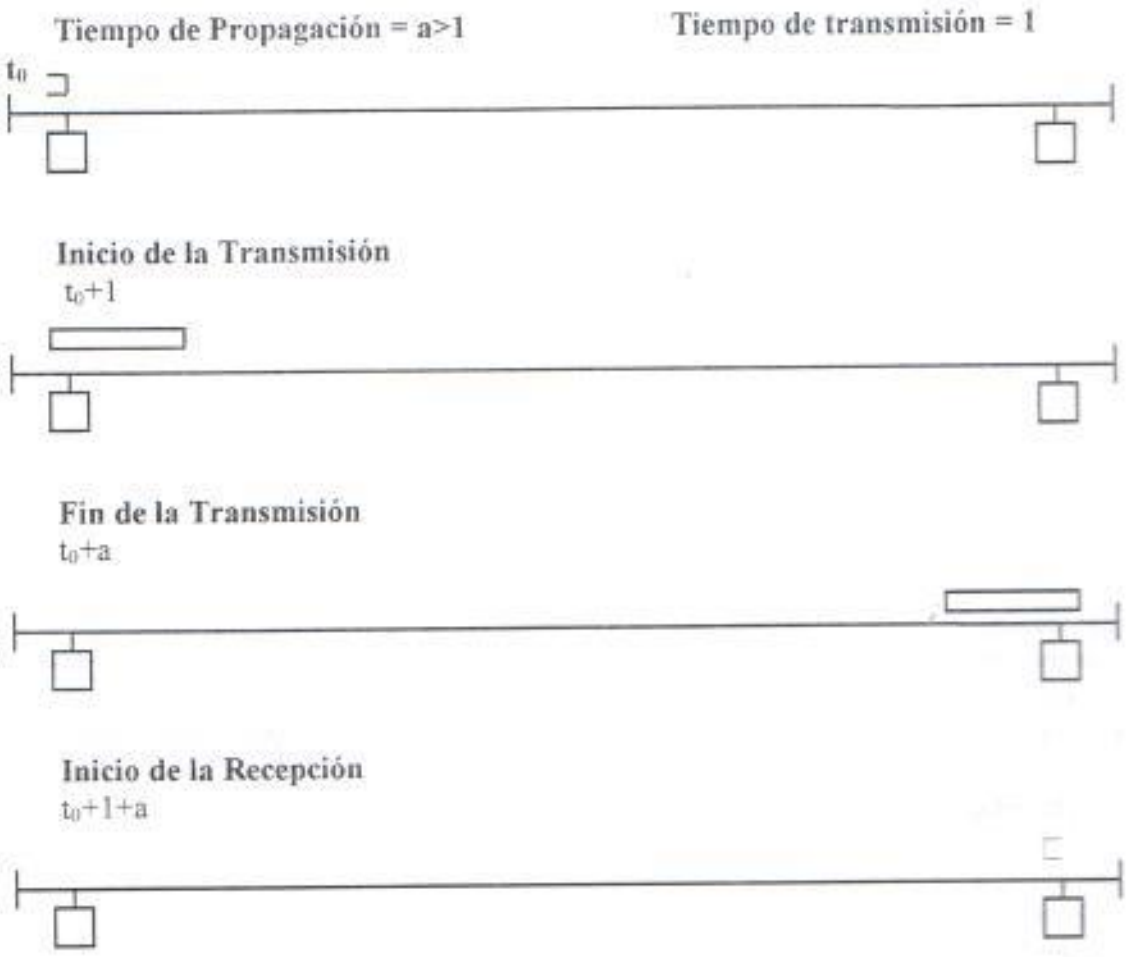
Inicio de la Recepción



Fin de la Transmisión

Fin de la Recepción

***Tiempo de Transmisión del Paquete*= 1**
***Tiempo del Bus en uso*= 1+a**
***Eficiencia*= 1/(1+a)**



Tiempo de Transmisión de Paquetes= 1
Tiempo del bus en uso= 1+a
Eficiencia= 1/(1+a)

Figura 76: Efecto de a en la Utilización: bus bandabase

El evento 2 ocurre después del evento 3 si a>1.0. En cualquier caso, el tiempo total para un "turno" es 1+a, pero el tiempo de transmisión es solamente 1, para una utilización de 1/(1+a).

2.7.2 FACTORES QUE AFECTAN EL RENDIMIENTO

Aqui se lista los factores que afectan el rendimiento de una LAN. Aqui se trata la parte que es independiente de los dispositivos conectados, esos factores que están exclusivamente bajo el control del diseñador de la red local. Los factores más importantes son:

- Capacidad
- Retardo de propagación
- Número de bits por frame
- Protocolos de red local
- Carga ofrecida
- Número de estaciones

Los primeros tres términos ya han sido analizados; ellos determinan el valor de a.

Los siguientes son los protocolos de red local: fisico, acceso al medio y enlace. La capa fisica no es un gran factor; generalmente pueden mantenerse con transmisiones y recepciones con retardos pequeños. La capa de enlace añadirá algunos bits de overhead a cada frame y algo de overhead administrativo, tal como manejo de circuitos virtuales y reconocimientos. Esto deja a la capa de acceso al medio, la cual puede tener un efecto significante en el efecto de la red. Esto se verá más adelante.

Se puede observar que los 3 primeros factores listados que caracterizan a la red son generalmente tratados como constantes o valores dados. El protocolo de red local es el centro del esfuerzo de diseño, la elección que debe ser tomada. Los siguientes dos factores la carga ofrecida y el número de estaciones, tienen que ver con la determinación del rendimiento como una función de estas 2 variables. Note que estas dos variables debe ser tratadas separadamente. Ciertamente es verdad que para una carga fija ofrecida por estación, la carga total ofrecida se incrementa proporcionalmente al número de estaciones. El mismo incremento podria ser alcanzado manteniendo el número de estaciones fijas pero incrementado la carga ofrecida por estación. Sin embargo como se observa, el rendimiento de la red será diferente para estos 2 casos.

Un factor que no estaba en la lista es la tasa de error del canal. Un error en la transmisión necesita una retransmisión. Ya que la tasa de error en las redes locales es baja, esto no es un factor significante.

2.7.3 LÍMITES DEL RENDIMIENTO

El propósito es presentar una técnica simple para determinar los límites del rendimiento de la LAN.

En cualquier LAN hay 3 regiones de operación, basadas en la magnitud de la carga ofrecida.

1. Una región de bajo retardo a través de la red, donde la capacidad es más que la adecuada para manejar la carga ofrecida.
2. Una región de alto retardo, donde la red se vuelve un cuello de botella. En esta región, relativamente se toma más tiempo controlando el acceso a la red y menos en la transmisión de datos actual comparado con la región de bajo retardo.
3. Una región de retardo ilimitado, donde la carga ofrecida excede la capacidad del sistema.

Esta última región es fácilmente identificada. Por ejemplo, considere la siguiente red:

- Capacidad= 1Mbps
- Número de estaciones= 1000
- Tamaño de frame= 1000 bits

Si, en promedio, cada estación genera datos a una tasa excediendo 1 frame/seg, entonces el total de carga ofrecida se excede en 1 Mbps. El retardo en cada estación se reforzará sin límite.

La tercera región es claramente evitada. Pero casi siempre el diseñador deseará evitar aún la segunda región. La segunda región implica un uso ineficiente de la red. Más aún un repentino surgimiento de datos mientras se está en la segunda región ocasionaria los correspondientes incrementos en el ya alto retardo. En la primera región la red no es un cuello de botella, y contribuirá tipicamente solamente con una pequeña cantidad al retardo terminal a terminal.

Así la pregunta crucial es: ¿En qué región operará la red, basado en la carga proyectada y las características de red? La tercera región es fácilmente identificada y evitada; es el límite entre las primeras dos regiones que deben ser identificadas. Si la red opera bajo ese límite no debería ocasionar un cuello de botella de comunicaciones. Se opera sobre el límite, entonces hay una razón para preocuparse y considerar un rediseño. Ahora, el punto es: ¿Cuán precisamente se necesita conocer el límite? La carga en la red variará en el tiempo y sólo puede ser estimada. Ya que la carga estimada no es precisa, no es necesario conocer exactamente dónde está ese límite. Si una buena aproximación del límite puede ser desarrollada, entonces la red puede ser dimensionada de tal manera que la carga estimada esté bajo ese límite. En el ejemplo recién descrito, la carga estimada es 1 Mbps. Si la capacidad de la LAN es

tal que el límite es aproximadamente 4 Mbps, el diseñador puede asegurar que la red no será un cuello de botella.

Con los puntos anteriores en mente, se presenta una técnica para estimar los límites del rendimiento, basado en la aproximación tomada por el comité IEEE 812. Para comenzar, se ignora el protocolo de control de acceso al medio y se desarrolla límites para el Throughput y el retardo como una función del número de estaciones activas. Se necesitan 4 cantidades:

T_{idle}= el tiempo medio en que una estación está inactiva entre los intentos de transmisión: la estación no tiene mensajes en espera de transmisión.

T_{msg}= el tiempo requerido para transmitir un mensaje una vez que se obtiene el acceso al medio.

T_{delay}= el retardo promedio desde el momento en que una estación tiene un paquete para transmitir hasta que se complete la transmisión; incluye tiempo de encolamiento y tiempo de transmisión.

THRU= el throughput total medio en la red de mensajes por unidad de tiempo.

Se asume que hay N estaciones activas, cada una con los mismos requerimientos de generación de carga. Para encontrar un límite superior en el throughput total, considere el caso ideal donde no hay retardo de encolamiento: cada estación transmite cuando está lista. De aquí en adelante cada estación alterna entre inactividad y transmisión con un throughput de $1/(T_{idle} + T_{msg})$. El throughput máximo posible es la suma de los throughput de todas las N estaciones:

$$\mathbf{THRU} \leq \mathbf{N/(T_{idle} + T_{msg})}$$

Este límite se increm7enta a medida que N incrementa, pero es razonable sólo hasta el punto de capacidad propia de la red, la cual puede ser expresada así:

$$\mathbf{THRU} \leq \mathbf{1/T_{msg}}$$

El punto de quiebre entre estos dos límites ocurre en:

$$\mathbf{N/(T_{idle} + T_{msg}) = 1/T_{msg}}$$

$$\mathbf{N= (T_{idle} + T_{msg}) / T_{msg}}$$

Este punto de quiebre define dos regiones de operación. Con el número de estaciones bajo este punto, el sistema no genera suficiente carga para utilizar la capacidad total del sistema. Sin embargo, sobre este punto, la red está saturada: está completamente utilizada y no es posible establecer las demandas de las estaciones conectadas.

Para ver la racionalidad de este punto de quiebre, considere que la capacidad de la red es $1/T_{msg}$. Por ejemplo, si toma un microsegundo transmitir un mensaje, la tasa de datos es 10^6 mensajes por segundo. La cantidad de tráfico generada por N estaciones es $N/(T_{idle} + T_{msg})$. Si el tráfico excede la capacidad de la red, se incrementa el retardo. Note también que el tráfico se incrementa ya sea incrementando el número de estaciones (N) o incrementando la tasa a la que las estaciones transmiten los mensajes (se reduce T_{idle}).

Estas mismas consideraciones permiten tener un límite menor en el retardo.

Claramente
$\mathbf{T_{delay} \geq T_{msg}}$ **(*)**

Ahora, considere que con cualquier carga se mantiene la siguiente relación:
$\mathbf{THRU = N/(T_{idle} + T_{delay})}$ **(**)**

ya que $1/(T_{idle} + T_{delay})$ es el throughput de cada estación, combinando las fórmulas anteriores se tiene
$\mathbf{T_{delay} \geq NT_{msg} - T_{idle}}$

El cálculo de punto de quiebre se obtiene combinando la ecuación anterior y la ecuación (*) se obtiene el mismo resultado que antes.

Tenga en mente que estos límites son asíntotas del verdadero retardo y curvas throughput. El punto de quiebre delimita dos regiones. Bajo el punto de quiebre, la capacidad es sobreutilizada y el retardo es bajo. Sobre el punto de quiebre, la capacidad se satura y el retardo aumenta. En la actualidad, los cambios son más bien graduales que abruptos.

Los límites del otro lado son fácilmente encontrados. El retardo sería maximizado si las N estaciones tuvieran que transmitir un mensaje simultáneamente.
$\mathbf{T_{delay} \leq NT_{msg}}$

Combinando con (**) se obtiene:

$\mathbf{THRU \geq N/(T_{idle} + NT_{msg})}$

Estos límites dan una idea del comportamiento del sistema. Permiten hacer un cálculo simple para determinar si un sistema propuesto está dentro de los límites razonables. Si la respuesta es no, mucho análisis se puede ahorrar. Si es sí, el análisis debe ser más profundo.

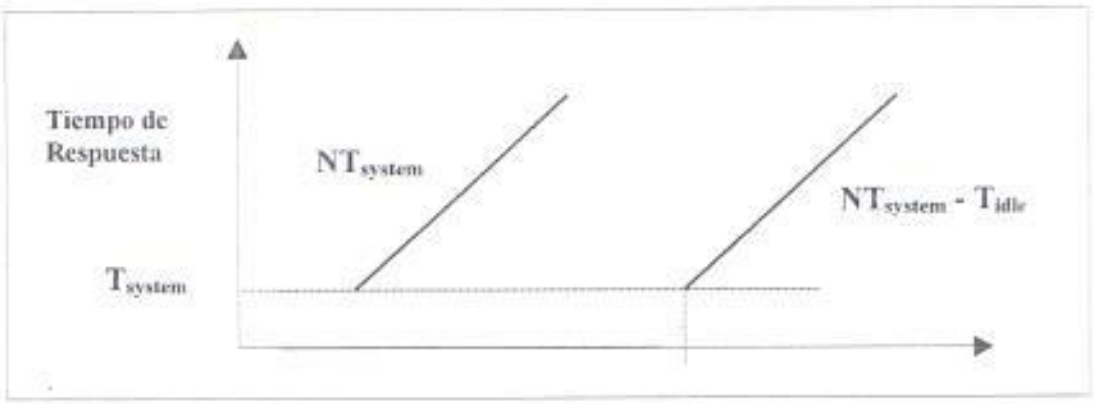


Figura 77: Gráfico de límites de operación en una LAN

Dos ejemplos aclararán el uso de estas estaciones. Primero, considere una estación de trabajo conectada a una red 1 Mbps que genera, en promedio, 3 mensajes por minuto, con mensajes promedios de 500 bit. Con el tiempo de transmisión de mensajes igual a 500μseg, el tiempo de inactividad medio es 20 segundos. El punto de quiebre de las estaciones es:

$N=20/500x10^{-6}$ = 40.000 estaciones

Si el número de estaciones es menor que esto, es decir 1000, la congestión no sería un problema. Si es mucho más, 100.000, la congestión podría ser un problema.

Segundo, considere un conjunto de estaciones que generan paquetes de voz digitalizada PCM en una red local de 10 Mbps. Los datos son generados a una tasa de 64 Kbps. Para 0.1 paquetes, se tiene un tiempo de transmisión por paquete de 640 μseg. Así

$N= 0.1/(640x10^{-6})$ = 156 estaciones

Generalmente, no se espera que todas las estaciones de voz (teléfonos) estén activas al mismo tiempo; probablemente ¼ de ellas es una estimación razonable, así que el punto de quiebre está alrededor de 600 estaciones.

Note que en ambos ejemplos, rápidamente se ha llegado al dimensionamiento de primer orden del sistema con un planeamiento perfecto. Una manera de incluir el overhead es reemplazar T_{msg} con T_{sys} donde la última cantidad incluye una estimación del overhead por paquete.

Se puede tener un manejo del rendimiento más preciso, considerando el protocolo involucrado.

2.8 EQUIPOS DE COMUNICACIÓN:BRIDGES

- Dispositivos que permiten descongestionar el tráfico, creando segmentos independientes en una Red.

- Mejorando tiempo de respuesta de la Red y su rendimiento total.

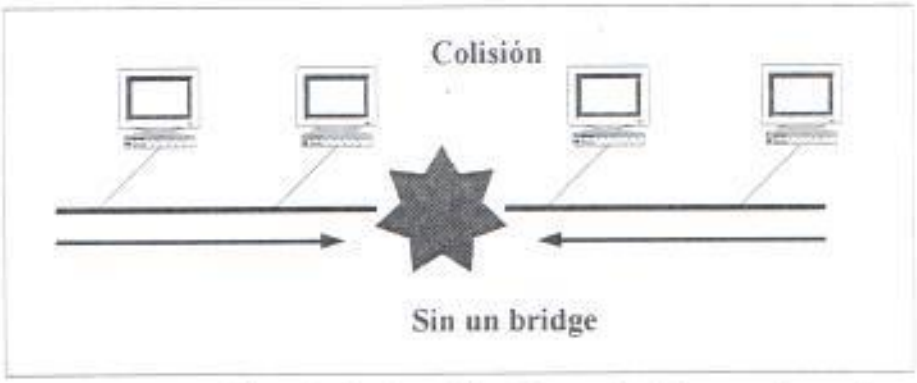


Figura 78: Ilustración de la función de un bridge en la red

Los dispositivos más simples de redes LAN es el brigde. Este dispositivo se diseña para el uso entre las redes de área local (LANS) que usa protocolos idénticos para las capas de acceso físico y de medio. Porque todos estos dispositivos usan los mismos protocolos, la cantidad requerido de procesamiento del bridge es mínima.

El bridge desempeña las funciones siguientes:

- Lee todos los paquetes de datos transmitidos hacia A, y aceptar estas direcciones en las estaciones en B.
- Usando el protocolo de control de acceso al medio para B, retransmitir los paquetes de datos hacia B.
- Hacer lo mismo para el tránsito de B hacia A.

El bridge provee una extensión a la LAN, que no requiere modificación en el software de comunicaciones en las estaciones adjuntas a las LANs. En todas las estaciones en dos o más LAN en que cada estación tiene una dirección única. La estación que usan una dirección única y no necesita explícitamente discriminarse entre estaciones sobre la misma LAN y estaciones sobre otras LANs; los bridges tienen cuidado de esto.

El bridge sólo tiene dos capas únicas 1 y 2 en el modelo OSI. En el efecto, el bridge opera en la capa 2. La capa 3 y más arriba deben ser idéntificadas en los dos sistemas para finalizar exitosamente la comunicación.

El bridge es usado en una situación en el cual todas las LAN tienen las mismas caracteristicas, el lector puede preguntarse por que dividir a la LAN en varias partes y por que no hacer una simple LAN. Dependiendo de las circunstancias, aquí hay varias razones para el uso de múltiples LANs conectadas por bridges.

Confiabilidad.- El peligro en conectar todos los dispositivos de datos en una organización y tener el peligro en que una falla sobre la red y esto puede causar desabilitar la comunicación en toda la red. Por bridges, la red puede ser particionada.

Performace.- En general, el desempeño sobre un LAN declina con el incremento en el número de dispositivos. Un número menor de LANs dará frecuentemente mejor desempeño.

Seguridad.- El establecimiento de múltiples LANs puede mejorar la seguridad de comunicaciones. Es deseable para guardar diferentes tipos de tráfico que necesitan diferente seguridad y deben estar separados fisicamente por medios. A la vez, los diferentes usuarios con niveles diferentes de seguridad necesitan comunicar con mecanismos controlados y monitoreados.

Geografia.- Claramente, dos LANS separadas se necesitan apoyar en dispositivos agrupados en dos ubicaciones geográficamente distantes. En el caso de dos de edificios separado por una carretera, puede ser lejos más fácil usar un enlace de microonda que intentar usar un cable coaxial entre dos edificios. En el caso de redes ampliamente separadas, dos " bridges" se necesitan.

La descripción de arriba ha aplicado al tipo de los más simple bridges. Los puentes más sofisticados pueden usarse en más complejas redes de area local (LANs). Estos incluirian funciones adicionales, tal como:

Cada bridge puede mantener la información en otros bridges, ambos con el costo y número de saltos de bridge a brigde requeridos para unir cada red. Esta información puede ser actualizada por cambios periódo de información entre bridges. Esto permite que los bridges puedan desempeñar una función de ruteo derrotando.

Un control de mecanismo puede administrar bancos de datos en cada bridge para superar congestión. Bajo las condiciones de saturación, el puente puede dar la prioridad a paquetes, en ruta a nuevos paquetes que simplemente van entrando en el Internet desde un LAN adjunta, asi conservando la inversión la anchura de banda de linea y procesar el tiempo que hace para enrutar el paquete.

2.8.1 ARQUITECTURA DEL PROTOCOLO USADO POR BRIDGE

La especificación de IEEE 802.1D define la arquitectura del protocolo para la MAC de los bridges. Además, el estándar sugiere formatos para una administración globalde estaciones de direcciones MAC a través de múltiples LANs homogéneas. En esta subsección se examina la arquitectura del protocolo de estos bridges dentro de la arquitectura 802, las estaciones de dirección esta diseñada en el nivel MAC. En el nivel LLC, solo la dirección SAP es especificada. Asi está en el nivel MAC que un bridge puede funcionar. La figura 14.2 muestra el caso más simple, que consiste de dos LANS conectado por un puente único. El LANs emplea el mismos protocolos MAC y LLC. El bridge opera como se describe anterioramente. Un paquete MAC cuando el destino no esta en la LAN inmediata es capturado por el bridge, temporalmente en el base, y entonces transmitido por otro LAN. Hasta la capa LLC es importante, aqui existe un diálogo entre la LLC y los puntos finales de la estación. El bridge no necesita contener una capa LLC, puesto que meramente esta trasmitiendo los paquetes de datos MAC.

La figura 14.2b indica la manera en que datos son encapsulados usando un bridge. Los Datos son proveidos por algún usuario a LLC. La entidad LLC añade una cabecera y pasa la unidad resultante de datos a la entidad MAC, el cual añade una cabecera el lleva a formar un paquetes de datos MAC. En base del destino de la dirección MAC, es capturado por el bridge. El puente no despoja fuera los campos MAC; su función está transmitir los paquetes de datos MAC intacto hacia el destino LAN. Asi el paquete de datos depositado en el destino LAN y capturado por la estación de destino.

2.8.2 EL ENLACE CON BRIDGES

En la configuración de la figura 14.1, el bridge tiene la decisión de transmitir un paquete de datos basándose en la dirección destino MAC. En una más compleja configuración, solo tiene la misión de enviar los datos. Considere la configuración de figura 14.5. Suponga que la estación 1 transmite un paquete de datos en una LAN destinada a la estación 5. El paquete de datos será leido por ambos bridges 101 y 102. Para cada bridge la estación dirigida no esta sobre un LAN al que el puente esta adjunto. Por lo tanto, cada bridge debe hacer una decisión con respecto a si mismo o no retrasmitir el paquete de datos sobre otra LAN, con el proposito de cerrar el enlace lo más rapido posible llegando al destino indicado. En este caso, el puente 101 deberia repetir el paquete de datos sobre LAN B, considerando el bridge 102 deberia repetir la retransmisión del paquete de datos. Una vez el paquete de datos se ha transmitido sobre LAN B, será recobrado por ambos puentes 103 y 104. Nuevamente, cada uno debe decidir si remitir o no el paquete de datos. En este caso, el puente 104 deberia retransmitir el paquete de datos sobre la LAN E, donde será recibido por el destino, estacionado 5.

Asi se observa que en el caso general, el bridge debe equiparse con una capacidad de enviar. Cuando un bridge recibe un paquete de datos, debe decidir si remitir o no el paqeute de datos. Si el bridge es adjunto a dos o más redes, debe decidir si o no remitir el paqeute de datos, y asi, sobre cual LAN el paquete de datos deberia transmitirse.

La decisión enviar no puede ser siempre simple. En la figura 14.6, el puente 107 se agrega a la configuración previa, directamente vinculando LAN A y LAN E. En este caso, si la estación 1 transmite un paquete de datos sobre LAN A destinada a estación 5 sobre LAN E, otro bridge 101 o bridge 107 podra remitir el paquete de datos. Apareceria preferible que el puente 107 remita el paquete de datos, esto involucrará uno único "brinca", considerando si el paquete de datos viaja mediante el puente 101, debe sufrir dos brincos. Otra consideración es que puede haber cambios en la configuración. Se puede decir que la capacidad enviar debe tomar en cuenta la topologia de la red y se puede necesitar alterar dinámicamente.

Un bridge sabe la identificación de cada estación sobre cada LAN. En una configuración grande, tal arreglo es abultado, además, como las estaciones se agregan a y bajadas desde LANs, todas las estaciones de todos los directorios deben ser actualizada. Facilitaria el desarrollo de una capacidad de enviar si todos los niveles de las direcciones MAC. Por ejemplo, el estándar 802.5 sugiere 16 bits para las direcciones MAC estas consisten de una 7 bits número de la LAN y 8 bits del número de la estación y la dirección de 48 bits, consiste de 14 bits para número de la LAN y 32 bits para el número de la estación.

Una variedad de estrategias para enviar ha sido implementada en el año reciente. La más simple y común estrategia, es fijar enlaces. Esta estrategia es apropiada para redes pequeñas de Internet y para redes que son relativamente estables. Recientemente, dos grupos en el comité IEEE 802 desarrolló especificaciones para diseñar derrotar estrategias. El grupo IEEE 802.1 ha emitido una estrategia para enviar paquetes de datos usando algoritmo. El comité Token Ring, IEEE 802.5, ha emitido su propia especificación, referido al envió de la fuente. Se observa que estas tres de estrategias a la vez.

2.8.3 RELACION DE LOS BRIDGES CON IEEE 802

- Un bridge opera al nivel de capa MAC:
  - Sólo "interpreta" direcciones MAC.
  - No le interesan las direcciones de capas superiores.
    - Direcciones de capa de red y de mayor nivel.

- Muchas veces se los llaman "dispositivos independientes de protocolo"
  - Quiere decir independiente de los Protocolos de Red.
  - En realidad si son dependientes, pero los protocolos de capa MAC.

2.8.4 DISPOSITIVOS DEPENDIENTES DEL PROTOCOLO

- Dependen de si "entienden o no" los protocolos MAC de las interfaces conectadas (802.3, 802.5, FDDI, etc.)
- Los bridges tienen la "opción" de "traducir o no" de un protocolo MAC u otro, aunque no siempre toman esa opción.

Figura 79: Ilustración de la comunicación entre el bridge y las subredes

2.8.5 CLASIFICACION Y APLICACIONES

- Los bridges prácticamente han dejado de existir como dispositivos dedicados a la tarea de "puenteo".
  - Excepciones: ambientes Token-Ring.
- Actualmente los bridges han sido reemplazados por los Switching Hubs.
- Sin embargo, la función de puenteo no ha desaparecido, y viene incluida en los routers.
  - Dispositivos pueden ser configurados como B. O R.
- Por su forma de ruteo.
  - Transparent/Spanning-tree.
  - Source Routing.
  - Source Routing Transparent(SRT).

2.8.6 BRIDGES TRANSPARENT/SPANNING-TREE

- Diseñado para operar en ambientes Ethernet.
- Mantiene una Tabla de Direcciones con los segmentos y sus respectivos nodos.
- Las interfases de un B.T. siempre operan en modo promiscuo osea capturan todo paquete que llega a ellos.
  - Aceptan todo paquete que llega.
  - Una interfase "normal" rechazaria un paquete que no está dirigido a ella.
- La promiscuidad es una de las claves de la operación de un B.T.
  - Es lo que le permite construir su Tabla de Direcciones.
  - Al encendido, la Tabla está vacia, por lo que tiene que aplicar procedimiento de aprender direcciones.
  - Por cada paquete Rx , almacena en la Tabla su dirección y el puerto por el que llegó.
  - Se realiza un broadcast cuando ningún terminal no transmite nada y el bridge pregunta la dirección fisica a cada terminal.
- Llamados transparentes por 2 motivos:
  - No cambian el contenido de los paquetes.
    - Paquetes circulan sin alteraciones.
    - "Inteligencia de ruteo" (Tabla de direcciones y la lógica para procesarla) reside en el Bridge.
- Llamados Spanning-Tree ya que usan algoritmo de eliminación de lazos del mismo nombre.

2.8.7 ALGORITMO SPANNING TREE

- Lazos pueden ser buenos.
  - Aumentan la confiabilidad general del sistema.
    - Ofrecen caminos alternos para llegar de una red a otra.
    - Si uno falla, el otro lo reemplazaria.
- El problema es que el lazo puede volverse infinito.
- Algoritmo descompone los lazos, generando un árbol.

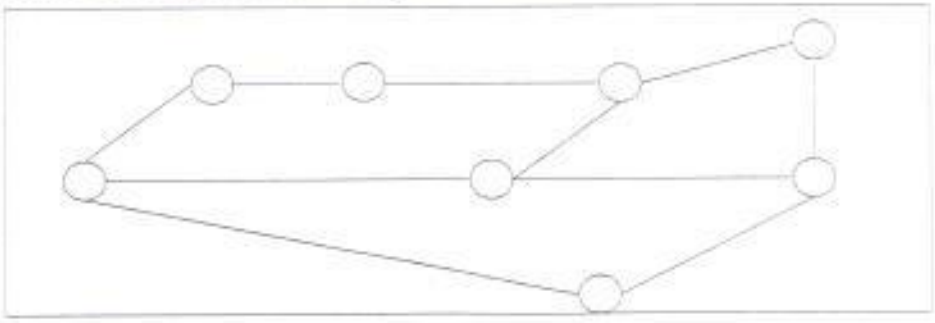


Figura 80: Ilustración de una red antes de aplicar el algoritmo de Spanning Tree

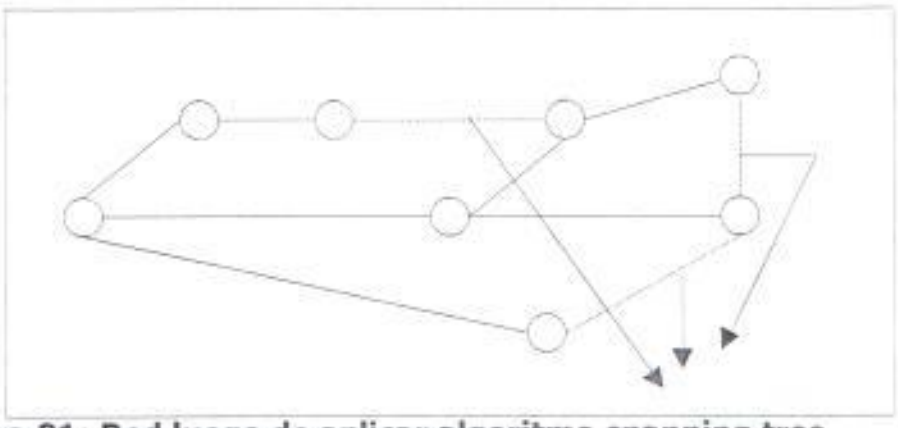


Figura 81: Red luego de aplicar algoritmo spanning tree

2.8.8 EFECTOS DE LOS BROADCASTS

- Los broadcast solucionan un problema, pero generan otros:
  - Exceso de tráfico.
    - Resta posibilidades de transmitir a otros nodos.
    - Pobre utilización efectiva de Enlaces Remotos.
- Interrupción del CPU.

Solución al problema de los broadcasts:

- Para "eliminar" el tráfico "broadcast", espcialmente de enlaces remotos es usar ruteadores.
  - No "repite" los paquetes a otro segmento, al menos que su Dirección de Red (IP, IPX) así lo indique.

- Los puertos deshabilitados son habilitados automáticamente, en caso de falla de puerto principal.
- Busca que las ramas tengan longuitud mínima.

2.9 RUTEADORES

- Los ruteadores son dispositivos que operan al nivel de la capa de la red.
  - Deben saber que están ruteando.
  - Los protocolos soportados deben ser ruteables.
- Realiza 2 tareas principales:
  - Conmutación de paquetes
  - La determinación de direcciones

Los ruteadores en una red de internet son responsables por recibir y enviar paquetes en un conjunto interconectado de subredes. Cada ruteador está diseñado para tomar

decisiones basado en el conocimiento de la topologia y condiciones de la red internet. En una simple red de internet, es posible un enlace fijo. En internet más complejas, un grado de cooperación dinámica se necesita entre los ruteadores. En particular, el ruteador debe enviar porciones de la red para que no falle y para descongestionar la red. Para realizar tales decisiones dinámicamente, los ruteadores cambian la información de ruteo usando un protocolo especial de ruteo para este propósito. Esta información se necesita para saber la condición de la red Internet, en términos de cuáles redes pueden ser accesadas por los ruteadores, y las caracteristicas de demora de diversas rutas.

En consideración la función de enviar de los ruteadores, es importante para distinguir dos de estos conceptos:

- **La información de enlace**: la información sobre las topologias y retardos de la red de internet.

- **Algoritmo de ruteo**: el algoritmo usado para tomar una decisión de ruteo para un datagrama en particular, basado en el flujo de información.

Hay otra manera de particionar el problema en forma útil desde el punto de vista de ambas localidades de funciones de ruteo y una estandarización efectiva. Esta es la función de partición de ruteo:

- Ruteo entre sistemas de Terminales (ESs) y ruteadores.
- Ruteo entre ruteadores.

La razón para la partición es que hay las diferencias fundamentales entre un ES conocido para el envio de paquetes y un ruteador conocido. En el caso de un ES, debe el primero saber si el destino ES es el mismo de la subred. Y asi, los datos pueden entregarse directamente usando el protocolo de subred de acceso. Si no, los ES deben remitir los datos al ruteador adjunto al mismo subred. Si hay más de un ruteador, es simplemente una manera de elegir uno. Los datagramas enviados por el ruteador en nombre de otros sistemas y necesitan tener alguna idea de la topologia de la red a fin de tomar una decisión de ruteo global.

El propósito general de este dispositivo es que puede usarse para conectar redes no semejantes y que opera en la capa 3 del modelo OSI y que es conocido como ruteador. El ruteador deber ser capaz de arreglar con una variedad de diferencias entre redes, incluyendo:

- **Direccionamiento de esquemas-** Las redes pueden usar diferentes esquemas para la asignación de direcciones para los dispositivos. Por ejemplo, en la LAN IEEE 802 usa direcciones de 16 o 48 bits en binario por cada dispositivo adjunto. Alguna forma de proveer el direccionamiento global de la red, es tener un buen servicio de direccionamiento.

- **El tamaño máximo de los datos**. - Los paquetes desde una red tienen que ser repartidos en partes menores para ser transmitidos sobre otra red, un proceso conocido como segmentación. Por ejemplo, Ethernet impone un tamaño máximo de datos de 1500 bytes.

- **Interfaces**. - Las interfaces de software y hardware para diferentes redes. El concepto de ruteador debe ser independiente de estas diferencias.

- **Confiabilidad**. - Varios servicios de red pueden proveer cualquier cosa con el fin de que sea confiable el circuito virtual punto a punto en un servicio no confiable. La operatividad de los ruteadores no depende de una suposición de la confiabilidad de la red.

El bridge puede distinguir segmentos, pero no "redes lógicas". Para poder "crear y diferenciar" Redes lógicas, se usan Ruteadores.
El ruteador opera al nivel de Capa de Red.

- No le importa si las capas MAC son distintas.

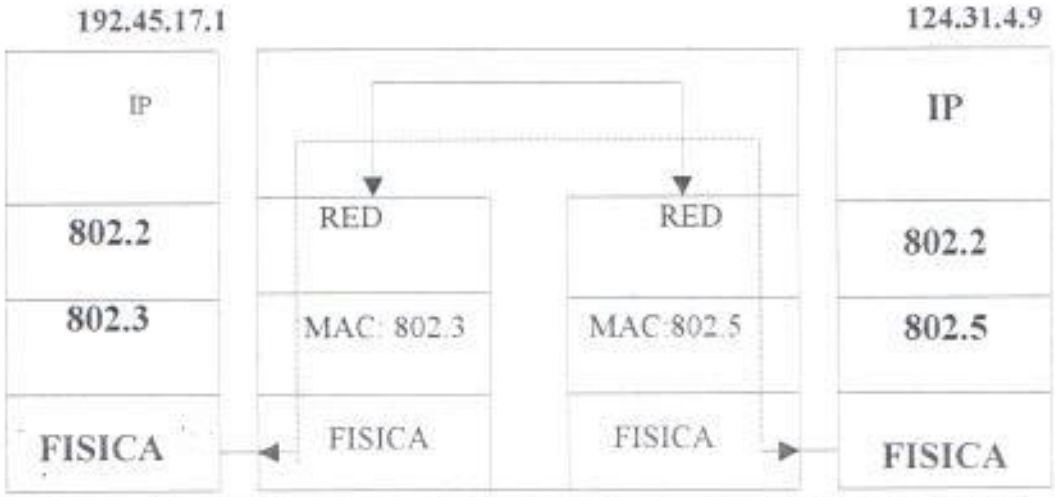


Figura 82: Ilustración de la comunicación entre el router y la red

2.9.1 FUNCIONES PRINCIPALES DE LOS RUTEADORES

- La segmentación lógica de redes
  - Mantenimiento de direcciones lógicas únicas de las redes, y de los nodos dentro de ellas.
- Control de Congestión
  - En dos formas: Segmentación + Reducción del Broadcast
- Enrutamiento

- Redundancia, balanceo de carga
- Control de seguridad

Permite definir quién puede, y quién no puede tener acceso a determinadas subredes o nodos.

Qué necesita el ruteador?

- Manejar protocolos de capa física y de enlace de datos necesarios en sus puertos.
- Entender direcciones físicas.
- Manejar direcciones lógicas.
- Resolver de direcciones físicas a lógicas y viceversa.

2.9.2 TIPOS DE RUTEO

- Cada red puede tener diferente topología y características físicas.
- Ruteo directo
  - Tiene que ver con la transmisión de paquetes en una misma red física.
- Ruteo indirecto
  - Tiene que ver con la transmisión de paquetes entre 2 máquinas que se encuentran en redes IP diferentes.

2.9.3 CLASIFICACION DE ROUTERS

- Por la capacidad y/o tamaño.
  - Centrales, más número de puertos, mayor poder de procesamiento.
  - Periféricos (Dedicados y Dial Up), organiza de un banco 2 o 3 redes de área local.

- Por la forma de implementación:
  - Software Based (computador + software de emulación).
  - Hardware Based (dispositivo dedicado).

- Por el alcance.
  - Internos.
  - De frontera.
  - De Backbone.

2.9.3.1 ROUTERS SEGÚN EL ALCANCE

- Interiores
  - Segmentos (redes) directos, pertenecen a la misma area
    - Ruteo sólo para su area: Transmisiones fuera de su area son enviadas al Router de Frontera de Area. (Si existe)

- Frontera de Area.
  - Segmentos directos, pertenecen a más de un Area.
    - Ruteo para todas las Areas, y para el Router de Backbone.
      - Si existiera

- Backbone.
  - Conecta a todas las Areas de la Red.

Otras caracteristicas de routers:
- Redes multiprotocolo.
- Gran capacidad de procesamiento.
  - Medida en PPS (paquetes por segundo)
- Facilidad de administración.
  - Via terminal (basado en texto) o Gráfica.
- Traslación de direcciones.
- Expandibilidad.
  - Número de puertos, memoria, funcionalidad.

2.9.4 CARACTERISTICAS DE PROTOCOLOS DE RUTEO

- Simple.
- Preciso: Decisiones consistentes y acertadas.
- Confiable (rápida recuperación, robusto)
- Adaptable (rápido y eficiente para adaptarse a cambios topológicos).

2.9.5 PROTOCOLOS RUTEABLES VS PROTOCOLOS DE RUTEO

- Una "confusión" muy común se produce con los términos "Protocolos de ruteo" y "Protocolos ruteables"

- Los protocolos de ruteo, son aquellos que permiten generar y propagar las Tablas de ruteo de on ruteador.

2.10 SWITCHING HUBS

- Los switching Hubs son semejantes a los bridges.
  - Operan al nivel de MAC.
  - Comparten algunas de sus limitaciones.
    - Direcciones lógicas.

- Actualmente muchos fabricantes de Switching Hubs los están haciendo semejantes a Routers.
  - Ya no operarian sólo a nivel MAC, sino también a nivel de Capa de Red.
    - Capacidad de entender direcciones de capa de red.
  - Serian casi equivalentes a un routers, aunque sin llegar a tener otras propiedades inportante de los ruteadores.
    - Tienen limitado control de seguridad.
- Dispositivos conocidos como Switch Routers.
- Combinan las ventajas de Ruteadores y Switches.
  Ejemplo: IBM 8273 permiten tener redes virtuales.

2.10.1 CLASIFICACION DE SWITCHING HUBS

- Por su capacidad: Numero de dispositivos soportados.
  - Trabajo en grupo: Pocos puertos y poca capacidad del Backplane. Util para un grupo pequeño de usuarios (pequeña empresa).
  - Departamental: Empresas más grandes (100-500 usuarios)
  - Enterprise: Para empresas de gran tamaño.

- Por los tipos de puertos empleados.
  - Segmentado: soporta varios nodos en un puerto del Hub.
  - Puertos: permite un solo nodo por puerto del Hub.
  - Full-Duplex: igual que puertos, permitiendo transmisión y recepción a la vez.

- Por la tecnologia de commutación:

2.10.1.1 STORE & FORWARD.

- Almacenan temporalmente los paquetes recibidos, a fin de verificar posibles errores (CRC).
- Equivalentes a un Bridge (requieren tablas de direcciones).
- Ventajas.
  - No propagan los errores.
  - Permiten interfaces de diferentes velocidades.

- Soportan funciones avanzadas. Como por ejemplo virtual LANs y tiene un control de seguridad.
- Desventajas.
  - Alto tiempo de conmutación: 51 – 1.200 microseg.
- Alta latencia.
- No propagan errores.
- Gran funcionalidad.
- Permite interfaces de distintas velocidades.
- Pueden combinar diferentes tecnologías LAN: Ethernet, FDDI, etc.

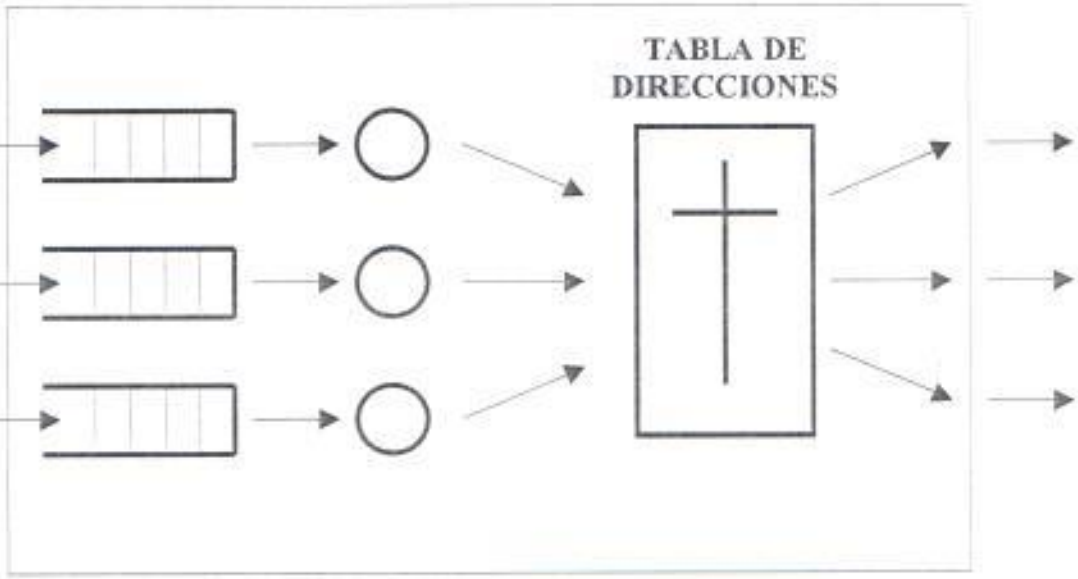


Figura 83: Ilustración de almacenamiento en Buffer temporal hasta que todo el Paquete halla llegado. Delay: 51 – 1.200 micro seg.

2.10.1..2 CUT-THROUGH

- No almacenan el paquete completo.
- Sólo verifican los primeros bytes (La cabecera que contiene la dirección) e inmediatamente hacen el respectivo Switch.
- Ventajas:
  - Bajo tiempo de conmutación: 40 – 70 microseg.
  - Hasta 30 veces más rápido que Store & Forward.
  - No significa que la red operará 30 veces más rápido.
- Desventajas
  - Propagan los frames de errores.
    - No es tan grave sino mayores problemas de ruido.
  - Todas las interfaces deben ser de igual velocidad.
  - Menor funcionalidad que un Switch Store & Forward.

- Baja latencia.
- Propagan errores.
- Limitada funcionalidad.
- Sus interfaces deben ser de igual velocidad.
- Todo puerto debe ser de la misma tecnología.

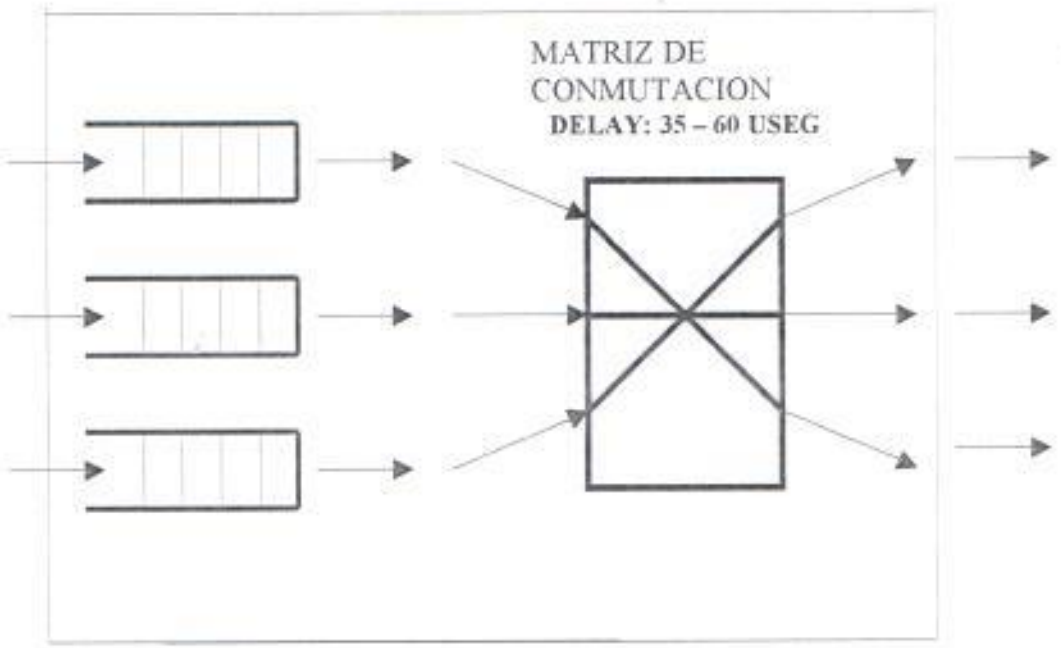


Figura 84: Ilustración del Cut-Through. Sólo basta con recibir los Primeros 8 bytes. Delay: – 6.4 micro seg.

3. DESCRIPCION, ANALISIS Y DIAGNOSTICO DE LA RED ACTUAL

Aqui podemos observar un diagrama general de la red. En primer lugar distinguimos que es una topologia de barra. Al observar los enlaces, vemos que son 3 satelitales: dos en Guayaquil y 1 en Quito. El enlace en Quito tiene las mismas caracteristicas y posición que uno de Guayaquil, el que está conectado con el PanAmSat, que veremos posteriormente. Se tienen dos enlaces satelitales, en caso de no contar con alguno, todos los clientes se conectarian internacionalmente por sólo 1 satélite. Ambos están enlazados con Miami, donde podemos navegar en toda la gran red mundial de Internet. Asi también descongestionamos el enlace y además la conexión va a ser mucho más rápida para el cliente. También posee otros 2 enlaces: el primero microondas, el cual tiene la prioridad, para comunicar los equipos de Kennedy con Urdesa. A través de este enlace se puede enviar voz, datos, fax, video, etc. Tiene una mayor capacidad de envio de datos. El otro enlace es alternativo, porque a pesar de tener mayor velocidad, 2 Mbps, sólo tiene capacidad de enviar datos y tiene menor capacidad de magnitud de paquetes. Posteriormente explicaremos detalladamente las rutas que tomaremos.

Además, existe una consola en Urdesa con lenguaje Unix, desde la cual monitoreamos, cambiamos rutas, controlamos equipos y enlaces, configuramos la entrada y salida de la red de los clientes. En Kennedy, existen otros terminales para realizar estas mismas funciones mencionadas. Además observamos las velocidades a las que trabajamos, y los medio que usamos como cable coaxial, canal digital, par trenzado para el sistema telefónico, y de acuerdo a los equipos utilizados, los cuales describiremos posteriormente, utilizamos conectores RJ-45 EIA/TIA 568, RJ11, interfaces V.35 para puertos sincrónicos, V.34 para puertos asincrónicos

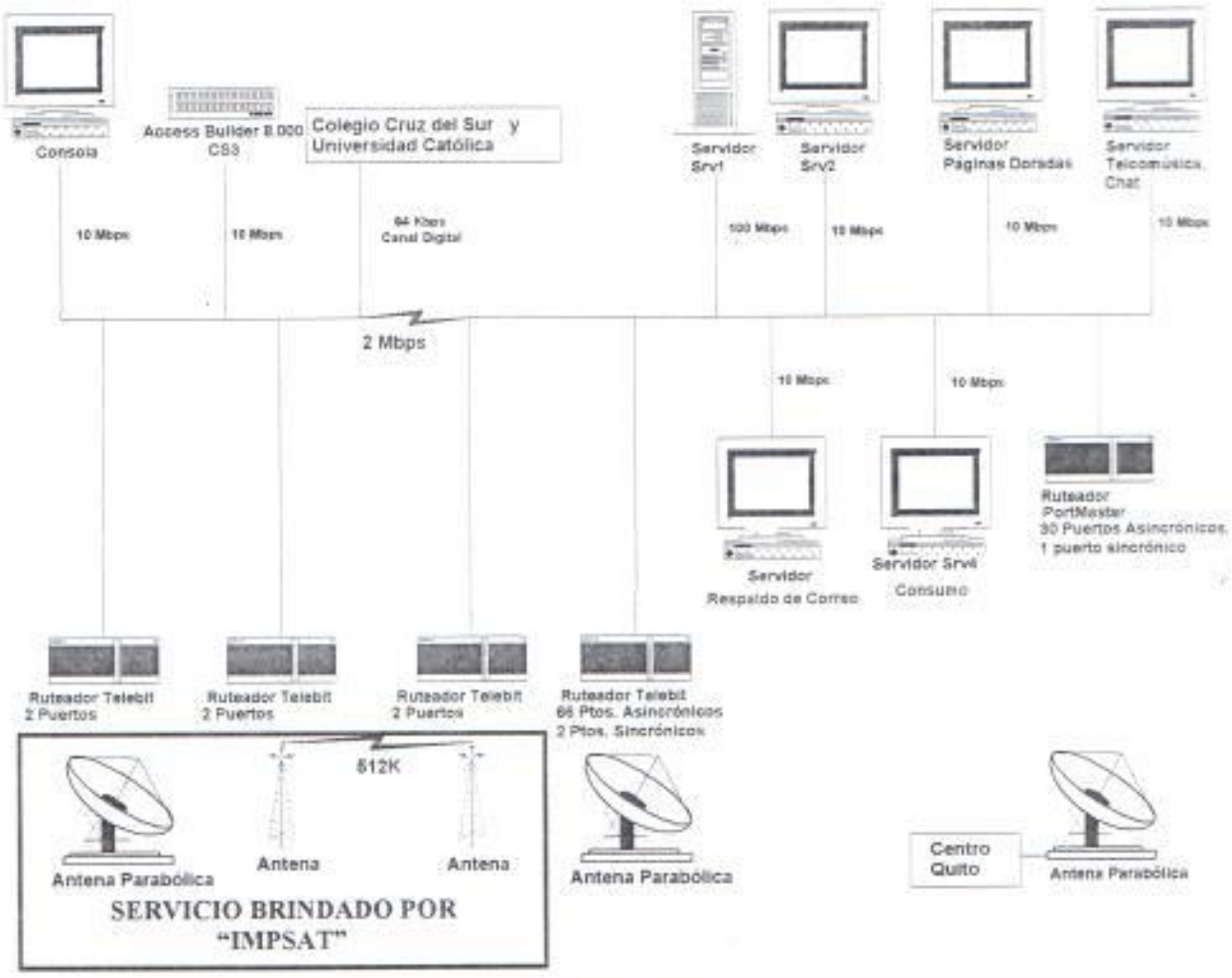


Figura 85: Ilustración General de la Red

3.1. SISTEMA TELEFÓNICO DE URDESA Y KENNEDY

El gráfico mostrado pertenece a los equipos de lineas analógicas, que luego fueron cambiadas a digitales por la Empresa Estatal de Telecomunicaciones (EMETEL) ahora PACIFCTEL, que son 86, por ello utilizan 4 Paneles Telefónicos "Patch Panel" Ortronics de 24 pares telefónicos, que nos dan en total 96, por lo que 10 pares quedan libres. Pacifictel nos genera los 86 pares en cable par trenzado, conectándose los usuarios a través del número 299777. Los 86 pares son el número de usuarios que pueden conectarse al mismo tiempo via dial-up, y para hacerlo, los clientes deben poseer un módem en su computadora personal, y se comunican con uno los 86 módem de 28.8 K de velocidad que especificamos en el gráfico.

Figura 86: Sistema telefónico

Estos módem, una vez enlazados, están directamente conectados con los 2 ruteadores, uno Telebit de 66 puertos asincrónicos y otro Livingston de 30 puertos asincrónicos que nos dan un total de 96. Así tenemos una conexión permanente con el usuario. Ambos ruteadores están conectados a un LinkSwitch 3000, así como todos los servidores. El ruteador Telebit está conectado sincrónicamente al Módem Satelital, a través de V.35. Aquí también podemos observar otro ruteador Telebit de 2 puertos sincrónicos, que nos sirve para conectarnos al módem sincrónico digital (radial), para el enlace microondas, a través de V.35. Esta parte se encuentra en los equipos que se encuentran en la Central Kennedy. Los módem y ruteadores están descritos posteriormente.

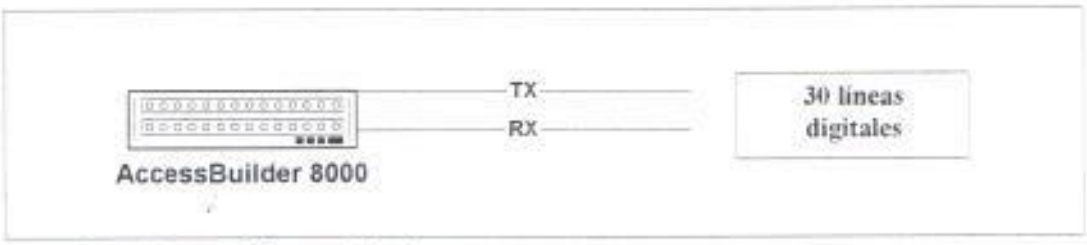


Figura 87: Conexión en Urdesa

En la central Urdesa, la forma de conexión es diferente. Tenemos 30 líneas digitales, que nos envía Pacifictel en 2 cables coaxiales, uno para transmisión y otro para recepción, en forma multiplexada, y que este equipo, AccesBuilder 8000 nos demultiplexa, enlaza a través de los módem a los usuarios, al mismo tiempo nos rutea y trabaja como servidor de comunicaciones. Así vemos la diferencia con la anterior forma analógica de conexión. Las características del AccesBuilder 8000 también se describen posteriormente en forma detallada.

Como vemos, la mejor forma de conexión, tanto por el ahorro de equipos y por rapidez de conexión, es de esta manera con líneas digitales.

3.2. SISTEMA SATELITAL DE URDESA Y KENNEDY

El sistema satelital consta de 2 enlaces con Miami: el uno brindado por PanAmSat y el otro por Impsat. El gráfico muestra las características técnicas del enlace con PanAmSat. Las frecuencias son: 6 GHz de subida y 4 GHz de bajada. La antena se encuentra ubicada en la Central Kennedy.

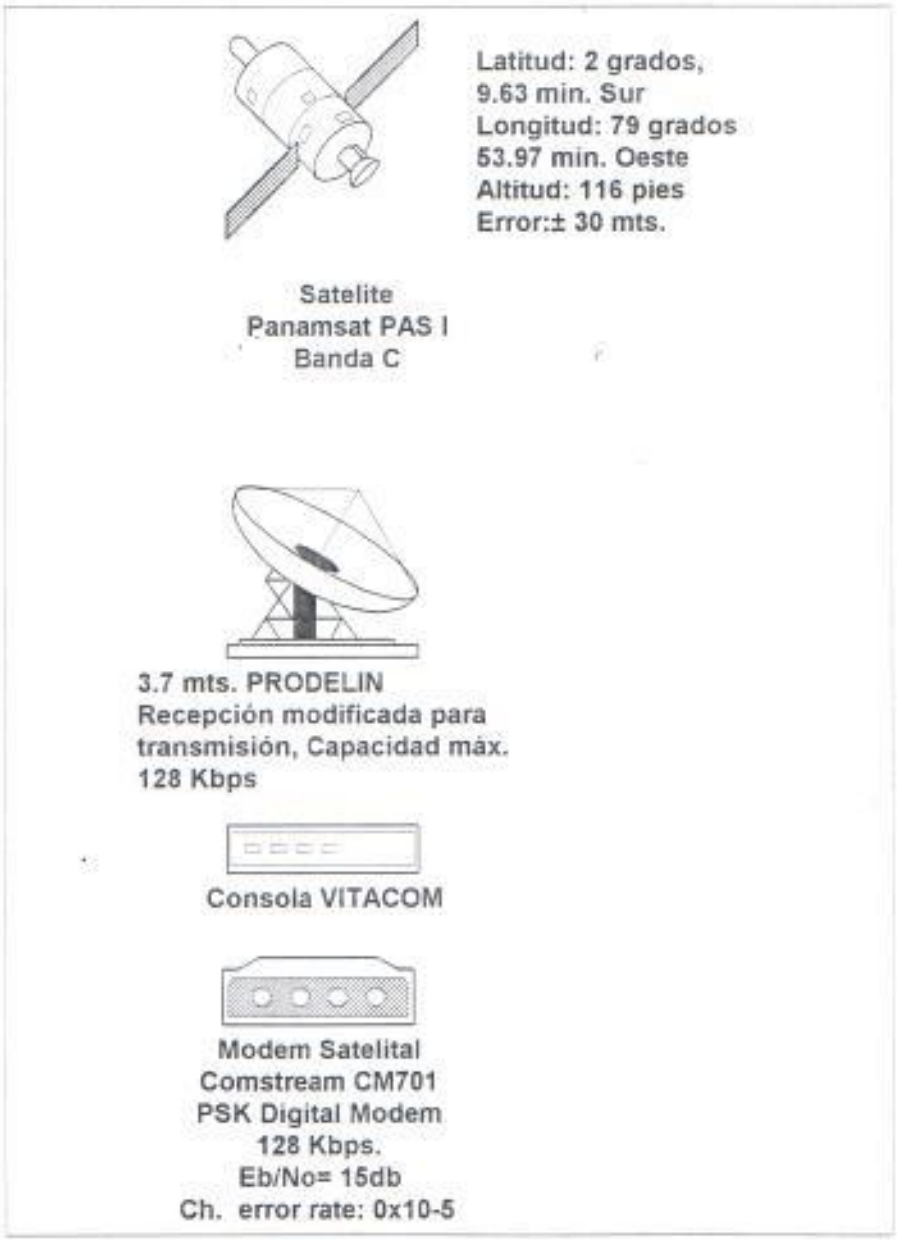


Figura 88: Ilustración del enlace satelital

El módem satelital está conectado al puerto sincrónico del ruteador Telebit Netblazer. En Quito, la conexión satelital es exactamente igual, inclusive la ubicación de su antena y características son las mismas. El otro servicio satelital es brindado por Impsat, tiene una velocidad de 128Kbps.

3.3. SISTEMA DE RADIO

- **Enlace Microondas**

La velocidad del enlace es 512K y tiene un frecuencia de operación de 23 GHz. Posee mayor área de cobertura por su gran anchura de banda. Su transmisión es síncronica. Sus usos son para servicios telefónicos, datos, voz, fax. El enlace está direccionado desde la Central Kennedy hasta la de Urdesa.

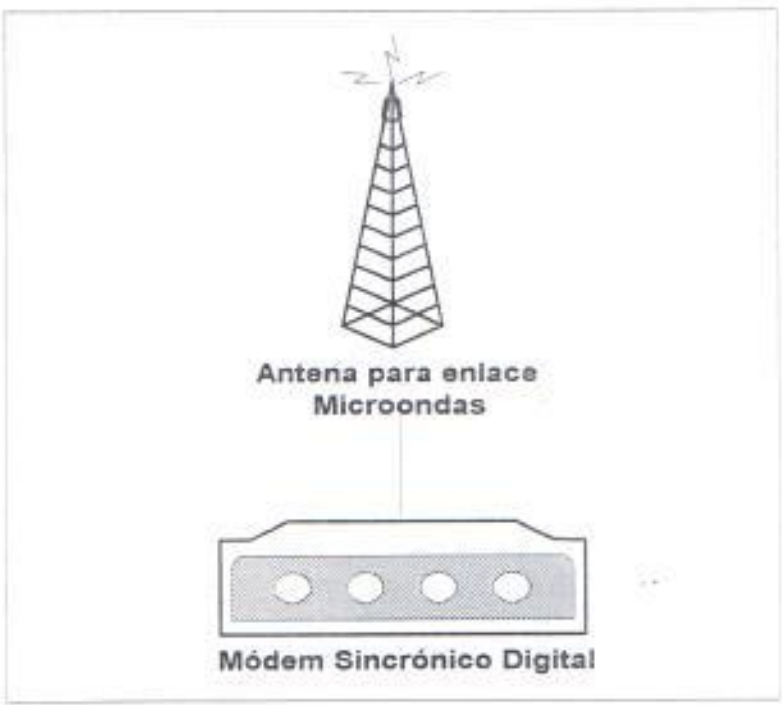
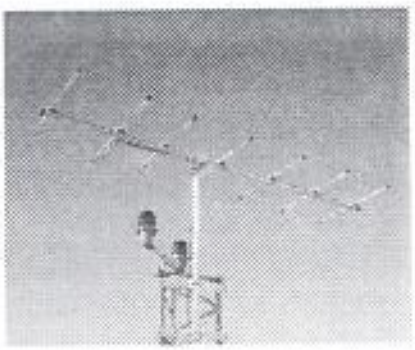


Figura 89: Enlace Microondas

➢ **Enlace Radial**

Este enlace trabaja a una velocidad de 2 Mbps. También comunica la Central Kennedy con Urdesa, con la gran diferencia que éste es un enlace alternativo, que sólo transmite datos, más no fax, voz, telefonía. No tiene gran cobertura por no posee un gran frecuencia de operación, que es de 2.4 GHz. La transmisión es asincrónica.



Antena Direccional

Bridge Radial "Aironet"

Figura 90: Enlace Radial

3.4. INTERCONEXION DE EQUIPOS DE LA CENTRAL KENNEDY

Aqui podemos observar los detalles de la red de la Central Kennedy, y básicamente la mayoria de servidores se encuentran aqui. Es donde se almacena correo, páginas Web, consulta de consumo, chat, FTP y otros servicios para los clientes. Los equipos, tanto ruteadores como servidores, están conectados al LinkSwitch 3Com, el que tiene los puertos para los servidores: 26 para srv1, 11 y 23 para srv2, 20 para Zeus, 24 para Srv4

La red no tiene un control de tráfico, un equipo que haga dichas funciones, sino que estan directamente interconectados. También son importantes las velocidades. Las caracteristicas de estos equipos se detallan más adelante.

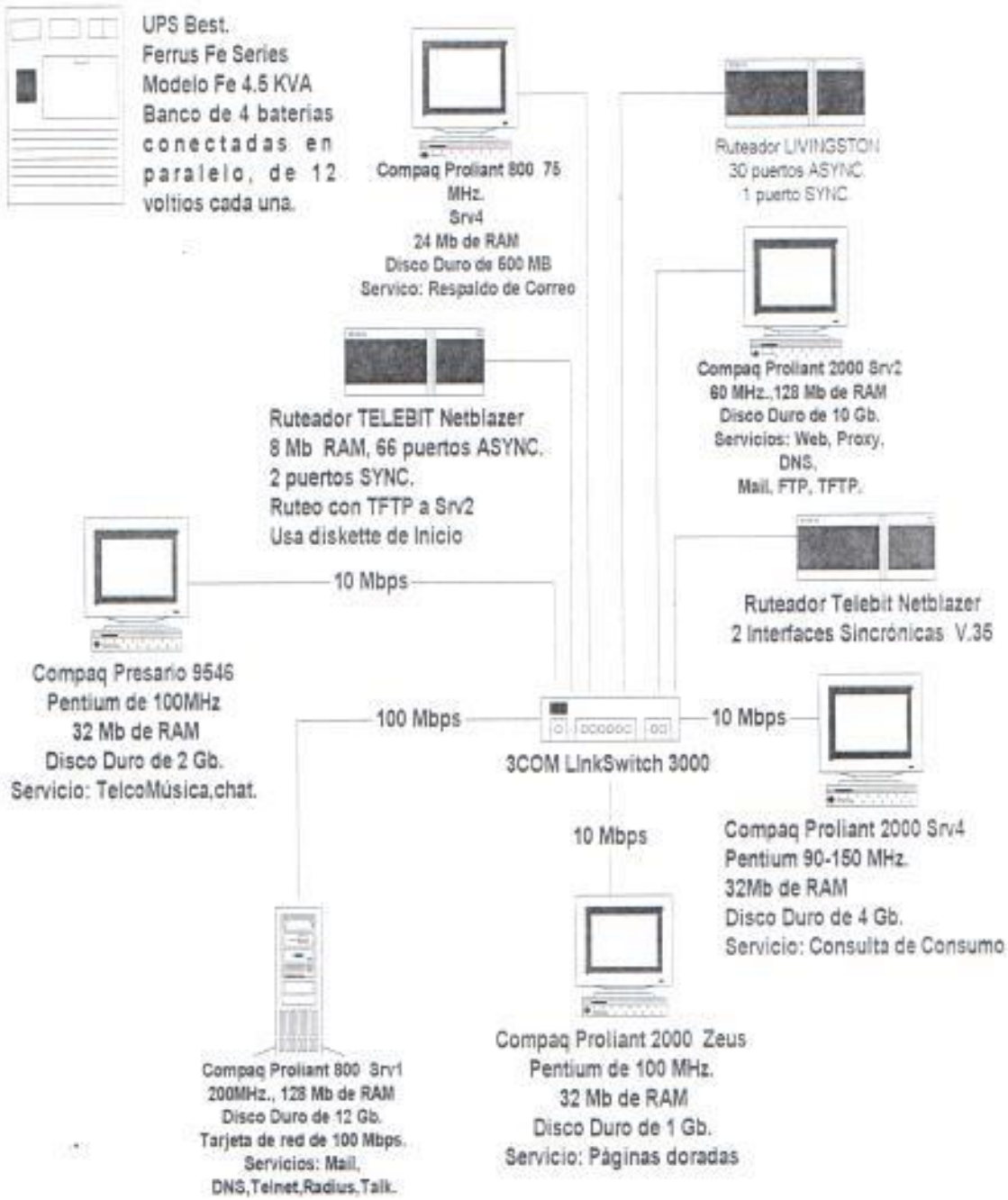


Figura 91: Red Kennedy

3.5 INTERCONEXION DE EQUIPOS DE LA CENTRAL URDESA

Esta central es diferente a la de Kennedy, debido a que aquí contamos con líneas digitales, ya que el AccessBuilder 8000 es un equipo multifunción, demultiplexa las líneas digitales que vienen de Pacifictel, rutea y modula-demodula la información. También tenemos la conexión con las 2 instituciones educativas a las cuales se les brinda servicio directo de red. Se lo hace con dos Dtu, con la finalidad de que actúen como DCE, para poder conectarse a la red. La conexión es a través de canal digital a 64 Kbps, servicio brindado por Teleholding. Así, estos dos centros educativos pueden conectar su red interna con la red de Internet, sin necesidad de hacerlo vía dial-up. Así gana velocidad y seguridad en la conexión. Los dos ruteadores Telebit son para la conexión y enlace con el satélite y microondas para el servicio de IMPSAT. Todos estos equipos serán descritos posteriormente.

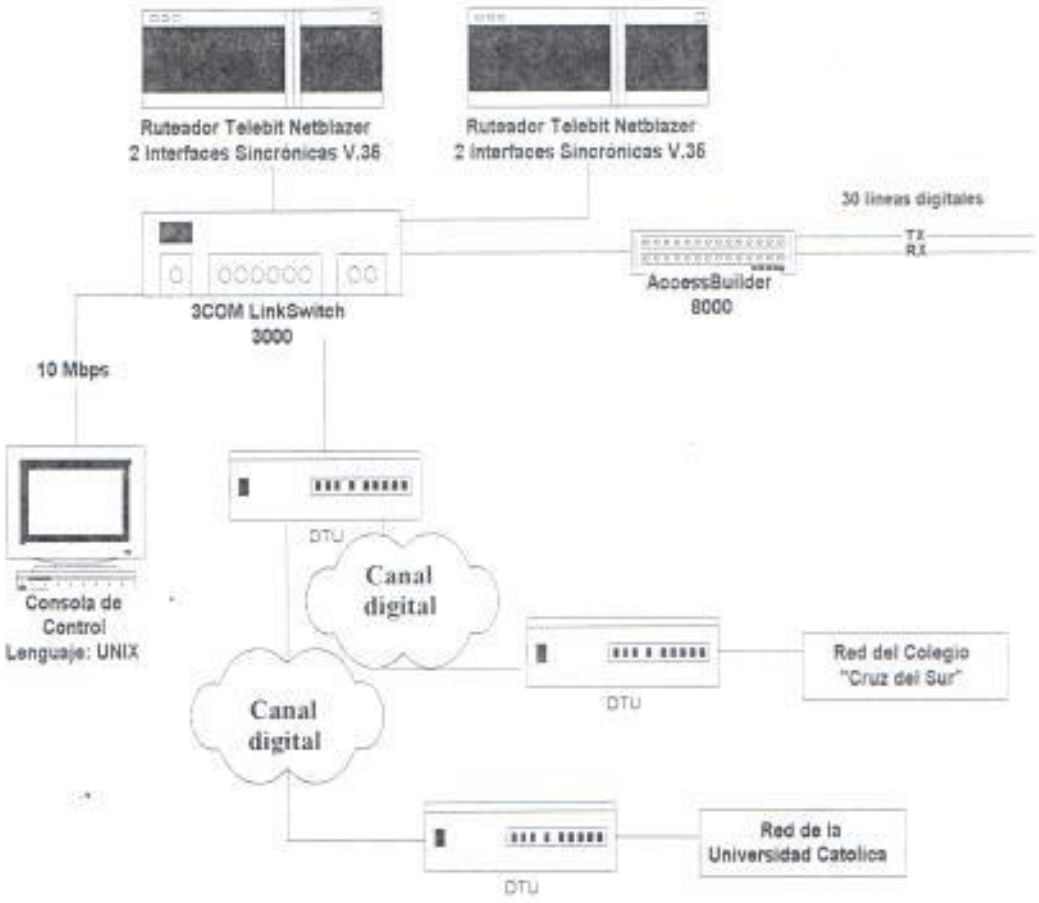


Figura 92: Red Urdesa

3.6. MODOS DE CONEXIÓN A LA RED

Actualmente, nos podemos conectar remotamente de dos maneras:

- Vía dial-up
- Canal digital

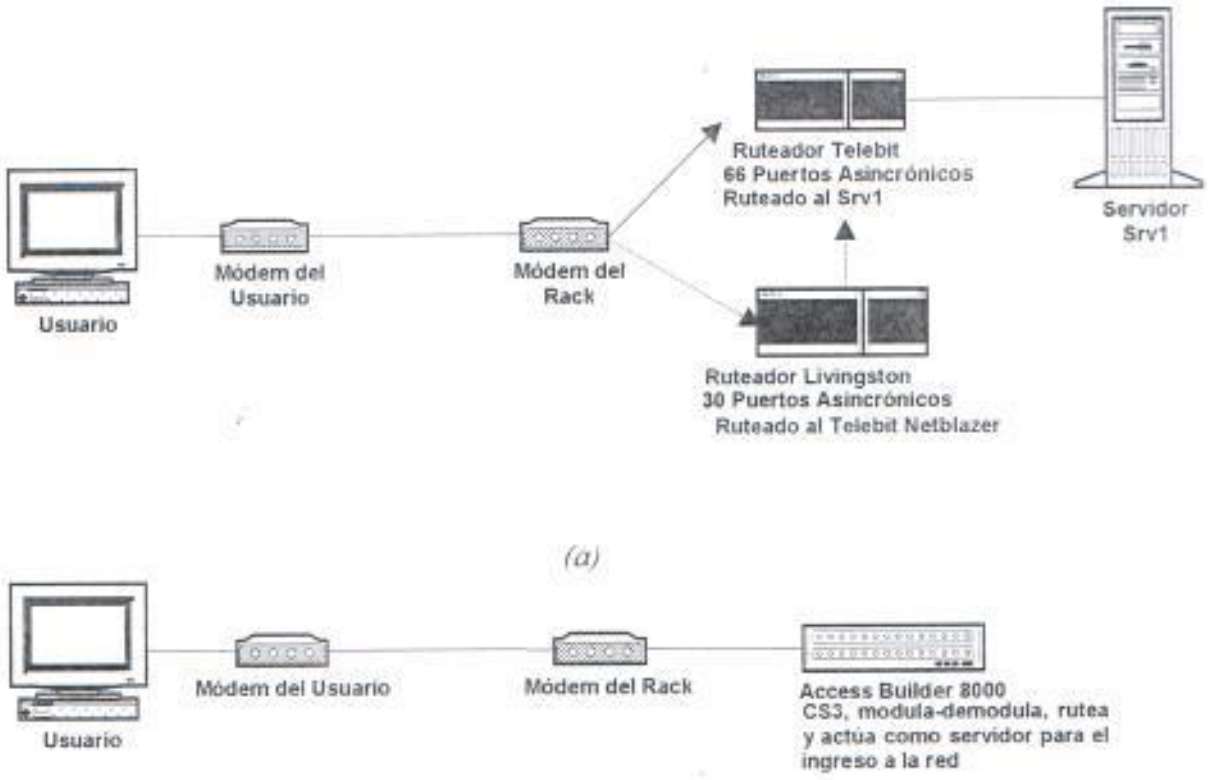


Figura 93: Modos de Conexión a la red vía dial-up

Como mencionamos anteriormente, la *vía dial-up* es el medio más cómodo para que un usuario desde sus hogares u oficinas se conecten a la red. En el caso (a) de la figura, hay 2 formas de comunicarse, la cual se realiza a través de 2 ruteadores: Telebit y Livingston, ya que cada uno utiliza conexión asincrónica a través de sus puertos para comunicarse con los 66 y 30 módem que tienen disponibles cada uno. Una vez realizada la conexión, si el usuario se conecta a través del Ruteador Telebit Netblazer, éste se comunica directamente con el servidor Srv1 a través del cual el usuario puede ingresar a la red, digitando su respectivo user y password. El otro caso es que si el usuario se conecta a través del Ruteador Livingston, como observamos en la figura caso (a), en líneas

punteadas describimos el camino que toma en esta situación. Este se conecta con el Ruteador Telebit, que se comunica con el Servidor Srv1, e ingresamos a la red. Estos equipos se encuentran ubicados en la central Kennedy.

En el caso (b) de la figura, la conexión se realiza con la central Urdesa. El usuario se conecta directamente con el Access Builder 8000, el cual posee 30 módem, realiza el enlace con el cliente, rutea y sirve como servidor de comunicaciones, el cual permite su ingreso a la red.

El *canal digital* es otro medio utilizado para conectar sitios donde existe una gran demanda de usuarios, que desean una conexión diferente y que brinde mejor servicio, que posean una mayor confiabilidad que las líneas telefónicas que pueden ocasionar problemas. Al momento la empresa brinda este servicio a 1 Colegio y a 1 Universidad. El usuario de la red se conecta a través de los DTUs, que funcionan como DCE, utilizando el canal digital a 64k con el Access Builder que es el servidor de comunicaciones para ingresar a la red. Utilizan una interface V.35 Sincrónico, a través del conector DB-25. Todas estas características están descritas posteriormente. Así, a futuro, podría brindarse servicio con este medio a otras empresas importantes.

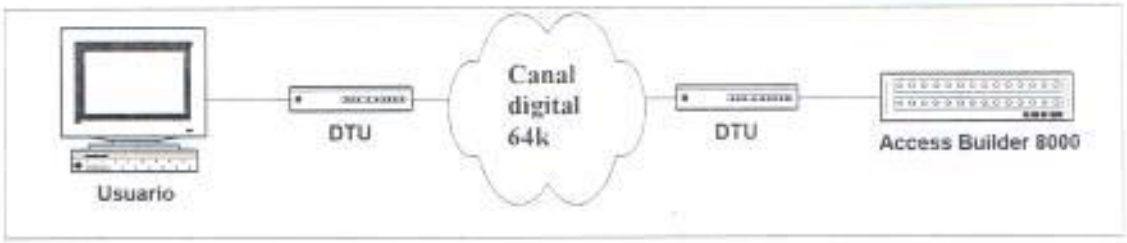


Figura 94: Modos de Conexión a la red vía Canal Digital

3.7 CAPACIDAD Y VELOCIDAD DE LOS EQUIPOS DE COMUNICACIONES

a) RUTEADORES

Los ruteadores que la red utiliza son:

- **RUTEADOR TELEBIT NETBLAZER 40I**

Escalable – El 40i es un chasis modular que tienen las ranuras de expansión para tener más opciones de hardware.

Versátil – El 40i puede configurarse para encontrar todo acceso remoto que usted necesite, bien sea dial-up, ISDN, Frame Relay.

Robusto – El 40i poder manejar desde 2 hasta 66 puertos asincrónicos, es decir, conexiones así como también un máximo de 10 puertos sincrónicos, 12 conexiones ISDN BRI y 3 interfaces LAN.

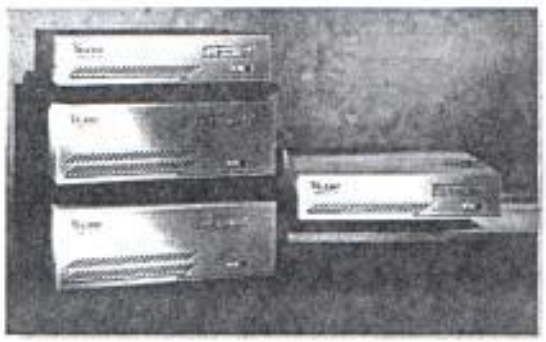


Figura 95: Ruteador Telebit Netblazer 40I

Descripción
Los Sitios Regionales y centrales extienden sus redes para incluir usuarios remotos, clientes, y socios de negocios. Este producto permite una red remota económica para el acceso de todos los usuarios dentro de una empresa. Con sus diseños modulares, el 40i puede configurarse para encontrar todo el acceso remoto de red que se necesita con flexibilidad y potencia.

El 40i incluye múltiples protocolos TCP/IP, NetWare IPX y Microsoft NetBEUI y son disponibles con interfaces Ethernet o Token Ring para LAN. Estos NetBlazer ofrecen una demanda de ruteo en LAN-a-LAN sobre enlaces tales como ISDN, Frame Relay, arrendamiento de líneas para T1/E1 y módem analógicos rápidos.

Todo NetBlazer soporta clientes de acceso a LAN por medio de accesos remotos como SLIP o PPP. Sus arquitecturas escalables pueden soportar como 60 usuarios remotos sobre ISDN o módem asincrónicos.

Cada modelo viene con una tarjeta Ethernet UTP, BNC, y AUI, 4 MB de RAM, 2 puertos seriales asincrónicos, todo el software para el NetBlazer y ranuras de expansión. El 40i tiene 6 ranuras de expansión para el uso de tarjetas opcionales en el NetBlazer.

Datos técnicos

Interfaces LAN	Netblazer 40i
Estándar	1 Ethernet
Máximo	3 Ethernet o Token Ring
Interfaces asincrónicas	
Estándar	2
Máximo	24 sin MTA-32 66 con MTA-32
Interfaces sincrónicas	
T1/E1	Hasta 3 (EIA-232/449/530, V.35, X.21) Hasta 10 (EIA-232/449/530, V.35, X.21)
Dimensiones	
Altura	172 mm
Ancho	427 mm
Profundidad	413 mm
Regletas de expansión	6
Arquitectura	486DX2 100MHz
Peso	10.4 Kg

Tabla 19: Descripción Técnica del ruteador Telebit Netblazer

Requerimientos

Se reinicia por medio de un diskette de alta densidad de 1.44MB.
El requerimiento de potencia y consuno son de 90 a 132 VAC/180 a 240 VAC, 47 a 63 Hz y 250 W AC
El rango de operación es de 0 a 50 grados celsius, 15 grados celsius por hora máximo

Protocolos soportados

Ruteando de LAN-a-LAN:
TCP/IP, IPX, NetBEUI
Acceso de cliente a LAN:

PPP (con TCP/IP, IPX, NetBEUI), SLIP (se usa con IP).

Características utilizadas

- 8 Mb. de memoria RAM
- 66 Puertos Asincrónicos, los cuales son utilizados para la conexión con los puertos Asincrónicos de los módem, que son los que comunican al usuario con la red. Así aseguramos en esta red la conexión de hasta 66 clientes a la vez.
- 2 Puertos Sincrónicos. Los utiliza para la conexión sincrónica con el Módem Satelital del enlace hacia el Pass 1.
- Sirve de Ruteo hacia el servidor ESPOL 2.
- Utiliza diskette de arranque
- Utiliza filtros
- Número de ruteadores utilizados: 1

Características utilizadas

- 8 Mb. de memoria RAM
- 2 Puertos Asincrónicos
- 2 Puertos Sincrónicos
- Utiliza diskette de arranque
- Utiliza filtros
- Número de ruteadores utilizados: 2, uno para la comunicación desde el Puerto Sincrónico del ruteador hasta el módem radial y otro hasta el módem satelital para las comunicaciones vía microondas y satelital.

➢ RUTEADOR LIVINGSTON PORTMASTER 2ER

El servidor de comunicaciones PortMaster 2ER viene con un estándar de 10 puertos seriales incrónicos y dos ranuras de expansión que aceptarán 10 puertos adicionales en cada módulo, dos módulos de ISDN. El PortMaster 2ER también incluye un puerto asincrónico T1/E1 para líneas arrendadas o Frame Relay conectado a una WAN o un proveedor de servicios de internet (ISP). El PortMaster 2ER provee una vía eficiente y económica para ISP o corporaciones para proveen un acceso vía dial para puntos locales múltiples de presencia (POP), estos últimos se usan en líneas ISDN.

Figura 96: Ruteador Livingston PortMaster 2ER

El PortMaster 2ER soporta el RADIUS (Es una Autenticación de un Dial remoto en un servicio de usuario), protocolo para la máxima seguridad del dial. Ellos sólo se caracterizan por el avanzado filtrado, que nos permite controlar exactamente que tipo de tránsito puede entrar y salir de la red. Y ellos incluyen "Livingston ChoiceNet", una tecnología de filtrado centralizado que nos permite escoger los sitios de Internet, las aplicaciones y servicios que desearíamos hacer para disponibilidad de los usuarios. La combinación de ChoiceNet, RADIUS, y nuestro filtrado es ideal para construir un servicio de aplicaciones personalizado de Internet.

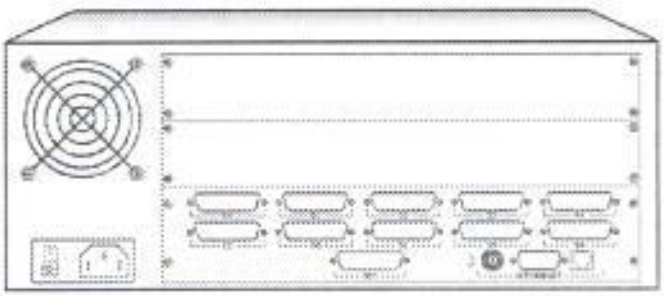


Figura 97: Parte posterior del Ruteador

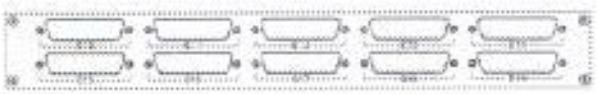


Figura 98: Puertos asincrónicos adicionales

Especificaciones
Protocolos Soportados
TCP, IP, IPX, SLIP
Telnet, PPP

Soporte de Ruteo
TCP/IP y Novell IPX

10, 20, o 30 puertos asincrónicos
Hasta 115.2 Kbps
Interface RS – 423/232
DTR, DSR, DCD, RTS, CTS, TxD, RxD
Conectores DB-25

Un puerto serial sincrónico
RS – 232, V.35, X.21, interfaces eléctricas
Acelera a T1/E1
Interface física DB-25
Interface física V.35

Dimensiones
La longitud: 29.2cm
La anchura: 42.7 cm
La altura: 16.5 cm
Peso: 8.6 kg

Potencia
110 VAC +/- 10%, 47-63 Hz
240 VAC +/- 10%, 47-63 Hz

Rango de operación
La temperatura: 41grados celsius a 113 grados celsius
La humedad: 20% a 80%

Características Utilizadas:

- 8 Mb. de memoria RAM
- 30 Puertos Asincrónicos, los cuales son utilizados para la conexión con los puertos Asincrónicos de los módem, que son los que comunican al usuario con la red. Así aseguramos en esta red la conexión de hasta 30 clientes a la vez.
- 1 Puerto Sincrónico
- Número de Ruteadores utilizados: 1

b) SWITCHING HUBS

➢ 3COM SUPERSTACK II LINKSWITCH 3000

El nuevo Fast Ethernet SuperStack II Switch 3000, es la solución ideal para la conexión de switches Fast Ethernet, Hubs Fast Ethernet y servidores de alta velocidad. Se pueden cambiar los cinco puertos de fibra 100BASE-FX con un puerto Ethernet 100BASE-TX para una conexión local de servidor, o los ocho puertos del switch de par trenzado 100BASE –TX. Ambos tienen una ranura opcional para un módulo Fast Ethernet o ATM. La arquitectura BRASICA 3Com provee anchura de banda completa sobre todos los puertos, y soporta arriba de 4,080 direcciones MAC, el switch maneja redes virtuales de cualquier tamaño. La Gestión Inteligente de flujo provee control de congestión para

eliminar pérdida de datos, y el soporte de LAN virtual (VLAN) que simplifica el manejo de la red. El switch 3000 provee manejo completo de SNMP.

La arquitectura BRASICA 3Com provee un bus interno de ancho de banda de 800 Mbps para obtener el más alto rendimiento.

La ranura del módulo provee un puerto opcional de alta velocidad para una conexión de fibra Fast Ethernet (100BASE-FX) o cobre (100BASE-TX) o ATM (OC-3C 155 Mbps); el SuperStack II Switch 3000 FX también soporta conexión de conmutación para LANs de 10 Mbps por medio de un transceiver que actúa como un módulo de interface.

Figura 99: LinkSwitch 3000

c) DTU

Figura 100: DTUs, 2603 Mainstreet Newbridge

Unidades de terminación de red (DTUs)

- Diseñado para aplicaciones internas con cableado de par trenzado, los DTUs NewBridge pueden transportar servicios hasta 7 Km. Todos los DTUs MainStreet

son configurables por software de manera remota, o en algunos casos local y remotamente.

- Todos los parámetros de operación son configurables local o remotamente usando un canal de control dedicado.
- Los puertos del conector pueden ser configurados como DTE o DCE y pueden acomodar datos sincrónicos o asincrónicos en un completo rango de velocidades.
- Todas las velocidades de subtasa son soportadas con una tasa eficiente HCM (multiplexamiento de alta capacidad) en pasos de 800 bit/seg.

Administración central y mantenimiento

Los DTUs MainStreet pueden ser controlados remotamente desde un administrador de red series NewBridge 4600 o 46000 MainStreet, ofreciendo las siguientes funciones:

- Configuración (Por ejemplo, velocidad de interface, paridad)
- Seteo y Monitoreo del estado de control
- Conjunto completo de Loopbacks
- Pérdida de sincronismo
- Probador Bert Integral
- Todos los DTUs operan de 0 a 50° C.

Distancia	Velocidad	Interfaces	Número de circuitos
3 Km.	**128 Kbit/s**	**V.35 + V.35**	**6 ó 12 circuitos por ranura**

Tabla 20: Características del DTU

- Puertos: dual V.35
- Conectores: DB25
- Interfaces físicas: CCITT V.35, ISO 2593
- Modo de operación: DTE/DCE
- Señales de control soportados: RTS, CTS, ALB, RDL, DCD, DRS, DTR, RI
- Tasas de datos seleccionables por software
- Genera Estadísticas de rendimiento de datos
- Auto-Diagnóstico automático
- Operación asincrónica y/o sincrónica
- Loopback en la red

d) **MODEMS.**

Rack de modems:

- 53 modems Telebit 28.8 kbps V.34

- 33 modems Microcom DeskPorte 28.8 Kbps V.334.

➢ Microcom DeskPorte 28.8P V.34

Microcom DeskPorte 28.8P ofrece un buen desempeño, documentación fácil de usar, una garantía de 5 años. Ofrece un puerto paralelo para la conexión, lo cual va a conseguir un alto rendimiento en el puerto serial V.34. Tiene una velocidad de 28.8 Kbps.

Desgraciadamente, el DeskPorte 28.8P tiene un gran problema: no conectaría a todos en nuestra línea rural a que se somete a prueba. Mientras la mayoría de la gente se encuentra con tales condiciones tan raramente que nosotros no consideramos el desempeño en estas pruebas en nuestras clasificaciones totales, cuando existe fuerte tempestad o la compañía de teléfono falla, nosotros no queremos ser interrumpidos completamente. Por esto, nosotros no recomendamos el DeskPorte 28.8P.

En esta red contamos al momento con 33 Módem Microcom Deskporte 28.8P V.34.

Figura 101: Microcom DeskPorte

➢ Telebit TeleBlazer

Velocidad alta, libre de errores de comunicaciones. El Telebit TeleBlazer es un módem que se caracteriza por transmitir a 28800 bps y que soporta ambos estándares internacionales como el V.34 y el V.Fast Class, son estándares muy rápidos y tienen un cómodo costo y eficiencia para la transmisión de datos.

- Soporta estándares V.34 y V.FC para velocidades hasta 28800 bps.
- Capaz de enviar y recibir fax a 14400 bps.
- Sensa velocidades de los DTE hasta 115200 bps.

- Incluye V.42 bis y MNP 5 para compresión de datos para el rendimiento de los datos hasta 115200 bps
- Provee corrección de errores V.42 y MNP 2-4.
- MNP 10 para conexiones celulares confiables.
- 15 leds indicadores y un parlante con un software para el control de volumen.

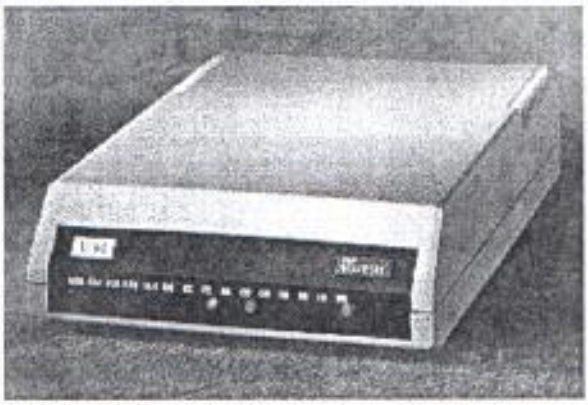


Figura 102: Telebit TeleBlazer

Características del módem

Con la demanda de los módem Telebit TeleBlazer V.34, sus transmisiones pueden correr a través de líneas dial-up hasta rangos de 28800 bps cuando se está comunicando con otro módem V.34 o V.FC. Con tecnología de compresión de datos V.42 bis, usted puede transmitir datos hasta rangos de 115200 bps. Si usted necesita comunicarse con módem más lentos, el TeleBlazer automáticamente escoge la más alta velocidad que mutuamente pueden soportar para la transmisión de datos.

Compatibilidad con módem

- El TeleBlazer es totalmente compatible con todo V.34, V.FC, V.32 bis, V.32, V.22 bis, V.22, V.23 y V.21.
- Capaces de enviar y recibir fax.
- El TeleBlazer es capaz de enviar y recibir fax a 14400 bps. El TeleBlazer viene empaquetado con software de fax para Windows y DOS.

Compresión de datos

El TeleBlazer incorpora V.42 bis y MNP 5 para la compresión de datos con el fin de aumentar al máximo el rendimiento de los datos, ahorrando asi cargas valiosas de linea telefónica y tiempo.

El V.42 y MNP 2-4 para corrección de errores, proporcionan un desempeño superior en la comunicación de datos libres de errores sobre pobres conexiones de lineas telefónicas. El TeleBlazer soporta MNP 10 para la transmisión confiable sobre el teléfono celular y el sistema telefónico rural.

El TeleBlazer sólo esta provisto de respuesta automática, asi como también selecciona la linea que sea de pulso o analógica.

Características

- ITU - T V.42 bis para compresión de datos.
- De acuerdo con ITU – T V.42 y MNP 2-4 para el control de errores.
- Compatibilidad total con V.34, V.FC, V.32 bis, V.32, V.22 bis, V.22, V.23 y V.21.
- Capaz de enviar y recibir fax a 14400 bps.

Beneficios

- Aumenta la velocidad de datos hasta 115200 bps, ahorrando tiempo y cargas costosas de linea telefónica.
- Provistos con un desempeño superior y libres de errores en la comunicación de datos sobre una pobre calidad de lineas telefónicas y asegura la compatibilidad con una ancha gama de módem.
- Permite aplicaciones para operar sobre lineas telefónicas ordinarias a velocidades rápidas.
- Provisto de una manera más rápida y más fácil para enviar directamente fax desde la computadora personal.

Especificaciones técnicas

- **Compatibilidad**

  ITU - T V.34 y V.FC (28800 bps, 26400, 24000, 21600, 19200, 16800 14400);
  ITU - T V.32 bis (14400 bps, 12000, 7200);
  ITU - T V.32 (9600 bps, 4800) ITU-T V.22 bis (2400 bps) ITU-T V.22 (1200 bps);
  ITU - T V.23 (1200/75 bps);
  ITU - T V.21 (300 bps);

- **Compatibilidad con fax**
  ITU - T V.17 (14400, 12000, 9600, 7200 bps);
  ITU - T V.33 (14400, 12000 bps);
  ITU - T V.29 (9600, 7200 bps);
  ITU - T V.21 canal 2 (300 bps)

- **Aplicación**
  Full Duplex sobre lineas conmutadas.

- **Corrección de errores**
  ITU - T V.42 y MNP 2-4

- **Compresión de datos**
  ITU - T V.42BIS y MNP 5

- **Rangos de datos de los dtes**
  115200 a 300 bps

- **Interface dte**
  ITU - T V.24 (EIA-232-D)

- **Interface de linea telefónica**
  Dial-up RJ-11

- **Potencia**
  105 V DE CA, 60 Hz de entrada.

- **Dimensiones físicas**
  6.125"(W) x 8.5"(L) x 1.625"(H)

  En esta red contamos al momento con 53 Módem Telebit Teleblazer.

➢ MÓDEM SATELITAL COMSTREAM CM701

En esta red contamos con 2 módem satelitales los cuales describimos a continuación.

Es un módem digital PSK de alto rendimiento usado en las aplicaciones de comunicación satelital que requieren transmisión y recepción continua. El CM701 es sumamente versátil para proveer al módem el mejor desempeño en la industria. El desempeño contribuye directamente a costos de operación bajos de circuitos satelitales.

El CM701 incluye lo siguiente:

- Comunicación con cualquier otro módem de una red cerrada.
- Capacidad para ser configurado para la aplicación de una red abierta.
- Selección de configuración local hecha desde un panel de control o un terminal remoto.
- Monitoreo y reportes por medio de un panel de control o un controlador remoto.
- Se puede hacer un diagnóstico, que se caracteriza por detectar fallas en la trayectoria de ambos circuitos internos y el enlace externo de comunicaciones satelitales.

Figura 103: Módem Satelital Comstream CM701

La Configuración estándar. El CM 701 contiene:

- Un modulador.
- Un demodulador.
- Una tarjeta de entrada/salida.
- Una tarjeta de control y monitoreo.

El Control del satélite, está constituido de un canal de datos para controlar el equipo de la estación terrena remota.

e) SERVIDORES

➢ SERVIDOR COMPAQ PROLIANT 2000

Características:

- Hasta dos Pentium de 60 MHz o Pentium de 90 MHz en la tarjeta del sistema.
- 32 MB (Pentium) de ECC RAM avanzado, expansible a 512 MB.
- Modelos redundantes de suministrador de poder.

- 2 Controladores Fast SCSI.
- Controlador del CD-ROM y dispositivo preinstalado
- Controlador SCSI para arreglos.
- Ocho ranuras de expansión EISA de 8/16/32 bit.
- Sistema operativo soportado por redes de área local: Netware, UNIX, Windows NT, OS/2, LAN Manager.

Figura 104: Servidor Compaq Proliant 2000

Los Servidores utilizados en nuestra red tienen las siguientes caracteristicas:

SERVIDOR SRV2 Compaq Proliant 2000

- 60 MHz.
- RAM 128 MB.
- 10 Gb de disco duro

Servicios: WEB, PROXY, DNS, Mail, FTP, TFTP.
Conexión: Este servidor está conectado al 3COM LinkSwitch 1000 a una velocidad de 10Mbps por medio de la interface RJ45.

SERVIDOR SRV4 Compaq Proliant 2000

- Pentium 90 – 150 MHz.
- RAM 32 Mb
- 4 Gb de disco duro
- Tarjeta de red de 10 Mbps.

Servicio: Consumo

Conexión: Este servidor está conectado al 3COM LinkSwitch 1000 a una velocidad de 10Mbps por medio de la interface RJ45.

SERVIDOR PAGINAS DORADAS **Compaq Proliant 2000**

- Pentium 100 MHz.
- RAM 32 Mb.
- 1 Gb de disco duro.
- Tarjeta de red de 10 Mbps.

Servicio: Páginas doradas
Conexión: Este servidor está conectado al 3COM LinkSwitch 1000 a una velocidad de 10Mbps por medio de la interface RJ45.

➢ **COMPAQ PROLIANT 800**

Características:

- Fuente de alimentación de 240 W
- Ranuras de expansión (5 PCI, 2 ISA)
- Tarjeta de video PCI
- Disco duro SCSI-2 Fast Wide
- Unidad de disquetes de 1,44 MB
- Unidad de CD-ROM 8X
- Procesador Pentium Pro a 180 ó 200 MHz
- 256K de caché integrada de nivel 2
- Capacidad de procesador dual para mayor rendimiento y confiabilidad
- 32 MB de memoria ECC, ampliable a 512 MB con módulos DIMM de memoria EDO sin memoria intermedia.
- Tarjeta controladora de interfaz de red 10Base T integrada, actualizable a 100TX
- Tarjeta controladora SCSI Wide-Ultra integrada

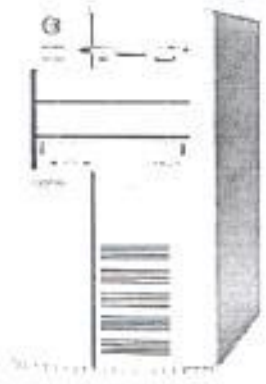


Figura 105: Servidor Compaq Proliant 800

Los servidores de esta categoría en nuestra red son:

SERVIDOR SRV1 Compaq Proliant 800

- Pentium 200 MHz.
- RAM 128 Mb.
- 12 Gb de disco duro.
- Tarjeta de Red de 100 Mbps.

Servicios: Mail, DNS, Radius, Telnet, Talk.
Conexión: Este servidor está conectado al 3COM LinkSwitch 1000 a una velocidad de 100 Mbps por medio de la interface RJ45.

SERVIDOR Compaq Proliant 800

- Pentium 75 MHz.
- RAM 42 Mb.
- 500 Mb de disco duro.
- Tarjeta de red de 10 Mbps.

Servicio: Respaldo de correo.
Conexión: Este servidor está conectado al 3COM LinkSwitch 1000 a una velocidad de 100 Mbps por medio de la interface RJ45.

➢ COMPAQ PRESARIO 9546

Características

- Procesador Intel Pentium 100 MHz.
- CD - ROM
- 1.06 GB de disco duro
- 8 MB RAM, expansible a 136 MB
- Cache interna de 16 KB
- Sonido interno integrado 16 bit
- Bus de vídeo local es de 64 bit (PCI)
- Compatible plug and play
- Soporta hasta 4 dispositivos IDE.
- Full Dúplex.
- Fax/Módem 19.2/14.4.
- El Centro mensajes personales
- Máquina contestadora telefónica.
- Direcciones electrónicas con velocidad de marcado.
- Incluye ratón, teclado y monitor con micrófono incluido.

Figura 106: Servidor Compaq Presario 9546

El servidor de esta categoría que tenemos en nuestra red tiene las siguientes características:

SERVIDOR **Compaq Presario 9546**

- Pentium de 100 MHz.
- 32 Mb de RAM
- 2 Gb de disco duro.

- Tarjeta de red de 10 Mbps.

Servicios: Music, chat.
Conexión: Este servidor está conectado al 3COM LinkSwitch 1000 a una velocidad de 100 Mbps por medio de la interface RJ45.

f) BRIDGE

Los Aironet son productos inalámbricos para red de computadoras de área local. Comunicaciones Inalámbricas Aironet, S.A. provee puntos de acceso inalámbrico, adaptadores de cliente, bridges, y radios OEM.

Los bridges Inalámbricos se usan para conectar LANs, típicamente en edificios diferentes. Los bridges inalámbricos son una alternativa eficiente y de costo mínimo en comparación a líneas telefónicas contratadas las cuales representan un costo elevado. Pueden usarse en lugar de líneas dedicados, o en aplicaciones donde cableado es imposible. Los bridges inalámbricos Aironet pueden usarse para conectar equipos a distancias mayores de 25 millas de distancia.

Los Radios OEM están disponibles para la integración en dispositivos inalámbricos re tales como computadoras de mano, dispositivos de almacenamiento de datos, y robots. Radios Aironets son disponibles en 900 MHz y 2.4 GHz

Figura 107: Productos Aironet

Estas unidades pueden ubicarse en cualquier lugar a lo largo de una red cableada Ethernet, para aumentar el área de cobertura. Los usuarios móviles pueden movilizarse libremente a lo largo del área de cobertura siempre manteniendo una conexión continua con la red LAN.

Rango de operación de frecuencia:	2.4 - 2.4835 GHz
Rango de datos de radio:	1 Mbps
Cobertura Tipica por microcelda:	4,500 sq.m. (50,000 sq. ft)
Rango Omni – Direccional interior:	Hasta 500 ft.
Rango Omni - Direccional exterior:	Hasta 1000 ft.
La Antena estándar:	Dos dipolos de 2.15 dB.
Caracteristicas de modulación:	2GFSK
Potencia externa:	250 mW, 100 mW, 50 mW
Sensibilidad:	80 dBm por 1 Mbps
Tiempo de recibir y transmitir:	5µsec
El número máximo de usuarios	68
Por punto de acceso:	2043
Configuración Local por medio de:	(RS - 232C a DB-9 hembra)
Configuración Remota por medio de:	Telnet, FTP, o SNMP

Caracteristicas Fisicas:

- Las dimensiones (sin la antena) :20 cm x 15 cm x 5 cm
- Peso: 0.7 Kg
- La temperatura de funcionamiento Oscila: 20° C a +50° C (- 4° F a 122° F)
- La Humedad Relativa: 95% no - condensado
- La fuente de alimentación: 90-260 VAC, 50/60 Hz, 18 VDC 1A
- Cumplimiento estándar IEEE 802.11

El estándar IEEE 802.11 se diseño con el objetivo establecer reglas para el diseño de equipos que conforman una red Inalámbrica de redes de área local, para que puedan operar entre ellos.

La cobertura de redes inalámbricas de área local es una función de la ganancia de antena, ubicación, y el tipo, así como también densidad y construcción del edificio. La cobertura tipica mostrada está para un ambiente de fábrica u oficina. La linea de vista puede variar de acuerdo a la elección de la antena.

g) ANTENA PARABOLICA

Las Antenas de Estaciones Terrestres Satelitales, son de construcción segmentada, los segmentos son moldeados por compresión a alta presión. Esta construcción usa un tipo de material, llamado thermoset FRP (fibra de vidrio reforzada de plástico)

La antena de nuestra estación tiene las siguientes características:

- Diámetro de 3.7 metros.
- La capacidad máxima de transmisión es de 128 Kbps
- Amplificador de bajo ruido

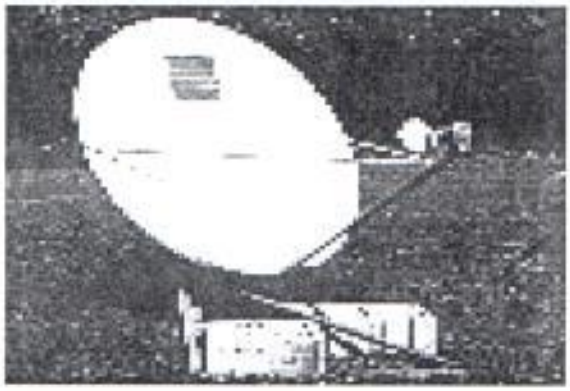


Figura 108: Antena Parabólica

Esta antena esta conectada a la consola VITACOM LCS 710 que tiene las siguientes características:

- Potencia de salida (dBm). 36.22
- Alimentación (VDC) 10.55
- Temperatura ambiente (°C) 39
- Frecuencia UpConverter (MHz) 6040
- Atenuación UpConverter (dB) 15
- Temperatura UpConverter (°C) 47
- Potencia de salida UpConverter (dB) -33.55
- Corriente del UpConverter (mA) 131
- Atenuación DownConverter (dB) 15
- Corriente Down Converter (mA) 196
- Corriente entrada del LNA (mA) 125.

h) SATÉLITE

PanAmSat es una parte integral de los super caminos de la información global, transmitiendo información digital alrededor del mundo para compañías de telecomunicaciones, negocios y proveedores de servicios de Internet.

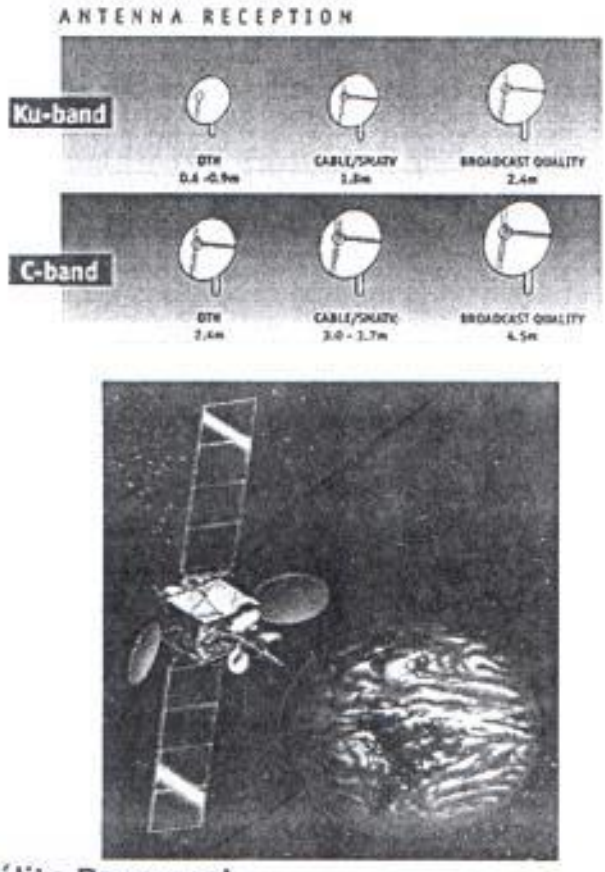


Figura 109: Satélite Panamsat

La empresa privada en el espacio

El decenio de 1960 fue el advenimiento de sistemas de satélite de comunicaciones. Estos sistemas se diseñaron primariamente para las comunicaciones telefónicas y no para aplicaciones modernas tales como transmisiones de datos. Aunque estos satélites tienen amplia cobertura geográfica, las señales proporcionadas son relativamente débiles lo que requiera el uso de "gateways" y grandes estaciones de tierra. Hasta la década de 1980, los usuarios internacionales de satélite tengan que confiar en sistemas anticuados. PanAmSat se fundó en 1984 para responder a las necesidades de cambio en la industria

de telecomunicaciones. Esta fue posible en 1985 mediante una decisión de la Comisión Federal de Comunicaciones de EE.U que le permiten al nuevo servicio de proveedores lanzar su propio sistema internacional de satélite.

PanAmSat revolucionó la Industria de telecomunicaciones en 1988 con el lanzamiento de PAS-1. El satélite PAS-1 permitió a corporaciones y usuarios de comunicaciones desarrollar las redes privadas personalizadas que usen antenas pequeñas y económicas.

Sistema global de satélite panamsat

El Sistema PanAmSat, está comprendido de PAS-1, un satélite GE Astro series 3000, y tres nuevos satélites Hughes HS 601. Ellos son: PAS-1, PAS-2, PAS-3 y PAS-4.

El Pas-1 actualmente provee cobertura en América del Norte, Centroamérica, Sudamérica, Caribe y Europa.

El equipo de científico de PanAmSat, junto con los expertos en satélite de Hughes, ha diseñado el satélite Hughes HS 601 para optimizar la flexibilidad y alta potencia. El PanAmSat de satélites emplean los más últimos adelantos en la tecnología de satélite incluyendo: emisores reflectores, emisores conmutables. Además, todos los transpondedores del satélite Hughes HS 601 utilizan la más avanzada tecnología que permite transmisiones multi-acarreo óptimo digital. El uso de estos avances disminuye la distorsión de cada transportador digital, y por lo tanto minimiza cualquier interferencia disociadora entre los diversos transportadores cuando comparten el mismo transpondeador.

Características

Manufactura: Compañía Hughes Aircraft	**Bus del Satélite: HS 601**	
Transpondedores:	**Banda Ku 16 x 54 MHz**	**Banda C 16 x 54 MHz**
Capacidad:	**Hasta 8 Transpondedores de Ku a C**	**Hasta 8 Transpondedores de C a Ku**
Potencia de Salida del Transpondeador:	**63 Watt**	**34 Watt**
Emisores:	**3 Subida 5 Bajada**	**3 Subida 5 Bajada**

Tabla 21: Características del PanAmSat

El Satélite PAS-1 opera en la Región del Océano Atlántico, con una localización Orbital de 45° Longitud Oeste/ 315° Longitud Este.

Servicios del PanAmSat

- Servicios Corporativos
- Aplicaciones IDS y DDS
- Servicio VSAT
- Voz
- Transmisión de Datos

Los Servicios Regionales y Domésticos

Los servicios que brinda son: para la emisión de Televisión, comunicaciones de datos, gobierno y propósitos educativos, o telefonía rural. El satélite cubre regiones densamente pobladas y regiones remotas, y los paises ahora tienen la oportunidad de usar el satélite PanAmSat como su sistema de satélite doméstico propio.

Transmisión de Datos

Además de redes bidireccionales de datos, PanAmSat ofrece una gama llena de opciones de ancho de banda para transmisión de datos en una sola dirección. La transmisión de una sola dirección es ideal para aplicaciones tal como noticias domésticas e internacional, cotizaciones financieras, información de tiempo, información deportiva e información de servicios.

Servicios de Datos

Los Transpondedores del PanAmSat se han perfeccionado para usos digitales de multitransporte incluyendo datos digitales internacionales, regionales y servicios domésticos. Con una combinación de señales regionales anchas y emisión de señales de alta potencia, los negocios son capaces de desarrollar redes privadas extensibles personalizadas para conectar ubicaciones en diferentes áreas del mundo. Los servicios incluyen Servicio de Datos Internacionales y Domésticos (IDS y DDS), VSAT, Circuitos Privados de Linea, y Voz.

Caracteristicas:

Latitud:	2°, 9.63 min. Sur
Longitud:	79°, 53.97 min. Oeste
Altitud:	116 pies, con un error de ± 30 metros.
Transpondedores:	9
Ancho de banda:	128Kbps. Banda C.
Rango de frecuencia Up:	6.0GHz.
Rango de frecuencia Down:	4.0GHz.

i) ACCESSBUILDER 8000

Tarjetas de Multifunción que pueden ser reconfiguradas mediante el software para asegurar el aprovisionamiento flexible de capacidades del AccessBuilder 8000.

El sistema remoto AccessBuilder 8000 se diseña para proveedores de servicio de red, lo que permiten entregar una gama llena de capacidades para el acceso vía dial al Internet y otros servicios conectados, redes inalámbricas, y redes de transacción. El sistema se conforma con T1, E1, PRI e interfaces analógicas para la red telefónica pública conmutada (PSTN); adaptadores terminales ISDN; x2™; 56 Kbps, V.34, conexión de módem celular y de transacción; y LAN de alta velocidad e interfaces WAN, incluyendo TCP/IP y X.25.

Como software para plataformas de acceso remoto, el sistema AccessBuilder 8000 reemplaza muchas funciones de dispositivos de hardware para reducir costos y simplificar muchas acciones, cambios de configuración, y gestión de red.

A continuación mostramos algunos de los beneficios claves de esta plataforma de clase de transporte (acarreo):

- La capacidad del "Puerto Universal" le permite al sistema dinámicamente reconfigurar para aceptar llamadas de módem e ISDN sobre el mismo puerto.
- Nuevos servicios de acceso para permitir modificaciones por software para el control de un centro de red sin cambios de hardware.
- Rebaja costos de operación mediante la gestión centralizada remota, reduce requerimientos de espacio en las instalaciones de la red, eliminación de cableado entre componentes discretos, y uso de una plataforma para soportar aplicaciones múltiples.
- Provee sistema escalable de alta - densidad con hasta 300 puertos para la flexibilidad en el despliegue de red.

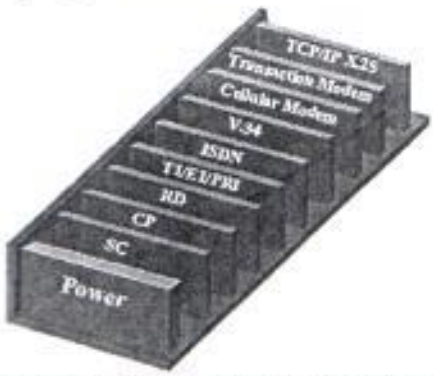


Figura 110: El Sistema Integrado de Acceso Remoto

- Todo digital, la arquitectura redundante mejora la calidad de servicio, y gestión en tiempo real aislando problemas antes que ellos afecten a los usuarios.
- Transmite confiabilidad en el transporte con aspectos tales como tarjetas para nivel de redundancia, y gestión remota en total tiempo real con un agente SNMP.

Solución para clase de acarreo (transporte) del accessbuilder 8000

El AccessBuilder 8000 se diseña para transporte en redes. La plataforma se caracteriza por la fuente de alimentación redundante, lógica común y ruteadores para asegurar la disponibilidad más alta posible del sistema. Todos los componentes deben tener el MTBFs mayor que 50,000 horas. El AccessBuilder 8000 soporta administración de SNMP.

Especificaciones del producto accessbuilder 8000

Interfaces para la red telefónica

- T1
- E1
- Analógica

Señales isdn

- Interface de rango Primario ISDN (PRI) 23B+D
- ISDN - 2(NI-2)
- EURO-ISDN
- Señalización A&T 5ESS y Nortel DMS-100 ISDN
- Circuitos conmutados para llamadas de datos y voz

Protocolos de modulación

- x2
- V.34
- V.32, V.22bis, V.22
- Corrección de error: V.42
- Compresión de Datos: V.42bis
- SDLC especificado para transacciones

Interfaces para la red de datos

- TCP/IP PPP, SLIP, CSLIP, Telnet y Rlogin
- PPTP
- X.25
- Interface Ethernet 10Base-T

- Interface (V.35) serial de alta velocidad
- RS - 232/V.35/EIA530

Arquitectura global

La arquitectura del Accessbuilder 8000 se diseña para instalaciones internacionales y soporta:

- Acción y Recepción de las capacidades de digito usadas con señales R1 y R2
- 110 y 220 de voltaje

Administración del accessbuilder 8000

- Soporta agente SNMP.
- Gestión de configuración Remota y diagnósticos vía AccessView.
- Diagnósticos de ciclos completos de potencia.
- Las configuraciones redundantes con automáticas.
- Localización de averías y diagnósticos remotos de respaldo vía dial-up a través de módem.

Componentes del accessbuilder 8000

Los Sistemas Transportadores 3Com producen una variedad de software para definición de aplicaciones de acceso que se encuentran en la plataforma del AccessBuilder 8000. El AccessBuilder 8000 tiene una alta capacidad, con sistema multiestrato diseñado para ambientes en que la confiabilidad, escalabilidad y la tolerancia de falla son obligatorias.

El AccessBuilder 8000 consta de uno o más chasis manteniendo niveles de software para los elementos funcionales definidos en los cuales las aplicaciones se ejecutan.

Este hardware incluye:

- Módem con Software para su definición
- Interfaces T1/E1
- Servidor de Comunicación TCP/IP y X.25
- AccessView NMS

Software para definir módem

- Soporta V.34 y x2 56kbps
- Soporta módem celular con técnicas mejoradas.
- TraxModem para POS, redes públicas.
- Software configurable sobre procesadores de señal digital de alto rendimiento.

El software, soporta puerto dual DSPs x2 (56 Kbps), módem de alta velocidad V.34 (33.6 Kbps); módem celular de técnicas mejoradas; y funciones de módem de

transacción especializados en redes de puntos de venta/ puntos de servicios (POS). El software para DSPs puede también estar definido para funcionar con adaptadores terminales ISDN.

Figura 111: Diagrama de bloques

Puerto universal
Uno de los aspectos que diferencia al sistema AccessBuilder 8000 es el Puerto Universal, que tiene la capacidad para aceptar V.34 asíncrono y llamada de módem x2 así como también llamadas ISDN/ PPP Sincrónico sobre el mismo puerto. Con este robusto y flexible software multifunción es simple configurar.

Interfaces digitales y analógicas
Los módem del AccessBuilder 8000 pueden conectarse al PSTN mediante tramas digitales (T1 o E1) o analógicas. Las conexiones digitales se realizan mediante otro elemento funcional del AccessBuilder 8000, la tarjeta de interfaces T1 o E1. Las conexiones analógicas se han hecho mediante un panel optativo I/O que se inserta en la parte posterior del aparato. Esta tarjeta de interfaces provee dos conectores RJ11 para líneas PSTN y, opcionalmente, dos conectores DB25 DTE para el uso con dispositivos externos.
Soportado por múltiples aplicaciones
Alta velocidad

Los módem del AccessBuilder 8000 soportan velocidades de transmisión de hasta 56 Kbps usando tecnología propia 3Com x2. El módem automáticamente retrocede a bajas velocidades para asegurar la interoperabilidad con módem más lentos. Las características del módem V.34 Trellis que codifica para todo tipo de enlace y aumenta al máximo el rango de enlace que el canal puede soportar el canal mediante sondeos y técnicas adaptables. La constelación de soportes de módem desarrollados y avanzados aspectos han servido para compensar la distorsión de amplitud y ruido proporcional.

Inalámbrico
El AccessBuilder 8000 soporta técnicas para el aumento popular de datos celulares para proveer confiabilidad, alta velocidad, y conexiones transparentes entre empresarios con módem celulares móviles y módem fijos o redes de paquetes conmutados. Los transportadores celulares tienen ampliamente desplegado al AccessBuilder 8000 en una configuración celular directa que les permite ofrecer a sus clientes móviles un servicio para conectar módem celulares a módem fijos sin preocupar sobre equiparar módem en ambos terminales.

Transacción
Los módem de transacción (TraxModem) del AccessBuilder 8000 soportan ambos Asincrónicos (Visa y transparente) y terminales de transacción SDLC. El tipo de llamado requerido que se procesa se detecta automáticamente y el módem es reconfigurado basándose en llamada a llamada. El TraxModem se perfecciona para reducir el tiempo total de conexión que se necesita para transacciones como máximo de 10 segundos. En 950 redes, el TraxModem está presente con el DNIS e inmediatamente lo encamina a la aplicación de la transacción PAD (relleno) (TraxPAD) en la tarjeta DCP del AccessBuilder 8000. El TraxPAD determina cómo el llamado debería manejarse y además establece un circuito virtual conmutado en X.25 igual como el TraxModem y el terminal POS. Esto perfecciona la transacción total el tiempo de proceso.

Especificaciones
- Modulaciones x2, V.34, V.32bis, V.32, V.22bis, V.22
- Incremento Celular
- Corrección de Error V.42
- Compresión de Datos V.42bis
- Soporta Visa I/II y SDLC
- Soporta conjunto de comandos estándares AT

Interfaces t1/e1
- Tarjetas de interfaces con software configurable
- Múltiples tarjetas instaladas en un mismo AccessBuilder 8000
- Control completo, pruebas y diagnósticos de enlaces con T1/E1

La linea de productos de la interface T1/E1 incluye una tarjeta de interface T1 que soporta 1.544 Mbps de velocidad en la línea que llevan 24 canales y una tarjeta de interface E1 que soporta 2.048 Mbps que lleva 30 canales.

Banco de canales con funcionalidad integrada
Las interfaces T1 y E1 se conectan al software para definición de módem del AccessBuilder 8000 e interfaces de red de datos para proveer una solución integrada para

la central de acceso al sitio de la red. Cuando un llamado llega a la interface T1 o E1, es demultiplexado y encaminado del bus interno del AccessBuilder 8000 al módem digital, al DSU u otro elemento funcional.

Completa verificación, prueba & diagnósticos
Las interfaces T1 y E1 soportan una variedad de modos de prueba "loopback" incluyendo "loopback" remotos y locales.

El sistema de gestión de red AccessView ofrece una gama llena de aprovisionamiento, capacidades de alarma y verificación. Las pantallas de configuración permiten al operador configurar líneas para T1/E1 y asigna conexiones de módem para cada canal y parámetros al canal. Las pantallas de diagnóstico le permiten al operador controlar los diversos estados de las tarjetas incluyendo alarmas, frames erróneos, frames perdidos y errores CRC. Las pantallas de definición de canales le permiten a los operadores definir variaciones de señales.

La interface E1 soporta canales asociados de señales R2 y software flexible y configurable R2 para registro de señales para ITU - T Q.421. La capacidad para configurar el software de señalización R2 es crítica porque las combinaciones de tono tienen interpretaciones diferentes para PTTs locales. La interface local de señalización R2 puede fácilmente personalizarse para la implementación en el país específico.

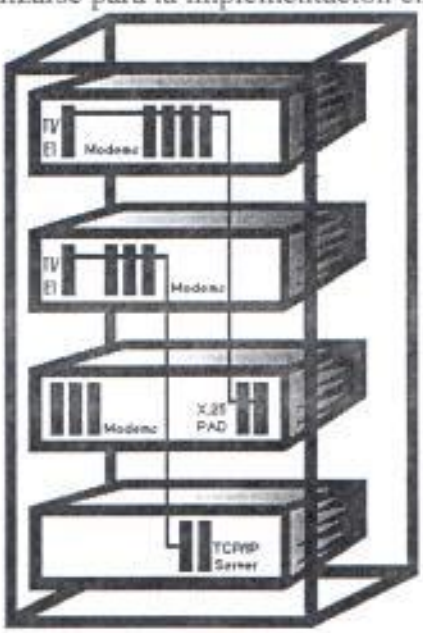


Figura 112: Conexión en Cascada del Access Builder 8000

La interface E1 se diseña para satisfacer estrictas normas Comunitarias Europeas de seguridad y estandarización.

Especificaciones

Software de T1

- Formatos de Frame D3/D4 y ESF
- La señalización E&M incluye:
  - Dirección de señalización DNI y ANI
  - Inicio parpadeante o inicio inmediato
  - Inicio de conexión e inicio de enlace
  - Loopback Local y Remoto
  - Rango de la linea de la interface desde 56 Kbps a 1.544Mbps

Tarjeta de Interface T1

- Procesador de 16 MHz I80152
- Frame soportado por el chip MT8976
- Interface de I/O soporta 100 ohm en par trenzado (conector DB15)

Software de E1

- Frames Doble y formatos de frame multiframe CRC4
- La Señalización de linea codificada R2 esta soportada bajo ITU - T Q.421
- Registro de señalización MFC R2 soportada bajo ITU - T Q.441
- Loopback Local y Remoto
- Rango de la Linea de la interface desde 56 Kbps a 2.048 Mbps

Tarjeta de Interface E1

- Procesador de 16 MHz I80152
- Frames soportado por chip MT8979
- La señalización RAM está soportada por un chip RAM de puerto dual
- La Interface I/O soportan una impedancia desbalanceada de 75 Ohm en la linea de la interface (coaxial)
- (Conector BNC) o 120 ohm de impedancia en la linea de interface (conector DB15)
- Puerto para Diagnostico de rendimiento

Tcp/ip y x.25 servidores de comunicación

El AccessBuilder 8000 de 3Com caracteriza a los procesadores de comunicaciones y equipos servidores de comunicaciones para conectar usuarios a redes de datos en una

variedad de maneras. Además, el AccessBuilder 8000 se caracteriza por tener tarjetas RS-232 para conexiones a servidor de comunicaciones externas.

La plataforma del servidor de comunicaciones AccessBuilder 8000 incluyen:

- El ingreso a la Red de Datos/DCP2
- PAD (relleno) para X.25

El ingreso a la red de datos/dcp2

- Software basado en soporte para interactividad (Telnet y Rlogin) y acceso entre cliente –servidor (PPP, SLIP y CSLIP)
- PPTP (L2TP de llegada rápida)
- Procesador Powerful Intel i960 RISC superscalar
- 60 conexiones concurrentes de usuarios sobre una tarjeta única
- TACACS+ y RADIUS soportados por AAA
- Interfaces Ethernet (10BaseT, AUI) & serial (RS530) para conexiones de red de datos

El ingreso a la Red de Datos de 3Com (DNG) es un protocolo de alto rendimiento que procesa equipos totalmente integrados en la plataforma de acceso a la red del AccessBuilder 8000 para proveer acceso vía dial al Internet, LANs remotos y hosts. Diseñados para dar servicio de red a proveedores que operan con un gran número de llamadas en las redes, el DNG genera alto rendimiento para un gran número de usuarios remotos concurrentes y es completamente un software superior. El ingreso a la Red de Datos combina módulos de software para protocolos que se ejecutan sobre un poderoso procesador i960 basado en un procesador RISC para proveer escalabilidad, buen desempeño, y confiabilidad en la clase de transporte.

Software para definición de accesos

El ingreso a la Red de Datos soporta una amplia gama de usuarios cuyas aplicaciones oscilan desde el carácter simple ASCII - basadas en sesiones para aplicaciones en nodos remotos.

El módulo de software TCP/IP de DNG provee acceso a nodos remotos (PPP, SLIP y CSLIP) e interactividad (modo de línea Telnet y Rlogin) para conexiones a redes de datos de una variedad de líneas PSTN. Con el ingreso a la Red de Datos, el servicio de la red para proveedores pueden soportar ambos acceso asincrónico al texto - basados en recursos tal como Lynx, Gopher y Usenet que se ejecutan en hosts de Internet y accesos en redes TCP/IP para aplicaciones avanzadas tal como "World Wide Web" y GUI basado en trabajo de cliente- servidor.

Como módulo de software definido, el ingreso puede ser controlado, administrado, y mejorado remotamente desde un centro de control de red.

Procesador escalable
La tarjeta procesadora RISC i960 de 32 bit superescalar ofrece un desempeño significativamente superior a procesadores X86. Diseñado para alta densidad, alto rendimiento, una simple tarjeta DNG soporta hasta 60 usuarios concurrentes conectados en cada ejecución a 64 Kbps o 48 usuarios a 128Kbps. Las tarjetas múltiples DNG pueden insertarse en un solo sistema AccessBuilder 8000 para clientes con grandes requerimientos de sistema.

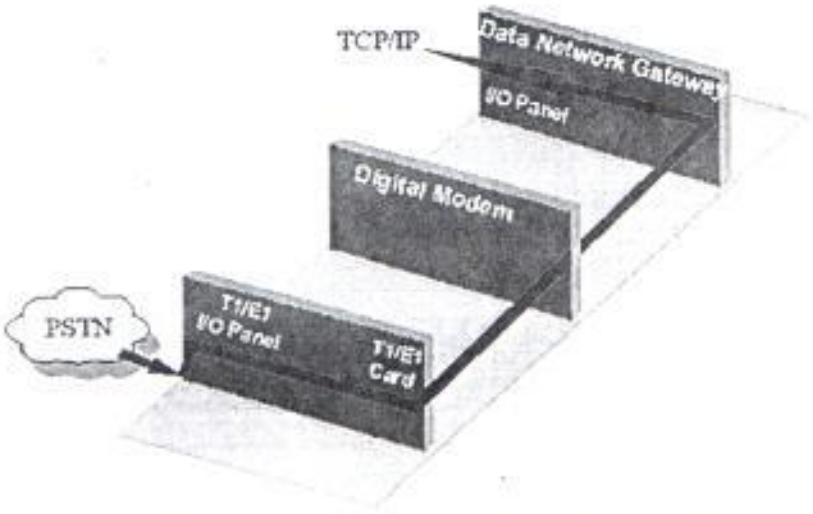


Figura 113: Clases de Transportador (acarreo) Confiable

El DNG se equipa con la clase de transportador de características requeridas por el proveedor de servicio de red, incluyendo tarjeta de nivel de redundancia y gestión remota integrada. En configuraciones redundantes, el AccessBuilder 8000 cambiará automáticamente las interfaces por el hardware de respaldo cuando una falla de red se detecta. Ethernet y las conexiones seriales están disponibles para la interface de la estructura principal de la red.

La gestión del AccessBuilder 8000 se realiza mediante SNMP (MIBII) y las Ventanas con un editor de configuración. Estos sistemas proveen registro de error, alarma, y otras herramientas para administrar las redes del AccessBuilder 8000 y para arreglar los problemas de sistema antes que ellos colisionen llamadas de usuarios.

Tacacs+/Radius

El ingreso a la Red de Datos requiere Autenticación, Autorización y Contabilidad (AAA) mediante ambos TACACS+ y Radio. El ingreso es compatible con una gama amplia de servidores de seguridad central y ofrecen completa flexibilidad para el control de llamadas y el conteo de llamadas.

Las redes privadas virtuales

El ingreso a la Red de Datos también provee soporte para Protocolo Punto a Punto que Traspasa (PPTP) para proveer corporaciones con seguridad, acceso a redes remotas usando una llamada local al Proveedor del Servicio de Internet (ISP). Esto rebaja costos para el acceso a la red mientras todavia emiten a los clientes un método conveniente de transportar datos sobre un medio seguro. En un futuro cercano el AB8000 soportará también L2TP, otro protocolo conocido.

Especificaciones del producto

Soporte de la red ip

- Protocolos IP, ICMP, ARP, TCP y UDP
- No sujeto a PPP, SLIP, CSLIP y Rlogin
- Temporal y dinámica asignación de direcciones IP para conexiones PPP
- Gran acceso interactivo
  - Telnet
  - Linea de Modo Telnet
  - Rlogin
- Interface Ethernet (DIX) para LAN
- Nombre del Host Local / base de datos de la dirección IP con hasta 5,000 entradas
- TACACS+/Radio para autenticación de cliente

Plataforma de proceso

- Procesador oi960CF superescalar RISC con la memoria cache dual
- El Sistema Base incluye 4MBs de código RAM con 2MB Flash
- 4-32 MB de RAM para I/O
- 96 PSTN independientes para usar conexiones en los canales de datos hasta 64Kbps cada uno
- MTBF: 75,000 + horas (estimadas)
- Arquitectura DMA para todos los dispositivos de I/O

- Interrumpe el proceso de no carga al usar los canales de los equipos para datos (módem, ISDN)

Interfaces de i/o

- Ethernet
  - Conector AUI DB15
  - Conector 10BaseT RJ45
  - LEDs para indicar condición de enlace y trafico.

Llamada al pad (relleno) de x.25

La plataforma del AccessBuilder 8000 está establecido en PAD (Relleno) Multi Protocolo que permite la conexión directa de hosts y redes. Con el RELLENO enlaza a su red de datos y la interface T1/E1 a la red pública, la plataforma del AccessBuilder 8000 provee un cable de entrada, uno de salida para la solución de la conectividad. Toda la funcionalidad del (PAD) Relleno radica en el software que se transmite a la tarjeta DCP del AccessBuilder 8000. Cada DCP ocupa una ranura única en el AccessBuilder 8000, y el DCPs múltiple puede instalarse sobre un soporte.

Los PAD (Relleno) X.3/X.28 pueden usarse para conectar usuarios asincronos a la red X.25. Se conecta un bus de alta velocidad del AccessBuilder 8000 a un DSPs individual el cual provee al módem o DSU la funcionalidad para equiparar el requerimiento del usuario terminal.
El RELLENO está disponible como una implementación del Relleno (Pad) por la norma ITU - T X.3/X.28 o como TraxPAD del 3Com. Alternativamente, el RELLENO puede personalizarse para encontrar las necesidades de los requerimientos de otros protocolos. El RELLENO X.3/X.28 convierte datos asincronos que llegan desde módem a datos para redes X.25 y viceversa.

Así un TraxPAD se usa conjuntamente con un AccessBuilder especial 8000 con software para módem de transacción para proveer un alto rendimiento para el acceso al sistema de transacciones del proceso de aplicaciones.

Los PAD X.3/X.28 (Rellenos) del AccessBuilder 8000 forman parte de las recomendaciones ITU - T 1988 para X.3, X.28, X.25 y X.121.

Los aspectos de estándares para RELLENO incluyen:

- Hasta 16 sesiones de RELLENO por DCP
- Terminales Asincronos a velocidades hasta 14.4Kbps
- Soporta estándares X.3/X.28/X.29
- Un puerto de red X.25 (hasta 64 Kbps)
- Provee la traducción de direcciones de DNIS-a-X.121 para el ruteo de red X.25

- Provee soporte para autollamado del sistema de configuración para X.25 basado en información DNIS

Los usuarios pueden situar las llamadas que usa el estándar X.28 por comandos de requerimientos de llamadas o usando direcciones mnemónicas. Adicionalmente, las llamadas pueden situarse trazando el camino DNIS o ANI desde la red pública a la ya configurada dirección X.121. Además de trazar el DNIS/ANI hacia la dirección X.121, el RELLENO puede proveer también a un usuario específico el perfil para cada DNIS/ANI.

El RELLENO soporta subdirecciones y los llamados pueden estar sujetos o no a la red pública. Mediante sistemas de gestión del AccessBuilder 8000, el Relleno X.3/X.28 se configura así:

1. *Canal de Usuario* - El punto de conexión para Relleno al módem del AccessBuilder 8000. Cada canal de usuario puede configurarse de manera diferente
2. *Relleno* - Configuración de información que es común para todos los usuarios en el RELLENO.
3. *Trama* - Configuración que determina como el Relleno obra reciprocamente con la red X.25 o el host.

Gestión de red accessview

La linea de productos AccessView provee diferentes clases de acarreo (transporte) para el manejo de la red para el sistema AccessBuilder 8000. El software del AccessView puede operar en una arquitectura cliente/servidor o sólo cliente, que le permite al sistema de gestión de red (NMS) escalar desde un ambiente pequeño hasta una operación de transporte (acarreo) con cientos de sistemas. Incluido en la linea de productos que son para el Cliente AccessView, Servidor, Elaborador de Informe y Agente SNMP.

Ventanas para interface con el usuario

Las Ventanas de interface del AccessView para Clientes provee acceso fácil a la información de gestión del AccessBuilder 8000 mediante menús, páginas de propiedades, y operaciones de configuración automatizadas.

Operación cliente o cliente/servidor

Las redes grandes de los sistemas del AccessBuilder 8000 son la mayoria efectivamente administrados para combinar el AccessView para Cliente y Servidor. Cada AccessView para Servidor soporta continua configuración, verificación, y diagnósticos para hasta 256 sistemas AccessBuilder 8000 simultáneamente. Los otros

aspectos claves para el servidor son el mantenimiento de archivos de registro en tiempo real mostrando todas las estadísticas de desempeño y sucesos, la capacidad para exportar estadísticas, y un agente SNMP. El agente SNMP le permite a cualquier plataforma de gestión SNMP proveer gestión de falla para una red de sistemas AccessBuilder 8000.

Característica de gestión

El software del AccessView provee ambas configuraciones conectada y fuera de línea, también remota o localmente. La configuración se efectúa rápida y eficientemente mediante configuraciones de falla, una biblioteca de configuraciones estándares, y una función de copia que permite a los operadores hacer cambios de configuración de gran volumen. La línea de productos AccessView ofrece verificación no - disociadora, alarma automática y reportes.

j) CARACTERISTICAS DEL UPS

Usos

- Computadoras personales Múltiples & Estaciones de Trabajo
- Redes de Area Local
- Sistemas de telecomunicaciones
- Unidades de Rackmount.

Regulación de voltaje activa.

FERRUPS tiene la capacidad para trabajar con todos los tipos de fuentes de entrada y cargas. La Regulación Activa de Voltaje convierte la potencia desde casi cualquier fuente de AC en la potencia del equipo.

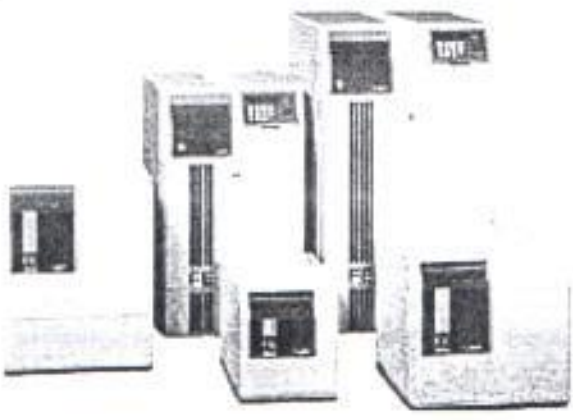


Figura 114: UPS

Mayor tiempo de trabajo.
FERRUPS provee voltaje regulado de salida sin la potencia de las baterías para entradas de voltaje hasta el 38 por ciento nominal (basado en el tamaño de la carga). Esto hace que las pilas permanezcan totalmente cargadas para protección contra los apagones.

Elimina armónicos.
FERRUPS detiene las corrientes armónicas nocivas generadas por el amplio uso de fuentes de alimentación en modo conmutado(SMPS) donde ellos podrían desorganizar las operaciones del equipo.

Carga compatible para la computadora.
FERRUPS garantiza seleccionar correctamente las demandas de las cargas de los equipos, incluyendo el factor de potencia corregido, modo conmutado, y fuentes de alimentación lineal.

Comunicaciones mejoradas.
FERRUPS trae aún más flexibilidad y energiza al equipo de mayor ganancia. En comunicaciones el UPS provee:

- Revisión de UPS y conjunto de Interfaces.
- Disponible para Redes Compatibles/SNMP
- Interfaces de Usuario RS232 mejorado

Confiabilidad aumentada.
El tiempo para que presente fallas (MTBF) oscilan en más de 160,000 horas.

Diagnósticos mejorados.
FERRUPS ejecuta encendido automático y programa de pruebas sobre las tarjetas lógicas, baterías, inversores, y otros sistemas críticos.

Especificaciones

- Rápida Protección. Cumple con las normas ANSI/IEEE C62.41 y C62.45, Categoría A y pruebas en la más alta de la Categoría B.
- Aislamiento: Completo en la línea. Menos de 2pF efectivo de capacitancia. El neutro en la salida afianzado con una conexión a tierra.
- Rechazo de Ruido: Modo Común - mayor de 120dB. Modo Transversal (Normal) - mayor de 60dB.
- Regulación: ±3% para entradas de voltaje desde +15% a -20% nominal. Si cualquier línea, carga, o las condiciones de pila exceden las normas de regulación de voltaje CBEMA y ANSI para regular el equipo.

- Continua no-ruptura de Potencia: FERRUPS provee permanente, sin ninguna ruptura de energia del completo o momentàneo suministro eléctrico.
- Potencia en onda Seno: FERRUPS provee en la onda senoidal, potencia gradual en el equipo con 5% o menos de Distorsión Armónica Total (THD) en la carga (KW). Cumple con la norma CSA C22.2 No. 107.1 para la distorsión armónica.
- Tipo de Fuente de alimentación en modo conmutado: La tipica fuente de alimentación en modo conmutado tiene un factor de potencia de 0.7 a 0.83 y un factor de cresta de 2.7 a 3.5. Garantiza la compatibilidad con carga total del equipo, incluyendo el factor de potencia corregido.
- Interface Interactivo inteligente: el puerto RS232 se caracteriza por tener una comunicación serial full-dúplex.
- Protección: Transformador genera protección contra sobrecarga (limitante de corriente). Algunos modelos tienen receptáculos protectores como cortadores de circuito o fusibles.
- Capacidad de Sobrecarga: 125% para 10 minutos en linea y 110% para 10 minutos para inversos.
- La frecuencia: 50Hz o 60Hz nominal. En linea - la frecuencia de salida trabaja dentro de limites ajustables (±0.01HZ a ±3HZ). En inversos es ±0.005HZ.
- Temperatura de funcionamiento: 0° a 40°C. Temperatura de Almacenaje: - 20° a +60°C (- 20° a +40°C si la bateria no es quitada). Humedad Relativa: 0 a 95% sin condensación.
- Requerimiento de Ventilación: Limpio, libre de quimicos de corrosión u otros contaminantes con la circulación apropiada de aire.
- Altitud para operación: La temperatura ambiente máxima para funcionamiento, el minimo es 1°C para 305 metros (1000 pies) sobre el nivel del mar siendo la altura máxima de 3050 metros (10,000 pies).

3.8. CONTROL, MONITOREO Y TIEMPOS DE RESPUESTA DE LA RED.

Para el control y monitoreo, la empresa no cuenta con un software adecuado que se encargue íntegramente a realizar permanentes pruebas a los equipos y enlaces para verificar su condición. Por este motivo, el control lo realizan manualmente. Es decir, que el operador permanentemente debe ejecutar los comandos para comprobar el funcionamiento correcto del sistema. Para ello, los comandos más utilizados son: *ping* y *tracerout*. El lenguaje utilizado por el sistema es UNIX, y desde allí realizan el control.

El comando *ping* es simplemente una llamada "*solicitud de eco*" que requiere de una "*respuesta de eco*". El terminal que en este caso envía un frame de prueba, el cual debe ser respondido. Si el terminal de origen recibe una respuesta, quiere decir que en su trayectoria o el equipo que se decidió realizar la prueba no tiene ningún problema. En caso de no recibir respuesta, el problema está en alguna parte de la trayectoria o en el equipo mismo. Entonces para ello, se verifica toda la trayectoria, hasta llegar al equipo, sea este local o remoto. A continuación se muestran algunos ejemplos del monitoreo que sse realizó desde un terminal de la red. En este caso, la prueba se hizo bajo Windows, ya que el terminal posee dicho software.

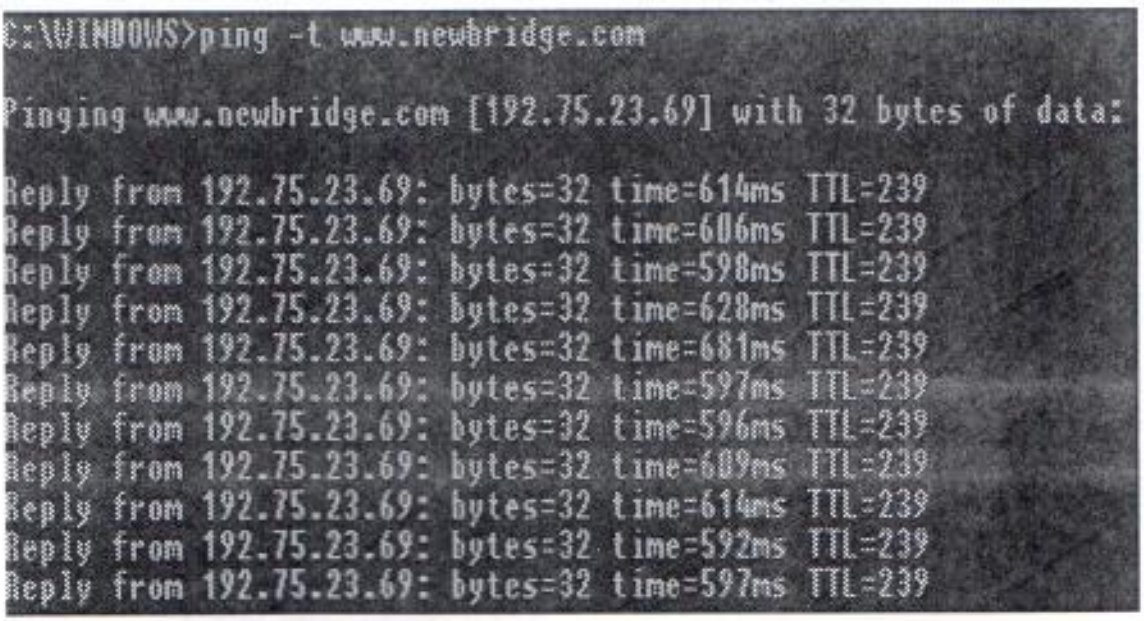


Figura 115: Ping a www.newbridge.com

En esta figura se puede observar la ejecución del comando *ping* en una dirección IP cualquiera, en este caso se ha tomado la dirección 192.75.23.69, que pertenece a www.newbridge.com. Se ha requerido el tiempo de respuesta que demora el requerimiento

en ir y volver, es decir, en llegar la solicitud y la respuesta del eco. Se observa algunos tiempos de respuesta, desde el más bajo que es 592 msegundos, hasta el más alto que es 628 msegundos. También se está garantizando que la red está enviando y recibiendo respuesta, con lo que se puede decir que los enlaces y equipos que se comunican con el exterior están funcionando bien. Pero, para evaluar el correcto funcionamiento de los demás equipos y enlaces, se debe seguir el diagrama de rutas y enlaces redundantes que después se describirá detalladamente. Si no se recibiera respuesta, se tendría que realizar *ping* en cada equipo de la red, especificando su dirección IP, y en el equipo o enlace que no se reciba señal de retorno, se sabrá que el problema está allí. La otra forma es realizando un *tracerout*, que muestra las direcciones IP por las que va pasando en su trayectoria. Aquí también se especifica las direcciones en las que no se pudo continuar.

En todos los casos, el tiempo de respuesta empleado es menor que el *"time out"*. Si se obtuviera un tiempo de respuesta mayor que el del *"time out"* que el equipo requiere, se estaría en el caso de una señalización de no-cumplimiento de dicho tiempo. En el siguiente ejemplo se analiza este caso.

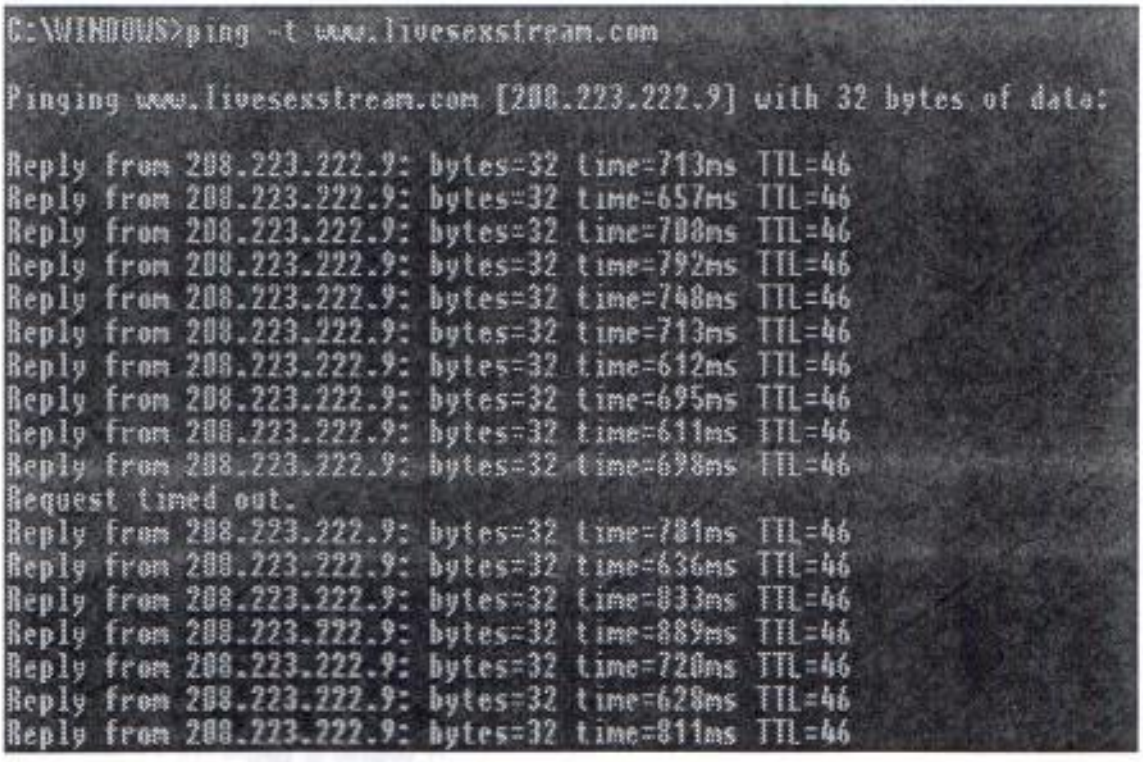


Figura 116: Ping a www.livesexstream.com

En este ejemplo, se ha realizado un *ping* a la dirección 208.223.222.9 que es el servidor donde se encuentra esta página web www.livesexstream.com. Se observa que existen varios tiempos de respuesta, desde el más alto que es 889 msegundos hasta el más bajo que es 611 msegundos, con la particularidad de encontrar un caso con *Request timed out*. Quiere decir que el tiempo de respuesta que se recibió fue mayor que el *time out* del sistema, debido al retardo. Se observa que los tiempos de respuesta en este caso son mayores a los anteriores.

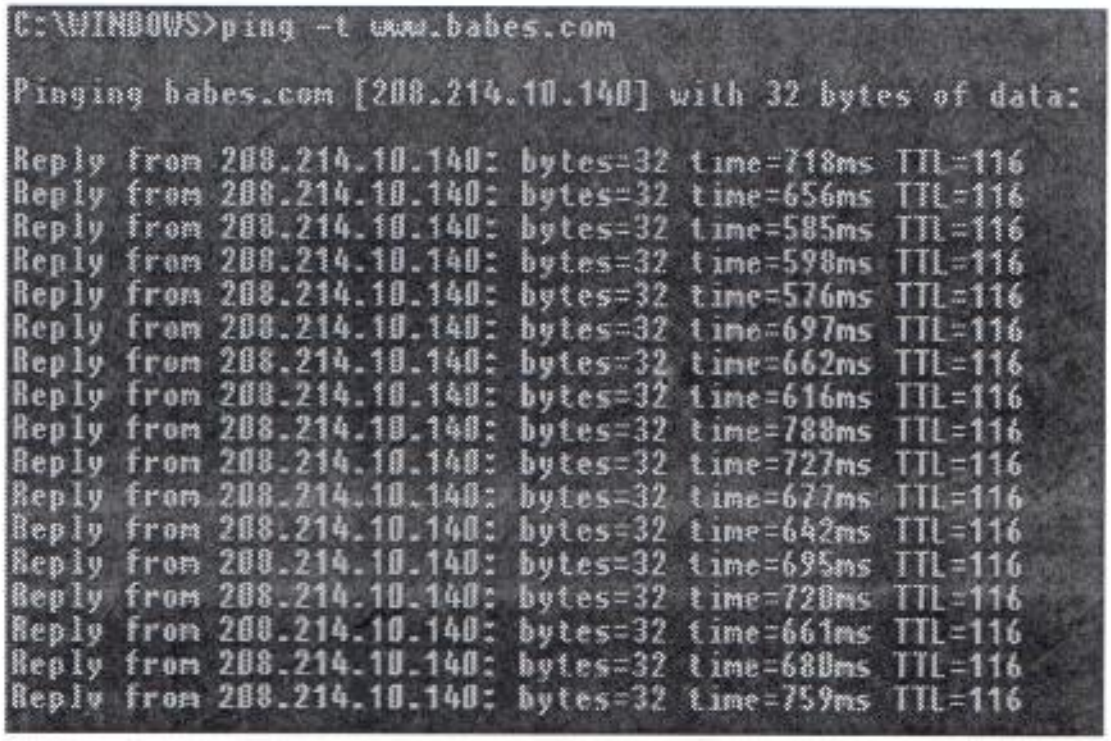


Figura 117: Ping a www.babes.com

Ahora se realizó un ping a la dirección 208.214.10.140 correspondiente al servidor donde se encuentra el web de www.babes.com. Los tiempos de respuesta en el caso más alto es 788 msegundos y el caso más bajo es 576 msegundos.

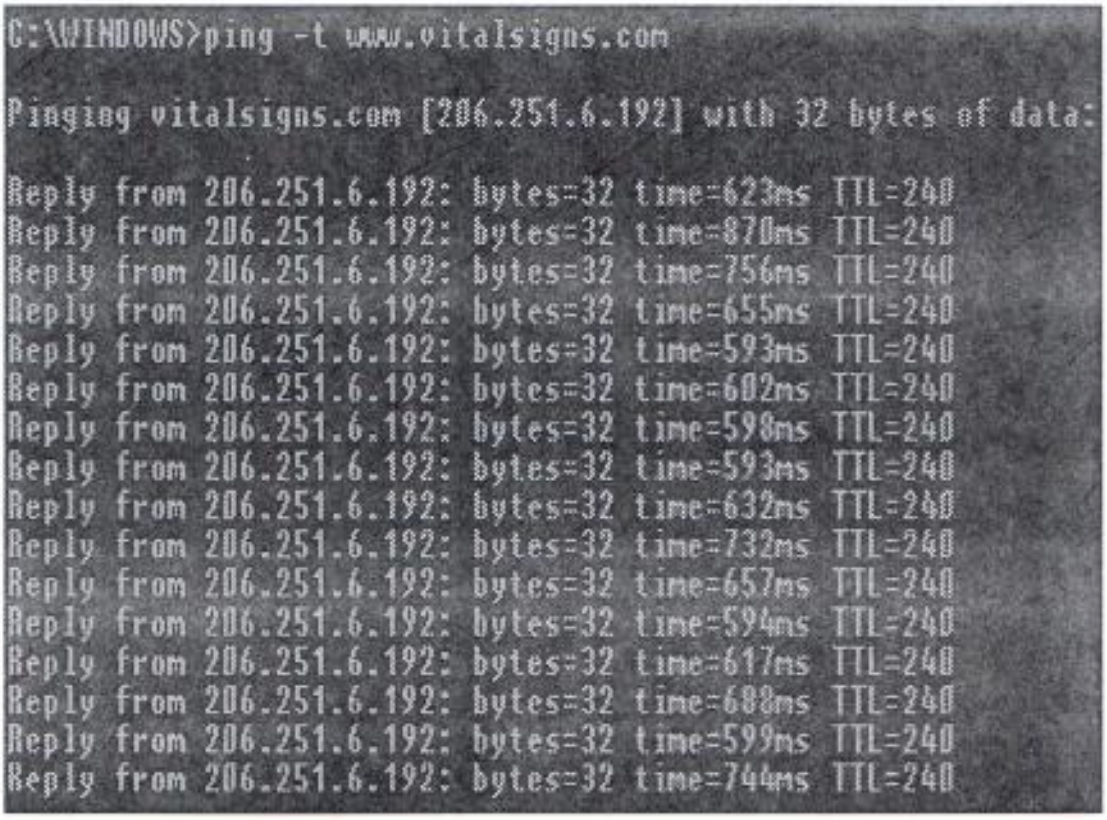


Figura 118: Ping a www.vitalsigns.com

El comando *ping* fue ejecutado hacia la dirección 206.251.6.192, servidor donde se encuentra la página web www.vitalsigns.com. El tiempo de respuesta mayor es 870 msegundos, y el menor es 593 msegundos.

Figura 119: Ping a ftp.eclipse.dk

Para este caso, el *ping* se realizó a la dirección 206.14.172.169 correspondiente al servidor donde almacena ftp.eclipse.dk. Los tiempos de respuesta desde el más alto que es 885 msegundos y el más bajo 698 msegundos.

En vista que la empresa no cuenta con un software adecuado, se lo buscó con la finalidad de que realice el monitoreo, y que mejore el análisis del control. Este software tiene el nombre de Net.Medic, el cual también se menciona en el capítulo 4. Tiene la capacidad de determinar cuántos saltos se ha realizado para llegar a la dirección IP destino, en el cuadro donde especifica los Hops. En este caso, aún no se lo ha logrado determinar , ya que en uno de ellos no es capaz de determinarlos debido a algún problema en la red remota. Cuando presenta problemas de conexión con la dirección IP destino, o en su trayectoria, el servidor dibujado a la derecha de Hops se presenta de color rojo intenso. Presenta los paquetes enviados y recibidos en kbps, en diagrama de barras, recuperación de paquetes en los servidores en valores de porcentaje, la utilización de la carga del CPU en porcentaje, utilización de memoria caché, velocidad del módem con capacidad de compresión de datos, porcentaje de tráfico tanto en la Intranet como en Internet. Inclusive, tiene la opción de mostrar ayuda e informes para cada problema presentado. Además, presenta un resumen en diagrama de barras del tráfico, tiempos de respuesta, retardos, velocidades, niveles de degradación.

A continuación, se presenta el monitoreo mientras se navegaba en la dirección ftp.eclipse.dk. En este caso el programa no puede determinar el número de saltos, porque

no reconoce la trayectoria entre los dos puntos en que existe mayor separación. Se puede observar el nivel de velocidad de envío y recepción de paquetes, ya que en este caso, se encontraba transfiriendo un software de 5 Mb. al terminal. Se ha observado que la recepción es muy marcada, en paquetes de medida variable, teniendo un límite de velocidad de 11.5 kbps para recepción y 0.8 kbps para transmisión. En ese momento, el porcentaje de carga del CPU es del 3%, con el porcentaje de recuperación del 99% en el servidor remoto y 1% en el servidor de la red. Utiliza un 83% de memoria caché. Existe el 1% de tráfico en el Internet.

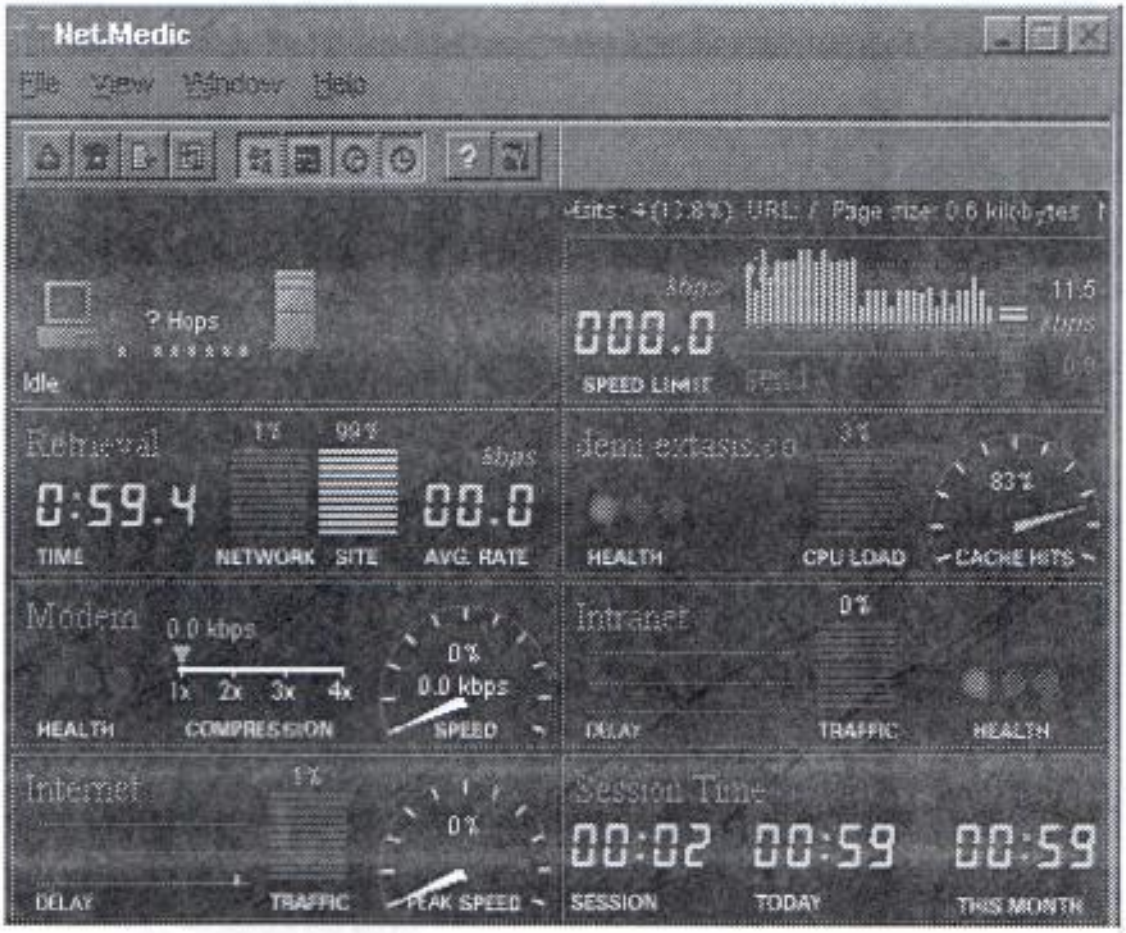


Figura 120: Monitoreo explorando ftp.eclipse.dk

En este instante, el nivel de límite de velocidad de 34.5 kbps para la recepción, y 1.7 para transmisión, debido al envío de paquetes provenientes de la dirección mencionada. El nivel de carga del CPU está en un 2%. Los restantes valores se mantienen.

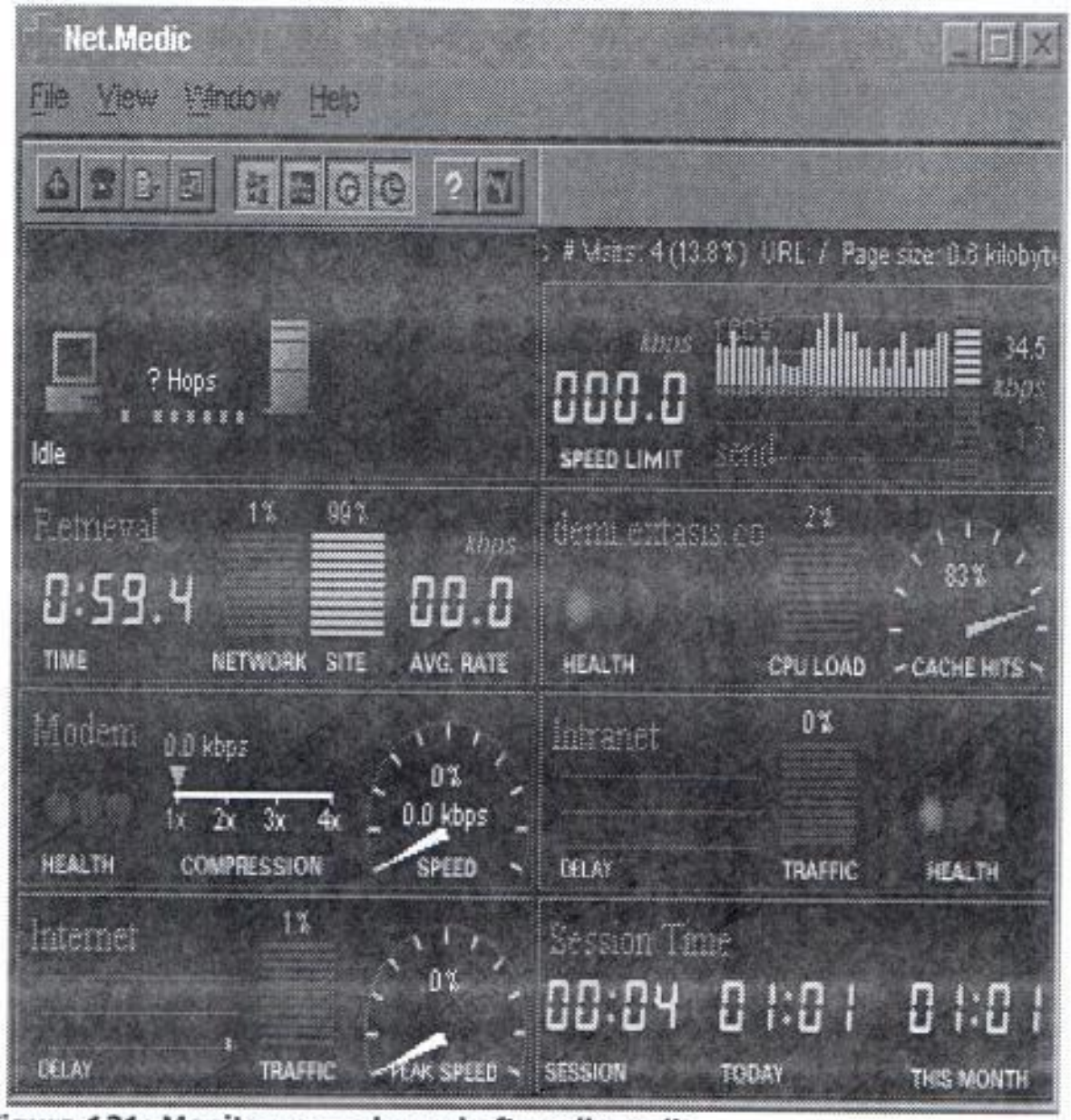


Figura 121: Monitoreo explorando ftp.eclipse.dk

Ahora, se ha visitado la dirección www.vitalsigns.com, en donde se observa la señal de transferencia de datos mostrando hojas volantes que representan al intercambio de información. Además no encuentra el número de saltos en su trayectoria. La velocidad de recepción es 32.7 kbps y de transmisión 4.8 kbps. El valor promedio de velocidad es de 21.3 kbps. El nivel de recepción es mucho mayor que el de transmisión, debido a que se estaba comunicando con el servidor de dicha dirección.

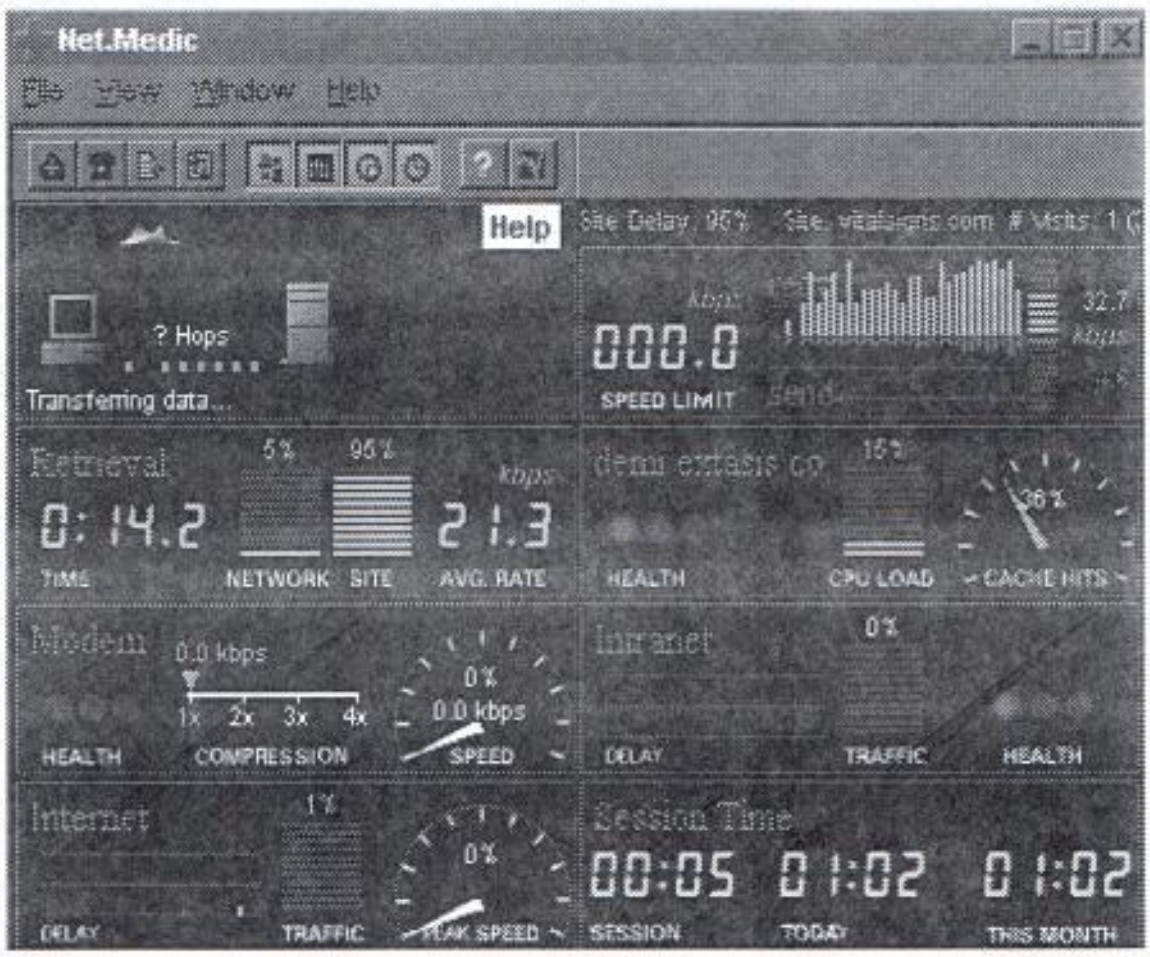


Figura 122: Monitoreo explorando www.vitalsigns.com

Al visitar la dirección www.babes.com, se observa que no se determinan el número de saltos. La velocidad es más variable que los anteriores casos, porque los datos en su gran mayoría ya han sido transferidos. De ahí, los paquetes oscilan entre 46.1 y en algunos casos hasta 0 kbps para la recepción y de 0 hasta 1.7 kbps. El valor promedio de velocidad es de 31 kbps. La recuperación es de 96% remotamente y 4% en el servidor local. Ocupa un 31% de caché, con un 21% de carga del CPU. Existe el 1% de tráfico en el Internet.

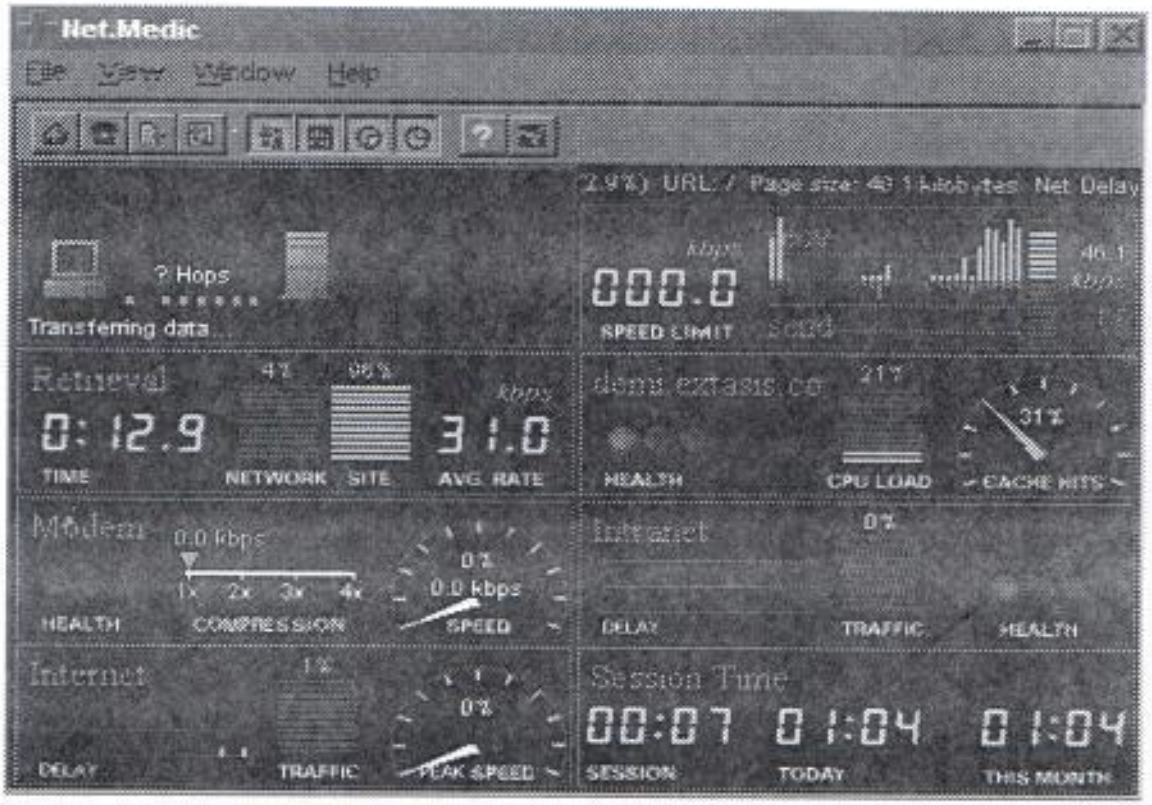


Figura 123: Monitoreo explorando www.babes.com

En esta ocasión se visitó la dirección www.livesexstream.com, que en su trayectoria ha dado 18 saltos. En este gráfico se observa que se encuentra en estado Idle, lo que quiere decir que ya ha terminado de transferir datos. Los niveles de velocidades de transmisión y recepción prácticamente han desaparecido, con muy pocas excepciones. Tiene un nivel de recuperación de 85% remotamente y 15% en la red. Tiene un nivel promedio de velocidad de 12.7 kbps. El nivel de carga del CPU es el 3%, utiliza un 27% de caché, con un aumento considerable en el Internet del 88%, mucho más grande con relación a muestreos anteriores.

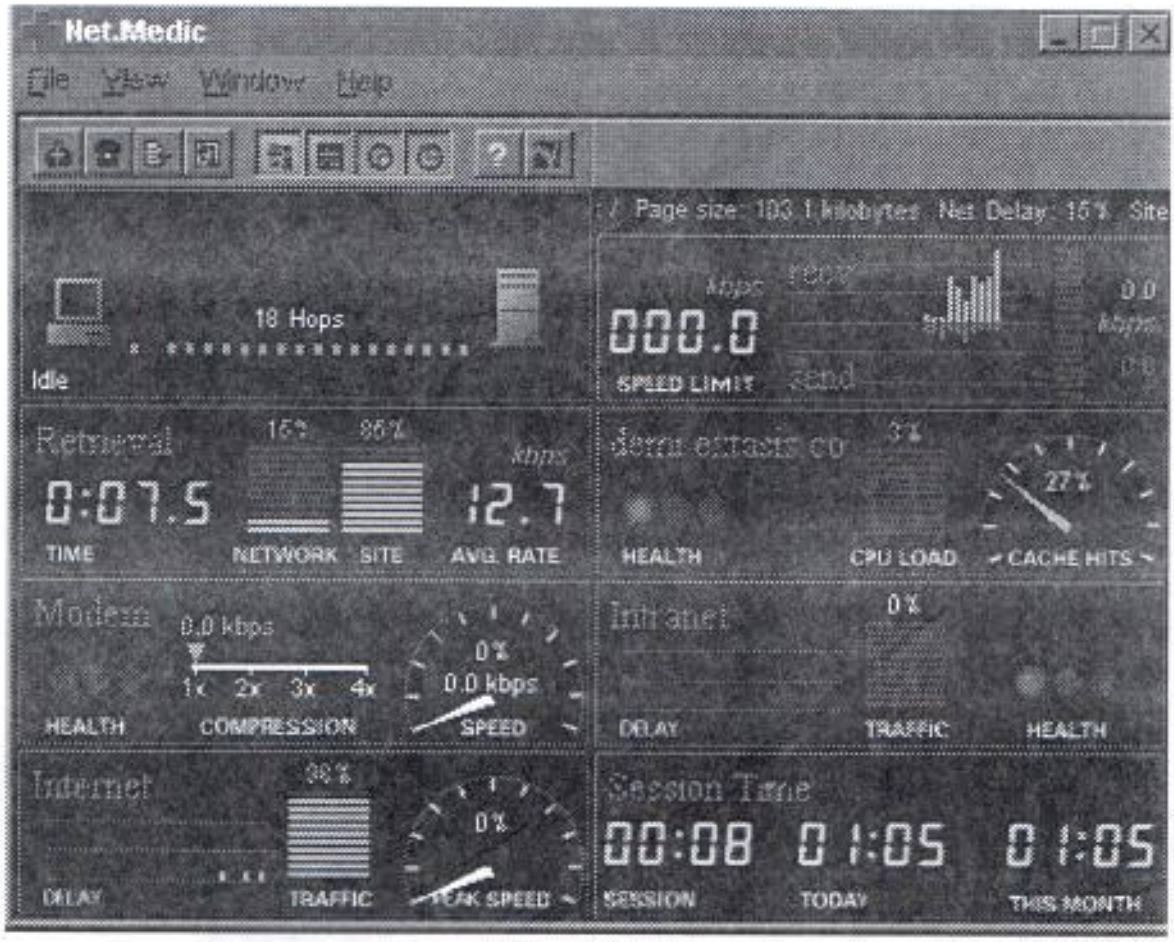


Figura 124: Monitoreo explorando www.livesexstream.com

En esta dirección visitada, www.newbridge.com, se puede observar que la transferencia de datos se está realizando es este momento, con niveles de transmisión y recepción variables, siendo 51.8 kbps para recepción y 7 kbps para transmisión. El valor promedio de velocidad es de 1.3 kbps, con un 93% de recuperación en el sitio remoto y 7% en la red. Utiliza el 14% de caché, con un 71% de carga del CPU. El tráfico en Internet es el 1%.

Figura 125: Monitoreo explorando www.newbridge.com

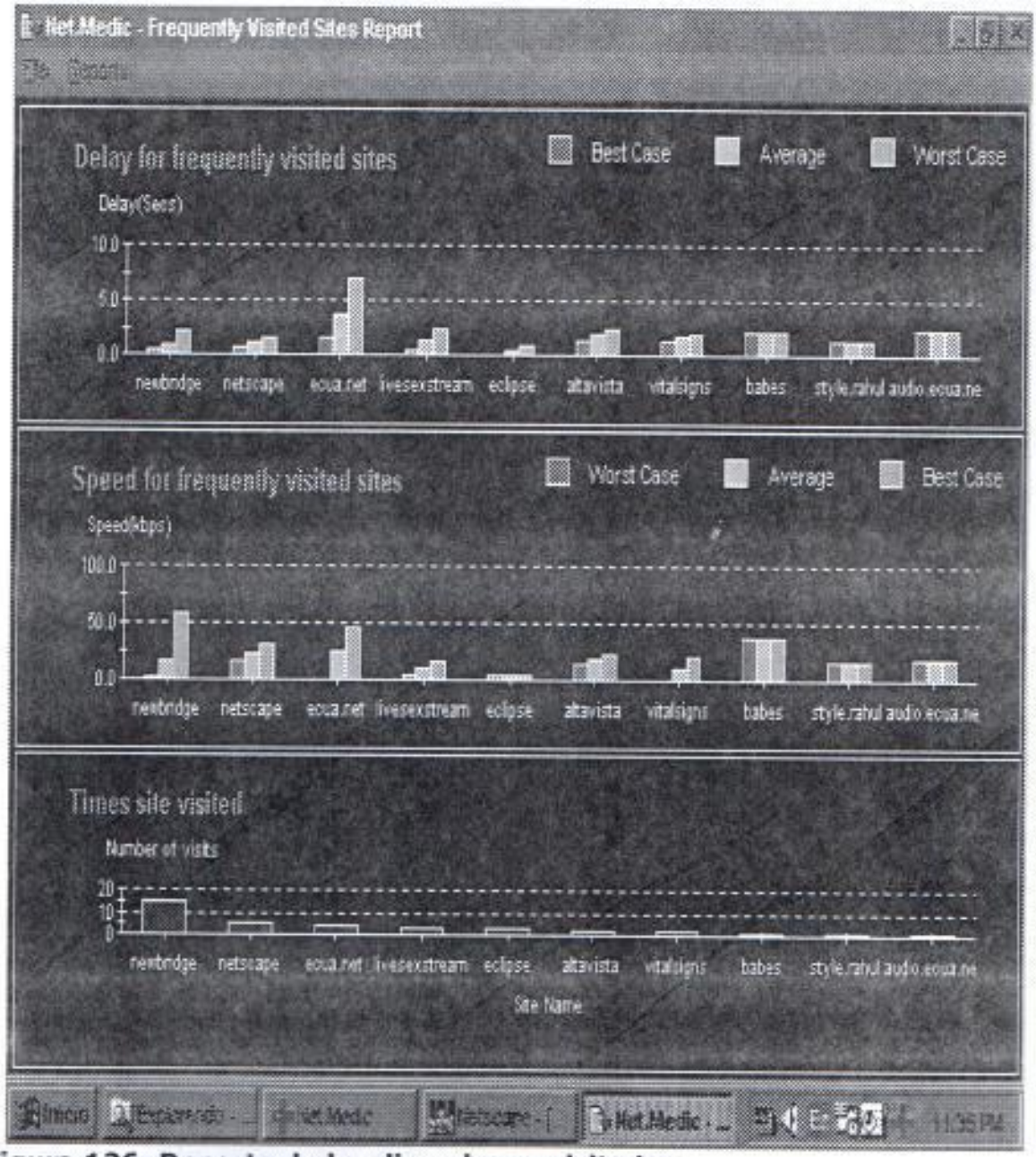


Figura 126: Reporte de las direcciones visitadas

Este gráfico muestra el resumen del monitoreo, presentando los gráficos de retardos, velocidad y el tiempo de visita en las direcciones. El primer diagrama especifica los retardos para cada sitio visitado, donde se aprecian los mejores y peores casos, incluyendo promedios. El peor caso es cuando se conecta con EcuaNet, otro proveedor local del servicio de Internet, donde llega a 7 segundos de respuesta, ya que es un tiempo

demasiado elevado. La razón es sencilla. En este medio no existe una conexión interna. Asi, si se desea conectarse con cualquier proveedor, sea de Guayaquil o de otra ciudad del país, la ruta que toma es via satélite, llegando hasta Miami para regresar nuevamente al destino, en este caso EcuaNet, respondiendo via Satélite hasta Miami, y por el mismo medio regresa la señal a la red, que finalmente la maneja el usuario. Por eso tiene el más alto retardo, por el doble salto satelital. En todos los demás casos, la red realiza un solo salto. El retardo también depende de los saltos que se encuentre en la trayectoria tomada. Depende del nivel de comunicación con las otras direcciones. Pero sin duda se debe mejorar el enlace local, lo cual en el capitulo 4 de optimización se detallará.

El mejor caso que se puede notar es la dirección ftp.eclipse.dk. La comunicación con este servidor es óptima.

En el segundo gráfico, se resumen las velocidades que se ha alcanzado en cada dirección. El mejor caso es www.newbridge.com, donde alcanza hasta 60kbps, y el caso más bajo es el ftp.eclipse.dk donde alcanza velocidades muy pequeñas.

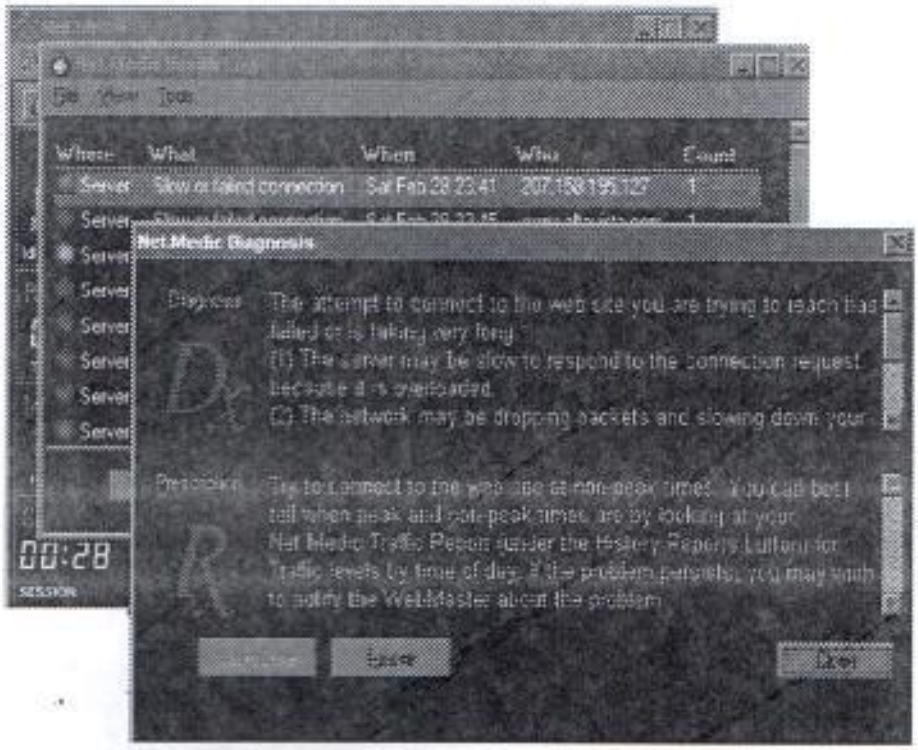


Figura 127: Detalle de problemas en la conexión y posibles soluciones

Aquí se muestra la explicación y ayuda de los problemas que se pueden presentar en los diversos servidores a los que se accesa. Muestra la causa del problema, fecha, hora, dirección y número de intentos de conexión. Presenta un diagnóstico y prescripción de lo que se puede hacer para solucionar el problema.

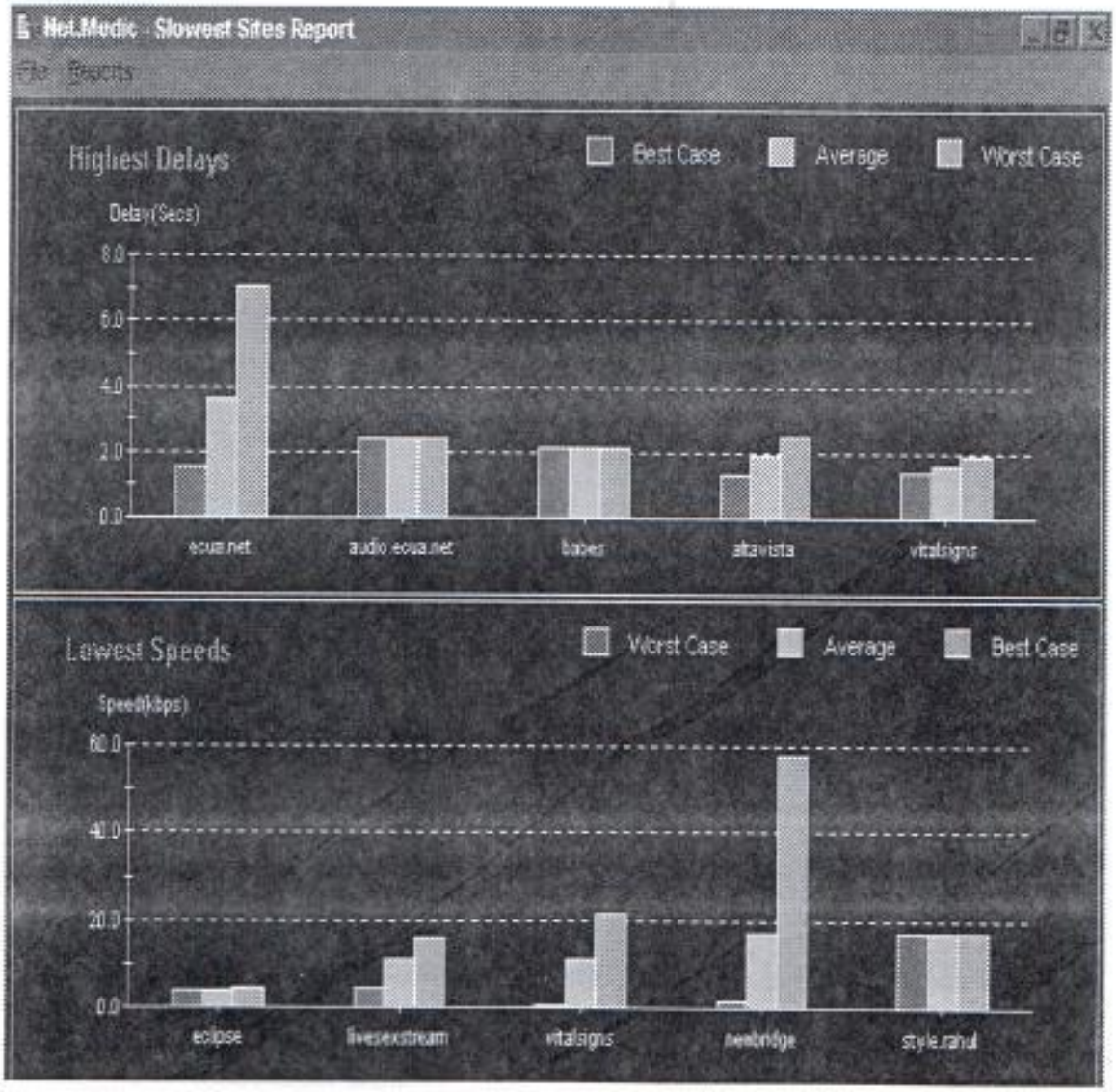


Figura 128: Reporte de los sitios de más altos retardos y más bajas velocidades

Se muestran dos gráficos. El primero especifica los más altos retardos, liderando el enlace con ecuanet. El segundo demuestra las más bajas velocidades. El más bajas velocidades pertenecen a la dirección www.newbridge.com. Se puede observar el mejor, peor y el caso promedio.

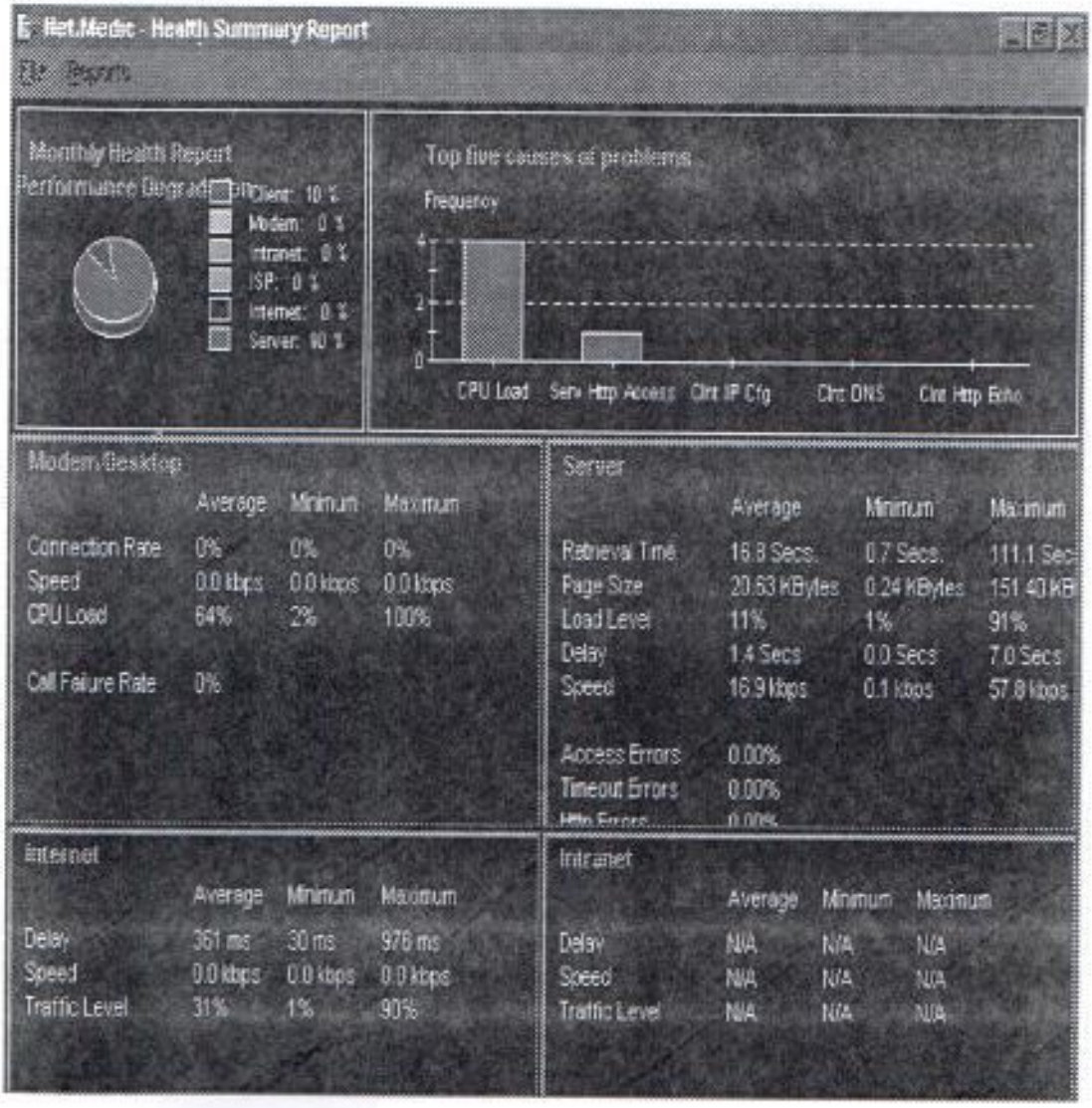


Figura 129: Resumen General

En diagrama de pastel se muestra el porcentaje de degradación, donde el 90% corresponde a los servidores y el 10% a los usuarios. Luego se muestra las 5 probables causas de los problemas ocasionados. En gran parte se le asigna a la carga

del CPU que oscila entre el 2% y el 100%, en segundo término a problemas con los servidores remotos.

Respecto a los servidores, se muestra los tiempos de recuperación, oscilando entre 0 0.7 y 111.1 segundos. Además se especifica las medidas de las páginas que se accesa, mostrando también niveles de carga que se encuentran entre el 1% y el 91%, con retardos que oscilan entre 0 y 7 segundos que ya se analizó anteriormente. La velocidad se encuentra entre los 0.1 y 57.8 kbps.

Los retardos en Internet oscilan entre los 30 a 976 msegundos, con un nivel de tráfico del 1% al 90%.

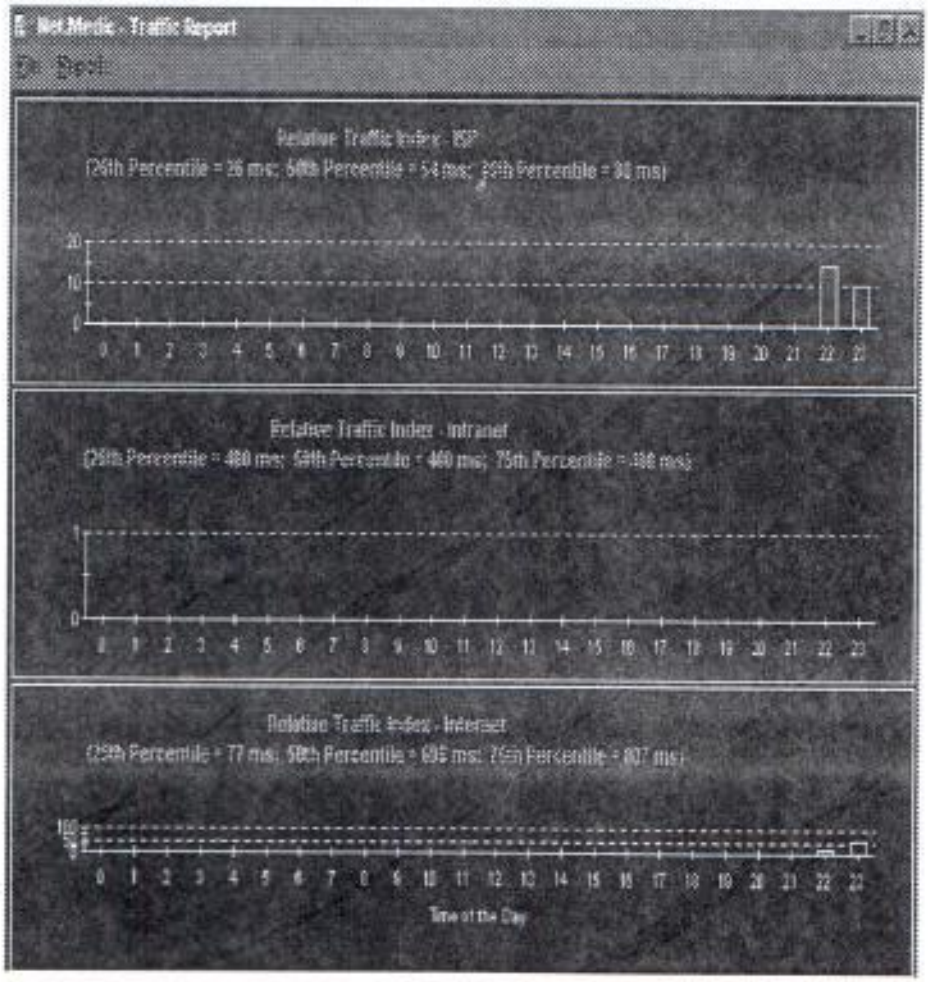


Figura 130: Reportes de Tráfico

Los indices relativo de tráfico para el proveedor está descrito en la primera parte del gráfico. Se observa que los tiempos relativos que son 26, 54 y 80 msegundos. Los indices relativo de tráfico en la Intranet es de 400 msegundos. Los indices relativos de tráfico para Internet son de 77, 696 y 807 msegundos.

3.9 RUTAS Y ENLACES REDUNDANTES

Al analizar esta red, se puede notar que existen rutas redundantes que permiten asegurar el funcionamiento de la red, asi existan problemas con ciertos enlaces.

Se ha realizado un estudio de las rutas más importantes, es decir, los recursos más utilizados por los clientes, los cuales son el correo electrónico y navegación.

Para empezar, cada equipo contiene una dirección IP correspondiente, y se clasifican en 2 grupos, 200.31.31.- y 206.72.133.-. Las direcciones del primer grupo pertenecen a los usuarios que se comunican via dial-up o en red con la central Urdesa, y las del segundo grupo corresponden a los usuarios que se comunican con la red de la central Kennedy. Asi, como se ha analizado anteriormente, los usuarios de Internet pueden comunicarse con cualquier servidor del mundo, a través de su dirección IP, mientras la red se lo permita, pero para ello, el requerimiento tiene que transportarse via satélite, mientras que la comunicación con servidores entre estos 2 grupos puede realizarse por las conexiones microondas y radial, sin necesidad de realizar el doble salto satelital.

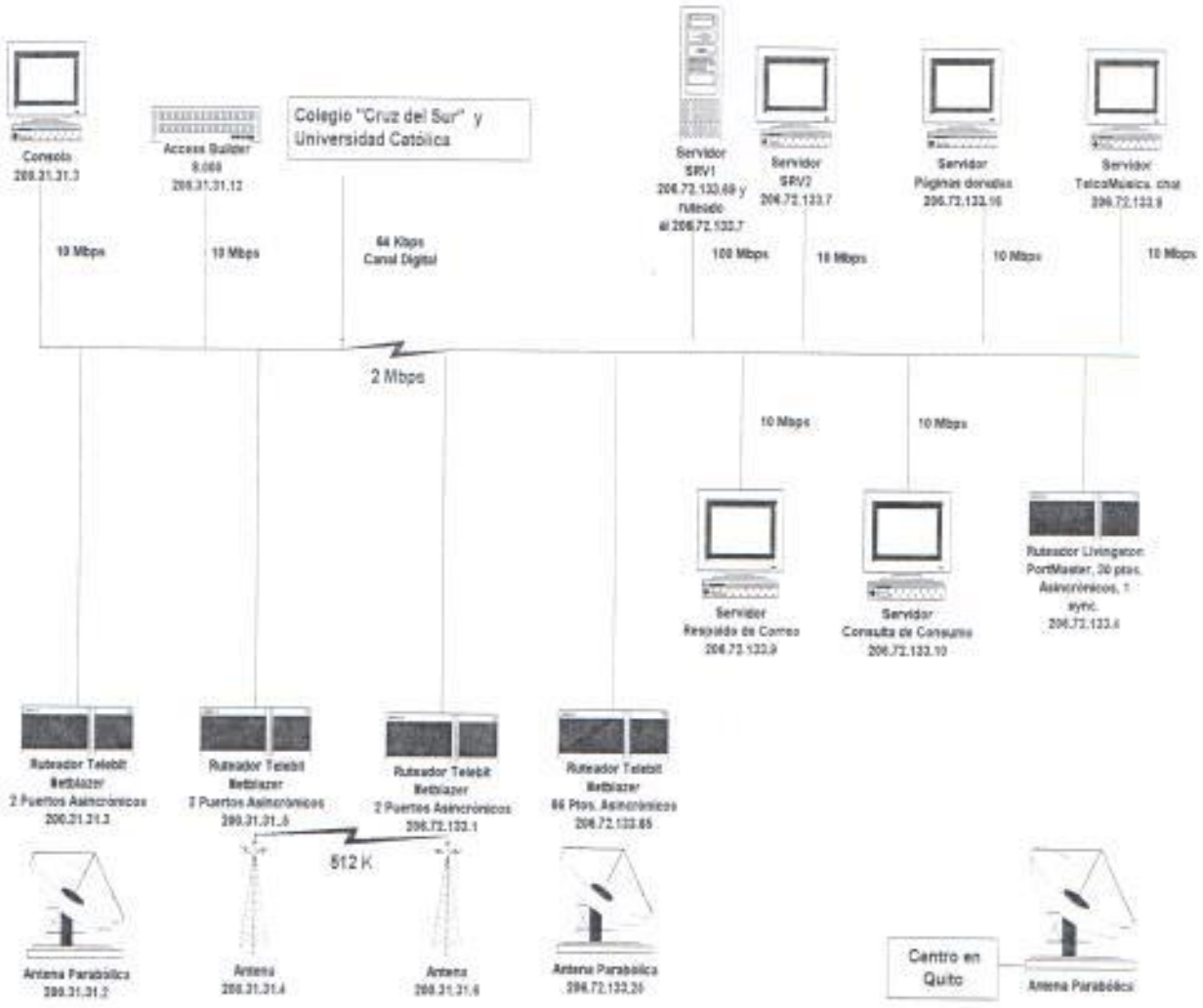


Figura 131: Esquema General de la Red

3.9.1 CORREO ELECTRONICO

Los servidores para brindar el servicio de correo electrónico son SRV1 y SRV2. Ambos se encuentran en la Central Kennedy, pero tienen direcciones de ambos diferentes.

Estas rutas se configuran a través del lenguaje utilizado por la red, en este caso, UNIX. Alli se realiza una tabla de las direcciones IP que deben tomar, incluyendo las rutas alternativas. Las rutas, en su orden de prioridad, son:

- **Si se conecta a través de la dirección 200.31.31.12 que pertenece al AccessBuilder 8000, que es el equipo que comunica vía dial-up, o en red como lo hacen el Colegio "Cruz del Sur" y la Universidad Católica. La ruta a seguir para leer el correo en el servidor SRV1 o SRV2 es:**

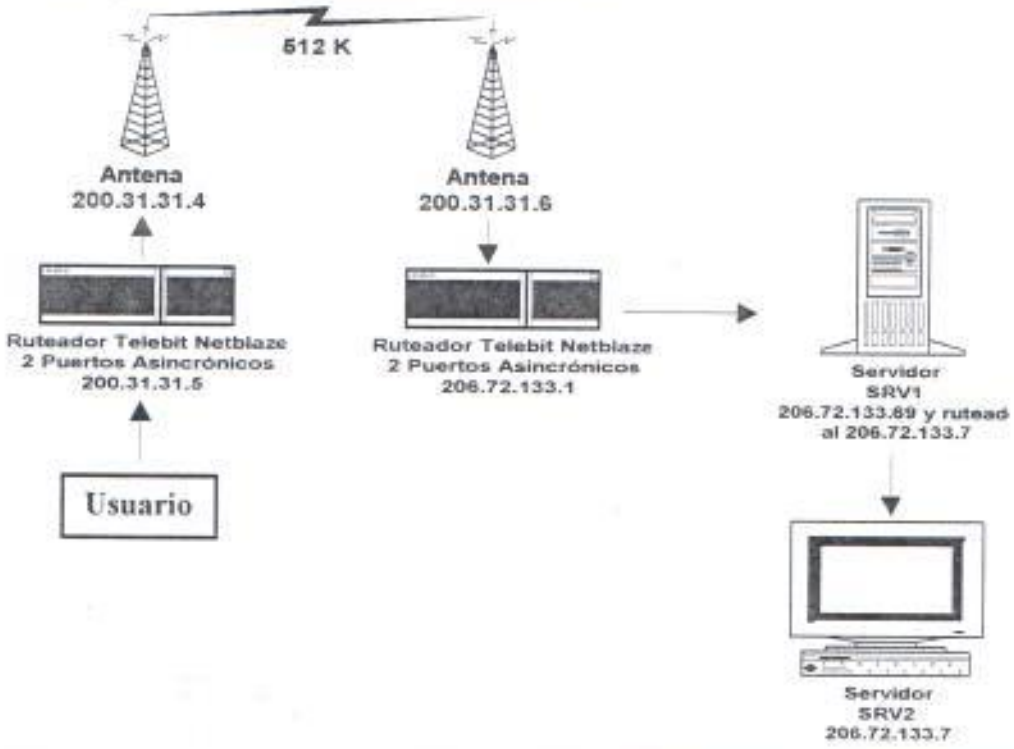


Figura 132: Ruta principal para un usuario conectado a la central Urdesa para leer su correo electrónico

- En caso de que el enlace vía microondas no se encuentre habilitado, la segunda opción para leer correo electrónico es el que se ha especificado a continuación, aunque la comunicación se volverá más lenta debido a que el microondas tiene un ancho de banda mayor que el radial.
-

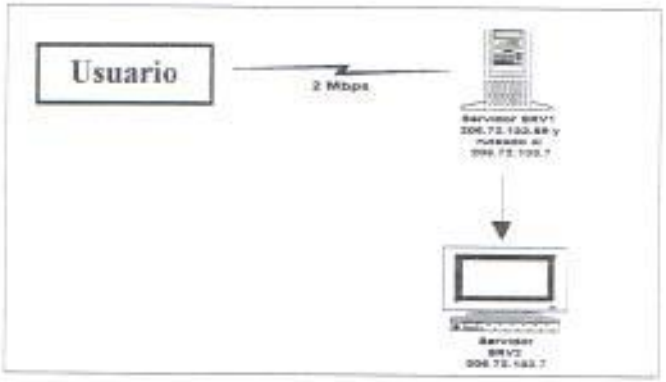


Figura 133: Segunda Ruta para un usuario conectado a la central Urdesa para leer su correo electrónico

- En caso de que ambos enlaces: microondas y radial, no se encuentren habilitados, la tercera opción es la que sigue a continuación, esta ruta va a ocasionar que el tiempo de respuesta es mayor que en los anteriores casos, debido al doble salto satelital.
-

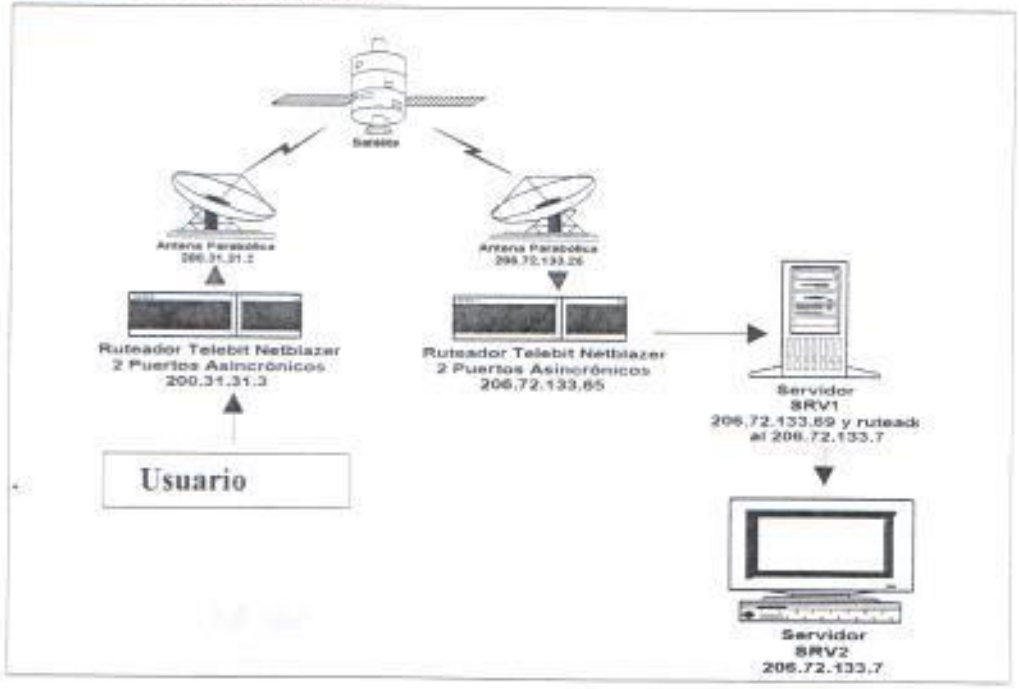


Figura 134: Tercera Ruta para un usuario conectado a la central Urdesa para leer su correo electrónico

3.9.2 CORREO ELECTRÓNICO DE USUARIOS QUE SE CONECTAN FUERA DE LA RED LOCAL.

Este caso ocurre cuando usuarios locales se encuentren fuera de la red y desean leer su correo electrónico.

- **La primera opción para la conexión es el enlace satelital a través de PanAmSat que enlaza directamente al ruteador Telebit (66 puertos asincrónicos) donde se encuentran los servidores SRV1 y SRV2. Se utiliza este enlace como prioridad ya que la conexión es directa dando como resultado el mejor tiempo de respuesta.**

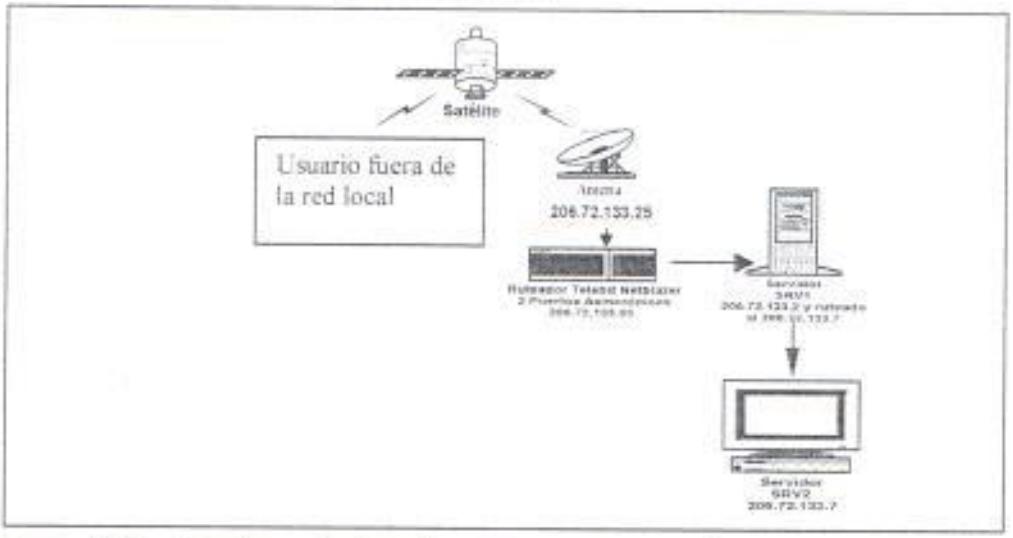


Figura 135: Ruta principal para un usuario que se encuentra conectado fuera de la red

- **Si el enlace con PanAmSat no se encuentra habilitado, la segunda opción es la conexión a través del enlace que provee Impsat con la Central Urdesa y de esta se utiliza el enlace de microondas para conectarse con la Central Kennedy.**

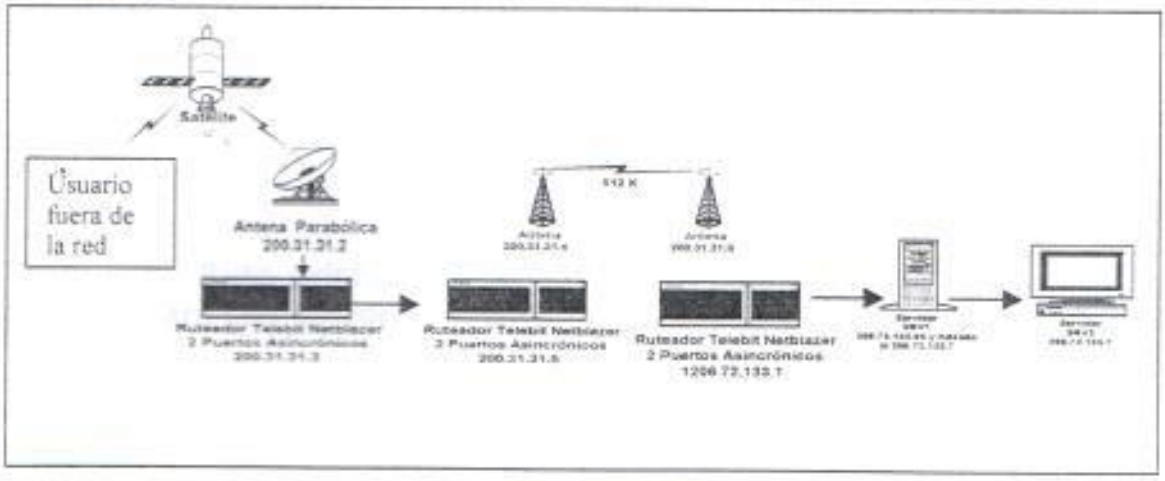


Figura 136: Segunda Ruta para un usuario que se encuentra conectado fuera de nuestra red

- En caso que el enlace de microondas no se encuentre habilitado se usa el enlace redundante entre la Central Kennedy y la Central Urdesa a través del enlace radial.

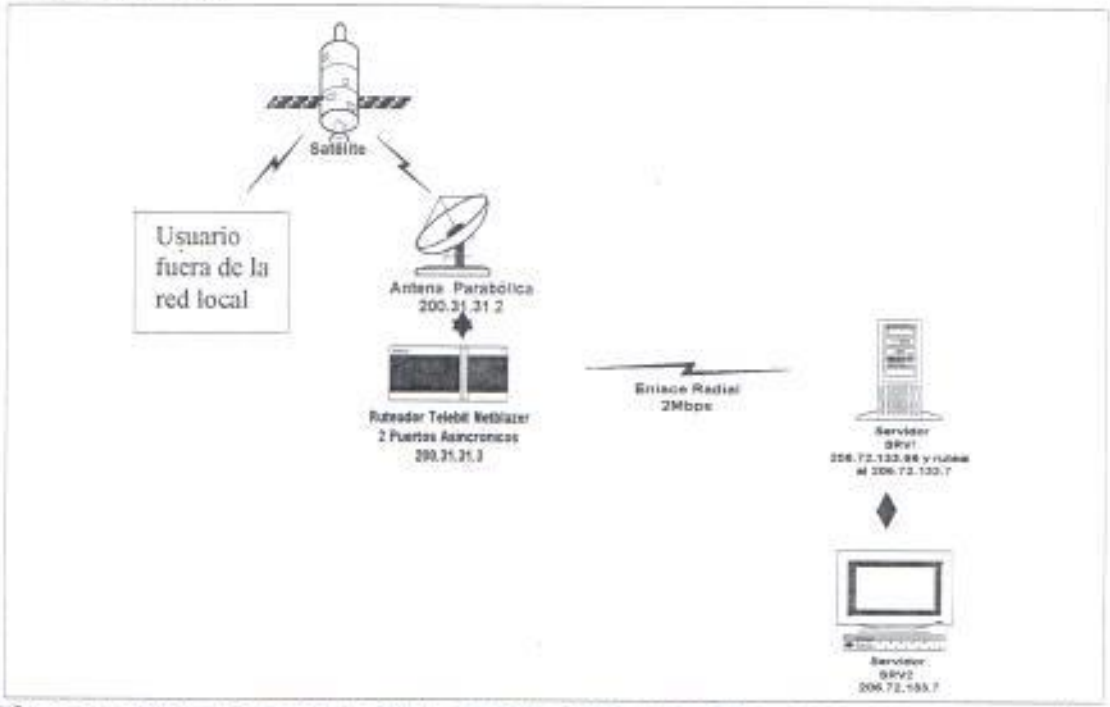


Figura 137: Tercera Ruta para un usuario que se encuentra conectado fuera de la red

3.9.3 CORREO ELECTRÓNICO EN CONEXIÓN DIRECTA A LA CENTRAL KENNEDY.

Un usuario que desea leer su correo electrónico en SRV1 o SRV2 puede hacerlo directamente vial dial-up a través de cualquiera de los ruteadores: 206.72.133.69 y 206.72.133.3. Para esta conexión no importa el estado de los enlaces satelitales, microondas y radial.

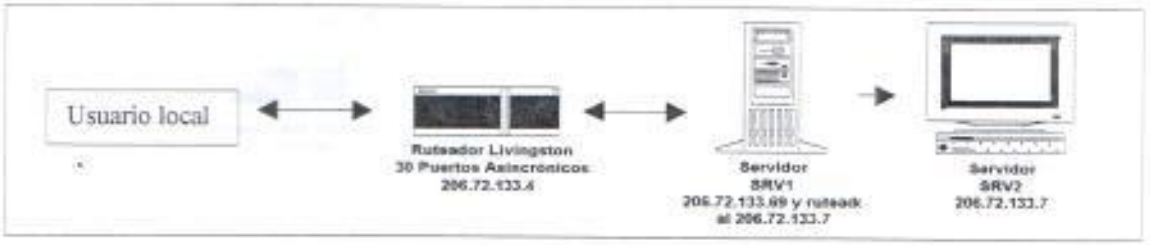


Figura 138: Ruta principal para un usuario conectado a la central Kennedy para leer su correo electrónico

3.9.4 CONEXIÓNES PARA NAVEGAR EN LA RED

- Se puede conectar a través de la Central Urdesa por medio del AccessBuilder usando los servicios de Impsat.

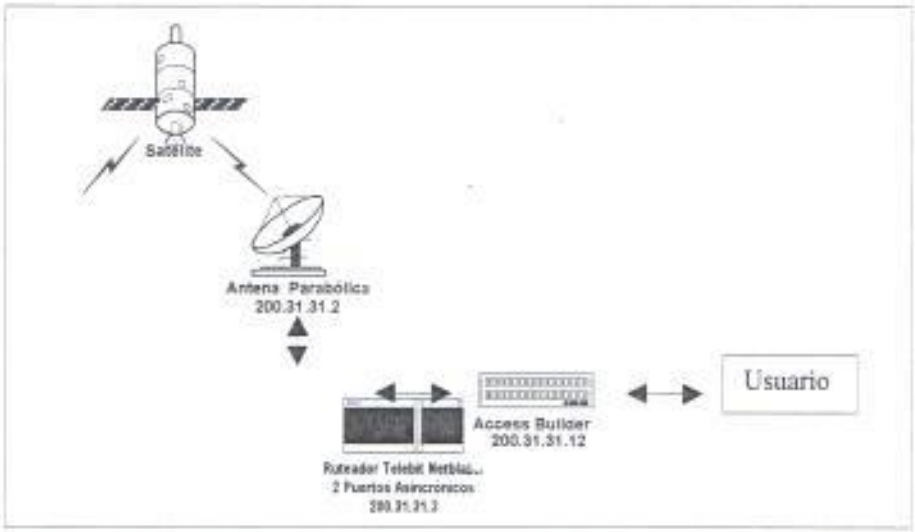


Figura 139: Ruta principal para un usuario conectado a la Central Urdesa para que pueda navegar

- En el caso de tener deshabilitado el enlace de Impsat se puede usar el enlace de microondas.

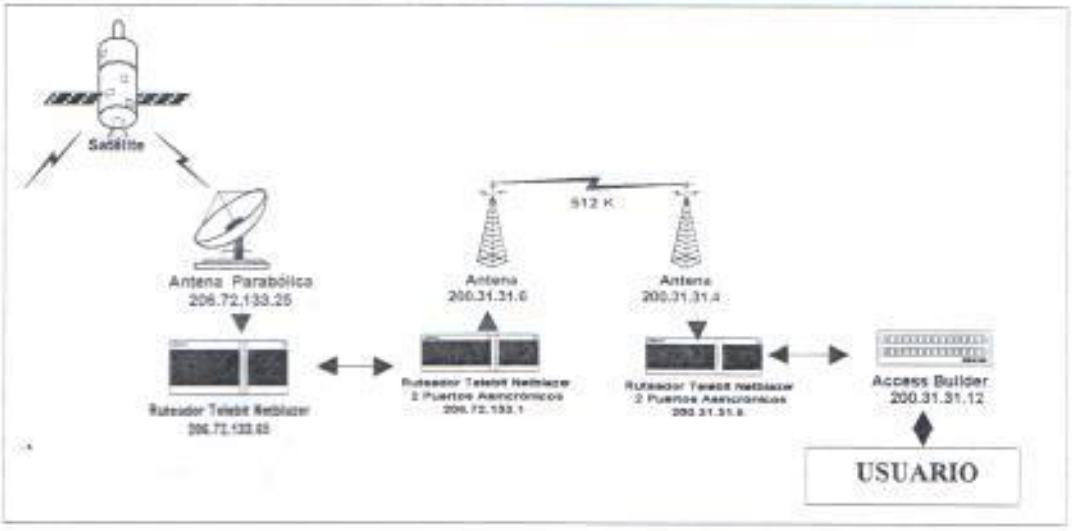


Figura 140: Ruta alterna para un usuario conectado a la Central Urdesa para que pueda navegar

3.10 JUSTIFICACION PARA OPTIMIZAR LA RED ORIGINAL

Se pueden mencionar muchas justificaciones que conlleven al mejoramiento parcial y total de la red. Todo está orientado hacia lo importante que es el cliente. Muchas veces, durante el tiempo en el departamento técnico en dicha empresa, se piensa que el cliente es el que siempre insistía con sus quejas. Se recabó las principales, entre las que Se tiene: pérdida de paquetes de datos que fueron enviados o recibidos, sin existir motivo o explicación valedera para el cliente. El tiempo que tardaban en lograr conectarse a la red en muchas horas del día, y en su gran mayoría, ya desistían de hacerlo debido a no encontrar cabida en las pocas líneas existentes, en comparación con el número de usuarios. Enlaces con servidores locales que demoran mucho más que con otros servidores internacionales. Falta de control permanente en el área de comunicaciones en la red.

Todo esto lleva a pensar que si se mejora todos estos puntos, e inclusive otros, se podría avanzar tecnológicamente, ya que Internet es la innovación del siglo. Con Internet se podrá comunicar constantemente con el mundo exterior, con el fin de intercambiar información, innovar, negociar, etc.

Lo importante comprender, es que para mejorar el servicio de Internet, debe mejorar el nivel de comunicación de las líneas telefónicas, su velocidad, seguridad de conexión. Inclusive tiene que mejorar el enlace nacional, para tener una confiable transferencia de datos.

3.11 RESULTADOS DEL DIAGNOSTICO

El estudio de esta red conlleva a deducir sus ventajas y desventajas. Las ventajas consisten en sus enlaces. Posee algunos enlaces redundantes, que dan facilidad de comunicación en caso de tener problemas con alguno. Se puede prescindir de uno de los dos enlaces satelitales, al igual que los enlaces microondas y de radio. No se puede prescindir de ambos, los 2 satelitales, o los otros dos a la vez.

Entre las desventajas se tiene la gran cantidad de usuarios y las pocas líneas telefónicas que se poseen para la conexión. La pérdida de paquetes de datos debido a que no existe un control de colisión de paquetes, especialmente en los servidores. La falta de un software de control de equipos y enlaces de comunicaciones, un control de la red. El alto tiempo de respuesta y retardo en las conexiones con servidores locales.

4. OPTIMIZACIÓN DE LA RED

4.1. MEDIOS DE COMUNICACIÓN

Con relación a la optimización del uso de los medios de comunicación, se puede describir de acuerdo a las prioridades de las necesidades.

La primordial es la pérdida de paquetes en muchas ocasiones, de mail y archivos importantes para los clientes. Esto se debe a la falta de un control de la colisión de paquetes, ya que la red LAN está toda conectada a un linkswitch, y de acuerdo a lo explicado, va a existir una gran colisión, especialmente en los servidores de comunicaciones, donde la información fluye en gran manera. Sus puertos se encuentran bastante saturados de información, a ciertas horas del dia, donde la colisión es bastante pronunciada, principalmente en horas laborables e inclusive en la noche, aproximadamente hasta las 22h00.

Una de las alternativas de solución que se brindan para este problema, en cuanto a los medios de comunicación, se las describe a continuación.

Otro de los grandes problemas de la red es la poca capacidad de usuarios que se pueden conectar al mismo tiempo con relación al número total de clientes. Por eso, otra de las necesidades primordiales de los medios de comunicación, es incrementar el número de lineas telefónicas en 200 a 300 adicionales a las existentes. Esta es una de las quejas de los clientes, la dificultad de conexión a ciertas horas. Actualmente las lineas son digitales, por lo que se adicionaria tarjetas de módem en el Access Builder 8000, que se los conecta en cascada, y no se gastaria en otro equipo nuevo.

4.1.1 ENLACE RADIAL

Una de las soluciones es poder reemplazar el enlace radial de 2 Mbps asincrónico, que brinda mucha inseguridad, ya que muchas veces el enlace se encuentra fuera de servicio debido a que un movimiento de la posición de los equipos de transmisión o recepción ocasiona la pérdida de la señal, por lo que hay que reemplazarlo por un enlace dial-up, que muchas veces ocasiona problema por la ineficacia de las líneas telefónicas.

El cambio que se plantea es el de este enlace por otro con fibra óptica, enlazado entre dos switch, uno en Kennedy y otro en Urdesa. Adicionalmente, se tiene que utilizar transceiver con la finalidad de convertir las señales eléctricas provenientes de los equipos de comunicación en señales de luz para que puedan ser transmitidas a través de la fibra óptica, que es un medio muy eficaz de gran ancho de banda y con pocas pérdidas, y cuyas caracteristicas ya fueron descritas anteriormente. Los equipos que se

describen son capaces de transmitir en fibra en distancias mucho mayores que esa. En el gráfico a continuación se muestra el planteamiento.

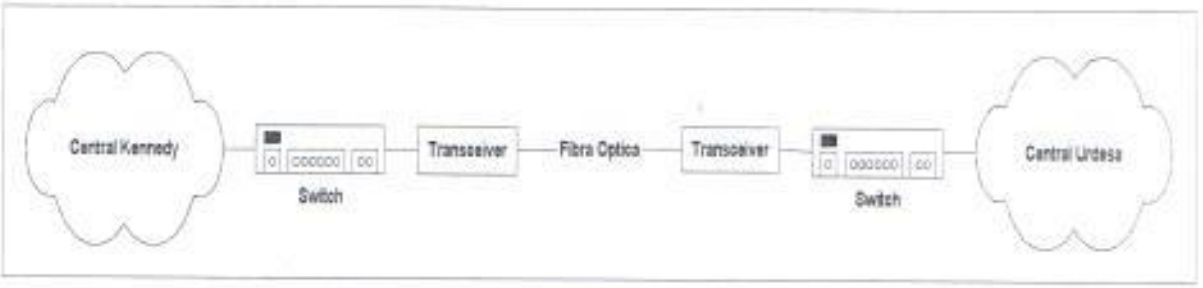


Figura 141: Ilustración del enlace con fibra óptica desde Kennedy hasta Urdesa

Así se tiene un gran control de colisión, lo que ya se explicó en el capítulo 1, se puede controlar en esta forma. Así no se tiene colisiones contando con el número de clientes de la empresa, pero si existe un aumento progresivo, se deben tomar otras medidas que se describirán posteriormente. También se tiene seguridad de conexión, porque la fibra es muy efectiva para la transmisión de datos.

A continuación se describen las características de los equipos que se utiliza en este tipo de conexión.

4.2. EQUIPOS DE COMUNICACIÓN

➢ NX300/S TRANSCEIVERS DE FIBRA OPTICA

Este equipo provee:

- Conexiones de Fibra multimodo y modo simple.
- 6 leds indicadores para el monitoreo de la transferencia de datos

- Switch de selección puede ser habilitado o deshabilitado (SQE)
- Switch de selección Half/Full Dúplex.

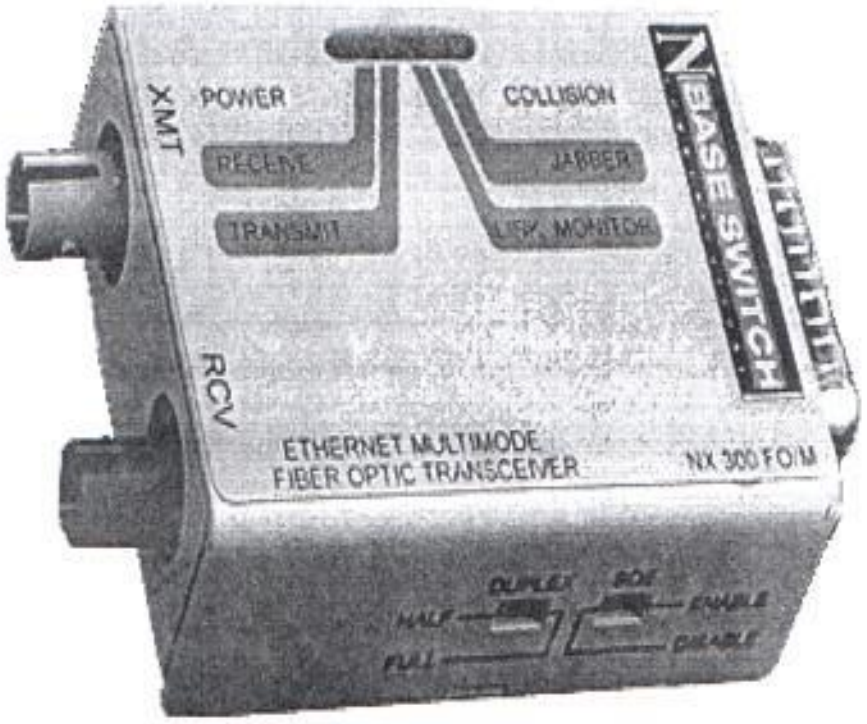


Figura 142: Transceiver

El NX 300 permite a sistemas con conectores AUI acceder directamente a sistemas de redes de Fibra Optica. NX300 esta disponible en la versión de multimodo o modo simple.

Ethernet Full Dúplex es una conexión punto a punto, permite transmisión libre de colisiones en distancias sin restricción por los 2 Km soportados por la Ethernet half dúplex. En el modo Full Dúplex requiere que los dispositivos conectados a la red también soporten Full Dúplex.

Indicadores

Los indicadores que aparecen en el panel de control son:

- Potencia
- Recepción.
- Transmisión.
- Monitoreo del enlace.

- Colisiones.

Opciones para seleccionar

- Conexión Ethernet normal, la recepción y transmisión no simultaneas.
- Modo Full Dúplex hasta 20 Mbit/seg. en punto a punto de mínimas colisiones.
- Seleccione la característica de prueba de SQE para usar cuando este conectado a una estación final, un Hub o repetidor.

Características

Estándares soportados

- IEEE 802.3
- 10 BASE-FL

Distancia: 0-18 Km

Tipo de Fibra: Modo simple de 1.300 mm

Conectores:

- 1 DB9
- 2 ST Fibra Optica

Potencia: 12 V +/- 15%; 0.150 A aplicado a través de un puerto del dispositivo AUI.

Temperatura: 0 °C a 50 °C

Dimensiones físicas: Alto: 2.03 cm; Ancho: 4.31 cm; Largo: 6.09 cm.

Peso: 58.5 gramos.

Humedad: 85% máximo no condensado.

➢ **MEGASWITCH II**

- Soporta EthernetGigabit por medio de módulos opcionales.
- Ocho puertos RJ-45 10Base - T / 100Base-TX.
- Dos ranuras de" Interfase de Red de alta velocidad" para módulos100Base-TX y 100Base-FX o enlaces altos ATM, Gigabit, o ISVLAN.
- La arquitectura directa de traslado desde el puerto fuente al puerto destino.
- El Control Selectivo de Flujo impide pérdida de paquetes sobre los dos puertos half y full dúplex.
- Configuración Full/Half dúplex por puerto.

- Transmisión sobre 110 Km con puertos 100Base-FX.
- Usa Filtrado y Redes Virtual
- Realiza pruebas y diagnósticos por sí mismo.

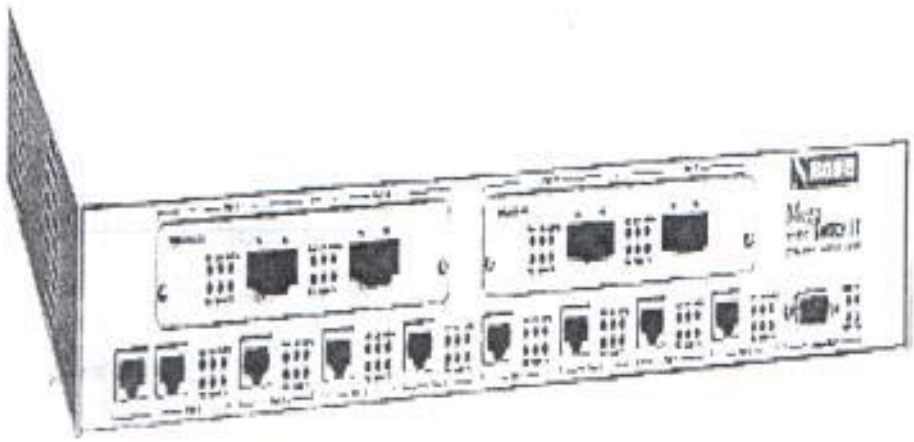


Figura 143: MegaSwitch

Aplicaciones típicas de red

- Interconexión de hubs Fast Ethernet (NBase NH108)
- Interconexión de Switches de grupos de trabajo 10/100/1000 (NBase NH208/215).
- Crear la estructura principal de Fast Ethernet.
- Extiende distancia de la Red.
- Maneja alto anchura de banda en aplicaciones de servidor.

Descripción

El MegaSwitch II es una arquitectura paralela de almacenamiento y transmisión, con el puerto de transferencia directa fuente-destino, elimina retardos en la transferencia de datos. Su hardware propietario permite al NH2012 manejar la recepción de velocidad de cable, incluyendo frames broadcast y multicast, y mantiene un rango de filtrado y envío de 1,000,000 paquetes /segundo. En conexiones punto a punto arriba de 200Mbps sobre un cableado estándar Fast Ethernet cablegrafiando puede lograrse con una tarjeta adaptadora Full Dúplex para soportar de estaciones de trabajo y aplicaciones finales.
Además, eliminando full dúplex la distancia se limita a 100 metros, permitiendo distancias de transmisión que exceden 110km sobre la fibra.

El Control de Flujo Selectivo Unico impide las perdidas de paquetes debido a sobrecarga del buffer, este es un aspecto crítico para protocolos de ventana deslizantes tales como TCP/IP y Novell 4.2. Además, NBase es el primero en ofrecer un switch con el control de flujo sobre enlaces Full Dúplex, dando su incomparable desempeño y calidad de servicio.

El MegaSwitch II soporta la creación de un dominio de seguridad Broadcast así como también para la seguridad de LANs virtuales. La creación de " Redes Virtuales" permite al operador de red para aumentar la seguridad de la red por prevenir el acceso de usuarios desde puertos especificos. Además, el administrador de red puede definir el uso de filtros especiales para estaciones de trabajo especificas y/o direcciones MAC. De esta manera los modelos de tráfico únicos pueden especificarse para estaciones de trabajo individuales.

Especificaciones técnicas

- Buffers: 64KB por puerto
- Interfaces: UTP RJ-45, RS232 DB-9, dos ranuras para módulos dual plug-in.
- Direcciones: De 1024 hasta 2048.
- Estándares soportados:
- 100 Base TX/FX Fast Ethernet.
- FDSE (Full Dúplex Switched Ethernet)
- IEEE 802.3u 10 Base TX/FX.
- IEEE 802.1d (Bridge/Spanning Tree)
- SNMP
- Provee un completo filtrado de errores en todos los paquetes. El control de flujo prevee la pérdida de paquetes.
- *Indicadores de estado*: recepción, transmisión, velocidad, enlace, control de flujo.
- *Temperatura de operación*: 0 – 50 grados Celcius.

Para el equipo de comunicación que se presentará a continuación, representa una gran alternativa de solución para dos problemas: colisión de paquetes en los servidores y control y monitoreo de la red.

Para la colisión de paquetes, se tiene que realizar un cambio pequeño en la estructura de la red. Se tiene que conectar un Hub al LinkSwitch 3000 que se encuentra en Kennedy, ya que en este Hub conectará todos los servidores así como también este equipo, el WSD (Web Server Director), con la finalidad de que tenga un control permanente sobre estos. Se puede entenderlo mejor observando la figura.

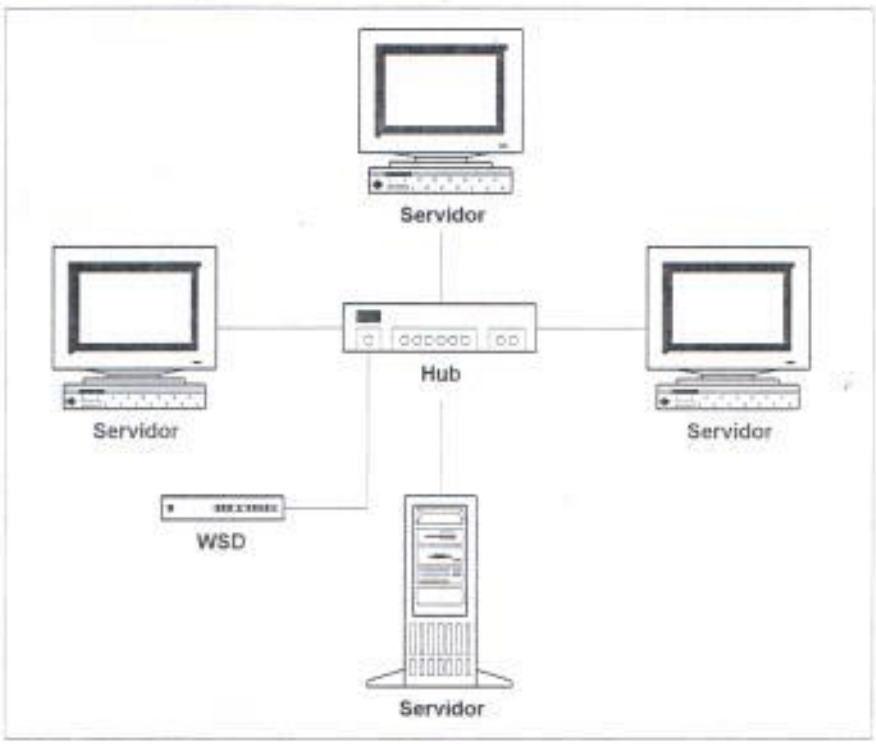


Figura 144: Conexión del WSD en la red

La ventaja que brinda este equipo es que ordena los paquetes, colocándolos en cola para que vayan ingresando uno a uno en los diferentes servidores, así evitando colisiones en sus puertos.

La otra ventaja es que contiene un software que realiza un control permanente sobre tráfico y servidores, lo que permite monitorear fácilmente la red.

➢ DIRECTOR RND DE SERVIDOR DE WEB

El WSD brinda a los clientes el mejor servicio posible: la conexión continua y el tiempo rapidísimo de respuesta sin tener que seleccionar desde una lista de servidores.

Con el WSD, usted se garantiza la utilización óptima de servidor y gestión centralizada.

Figura 145: WSD (Web Server Director)

Quejas	Solución
Acceso muy complicado a un lugar del Web • Múltiples Servidores en sitios del Web tienen múltiples direcciones IP. • Muchos usuarios del Web cambian a cual servidor va accesar.	Mejorar y simplificar el acceso a un sitio del Web. • Una simple dirección accesa a todos los servidores. • No necesita un cambio para el acceso a un sitio del Web, ya que necesita una dirección solamente.
La conexión es pobre a los sitios del Web. • La conexión pobre es causada por la sobrecarga en un servidor mientras no hay trafico en otro.	La conexión cambia a un lugar del Web. • La demanda para conexión es balanceada para el trafico cuando se optimiza el uso de cada servidor.
El sitio Web está fuera de servicio frecuentemente. • Mantenimiento y/o actualización requiere desconexión del servicio del cliente.	Funcionamiento continuo de lugares del Web. • El servicio nunca va ha ser interrumpido.

Tabla 22: Principales soluciones brindadas por el WSD

Descripción de la aplicación
El WSD provee una solución en la que se necesita accesar a una dirección IP individual con lo cual elimina múltiple servidores de web site. Solamente la dirección IP del WSD es necesaria para el acceso a los servidores del sitio web. El proveedor de servicio Internet puede agregar como muchos servidores tan necesarios, efectivamente creando una capacidad ilimitada para aumentar capacidad. Un puerto del WSD conecta al router de acceso a Internet, mientras el otro puerto o puertos de interfase en los servidores para conectar un switch o hub Ethernet, un servidor único, servidores múltiples o cualquier combinación anterior. Cuando los usuarios se registran sobre el WSD ellos se remiten con altos rendimientos y bajo nivel de tráfico para cualquiera de los servidores en el sitio, basándose en una carga sofisticada que comparte el algoritmo que toma en cuenta el poder de procesamiento de los servidores.

El WSD no solamente provee una solución local para un sitio único, pero en uno bien distribuido, en que varios sitios web en diferentes ubicaciones se benefician de sus servicios.

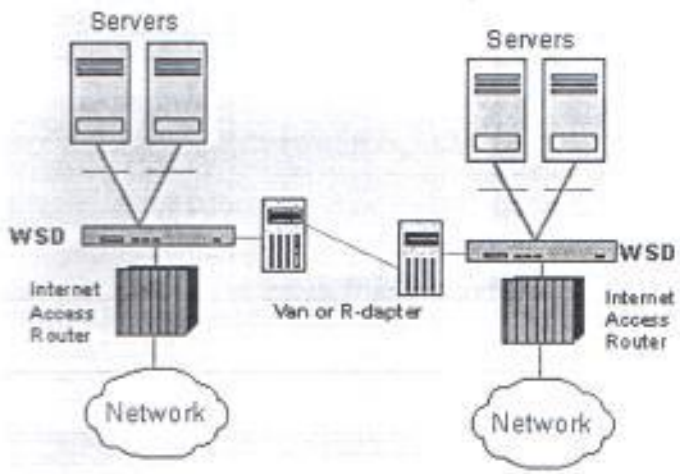


Figura 146: Soluciones locales y Distribuidas a los servidores

Características de alto rendimiento.
A causa de su diseño, el WSD provee una solución escalable. Como el tránsito aumenta y el sitio aumenta la capacidad, puede agregarse a la red WSDs adicionales para proveer más acceso así como también redundancia para la red. El WSD controla tránsito

entrante, mejorando seguridad de sistema por la entrada controladora en el sitio web y provee gestión principal en el registro del tránsito. Las diversas estadísticas pueden obtenerse, tales como carga en el servidor (en paquetes), clientes conectados por servidor, número de intentos fracasados al WSD (la tabla de clientes sobrecargada) etc.

Wsd beneficia al cliente como al operador del sitio web

- Utilización óptima de la garantía de los servidores Web.
- Acceso máximo de usuarios con un número mínimo de direcciones IP.
- Regulación del tráfico más efectiva.
- Fácil supervisión de numerosos servidores Web: el manejo de la centralización de los servidores localizada en algún segmento Ethernet.
- Servidores provistos con una capa adicional de protección.
- Topología redundante no esta provista con un punto de falla.
- Provee monitoreo y estadísticas.
- Provee control de acceso y seguridad.
- Provee escalabilidad mediante redundancia.

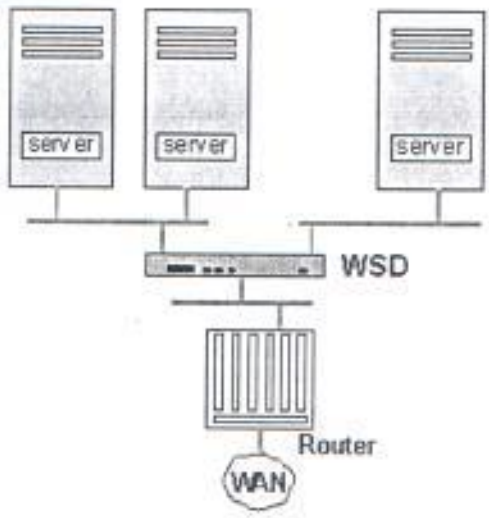


Figura 147: WSD en WAN

Wsd

- Los productos de la familia WSD revela la congestión debido al creciente tráfico de acceso por dirección IP
- El WSD actúa como un controlador transparente a algunos servidores proveyendo:

- Un servidor único accesa en una dirección a varios servidores.
- Balancea la carga.
- Acceso a servidor es tolerante a fallas.
- Protección de inversión y escalabilidad.

Características

- Un dispositivo compacto con la capacidad para soportar servidores virtuales: WSD hasta 100 o WSD-PRO hasta 50,000.
- Detección de falla de los servidores en las capas de aplicación e IP.
- Topología tolerante a fallas con alternativas locales y enlaces remotos.
- Control de acceso por una dirección MAC, dirección IP y aplicación

Beneficios

- Regulación del control de tráfico más efectivo. Fácil acceso a algunos servidores. Utilización óptima de la garantía de servidores Web o algunas aplicaciones en servidores Intranet.
- Acceso máximo de usuarios con un número mínimo de direcciones IP
- Direccionamiento flexible
- Alternativa eficiente de costos para pequeñas y grandes familias de servidores.
- Permite empleo de todos los servidores existentes
- Servidores provistos con una capa adicional de protección.
- Fácil supervisión de numerosos servidores Web.

Dirección de acceso único para un grupo de servidores

El WSD administra tráfico en grupos de servidores que tienen un acceso pesado. Los usuarios accesan al sitio y escriben en una dirección única para el grupo de servidores. El WSD controla la capacidad actual de servidor y carga y automáticamente distribuye el tránsito entre los servidores. Esto da al usuario el mejor tiempo de respuesta y una interfase de acceso simple, garantizando utilización óptima de los servidores.

Con el WSD, los servidores múltiples se benefician de la tolerancia de falla. Mediante la detección de fallas del servidor y la aplicación del monitoreo, el WSD redistribuye el tráfico cuando un servidor se cae o durante periodos de mantenimiento y mejoramiento. Cuando el tráfico de una lugar se incrementa, adicionalmente se puede añadir un WSD a la red para proveer más acceso y una buena redundancia para la red, asegurando un servicio sin interrupciones

Servidores de respaldo.
El WSD permite la definición de uno o más servidores virtuales en un grupo como respaldo a los servidores virtuales activos. Los servidores de respaldo entran en operación cuando el servidor principal deja de funcionar. El balanceo de carga se efectúa entre los servidores de respaldo.

Control de acceso.
El WSD ayuda para impedir acceso no solicitado a servidores de una compañía según el control de acceso total por direcciones MAC, direcciones y aplicaciones IP.

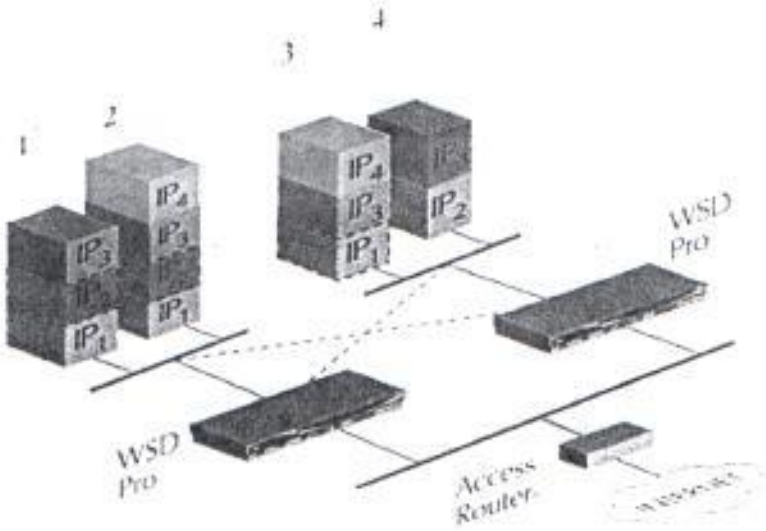


Figura 148: Control de Acceso del WSD

4.3 OPTIMIZACION FUTURA DE LA RED

➢ MEDIOS DE COMUNICACIÓN

Al analizar los tiempos de respuesta de la red original, se observa que el mayor de ellos es cuando se realizó enlaces con servidores locales, como es el caso de EcuaNet. Igual si un cliente se comunicara con la Central Quito, el tiempo de respuesta es tan alto como si se hiciera con EcuaNet.

Por esta razón, la recomendación a futuro es la comunicación nacional. Es decir, que los proveedores locales tengan una conexión entre ellos, para que los tiempos de respuestas se reduzcan visiblemente. Asi, cuando el cliente se enlace con EcuaNet, Quito o cualquier proveedor local, la conexión no tiene que realizarse con Miami sino que permita directamente comunicarse con el servidor local. Las conexiones pueden realizarse de muchas maneras, microondas, satelitales, fibra óptica, cable coaxial, canal digital, etc. Para conexiones en Guayaquil se deberia utilizar microondas o fibra óptica. Para enlaces nacionales, es decir con otras ciudades, se podria utilizar Microondas pero dependiendo de la distancia, porque para conexiones a mucha distancia se necesitarian muchas repetidoras, lo que ocasionaria un número mayor de equipos que ocasionan un mayor gasto. El enlace Satelital se recomendaria para grandes distancias.

Otra ventaja de esta interconexión nacional es que en el caso de que algún proveedor no sea capaz de dar servicio por algún motivo a través de sus enlaces, podria utilizar momentáneamente hacerlo a través de alguno de los otros proveedores, compartiendo su carga de datos entre los demás para no saturar sus enlaces. Así el servicio para los clientes seria óptimo.

La otra posibilidad para mejorar la comunicación con clientes especiales que se encuentran directamente conectados a la red, es enlazarlos a través de fibra óptica, en vez de darle prioridad al canal digital para que su comunicación sea rápida y segura. La conexión puede realizarse de la misma manera. Además, si se cambiara este medio de enlace, la empresa no tendria que gastar mensualmente en pagar a Teleholding por el servicio del canal digital. La idea seria la misma que la anterior. Se deben conectar dos switch entre la red y el cliente, unidos con fibra óptica a través de transceivers.

Este tipo de conexión se realizaria para clientes que cuentan con un gran número de usuarios y que requieran de excelente conexión, sin colisiones.

La idea es darle a los clientes dos alternativas de conexión: una muy segura y cómodo costo con fibra óptica, y la otra con canal digital de menor costo que la de fibra, pero que brinda buen servicio.

5. CONCLUSIONES Y RECOMENDACIONES

Al finalizar el estudio y optimización del presente proyecto, se ha cumplido con los objetivos propuestos en un principio. Se ha planteado las soluciones a las necesidades primordiales y futuras, que brindan seguridad en la red.

El cliente es la parte primordial de toda empresa, que brinda un servicio tecnológico que contribuye al desarrollo del país.

El alto índice de reclamos conlleva a generar algunas alternativas de solución, lo que justifica este proyecto. Uno de los más comunes es la pérdida de paquetes debido al alto nivel de colisión en la red, especialmente en los servidores. Se brindan 2 soluciones: controlando el tráfico de los servidores a través del WSD (Web Server Director), equipo cuyo costo en poco tiempo de trabajo puede ser recuperado, pero que vale la pena debido a su gran efectividad, escalabilidad y capacidad de control del tráfico. Muestra sus estadísticas, mejora el acceso a clientes, por lo que la red mejora con relación a la conexión con los clientes. En este caso, es una gran inversión el utilizar este equipo.

La otra alternativa de solución es colocar switch en cada central con la finalidad de evitar la colisión de paquetes, mediante conexión de fibra óptica. Así, si la empresa crece mucho más de lo esperado, la nueva red será capaz de soportar una mayor afluencia de usuarios. Sin embargo, el problema de lograr conectarse no permite alta velocidad, sino una dificultad en su conexión, debido al bajo número de líneas con relación al número total de clientes. También se tiene una mayor seguridad en la conexión, lo que el aironet no proporciona completamente.

Las alternativas a futuro, son una idealización del servicio, creando una conjunción técnica que serviría de respaldo, que mejoraría en gran manera los altos tiempos de respuesta presentados por los enlaces locales.

A pesar de que todas estas soluciones implican inversión, ésta no tiene comparación con los beneficios que representan para la compañía, situación que haría incrementar gradualmente el número de usuarios, pero que la inversión sería recuperada muy pronto.

Se puede aseverar que los planteamientos solucionarán todos los reclamos presentados.

ANEXO A

ESTANDARES DE COMUNICACIONES

V.110
Estándar CCITT (1984). Especifica cómo los equipos terminales de datos (DTE) con interfaces seriales asincrónicas o sincrónicas pueden ser soportados en una red SDN. Esta usa un índice de Adaptación el cual involucra una alineación bit a bit entre el DTE y el canal B ISDN.

V.120
Estándar CCITT (1988). Especifica cómo los DTEs, con interfaces seriales sincrónicas o asincrónicas pueden ser soportados en una red ISDN usando un protocolo (similar al LAPD) para encapsular los datos a ser transmitidos. Esto incluye la capacidad de usar multiplexación compartiendo la conexión del canal B entre múltiples DTEs.

V.17
Estándar CCITT (1991). Para transmisión de Fax que usa modulación TCM a 12.000 y 14.000 bps.

V.21
Estándar CCITT (1964). Para transmisión asincrónica 0 a 300 bps en módem full-duplex para uso de líneas dial-up. Usa modulación FSK.

V.22
Estándar CCITT (1980). Para transmisiones sincrónicas y asincrónicas de 600 y 1.200 bps módem full-duplex para uso de líneas dial-up. Usa modulación DPSK.

V.22bis
Estándar CCITT (1984). Para transmisiones sincrónicas y asincrónicas en módem full-duplex a 2.400 bps para uso en líneas dial-up y dedicadas de 2 hilos, con caída a V.22 operando a 1.200 bps. Usa modulación QAM.

V.23
Estándar CCITT (1964). Para transmisiones sincrónicas y asincrónicas 0-600 y 0-1200 bps, en módem full-duplex para uso de líneas dial-up. Este tiene un método opcional de compartir la velocidad de transmisión con un canal inverso de 0-75 bps (1.200/75, 75/1200 bps). Este usa modulación FSK.

V.24
Estándar CCITT (1964). Define las funciones de todos los circuitos para la interface RS-232. Este no describe los conectores o pines asignados, éstos son definidos en el estándar ISO 2110. En USA el EIA-232 incorpora la definición de señales de control de V.24, las características eléctricas de V.28 y los conectores y pines asignados son definidos en el ISO 2110.

V.25
Estándar CCITT (1968). Para llamadas automáticas I/O respuestas en líneas dial-up. Este usa circuitos paralelos y es similar en función al RS-366 usado en USA. El tono de respuesta definido en V.25 es lo primero que se escucha cuando está llamando un módem. Este tiene la función de identificar el equipo que responde y también deshabilitar el equipo que produce resonancia en la red tal que el módem full-duplex opere apropiadamente.

V.25bis
Estándar CCITT (1968). Para llamadas automáticas I/O respuestas en líneas dial-up. Este tiene 3 modos: asincrónico (raramente usado), sincrónico orientado a caracteres (bisync), y sincrónico orientado a bit (HDLC/SDLC). Ambas versiones sincrónicas son usadas en AS/400 de IBM y otros de pequeños a medianos tamaños de computadoras que llaman automáticamente para entrada remota de trabajo.

V.26
Estándar CCITT (1968). Para transmisiones sincrónicas a 2.400 bps en módem full-duplex para uso en líneas dedicadas en 4 alambres. Usa modulación DPSK e incluye una opción de canal de respaldo de 75 bps.

V.26bis
Estándar CCITT (1972). Para transmisiones sincrónicas a 1.200 y 4.200 bps en módem full-duplex para uso sobre líneas dial-up. Usa modulación DPSK e incluye una opción de canal de respaldo de 75 bps.

V.26ter
Estándar CCITT (1984). Para transmisiones sincrónicas y asincrónicas a 2.400 bps en módem full-duplex usando modulación DPSK sobre líneas dial-up y líneas dedicadas de 4 alambres. Este incluye una caída de velocidad de 1.200 bps y uso de cancelación de eco, permitiendo al módem una comunicación full-duplex para enviar y recibir sobre la misma frecuencia.

V.27
Estándar CCITT (1972). Para comunicación sincrónica a 4.800 bps, en módem full-duplex para uso sobre líneas dedicadas de 4 alambres. Usa modulación DPSK.

V.27bis
Estándar CCITT (1976). Para comunicaciones sincrónicas a 2.400 y 4.800 bps, en módem full-duplex usando modulación DPSK para uso de líneas dedicadas de 4 alambres. La principal diferencia entre el V.27 y el V.27bis es la adición de un equalizador automático adaptivo.

V.27ter
Estándar CCITT (1976). Para comunicaciones sincrónicas a 2.400 y 4.800 bps, en módem half-duplex usando modulación DPSK sobre líneas dial-up. Esto incluye un canal opcional de respaldo de 75 bps.

V.28
Estándar CCITT (1972). Define las funciones de todos los circuitos para la interface RS-232. En USA EIA-232 incorpora las definiciones de las señales eléctricas de V.28, las señales de control de V.25 y los conectores y pines asignados definidos en el ISO 2110.

V.29
Estándar CCITT (1976). Para comunicaciones sincrónicas a 4.800, 7.200 y 9.600 bps en módem full-duplex usando modulación QAM sobre líneas dedicadas de 4 alambres.

V.32
Estándar CCITT (1984). Para comunicaciones asincrónicas y sincrónicas a 4.800 y 9.600 bps, en módem full-duplex usando modulación TCM sobre líneas dial-up o líneas dedicadas de 2 alambres. TCM codificado puede ser opcionalmente agregado. V.32 usa cancelación de eco para lograr la transmisión full-duplex.

V.32bis
Estándar CCITT (1991). Para comunicaciones sincrónicas y asincrónicas a 4.800, 7.200, 9.600, 12.000 y 14.400 bps, en módem full-duplex usando modulación TCM y cancelación de eco. Soporta renegociación, lo cual permite a los módems cambiar a la velocidad requerida.

V.33
Estándar CCITT (1988). Para comunicaciones sincrónicas a 12.000 y 14.400 bps, en módem full-duplex para uso en líneas dedicadas de 4 alambres usando modulación QAM. Este incluye la opción de multiplexación por división de tiempo para compartir la línea de transmisión entre varios terminales.

V.35
Estándar CCITT (1968). Para grupos de módem que combinan el ancho de banda de varios circuitos telefónicos para alcanzar altas velocidades de datos. V.35 es conocido como la interface RS-232 de alta velocidad en vez de un tipo de módem. El conector rectangular V.35 nunca fue especificado pero viene siendo un estándar por efecto para esta interface.

V.42
Estándar CCITT (1989). Para módem de corrección de error que usan LAPM como protocolo primario y provee MNP clase 2 hasta 4 como un protocolo alternativo para compatibilidad.

V.42bis
Estándar CCITT (1989). Para módem de corrección de error y compresión de datos. Este usa el V.42 de corrección de error con una técnica de compresión que incrementa la velocidad de transmisión mayor de 4 veces el nivel de bps.

GLOSARIO

CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía) es una organización internacional concerniente con recomendaciones para redes internacionales de telecomunicaciones.

DNS Servidor de Nombre de Dominio

DTU Unidad de Terminación de Red

FTP Protocolo de transferencia de archivos

IP Protocolo Internet

ISO Organización Internacional de Estandarización

LLC Control Lógico de Enlace

LNA Amplificador de Bajo Ruido

LAN Redes de Area Local

MAC Control de acceso a los medios

NFS Sistemas de Archivos de Red

NIC Tarjeta de Interface de Red

SLIP Protocolo Internet para Enlaces Seriales

OSI Interconexión de Sistemas Abiertos

PPP Protocolo Punto a Punto

TCP Protocolo de Control de Transmisión

UDP Protocolo de Datagrama de Usuario

WAN Redes de Area Amplia

WSD Director de Servidor de WEB

BIBLIOGRAFIA

1. Manual de Tecnología de Redes LAN. Paginas 1 – 18, 26 – 67, 157 – 204.
   Publicado por Intranet

2. Manual de Intranet "Servicios y Aplicaciones". Paginas 1 – 6.
   Publicado por iCnet (Comunicaciones y Redes)

3. Manual de Intranet "En el Entorno a WAN". Paginas 11 – 20.
   Publicado por iCnet (Comunicaciones y Redes)

4. PC/TCP Interoperability. Paginas 1 – 8 de la Carpeta 1, 1 - 5 de la Carpeta 2, 1 – 18 de la Carpeta 3, 1 – 23 de la Carpeta 4.
   Publicado por FTP Software, Inc.

5. Technical Introduction To PC/TCP. Paginas 1 – 66 de la Carpeta 1, 1 – 23 de la Carpeta 2.
   Publicado por FTP Software, Inc.

6. Manual de Bridges, Routers y Switching Hubs. Paginas 1 – 162.
   Publicado por Intranet.

7. Seminario de Conceptos Básicos de Redes y Conectividad. Paginas 1 – 28 de la Carpeta 1, 1 – 27 de la Carpeta 2.
   Publicado por MAINT.

8. Redes Globales de Información con Internet y TCP/IP. Paginas 51 – 58 del Capítulo 3, 61 – 72 del Capítulo 4, 75 – 83 del Capítulo 5, 85 – 91 del Capítulo 6, 111 – 121 del Capítulo 8, 125 – 141 del Capitulo 9, 181 – 193 del Capítulo 12.
   Publicado por Douglas E. Comer.

9. **Información obtenida de Internet en la siguientes pagínas WEB:**

www.Netmedic.com
www.Netblazer.com
www.WSD.com
www.Telebit.com
www.Comstream.com
www.Compaq.com
www.Netbridge.com
www.3COM.com
www.Livingston.com
www.Aironet.com
www.Panansat.com

10. **Manual de Internet. Paginas 1 – 7 del Capítulo 1, 9 – 17 del capítulo 2.**

Publicado por CESERCOMP

11. **El Camino Fácil a Internet. Paginas 1 – 17 del Capítulo 1, 19 – 27 del Capítulo 2, 41 – 51 del Capítulo 4, 63 – 76 del capítulo 6, 81 – 89 del Capítulo 7,.**

Publicado por José Daniel Sánchez Navarro.