107

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

"A R A G O N"

DESARROLLO DE CORREO ELECTRONICO EN UNA RED TCP / IP.

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

RICARDO VARGAS LOPEZ

Asesor: Ing. Eleazar M. Pineda Díaz

MEXICO, D. F. ABRIL 2002

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

DIRECCIÓN

RICARDO VARGAS LÓPEZ
P R E S E N T E.

En contestación a la solicitud de fecha 26 de febrero del año en curso, relativa a la autorización que se le debe conceder para que el señor profesor, Ing. ELEAZAR MARGARITO PINEDA DÍAZ pueda dirigirle el trabajo de tesis denominado "DESARROLLO DE CORREO ELECTRÓNICO EN UNA RED TCP/IP", con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 14 de marzo del 2001
EL DIRECTOR

M en R.I. CARLOS EDUARDO LEVY VÁZQUEZ

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON UNAM
DIRECCION

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería Mecánica Eléctrica.
C p Asesor de Tesis.

CELV/AIR/vr

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN
JEFATURA DE CARRERA DE INGENIERÍA MECÁNICA ELÉCTRICA

LIC. ALBERTO IBARRA ROSAS
JEFE DE LA UNIDAD ACADÉMICA
PRESENTE

San Juán de Aragón, Estado de México a 09 de enero del 2002.
Por este conducto, me permito informarle a usted que el alumno de la carrera de Ingeniería Mecánica Eléctrica:

APELLIDO PATERNO	APELLIDO MATERNO	NOMBRE(S)	No. de Cuenta:
VARGAS	LÓPEZ	RICARDO	8816589-7

Ha concluido su trabajo de tesis denominado:

Desarrollo de correo electrónico en una red TCP/IP.

ENEP ARAGÓN
SECRETARÍA ACADÉMICA
09 ENE 2002

Considero que dicha tesis reune los requisitos necesarios para ser discutida en el Examen Profesional correspondiente. Por lo que le solicito, tenga a bien autorizar, la continuación de los trámites correspondientes para su titulación.

Sin más por el momento, y agradeciendo de antemano su atención, quedo a sus apreciables ordenes.

ATENTAMENTE:	Vo.Bo.
Ing. Eleazar Margarito Pineda Díaz Director de Tesis	**Ing. Raúl Barrón V.** Jefe de Carrera de IME

c.c.p. Ing. José Luis García E. Secretario Técnico de IME
Alumno

TESIS CON
FALLA DE ORIGEN

Agradecimientos

Para mi Esposa Sara:

Por que con ella he aprendido a luchar por ser mejor y por su apoyo incondicional, gracias amor. Tenemos muchos triunfos más que compartir y siempre vamos a lograrlo juntos. Te amo.

Para mis Padres Alfonso y Ma. Teresa:

Por el hogar maravilloso y el apoyo que me han brindado, durante mis estudios y en toda mi vida, Papá se que donde estas vas a estar orgulloso de mi, Mamá tu ejemplo de valor y fortaleza están conmigo siempre. Los quiero mucho.

Para mis Hermanos: Alfonso, Ana María, Alicia, Angélica y María Luisa:

Por todos los momentos felices y difíciles que hemos vivido juntos, y por que cada uno me ha brindado su apoyo, por tener confianza en mi.

Para mis sobrinos: Dayana, Adara, Yael, Abril, Iliana y Daniel:

Por ser lo mas jóvenes de la familia, por sus sonrisas y alegrías, se que van a lograr ser grandes profesionistas.

Agradecimientos

Para Mi Asesor Ing. Eleazar M. Pineda D.

Por su paciencia y apoyo, para realizar este trabajo, mi más sincero agradecimiento.

Para la Universidad Nacional Autónoma de México, E.N.E.P. Aragón:

Por la oportunidad de estudiar y aprender una carrera que me ha permitido desarrollarme mejor en todos los ámbitos de mi vida. Mi compromiso es poner en alto el nombre de esta gran Casa de estudios.

Índice.

Desarrollo de correo electrónico en una red TCP/IP.

Introducción.

Actualmente, estamos experimentando una creciente utilización de Internet y de las aplicaciones que se han desarrollado con esta red mundial, como el correo electrónico, debemos decir que cada organización, universidad, instituto, empresa, etc., necesita contar con un sistema de correo electrónico, para cubrir sus necesidades de comunicación. No podríamos entender que por alguna razón tecnológica no se cuente con un sistema de correo electrónico.

Para tener un marco de referencia de qué tanto cambia a una organización el utilizar un sistema de correo electrónico, podemos mencionar como ejemplos los sistemas gubernamentales de atención al público donde se difunde una cuenta de correo electrónico (atención@gobierno.org.mx) para recibir sugerencias, quejas, solicitar información especializada, realizar tramites, etc. Por otro lado están las organizaciones de tipo comercial que con gran entusiasmo realizan comercio electrónico por medio de Internet, regalando bajo ciertas reglas de uso una cuenta de correo electrónico y espacio para almacenar los correos de los usuarios. Sin dejar de mencionar a la Universidad Nacional Autónoma de México que otorga a sus alumnos, profesores, trabajadores y egresados una cuenta de correo electrónico para permitir el intercambio de información por este medio.

Objetivos

Por las razones mencionadas anteriormente, son varias las posibles soluciones para lograr que una organización cubra sus necesidades de comunicación por medio de mensajes electrónicos, una de ellas es utilizar los servicios de sistemas de correo electrónico públicos como Infosel, CompuServe, etc., además de múltiples empresas que venden este servicio a un costo razonable actualmente, otra solución es implementar un sistema de correo electrónico propietario, a la medida de los requerimientos que cada organización pudiera tener y que fue la principal razón para realizar este trabajo.

Como objetivos de este trabajo se tienen los siguientes:

- Dar una descripción general de las comunicaciones, de tal forma que el lector tenga los elementos necesarios para identificar los componentes de un sistema de comunicaciones.

- Dar una visión global del conjunto de protocolos de TCP/IP y sus aplicaciones, haciendo mayor énfasis en los protocolos de correo electrónico.

- Describir la metodología necesaria para hacer el análisis, donde se recaba información de la red y sus características, la factibilidad donde se fundamenta la inversión del proyecto, el diseño y administración de un sistema de correo electrónico que cumpla con los requerimientos que una organización plantea. Además de las políticas de seguridad que debe tener este tipo de sistemas.

Cabe mencionar que el tema es muy amplio pues cada día se publican nuevos protocolos que expanden las funciones de las versiones anteriores y surgen nuevas tecnologías en las redes de área local (LAN) y área extendida/amplia (WAN/MAN), que son más veloces y capaces de transportar todo tipo de tráfico como voz, datos, video, multimedia, etc., A altas velocidades.

Para presentar este trabajo se desarrollaron cuatro capítulos.

El *Capitulo I* trata principalmente de los conceptos básicos y generales que se requieren, como los elementos mínimos para establecer una comunicación, la teoría de información donde se describen varios conceptos, como ancho de banda, limite de transmisión, tipo de ruido que afecta a una señal, etc., además se explican algunos de los códigos de comunicación y codificación. Más adelante se describen las redes de datos, como los medios y técnicas de transmisión, además de los tipos de redes y topologías más sobresalientes en la industria, y los sistemas operativos de red que actualmente dominan en el mercado de las pequeñas y medianas empresas. Finalizando con una descripción clara y breve del modelo de referencia OSI, para la interconexión de sistemas abiertos, que es una referencia necesaria para el estudio de las comunicaciones.

El *Capitulo II* describe el conjunto de protocolos de TCP/IP, iniciando con la explicación del modelo general de TCP/IP, después describiendo cada uno de los niveles, comenzando con el nivel de Internet que muestra el formato de los paquetes IP y los diferentes tipos de direcciones usadas en este nivel. El siguiente nivel que es TCP, que en realidad se compone por TCP y UDP, el primero es encargado del control y flujo de las transmisiones proporcionando el transporte de datos orientado a conexión y el segundo que es el protocolo de datagrama de usuario, proporciona la operación en modo no orientado a la conexión. Terminando este capitulo con el nivel de aplicación que describe brevemente los diferentes protocolos que se han desarrollado y entre los cuales se mencionan los más representativos de Internet.

El *Capitulo III* se enfoca al correo electrónico, donde se da una breve historia de su origen, además se describe su funcionamiento desde el punto de vista conceptual, complementando con las ventajas y desventajas que el correo electrónico tiene con respecto a otros sistemas. El final de este capitulo se compone de los tres protocolos de correo electrónico más representativos, el primero X.400 desarrollado por el CCITT se explica su modelo funcional y forma de operar, el siguiente SMTP, el protocolo de transmisión de correo simple se describe en su modelo y comando de operación, y por último el protocolo POP 3, el protocolo de oficina postal versión 3, que se describe su estructura y funcionamiento.

El *Capitulo IV* es un estudio de los requerimientos y desarrollo de un sistema de correo electrónico, donde se hace uso de la metodología necesaria para realizar una implementación sencilla, clara y planeada, se inicia con el Análisis de una red y sus requerimientos, realizando algunas tareas como documentar la red y la información importante para este punto. Continuamos con un estudio de Factibilidad que en forma breve identifica si es posible llevar a cabo la implementación del sistema pues se realiza un calculo del tráfico que generara el sistema de correo electrónico, además de la factibilidad financiera que todo proyecto implícitamente contiene. El siguiente punto trata la Seguridad donde se describen los mecanismos y políticas necesarias para proyectos de este tipo. Por último el desarrollo del sistema de correo electrónico que se compone de tres partes el Diseño, la Implementación y Administración.

Capitulo I

Conceptos básicos.

I.I. Elementos de la comunicación digital

Existen tan sólo tres elementos que son esenciales para que exista cualquier comunicación:

- El emisor de la información
- El receptor de la información
- El medio por el cual la información es transmitida

Figura 1. Elementos para una comunicación.

La información se define como el conocimiento, la sabiduría o la realidad y puede ser en forma *analógica* (proporcional o continua), tal como la voz humana, información sobre una imagen de video, o música, o en forma *digital* (etapas discretas), tales como números codificados en binario, códigos alfanuméricos, símbolos gráficos, códigos operacionales de microprocesador o información de base de datos.

En los sistemas de comunicación digital, la información analógica se convierte a forma digital, antes de la transmisión, y con los sistemas de comunicación analógica, los datos digitales se convierten a señales analógicas antes de la transmisión.

La transmisión digital es la transmisión de pulsos digitales, entre dos o más puntos, de un sistema de comunicación. La información que se procesa y se organiza se llama datos. En el Emisor y Receptor, los datos están en forma digital, sin embargo, en el medio de transmisión, los datos pueden estar en forma digital o analógica.

I.I.1 Tipos de Información.

La información en el medio de transmisión, así como en los equipos emisor y receptor es de alguno de los siguientes dos tipos:

- Analógica, en donde los valores siguen una variación gradual (una señal variando continuamente tal como una onda senoidal).

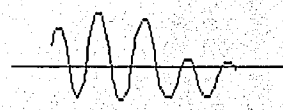

Figura 2. Señal Analógica.

- Digital, en donde solo se tienen 2 valores, que pueden ser el uno y el cero lógico.

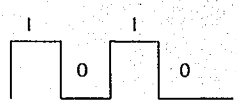

Figura 3. Señal Digital

Los sistemas de comunicación analógica fueron los primeros en desarrollarse; sin embargo, en los últimos años los sistemas de comunicación digital se han hecho más comunes de tal forma que son los que predominan en la actualidad y están siendo implementados en todos los campos de las comunicaciones.

I.I.2 Tipos de Sesión.

Una sesión es el proceso que se establece entre dos puntos para intercambiar información.

Existen dos tipos de sesiones: *sesión tipo datos* y *sesión tipo voz*.

La *sesión tipo datos* no es afectada seriamente por retrasos en el arribo de la información, no permite que exista ganancia o pérdida de información al ser transmitida, ocurre en ráfagas de transmisión entre períodos relativamente largos

de ausencia de transmisión, su duración es usualmente corta, y podemos reducir la duración de la sesión si ampliamos el ancho de banda disponible.

Las características de este tipo de sesión son:

- insensible a retrasos
- sensible a perdida /ganancia de información
- transmisión en ráfaga
- corta duración.

La *sesión tipo voz* es afectada si existen retrasos y variaciones en el arribo de la información, no es afectada seriamente por la ganancia o pérdida ligeras de información al ser transmitida, ocurre en forma continua, típicamente tiene duraciones mayores a la sesión tipo datos, y su duración no es afectada si se reduce o amplia el ancho de banda disponible.

Las características de este tipo de sesión son:

- sensible a retrasos
- insensible a perdida/ganancia de información
- transmisión continúa
- larga duración.

I.I.3 Sincronía.

La sincronía en comunicaciones es un termino representativo del hecho que ocurre cuando se coincide o se esta de acuerdo al mismo tiempo para transmitir información.

Existen tres tipos de sincronía de las transmisiones de información, y son: *asíncrona*, *síncrona* e *isócrona*:

a) En la transmisión *asíncrona* las unidades de información son de tamaño fijo (celdas) y ocurren en cualquier momento. Ejemplos de ella son las comunicaciones seriales de las PC's y las redes ATM

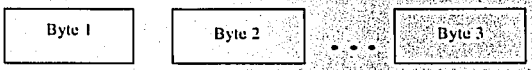

Figura 4. Transmisión *asíncrona*.

- Cada unidad cuenta con un bit de arranque y uno de final, el primer bit transmitido es el de arranque y siempre es un 0 lógico, el último bit

transmitido es el bit de parada, el cual siempre es un 1 lógico. Con los datos *asíncronos*, no es necesario que los relojes de transmisión y recepción se sincronicen continuamente. Sólo es necesario que operen aproximadamente a la misma tasa y sean sincronizados al inicio de cada transmisión.

b) En la transmisión *síncrona* se envían unidades de información variable (tramas) que requieren de cierto preámbulo o conjunto de bits para sincronizar el reloj del receptor con la información que está arribando

Figura 5. Transmisión *síncrona*.

- Al comienzo de cada transmisión se tiene una bandera o un carácter de sincronización único. El carácter o bandera de fin que se usa para el final de una transmisión varía con el tipo de protocolo utilizado. Con los datos sincronos los relojes de transmisión y recepción deben sincronizarse, por que la sincronización ocurre, sólo una vez al comienzo del mensaje.

c) En la transmisión *isócrona* se envían porciones de la información a ser transmitida en forma periódica (slots de tiempo), en donde cada sesión tiene asignado su *slot* independientemente si envía información o no lo hace.

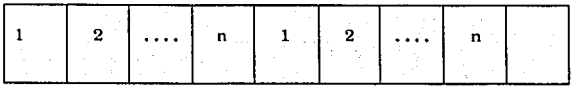

Figura 6. Transmisión *isócrona*

- Se refiere al proceso donde los datos deben ser entregados dentro de cierto tiempo, por ejemplo aplicaciones multimedia requieren un mecanismo de transporte *isócrono* para asegurar que la entrega de datos es tan rápida como se despliega en pantalla y que el audio esta sincronizado con el video.

Las transmisiones de datos *asíncronos* son más eficientes, para los mensajes cortos, y las transmisiones de datos *síncronos* son más eficientes para los mensajes largos. En cambio las transmisiones de datos *isócronos* son el contraste de *síncrono* y *asíncrono*.

I.I.4 Transmisión serial y paralela.

Si la información es enviada por un solo canal se le conoce como serial. Esto es, la transmisión es bit por bit en una sola línea de transmisión. En la siguiente figura vemos una descripción de la comunicación serial.

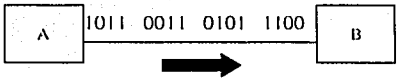

Figura 7. Comunicación Serial.

Si la información es enviada por más de un canal se le conoce como paralela, permitiendo reducir el tiempo de transmisión al enviar más de una información a la vez. De tal forma que cada bit tiene su propia línea de transmisión. En la siguiente figura vemos una descripción de la comunicación paralela.

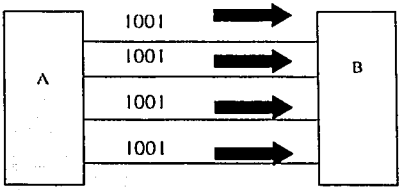

Figura 8. Comunicación Paralela

Obviamente, la diferencia principal entre la transmisión paralela y serial es la velocidad contra la simplicidad. La transmisión de datos se puede lograr mucho más rápido usando la transmisión paralela. Sin embargo, la transmisión paralela requiere más líneas entre fuente y destino. Como una regla general, la transmisión

paralela se usa para la comunicación a corta distancia, y dentro de una computadora, y la transmisión serial se usa para la comunicación de larga distancia.

I.I.5 Modos de transmisión.

Los sistemas de comunicaciones están diseñados de tal forma que la dirección de la información determina el modo de transmisión, teniendo principalmente tres sentidos o modos posibles de transmitir en un sistema: *simplex, half-duplex, y full-duplex.*

a) En una transmisión *simplex* solo existe un emisor y los receptores no pueden contestar. Con la operación *simplex*, las transmisiones pueden ocurrir sólo en una dirección. Algunas veces, llamados de un sentido, sólo para recibir o sólo para transmitir. Una ubicación puede ser un transmisor o un receptor, pero no ambos. Un ejemplo de la transmisión *simplex* es la radiodifusión de la radio comercial o de televisión; la estación de radio siempre transmite y el usuario siempre recibe. En la figura 9 vemos un diagrama de la operación *simplex*.

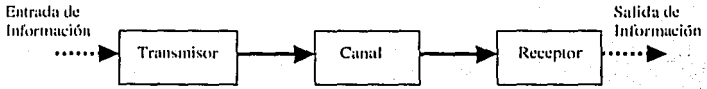

Figura 9. Transmisión *simplex*.

b) En la transmisión *half-duplex* el emisor y el receptor alternan sus roles, pero solo uno puede enviar a la vez, debiendo esperar a que termine el otro de transmitir para hacer lo propio él. Algunas veces se les llaman sistemas con alternativa de dos sentidos, cualquier sentido, o cambio y fuera. Una ubicación puede ser un transmisor y un receptor, pero no los dos al mismo tiempo. Los sistemas de radio de doble sentido, como los radios de banda civil y de banda policiaca son ejemplos de transmisión *half-duplex*. En la figura 10 vemos un diagrama de la operación *half-duplex*.

Figura 10. Transmisión *half-duplex*.

c) En la transmisión *full-duplex* ambos pueden transmitir y recibir simultáneamente. Algunas veces se les llaman líneas simultaneas de doble sentido, dúplex o de ambos sentidos. Una ubicación puede transmitir y recibir simultáneamente; sin embargo, la estación a la que está transmitiendo también debe ser la estación de la cual está recibiendo. Un sistema telefónico estándar es un ejemplo de transmisión *full-duplex*. En la figura 11 vemos un diagrama de la operación *full-duplex*.

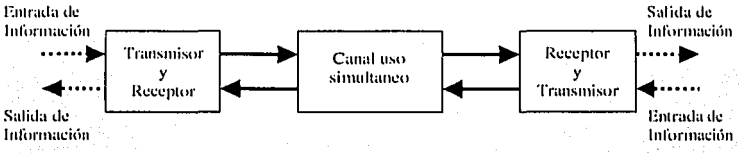

Figura 11. Transmisión *full-duplex*.

En resumen podemos decir que:

Simplex: los datos fluyen del emisor al receptor solamente.
Half-duplex: los datos fluyen entre ambos pero sólo en un sentido a la vez.
Full-duplex: los datos fluyen entre ambos simultáneamente.

I.II Teoría de la Información.

I.II.1 Capacidad

Las dos limitaciones más significativas en el funcionamiento de los sistemas de comunicaciones son: el *ruido* y el *ancho de banda*. De tal forma, que estos son la referencia para decir de la capacidad de información que un canal puede tener. En un sistema de comunicaciones la capacidad es una medida de la cantidad de información que la fuente puede transportar por el sistema, en un período determinado de tiempo. La cantidad de información que puede propagarse a través de un sistema de transmisión es una función del *ancho de banda* del sistema y el tiempo de transmisión.

La relación entre el ancho de banda, tiempo de transmisión y capacidad de información fue desarrollada en 1920 por R. Hartley de los Laboratorios Telefónicos Bell. De manera sencilla, la ley de Hartley es:

$$I \propto B \propto t$$

En donde:

I = capacidad de información
B = ancho de banda (Hz)
t = tiempo de transmisión (segundos)
$\propto$ = proporcional

La ecuación anterior muestra que la capacidad de información es una función lineal y directamente proporcional al ancho de banda del sistema y al tiempo de transmisión. Si se modifica el ancho de banda o el tiempo de transmisión, ocurrirá un cambio directamente proporcional en la capacidad de información.

I.II.2 Limite de Shannon

En 1948, C.E. Shannon (también de los Laboratorios de Teléfonos Bell), publicó un articulo en la revista Bell System Technical Journal relacionando la capacidad de información de un canal de comunicación con el ancho de banda y la relación *señal-a-ruido*. Matemáticamente, el *límite de Shannon para la capacidad de información* es:

$$I = B \log 2 (1 + S/N)$$

o

$$I = 3.32\ B \log 10 (1 + S/N)$$

Donde:

I = capacidad de información en (bps)
B = ancho de banda (Hz)
S/N = relación de potencia *señal-a-ruido* (sin unidades)

Como ejemplo, para un canal de comunicaciones de banda de voz estándar, con una relación de potencia *señal-a-ruido* de 1000 (30 dB) y un *ancho de banda* de 2.7 KHz, el límite de Shannon para la capacidad de información es:

$I = 2.7 \log 2 (1 + 1000)$
$I = 26.9$ Kbps

La formula de *Shannon* suele interpretarse mal, ya que los resultados del ejemplo anterior indican que 26.9 Kbps se pueden transferir a través de un canal de 2.7 KHz. Quizás esto sea cierto, pero no se puede hacer con un sistema binario. Para lograr una velocidad de transmisión para la información de 26.9 Kbps, a través de

un canal de 2.7 KHz, cada símbolo transmitido debe contener más de un bit de información. En consecuencia, para alcanzar el límite de Shannon para la capacidad de información, se deben utilizar los sistemas de transmisión digital que tienen más de dos condiciones de salida (símbolos). Estos sistemas incluyen técnicas de modulación.

En resumen podemos decir que:

- La tasa máxima de transmisión de un canal se le denomina su capacidad.
- La capacidad se mide en bits por segundo (bps).
- Muchas veces se le llama ancho de banda a lo que en realidad es su capacidad.

I.II.3 Ancho de Banda

El *ancho de banda* de un sistema de comunicaciones es la banda de paso mínima (rango de frecuencias) requerida para propagar la información de la fuente a través del sistema. El *ancho de banda* debe ser lo suficientemente grande para pasar todas las frecuencias significativas de la información que se requiere transmitir en el sistema.

Ancho de banda **B** es la diferencia entre la frecuencia máxima y la frecuencia minina permitida.

El oído humano registra un *ancho de banda* entre 20,000 Hz y 20 Hz, o sea, **B** = 19,980 Hz.

Más del 90 % de la energía de la voz humana se encuentra entre 3,400 Hz y 300 Hz, o sea, un *ancho de banda* de 3,100 Hz. Este es el *ancho de banda* de la red telefónica conmutada.

El *ancho de banda* de un canal determina la velocidad de la transmisión de datos, aun cuando el canal es perfecto.

I.II.4 Relación señal-a-ruido

Los canales digitales están limitados por la proporción señal a ruido. La relación *señal-a-ruido*, (***S/N***) es una relación matemática sencilla del nivel de la señal con respecto al nivel de ruido en un punto dado del sistema. La relación ***S/N*** puede expresarse como una relación de voltaje y una relación de potencia. Matemáticamente, ***S/N*** es:

S/N = (voltaje de la señal/voltaje del ruido)^2 = (**Vs/Vn**)^2

S/N = (potencia de la señal/potencia del ruido)^2 = (**Ps/Pn**)^2

La relación señal a ruido se expresa frecuentemente como una función logarítmica con la unidad de decibel.

Para las relaciones de voltaje, S/N (dB) = 20 log Vs/Vn.

Para las relaciones de potencia, S/N (dB) = 10 log Ps/Pn.

La relación señal-a-ruido probablemente sea el parámetro más importante y frecuentemente usado para evaluar el funcionamiento de un sistema de comunicaciones. Entre más alta sea la relación señal-a-ruido, mejor será el funcionamiento del sistema

Capacidad máxima del canal en bps = 3.32 x (**ancho de banda**) x lg (1 + **señal/ruido**).

I.II.5 Ruido

En general, el ruido eléctrico se define como cualquier energía eléctrica no deseada presente en la pasabanda útil de un circuito de comunicaciones. Por ejemplo, en una grabación de audio cualquier señal no deseada que cae en la banda de frecuencias, entre 0 y 15 Khz, es perceptible e interferirá con la información de audio.

La figura 12 muestra el efecto que el ruido tiene sobre una señal eléctrica.

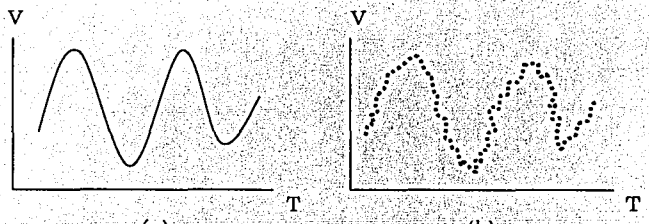

Figura 12. Efecto del ruido en una señal.

La figura (a) es una señal perfecta sin ruido y la figura (b) muestra la misma señal pero con ruido. La señal que ha sido contaminada con ruido esta distorsionada y obviamente contiene otras frecuencias además de la original.

Esencialmente, el ruido puede dividirse en dos categorías generales, *correlacionado* y *no correlacionado*. Correlación implica una relación entre la señal y el ruido. El *ruido no correlacionado* está presente en la ausencia de cualquier señal. (Esto quiere decir que, cuando está presente, la señal no tiene efecto sobre la magnitud del ruido). El *ruido correlacionado* es producido directamente como un resultado de la señal.

I.II.6 Codificación y Códigos de Comunicación.

Se dice que codificar es el proceso para enviar información digital por el medio, el cual genera (*codifica*) un conjunto de valores binarios según la información del emisor. En el otro extremo debe realizarse la función inversa (*decodificación*) para entregar la información al receptor.

Existen dos tipos de codificación:

- *analógico-digital*
- *digital-digital*

a) Codificación *analógico-digital*:

El transformar datos analógicos a un formato digital implica un proceso, al cual más correctamente nos podemos referir como digitalización. Las señales analógicas pueden digitalizarse obteniéndose muestras del valor de su amplitud. Las muestras deben realizarse en forma periódica, basándose en el teorema de muestreo (*Postulado de Nyquist*) que dice:

" Si una señal f(t) es muestreada a intervalos regulares de tiempo con una frecuencia mayor que el doble de la frecuencia significativa más alta de la señal, entonces las muestras así obtenidas contienen toda la información de la señal original. La función f(t) se puede reconstruir a partir de estas muestras mediante la utilización de un filtro pasa-baja ".

Es decir, se debe hacer un muestreo de la señal original con el doble de frecuencia que ella, y con los valores obtenidos, normalizándolos a un número de bits dado (por ejemplo, con 8 bits habría que distinguir entre 256 posibles valores de amplitud de la señal original a cuantificar) se ha podido codificar dicha señal. En el receptor, este proceso se invierte, pero por supuesto se ha perdido algo de información al codificar, por lo que la señal obtenida no es exactamente igual que la

original (se le ha introducido ruido de cuantización). Las desviaciones resultantes no son perceptibles, o al menos no impactan en la comunicación, debido a que su frecuencia es mayor que la máxima.

La primer codificación que se estandarizó fue la de la voz humana a través de la red telefónica conmutada, a la que se le denomino PCM. Al tener 3,100 Hz y una banda de guarda de 900 Hz para separar cada canal, el ancho de banda total es de 4,000 Hz. La frecuencia del muestreo es el doble del ancho de banda, o sea, 8,000 Hz. Se codifican hasta 256 diferentes valores de amplitud, por lo que se requieren 8 bits para cada valor. El canal debe tener una tasa de 8 bits X 8,000 Hz, esto es, la capacidad del canal para digitalizar la voz es de 64, 000 bits/seg. PCM se basa en el teorema de muestreo.

El teorema de *Nyquist* establece la mínima razón de muestreo (fs) que puede usarse para un sistema PCM, matemáticamente, la mínima razón de muestreo es:

$$fs \geq 2\ fa$$

En donde:

fs = mínima razón de muestreo de *Nyquist* (hertz)
fa = frecuencia más alta que se debe muestrear (hertz).

b) Codificación *digital-digital*:

Una señal es digital si consiste de una serie de pulsos de tensión. Para datos digitales no hay más que codificar cada pulso como un bit de datos.

La razón de datos de una señal es la velocidad de transmisión expresada en bits por segundo, a la que se transmiten los datos.

La razón de modulación es la velocidad con la que cambia el nivel de la señal, y depende del esquema de codificación elegido.

Las señales digitales son enviadas a través del medio por diferencias de voltaje o de intensidad luminosa.

Para mejorar las prestaciones del sistema de transmisión, se debe utilizar un buen esquema de codificación, que establece una correspondencia entre los bits de los datos y los elementos de señal.

Factores que se deben tener en cuenta para utilizar un buen sistema de codificación:

i. Espectro de la señal: La ausencia de componentes de altas frecuencias, disminuye el ancho de banda. La presencia de componente continua en la señal obliga a mantener una conexión física directa (propensa a algunas interferencias). Se debe concentrar la energía de la señal en el centro de la banda para que las interferencias sean las menores posibles.

ii. Sincronización : para separar un bit de otro, se puede utilizar una señal separada de reloj (lo cuál es muy costoso y lento) o bien que la propia señal porte la sincronización, lo cuál implica un sistema de codificación adecuado.

iii. Detección de errores: es necesaria la detección de errores ya en la capa física.

iv. Inmunidad al ruido e interferencias: hay códigos más robustos al ruido que otros.

v. Costo y complejidad: el costo aumenta con el aumento de la razón de elementos de señal.

Se utilizan distintos métodos según las características del medio, y los más comunes son:

- NRZ (Nonreturn-to-Zero-Level), la figura 13 muestra un ejemplo de este código, donde se aprecia como el nivel alto es un 1 y el nivel bajo es un 0.
  0 = nivel bajo
  1 = nivel alto

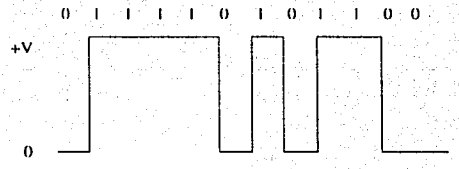

Fig. 13. Código sin Retorno a Cero (NRZ)

Considerado como un código básico, debido a que aparece en forma "natural" en los circuitos digitales sincrónos. El intervalo portador de información en el código NRZ es el máximo posible, es decir un intervalo de reloj. En caso de trenes largos de bits iguales, la información de sincronismo es poco densa y es muy difícil regenerar la señal de reloj en el receptor. La componente de corriente continua de la onda NRZ medida en secuencias largas y aleatorias es igual a la mitad del pico de amplitud

- RZ (Return-to-Zero-Level), como se muestra en la figura 14:

Fig. 14 Código con Retorno a Cero (RZ).

Similar al NRZ, excepto que la información esta contenida en la primera mitad del intervalo de bit, mientras que la segunda mitad esta siempre en el nivel "cero".

Es posible extraer en recepción, directamente el reloj de la señal recibida, sin embargo para secuencias largas de "ceros", es nuevamente imposible extraer el reloj para todo aquel período.

- NRZI (Nonreturn to Zero Inverted), como se muestra en la figura 15:
  0 = no-transición a un comienzo de intervalo (un intervalo de bit)
  1 = transición a un comienzo de intervalo

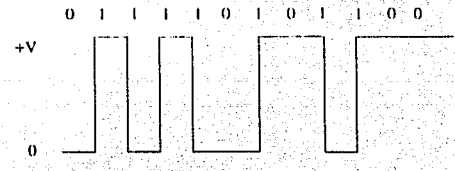

Fig. 15 Código sin Retorno a Cero Invertido (NRZI)

Es una variación de NRZ, mantiene un pulso constante de voltaje para la duración de un intervalo bit. Los datos son codificados por la presencia o ausencia de una transición de señal al comienzo del intervalo de bit. Una transición bajo a alto, o alto a bajo, al comienzo de un intervalo de bit denota un 1 binario para el intervalo de bit, no hay transición indica un 0 binario.

- Manchester, como se muestra en la figura 16:
  0 = transición de alto a bajo en medio del intervalo
  1 = transición de bajo a alto en medio del intervalo

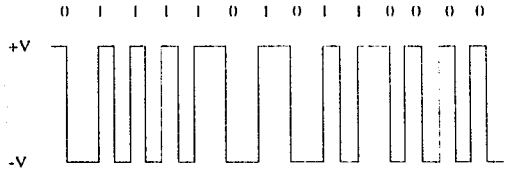

Fig. 16 Código Manchester

Los datos digitales son representados como sigue:

0 bit = +V voltaje en la primera mitad del bit y –V voltaje en la segunda mitad.

1 bit = -V voltaje en la primera mitad del bit y +V voltaje en la segunda mitad.

- Bipolar-AMI, como se aprecia en la figura 17:
  0 = no hay señal de línea
  1 = nivel positivo o negativo, alternancia para unos sucesivos
  Es un código Bipolar, por lo que la componente continua es nula.
  Se codifican "ceros" con el nivel cero.
  Se codifican "unos" con niveles positivos y negativos alternativamente.

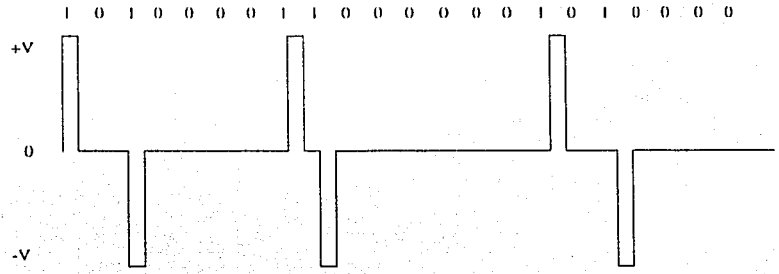

Fig. 17 Código de Marca Alternativa (AMI).

Es posible obtener la señal de sincronismo simplemente rectificando la señal recibida, al hacerla similar a la RZ.

Otra ventaja es la posibilidad de reconocer errores, si durante la transmisión por cable un pico de ruido se sumara a un "cero", y se tendría una violación del código.

Se presenta igualmente la dificultad de extracción del sincronismo en secuencias largas de "ceros".

- HDB3, como se muestra en la figura 18:
  Igual a Bipolar-AMI excepto que cualquier cadena de cuatro ceros es remplazada por una cadena con un código de violación.

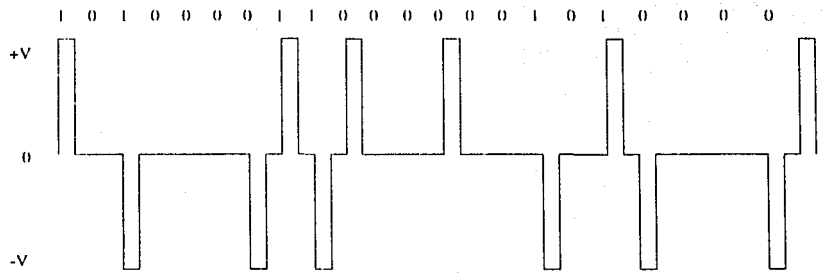

Fig. 18 Código HDB3.

Los "unos" son alternadamente positivos y negativos.
Permite extraer la señal de reloj también en presencia de largas secuencias de "ceros".
Cuando se tienen mas de tres "ceros" consecutivos, automáticamente se inserta un "uno" en el lugar del cuarto "cero", violando la polaridad (es decir se inserta un "uno" con la misma polaridad del último "uno" recibido) de forma que se pueda reconocer en recepción y poderlo eliminar.

Si entre dos violaciones consecutivas no existen "unos", o bien hay un número par de "unos", se inserta un bit adicional para mantener nula la componente continua. El reloj se extrae utilizando las transiciones que se suceden a la frecuencia del reloj o múltiplos de esta para sincronizar un oscilador local (VCO) oscilando a la frecuencia del reloj.

Los *códigos de comunicación de datos* son secuencias de bit prescritas, usadas para codificar caracteres y símbolos. Consecuentemente, los códigos de comunicación de datos frecuentemente se llaman *conjuntos de caracteres, códigos de caracteres, códigos de símbolo, o lenguajes de caracteres.* Esencialmente, existen sólo tres tipos de caracteres usados en los códigos de comunicación de datos: *caracteres de control de enlace de datos*, los cuales se usan para facilitar el flujo ordenado de información,

de una fuente a un destino; caracteres de control gráfico, lo cual involucra la síntesis o presentación de la información en la terminal de recepción, y caracteres *alfa/numéricos,* los cuales se usan para representar los múltiples símbolos usados para letras, números y puntuación en el lenguaje ingles.

Los tres conjuntos de caracteres, más comunes, actualmente usados para la codificación son: el *código* ***Baudot***, el *Código Estándar Americano para el Intercambio de Información* (**ASCII**) y el *Código de Intercambio de Decimal Codificado en Binario Extendido* (**EBCDIC**).

a) El código *Baudot* (a veces llamado código Teletex) fue el primer código de caracteres de tamaño fijo. El código *Baudot* fue desarrollado por un ingeniero postal francés. Thomas Murray, en 1875 y nombrado después Emile Baudot, un pionero en la impresión telegráfica. El código *Baudot* es un código de caracteres de 5 bits que se usa principalmente para equipo de teletipo de baja velocidad, tal como el sistema TWX/Telex. Con el código de 5 bits existen sólo 25 o 32 combinaciones posibles, lo cual es insuficiente para representar las 26 letras del alfabeto, los 10 dígitos y los diversos signos de puntuación, así como caracteres de control. Por lo tanto, el código *Baudot* usa caracteres de cambio de posición de letra, para expandir su capacidad a 58 caracteres. La última versión del código *Baudot* está recomendada por el CCITT como el Alfabeto Internacional No. 2. El código Baudot, aún lo usa la *Western Union Company* para el TWX y los sistemas de teletipo Telex. Los servicios de noticias, AP y UPI, por muchos años usaron el código Baudot para enviar la información de noticias a todo el mundo.

b) En 1963, en un esfuerzo por estandarizar los códigos de comunicaciones de datos, Estados Unidos adoptó el código de teletipo modelo 33, del Sistema Bell, como el código para Intercambio de Información Estándar de Estados Unidos de América (*USASCII*), mejor conocido como *ASCII*-63. Desde su adopción, *ASCII* ha progresado genéricamente por las versiones de 1965, 1967 y 1977, con la versión de 1977 recomendada por la CCITT como el Alfabeto Internacional No. 5. *ASCII*, es un conjunto de caracteres de 7 bits que tiene 2 ala 7 o 128 combinaciones. Con *ASCII*, el bit menos significativo (LSB) se designa como bo y el bit más significativo (MSB) se designa como b6. El b7 no es parte del código *ASCII*, pero generalmente se reserva para el bit de paridad. En realidad, con cualquier conjunto de caracteres, todos los bits son igualmente importantes, por que el código no representa un número binario con más peso. Es común con los códigos de caracteres referirse a bits por su orden; bo es el bit de orden cero, b1 es el bit de primer orden, b7 es el bit del séptimo orden, etc. Con la transmisión serial, el bit transmitido se llama LSB. Con *ASCII*, el bit de orden bajo (bo), es el LSB y se transmite primero. El *ASCII* es probablemente el código más frecuentemente usado hoy día.

c) *EBCDIC* es un código de caracteres de 8 bits, desarrollado por IBM y se usa, extensamente, en IBM y equipo compatible con IBM. Con 8 bits, son posibles 2 a la 8 o 256 combinaciones, haciendo que *EBCDIC* el LSB se designa como b7 y el MSB se designa como bo. Por lo tanto, con *EBCDIC*, el bit de orden alto (b7) se transmite primero y el bit de orden bajo (bo) se transmite al final. El código *EBCDIC* no facilita el uso de bit de paridad.

I.II.7 Control y Detección de Errores.

Un circuito de comunicación de datos puede ser tan corto ó de varios miles de kilómetros; el medio de transmisión puede ser tan sencillo, como un pedazo de cable o, tan complejo, como un sistema de microondas, satélite o fibra óptica. Por lo tanto, debido a las características, no ideales, que están asociadas con cualquier sistema de comunicación, es inevitable que ocurran errores y es necesario desarrollar e implantar procedimientos para el control de errores. El control de errores puede dividirse en dos categorías generales: *detección de errores* y *corrección de errores*.

a) Detección de Errores. Cuanto mayor es la información que se transmite, mayor es la probabilidad de que contenga algún error. Para detectar errores, se añade un código en función de los bits de la trama de forma que este código señale si se ha cambiado algún bit en el camino. Este código debe de ser conocido e interpretado tanto por el emisor como por el receptor

La detección de errores es simplemente el proceso de monitorear la información recibida y determinar cuando un error de transmisión ha ocurrido. Las técnicas de detección de errores no identifica cual bit (o bits) es erróneo, solamente indican que ha ocurrido un error. El propósito de la detección de errores no es impedir que ocurran errores, pero previene que los errores no detectados no ocurran. Cómo reacciona un sistema a los errores de transmisión, depende del sistema y varía considerablemente. Las técnicas de detección de errores más comunes usados para los circuitos de comunicación de datos son: redundancia, codificación de cuenta exacta, paridad, chequeo de redundancia vertical y longitudinal y chequeo de redundancia cíclica.

Redundancia:

La redundancia involucra transmitir cada carácter dos veces. Si el mismo carácter no se recibe dos veces sucesivamente, ha ocurrido un error de transmisión. El mismo concepto puede usarse para los mensajes. Si la misma secuencia de caracteres no se recibe dos veces sucesivamente, en exactamente el mismo orden, ha ocurrido un error de transmisión.

Codificación de cuenta exacta:

Con la codificación de cuenta exacta, el número de unos en cada carácter es el mismo. Un ejemplo de un esquema de la codificación de cuenta exacta es el código ARQ. Con el código ARQ, cada carácter tiene tres unos en él y, por tanto, una cuenta sencilla de la cantidad de unos recibidos, en cada carácter, determina si ha ocurrido un error de transmisión.

Paridad:

La *paridad* es probablemente el esquema de detección de error, más sencillo, usado para los sistemas de comunicación de datos y se usa con chequeo de redundancia vertical y horizontal. Con la paridad, un solo bit (llamado bit de paridad) se agrega a cada carácter para forzar el total de números unos en el carácter, incluyendo el bit de paridad, para que sea un número impar (paridad impar) o un número par (paridad par). Por ejemplo, el código ASCII para la letra "C" es 43 hex o P1000011 binario, con el bit P representando el bit de paridad. Hay tres unos en el código, no contando el bit de paridad. Si se usa la paridad impar, el bit P se hace un 0, manteniendo el número total de unos en tres, un número impar. Si se usa la paridad par, el bit P se convierte en 1 y el número total de unos es cuatro, un número par.

La ventaja principal de la paridad es la simplicidad. La desventaja es que cuando un número par de bits se recibe erróneamente, el checador de paridad no lo detectará. Consecuentemente, la paridad en un período largo de tiempo, detectará sólo el 50% de los errores de transmisión.

Chequeo de redundancia vertical y horizontal.

El chequeo de *redundancia vertical* (*VRC*), es un esquema de detección de errores que usa la paridad para determinar si un error de transmisión ha ocurrido dentro de un carácter. Por lo tanto, el *VRC* a veces se llama paridad de carácter. Con el *VRC*, cada carácter tiene un bit de paridad agregado a él, antes de la transmisión. Puede usar paridad par o impar.

El chequeo de *redundancia horizontal* (*HRC*) y *longitudinal* (*LRC*), es un esquema de detección de errores que utiliza la paridad para determinar si un error de transmisión ha ocurrido en un mensaje y, por lo tanto, a veces es llamada paridad de mensaje. Con el *LRC* cada posición de bit tiene un bit de paridad. Esencialmente, el *LRC* es el resultado de usar XOR (compuerta lógica, donde todas las entradas con unos o ceros, resulta la salida un cero), con los "caracteres" que componen un mensaje, mientras que el *VRC* es el uso de XOR en los bits con un solo carácter. Con el *LRC*, sólo la paridad par será usada.

La secuencia del bit en el *LRC* se calcula en el transmisor, antes de enviar la información, después se transmite como si fuera el último carácter del mensaje. En el receptor, el *LRC* sé recalcula en los datos y el *LRC* recalculado se compara con el *LRC* transmitido con el mensaje. Si son iguales, se asume que ningún error de transmisión ha ocurrido. Si son diferentes, un error de transmisión deber haber ocurrido.

Chequeo de redundancia cíclica:

Probablemente, el esquema más confiable para la detección de errores es el *chequeo de redundancia cíclica* (*CRC*). Con *CRC*, aproximadamente el 99.95 % de todos los errores de transmisión se detectan. El *CRC* se usa generalmente con códigos de 8 bits, tales como el *EBCDIC* o códigos de 7 bits, cuando no se usa la paridad.

El código *CRC* más común es el *CRC*-16, el cual es idéntico al estándar internacional, CCITT V.41. Con el CRC-16 se utilizan 16 bits. Esencialmente, el carácter CRC es el sobrante de un proceso de división. Un mensaje de datos polinómico *G(x)* se divide por una función de polinómico del generador *P(x),* el cociente se descarta, y el residuo se trunca en 16 bits y se agrega al mensaje como el *BCS (secuencia de chequeo de bloque).* Con la generación de CRC, la división no se logra con un proceso de división aritmética estándar. En vez de usar una resta común, el residuo se deriva de una operación de XOR. En el receptor, el flujo de datos y el *BCS* se dividen por la misma función de generación P(X). Si ningún error de transmisión ha ocurrido, el residuo será cero.

El polinomio generado para el CRC-16 es

$$P(x)= x16 + x\ 12 + x5 + x_0$$

En donde $x_0 = 1$

El número de bits en el código CRC es igual al exponente más alto del polinomio generado. Los exponentes identifican las posiciones del bit que contiene un 1.

b) Corrección de errores. Esencialmente, hay tres métodos de corrección de errores: *sustitución de símbolos, retransmisión y seguimiento de corrección de un error.*

Sustitución de símbolos:

La sustitución de símbolos se diseño para usarse en un ambiente humano. Con la sustitución de símbolos, si un carácter se recibe en error, en vez de revertirse

a un nivel superior de corrección de errores o mostrar el carácter incorrecto, un carácter único que es indefinido por el código de caracteres, tal como un signo de interrogación invertido, se sustituye por el carácter malo. Por ejemplo, si el mensaje "Nombre" tenía un error en el primer carácter, se mostraría como "?ombre", un operador puede discernir el mensaje correcto por inspección, y la retransmisión es necesaria. Sin embargo, sí el mensaje "$?,000.00" se recibiera, un operador no podría determinar el carácter correcto y la retransmisión sería requerida.

Retransmisión:

La *retransmisión*, es volver a enviar un mensaje, cuando es recibido en error, y la terminal de recepción automáticamente pide la retransmisión de todo el mensaje. La retransmisión frecuentemente se llama *ARQ*, que significa petición automática para retransmisión. *ARQ* es probablemente el método más confiable de corrección de errores, aunque no siempre es el más eficiente. Las dificultades en el medio de transmisión ocurren en ráfagas. Si se usan mensajes cortos, la probabilidad de que una dificultad ocurra, durante la transmisión, es pequeña. Sin embargo, los mensajes cortos requieren de más reconocimientos y regresos de línea que los mensajes largos. Los reconocimientos y regresos de línea para el control de errores son formas de encabezamientos (caracteres diferentes a los datos que se deben transmitir). Con los mensajes largos, menos tiempo de regreso es necesario, aunque la probabilidad de que un error de transmisión ocurra es mayor que para los mensajes cortos.

Seguimiento de corrección de error:

El *seguimiento de corrección de error* (*FEC*), es el único esquema de corrección de error que detecta y corrige los errores de transmisión, del lado receptor, sin pedir retransmisión.

Con *FEC*, se agregan bits al mensaje, antes de la transmisión. Un código de corrección de errores popular, es el código de *Hamming*, desarrollado por R. W. *Hamming*. El número de bits de Hamming que debe agregarse a un carácter se determina de la siguiente expresión:

$$2^n > m + n + 1$$

en donde n = número de bits de Hamming
m = número de bits en el carácter de datos.

El propósito de los códigos *FEC* es reducir o eliminar el tiempo gastado de retransmisiones. Sin embargo, la suma de los bits *FEC* a cada mensaje gasta el tiempo de transmisión. El *FEC* frecuentemente se usa para transmisiones sencillas a muchos receptores, cuando los reconocimientos no son prácticos.

I.III Redes de datos.

En tan solo unos años las redes de computadoras han pasado de ser algo casi desconocido y utilizado por unos pocos a ocupar un primer plano en cualquier medio informativo de carácter general.

Para estructurar los conceptos de Redes de Computadoras se ha desarrollado un amplio cuerpo de doctrina que cubre desde la abstracción de la arquitectura hasta la visión sistemática pasando por los fundamentos tecnológicos y la modelación matemática. Las Redes pueden analizarse desde las siguientes ópticas:

- Arquitectura, es decir, la definición abstracta de sus servicios y protocolos
- Características físicas y lógicas, como topología, sistemas de transmisión, acceso y conmutación y medios de transmisión.
- Modelos matemáticos del comportamiento de la red, para evaluar sus parámetros de calidad.

También hay que decir que, en la actualidad, hay tendencias para encontrar arquitecturas y tecnologías que sean aplicables a todo tipo de redes, sean LAN, MAN o WAN, así como a todo tipo de tráfico, datos, voz e imagen estática o animada.

La velocidad de transmisión y, en consecuencia, el ancho de banda requerido por las aplicaciones se ha incrementado notablemente a medida que han ido apareciendo aplicaciones más complejas.

I.III.1 Medios y técnicas de transmisión.

El medio de transmisión, es probablemente la parte más crítica en el diseño de una red, especialmente cuando se trata de redes locales. Además las inversiones que se hacen en infraestructura suelen ser la parte más importante de la red y la más difícil de modificar más adelante. Por otro lado, este es un campo que evoluciona con mucha rapidez, y lo que hoy puede parecer adecuado quizá no lo sea dentro de dos años; para tomar una decisión acertada es necesario hacer una estimación objetiva de las necesidades actuales y futuras, y una valoración adecuada de las tecnologías disponibles tomando en cuenta su relación costo/beneficio.

Este aspecto clave del diseño de una red, que es el medio físico que transporta la información, puede condicionar la distancia, velocidad de transferencia, topología e incluso el método de acceso.

Existen 5 tipos de medios utilizados más comúnmente en comunicaciones, agrupados en dos categorías: cables e inalámbricos:

- Cables
  a) Par Trenzado
  b) Coaxial
  c) Fibra Óptica

- Inalámbricos
  d) Radio
  e) Luz

Los parámetros más significativos a considerar en la selección del tipo de cable son los siguientes:

- Ancho de Banda
- Longitud
- Fiabilidad en la transferencia
- Seguridad
- Facilidad de instalación
- Costo.

El ancho de banda es función de las características del cable y de su longitud. Normalmente, para cada arquitectura y tipo de cable están definidas las distancias máximas utilizables.

La fiabilidad es la característica que determina la calidad de la transmisión, normalmente evaluada en porcentaje de errores por número de bits transmitidos, relacionada con la atenuación, así como la sensibilidad a las interferencias externas.

La seguridad indica el menor grado de dificultad con que las señales transportadas pueden ser interceptadas.

La facilidad de instalación está relacionada con la ligereza y diámetro del cable, así como por su sensibilidad a las operaciones que sobre él se realicen. En fibra óptica, por ejemplo, los optó acopladores son elementos muy críticos, por lo que su instalación y ajuste es muy complejo.

Obviamente, el costo es un criterio determinante en la selección del cable. El cable más económico es el par trenzado, siendo la fibra óptica el más costoso.

a) Cable de par trenzado.

Este es el medio de transmisión más común, por su bajo costo y sencillez de instalación, consiste en un par de hilos de cobre aislados, de alrededor de 1 milímetro de diámetro. Un cable suele llevar varios hilos (típicamente 4 u 8) que normalmente están doblados dos a dos (o cuádruple) hélice, por lo que se le suele denominar cable de par trenzado (twisted pair). Este trenzado helicoidal le hace menos susceptible a las interferencias externas y reduce la posibilidad de interferencias entre pares cuando éstos se agrupan en el mismo cable. La figura 19 muestra los cables de par trenzado.

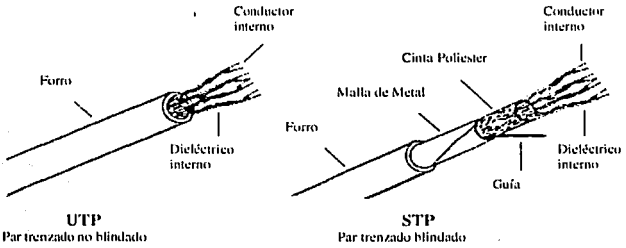

Figura 19. Cables de par trenzado.

El cable de par trenzado puede ser blindado o sin blindaje. Al cable blindado se le conoce frecuentemente por el acrónimo *STP* (*Shielded Twisted Pair)*, mientras que el cable no blindado es conocido como *UTP* (*Unshielded Twisted Pair)*. Por su menor sensibilidad a las interferencias y menor atenuación el cable *STP* es más adecuado para mayores distancias y velocidades de transmisión, así como para operación en entornos con interferencias, aunque la tendencia es utilizar *UTP*, por su bajo costo, sencillez de instalación y su utilización. Tanto el cable *UTP* como *STP* se utilizan actualmente a velocidades muy elevadas, incluso a 150 Mbps, con longitudes de cable no superiores a 100 m. La atenuación es del orden de 30dB/300 m a 100 Mhz. La impedancia característica es de 100 ohms para los cables *UTP* y de 120 a 150 ohms para los *STP*.

En el caso del cable UTP existen varías versiones denominadas categorías 2, 3, 4 y 5 que han sido normalizadas por la EIA (*Electronics Industries Association*) en 1991. Puesto que todas las categorías permiten la transmisión de voz y datos, se señalarán las diferencias más significativas relativas a la transmisión de datos.

De tal forma que antes haremos la distinción entre lo que es categoría y nivel.

- Categoría: son los cables que cumplen con la norma EIA/TIA 568 de alguna categoría tiene características mejores que los que sólo cumplen con las especificaciones del mismo nivel

- Nivel: los cables que sólo cumplen con los requerimientos de nivel pueden tener variaciones importantes en sus características eléctricas.

Conforme sube la categoría aumenta la densidad de vueltas y mejora la propagación de señales eléctricas de alta frecuencia. Por otro lado cuanto mayor es la frecuencia de la señal mayor es la atenuación y peor la propagación en un determinado cable, en la siguiente tabla se muestra las categorías y las frecuencias máximas correspondientes.

Categoría	Frecuencia Máxima	Vueltas/metro	Tipo cable
1	NA	0	UTP
2	1	0	UTP
3	16	10-16	UTP
4	20	16-26	UTP
5	100	26-33	UTP

Tabla 1. Categorías y frecuencias de los cables de par trenzado.

b) Cable coaxial

Un cable coaxial consta de un par de conductores de cobre o aluminio. Uno de ellos forma un alma central y está rodeado por el segundo conductor constituido por una malla muy fina de hilos trenzados o una lámina metálica cilíndrica. Como se muestra en la figura 20.

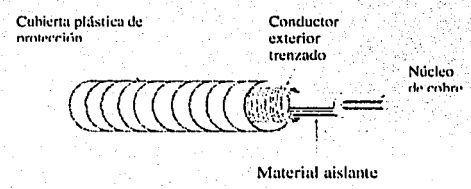

Figura 20. Cable coaxial.

La separación y aislamiento entre los dos conductores se realiza generalmente mediante un material dieléctrico de teflón o plástico. Todo el

cable esta cubierto por un aislamiento de protección para reducir las emisiones eléctricas.

El cable coaxial tiene normalmente un mayor ancho de banda que el cable de pares. Se utiliza tanto para transmisión de datos como para telefonía o señales de vídeo.

En redes de área local, el cable coaxial se emplea tanto con transmisión en banda base como en banda ancha, si bien la primera modalidad es la más utilizada. Es en las redes de tipo Ethernet donde su utilización ha sido la más extendida, si bien está siendo desplazada progresivamente y rápidamente por el cable UTP.

Los tipos de cable coaxial más empleados son los siguientes:

- Cable coaxial grueso. Sus características son: Impedancia de 50 ohms, conector tipo "N". Conocido como 10BASE5, implica una velocidad de operación de 10 Mbps, transmisión en banda base y una longitud máxima de un segmento de cable de 500 m

- Cable coaxial delgado. Sus características son: Impedancia de 50 ohms, conector tipo "BNC". Conocido como 10BASE2; es decir, operan a 10 Mbps, con transmisión en banda base y una longitud máxima de cable del orden de 200 m (realmente hasta 185 m).

- Cable coaxial de banda ancha. Sus características son: Impedancia de 75 ohms. Conocido como 10BROAND36; es decir, opera a 10 Mbps con transmisión en banda ancha y longitud máxima de extremo a extremo de 3,600 m.

Se podría decir además, que de los cables coaxiales por su variedad, solo se deben utilizar para redes Ethernet aquellos que sean específicamente marcados con la leyenda de IEEE802.3. En la tabla 2 se muestra los diferentes tipos de coaxiales más comunes.

Tipo de Cable	Impedancia (ohms)	Aplicación
802.3 y RG-58	50	Ethernet delgado
802.3, RG-58, RG-11, RG-213 y RG-24	50	Ethernet grueso
RG-58	53	No se debe usar
RG-59	75	CATV

Tabla 2. Cables coaxiales.

c) Cable de fibra óptica.

Constituye el medio de transmisión más reciente y el de mayor potencial para redes de alta velocidad. Como se observa en la figura 21, la fibra óptica está constituida por un núcleo circular muy fino de fibra de vidrio (silicio) transparente, capaz de conducir en su interior la energía óptica. Esta rodeado de un revestimiento de otro tipo de vidrio, con diferente índice de refracción. Todo el conjunto está envuelto con una cubierta opaca y absorbente de luz.

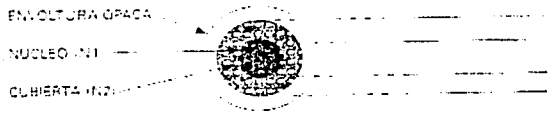

Figura 21. Núcleo de fibra óptica.

El sistema de transmisión óptica está formado por tres componentes, como se muestra en la figura 22.

- *Transmisor de energía óptica* con un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones), que se emite a través de la fibra óptica. Las fuentes luminosas pueden ser el LED –diodo emisor de luz- o láser, con una mayor capacidad.
- *La fibra óptica,* que se conecta a la fuente luminosa y al detector de energía óptica. El componente de la fibra es silicio.
- *Detector de energía óptica,* normalmente un foto diodo, que convierte la señal óptica recibida en electrones. Es necesario también un amplificador para regenerar la señal.

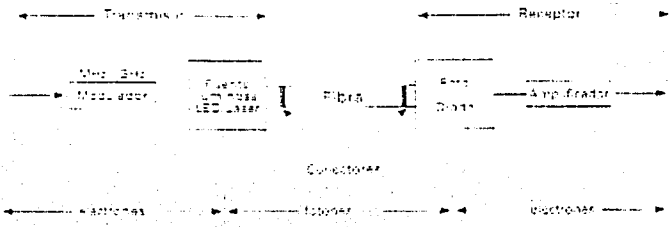

Figura 22. Componentes del sistema de transmisión óptica.

El principio de operación de la fibra óptica es el siguiente:

Los rayos ópticos que se transmiten a través del núcleo tienen un cierto ángulo con respecto al eje de éste. Así, al cabo de cierta distancia, alcanza el revestimiento, en el que se refractan, siguiendo la ley de Snell, que establece que los senos de los ángulos de refracción son inversamente proporcionales a la velocidad de propagación de la luz en cada uno de los medios, el cual, a su vez, es proporcional al denominado índice de refracción *n*, *n*= V/C, siendo V la velocidad de propagación en el medio y C la velocidad de propagación en el vacío.

El valor de *n* para el aire es próximo a 1, y para la fibra óptica es del orden de 1,5. Cuando el ángulo de refracción en el material con el índice de refracción más elevado alcanza un determinado valor, no se produce refracción, y toda la energía óptica se refleja. El ángulo de incidencia en el que se produce este fenómeno se denomina ángulo crítico. Para ángulos mayores (con respecto a la perpendicular del eje) hay reflexión y para ángulos menores refracción. Por consiguiente, para que la energía óptica se refleje en el revestimiento y no atraviese éste, el índice de refracción del núcleo debe ser mayor que el del revestimiento y los rayos deben de alcanzar éste con un ángulo superior al crítico, con respecto a la perpendicular al eje del núcleo. Típicamente el valor del índice de refracción del núcleo es del orden de 1,5 y el del revestimiento, del orden de 1,48.

De la forma expuesta, el rayo luminoso se propaga a través del núcleo, reflejándose en la frontera con la cubierta sin penetrar en el material de ésta. Sin embargo, como se ve en la fig. 23(a), la luz recorre diferentes caminos, según el ángulo de incidencia del rayo, lo cual produce que los rayos se agreguen en recepción con diferentes fases. A velocidades muy altas (tiempos de bit muy pequeños), la distorsión hace impracticable la transmisión. Este sistema se denomina *multimodo* con *índice escalonado* (n1 y n2). El producto de la velocidad (Mbps) por la distancia (Km) no puede ser mayor de 30. Así, para una velocidad de 10 Mbps la distancia máxima es del orden de 3 Km; sin embargo para una velocidad de 100 Mbps sólo se podrían alcanzar 300 m, por lo que no es adecuado.

La capacidad de la fibra puede mejorarse, por ejemplo, haciendo que el índice de refracción del núcleo sea variable, decreciendo desde el centro hacia la cubierta con una función parabólica. De esta forma, los rayos con menor ángulo con respecto al eje recorren una distancia menor, pero también atraviesan la fibra a una velocidad relativamente mayor que los rayos con mayor ángulo. Así se compensan los efectos, y las fases de llegada se aproximan. Este sistema se denomina *multimodo* con *índice gradual*, como se ve en la figura 23 (b).

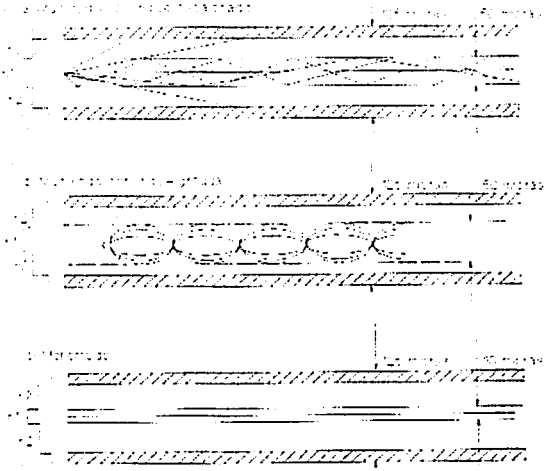

Figura 23. Tipos de fibras ópticas.

Los sistemas *multimodo* pueden operar con LED. Si se desea tener unos ángulos mínimos, para que prácticamente todos los rayos lleguen al destino sin reflexión, se debe utilizar luz coherente, generada con láser y reducir el tamaño del núcleo de 50 a un orden de 10 micras. Con ello, el límite de velocidad y distancia es de varios órdenes de magnitud superior y está condicionado por un fenómeno denominado dispersión cromática, sobre el que se está investigando, para obtener cada vez mayores capacidades. Por indicar un orden de magnitud, podemos hablar de un orden de 100 Gbps por Km. En la fig. 23 (c) se representa un sistema *monomodo*.

Las principales características de la fibra óptica son:

- Ancho de Banda muy elevado
- Tamaño pequeño y de poco peso
- Baja atenuación
- Aislamiento electromagnético

Su principal inconveniente es la complejidad y la sensibilidad de los optoacopladores. Por lo que las causas principales de pérdidas en un enlace de fibra óptica son los siguientes:

- Atenuación en la fibra

- Conectores
- Empalmes

La fibra en sus diferentes modalidades, como se menciono anteriormente cubre ciertas aplicaciones especificas por lo que podemos destacar lo siguiente:

- La fibra óptica *multimodo de índice escalonado* ya no se utiliza
- La fibra óptica *multimodo de índice gradual* se utiliza en redes de área local (LAN) con un segmento máximo de 2 Km
- La fibra óptica *monomodo* se utiliza en redes de área amplia (WAN) y metropolitana (MAN) con un segmento máximo de 60 Km

d) Inalámbricos (Tecnología de Radio.)

Las ondas de radio se propagan por diferentes medios físicos, como son el aire y el vacío, de tal forma que podemos distinguir tres tipos de redes comunicación por radio: inalámbricas, Terrenas, Satelitales.

Redes inalámbricas

En algunos de los entornos el tendido de cables puede resultar muy difícil o muy frecuente debido a los cambios de lugar de trabajo del personal. Una solución a este tipo de problemas puede ser la utilización de redes inalámbricas, sí bien, hasta la fecha, su despliegue es muy restringido.

Las principales técnicas utilizadas transmiten en los espectros de UHF (Ultra High Frecuency, de 300 Mhz a 3 GHz), microondas (banda SHF, Super High Frecuency, de 3 GHz a 30 GHz) o infrarrojos.

La mayoría de las redes inalámbricas que operan en el espectro de UHF utilizan la banda de 902 a 928 Mhz, usada también por los teléfonos móviles e inalámbricos. Operan con una cobertura de unos pocos de cientos de metros y velocidades de hasta 2 Mbps. Las limitaciones de velocidad son debidas a la necesidad de un gran ancho de banda por la utilización de un código denominado de expansión que es conocido por un único receptor capaz de descifrar la señal recibida.

Las redes que operan con microondas utilizan normalmente la banda de 18 GHz. Se pueden alcanzar velocidades de 10-15 Mbps y distancias del orden de 100 m

Las redes de infrarrojos exigen una línea de vista sin obstáculos, dada su propagación en línea recta. Pueden operar entre 4-10 Mbps, sí bien la máxima cobertura es de tan solo unas pocas decenas de metros.

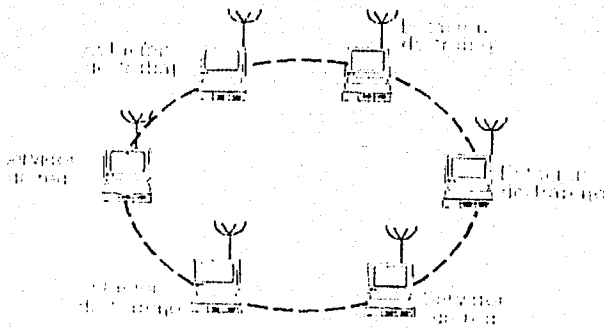

Figura 24. Red inalámbrica.

Puede decirse que la tecnología de redes inalámbricas es emergente y que comienza a utilizarse en entornos departamentales o de pequeñas oficinas, o bien en situaciones en que es necesario disponer de una "estación de trabajo" en localizaciones en las que no es accesible el cableado. La figura 24 muestra una red inalámbrica.

De las ventajas de este medio de transmisión tenemos:

- No se requiere cableado
- Movilidad y reubicación
- Muchas veces no se requiere línea de vista
- Puesta en marcha muy rápido
- No requiere asignación de frecuencia

Desventajas:

- 800 ft de distancia máxima entre estaciones
- Muchas de ellas operan a menos de 10 Mbps
- Más caro que instalar cable

Comunicación terrena por radio

Para este apartado existen dos opciones de frecuencias: radio y microondas, teniendo mayor alcance estas últimas. De tal forma que podemos mencionar entre sus ventajas y desventajas principales:

Ventajas:

- No se requiere cableado

- Grandes distancias
- Tasas medias y altas de transmisión

Desventajas:

- Infraestructura costosa
- Requiere línea de vista (incluyendo la primer zona de Fresnel)
- Puede requerir asignación de frecuencia
- La lluvia y el polvo afectan la calidad de la transmisión

Comunicación Satelital

Se utilizan estaciones terrenas de microondas apuntadas al satélite que las repetirá

Ventajas:

- No se requiere cableado
- Muy grandes distancias
- No se requiere línea de vista (solo al satélite)

Desventajas:

- Infraestructura muy costosa
- Tiempo de respuesta con retraso de más de medio segundo
- Tasas bajas de transmisión
- Requiere asignación de frecuencia
- La lluvia y el polvo afectan la calidad de la transmisión.

Técnicas de transmisión

En esta sección se analiza cómo se transmiten los datos de las estaciones de la red al medio físico. En las redes de área local se utilizan principalmente dos modalidades: *banda base* y *banda ancha.*

En *banda base*, la transmisión se realiza en forma digital, sin emplear técnicas de modulación. En *banda ancha*, la señal digital se modula y después se envía al medio.

En la actualidad, la técnica dominante en las redes de área local es la de banda base.

a) Banda base

En las redes de *banda base*, la señal se transmite sin modulación. En consecuencia, cada vez que se realiza una transmisión se utiliza todo el ancho de banda del medio. Por ello, deben emplearse técnicas de medio compartido para que éste pueda ser utilizado por múltiples estaciones.

La ventaja fundamental en *banda base* es su sencillez, puesto que no requiere moduladores/demoduladores. La desventaja es que, debido a la distorsión de la señal digital con la distancia, se requiere el empleo de repetidores para regenerar la señal a partir de una cierta distancia, que depende del tipo de medio utilizado, del tipo de red y de la velocidad de transmisión.

La señal es transmitida secuencialmente al medio en forma de trenes de bits "1" y "0". Si se hace corresponder un nivel de voltaje con un "1" y otro nivel con "0", existe el inconveniente de que no se producen transiciones en la red cuando se envían corrientes de "1" o corrientes de "0". Ello dificulta la recuperación de la señal por parte del receptor, dado que no hay ninguna indicación de cuando empieza y cuando termina un bit, al no haber cambios de nivel en la señal. Esta circunstancia hace que se pueda perder la sincronización entre el emisor y el receptor, con lo que la información recibida es errónea. Para resolver el problema de la sincronización, se utilizan los códigos, de los más utilizados es el Manchester.

b) Banda ancha

Las redes de banda ancha utilizan señales analógicas moduladas. Normalmente, el medio utilizado es un cable coaxial de 75 ohms de impedancia característica. Las frecuencias de transmisión suelen alcanzar los 300 ó 400 Mhz. El ancho de banda total del cable se puede dividir, mediante técnicas de multiplexión por división de frecuencias (FDM), en grupos de canales de banda más estrecha. Cada uno de estos canales puede ser utilizado independientemente para un determinado tipo de servicio.

I.III.2 Tipos de redes

Sí bien las clasificaciones de redes que se van a presentar en esta sección tienen como interés sintetizar su estudio, es obvio que en la realidad casi nunca se da uno de esos tipos de redes en estado puro.

Las redes se clasifican generalmente sobre la base de su cobertura

Existen tres diferentes tipos de redes

a) Redes de Area Local (*LAN*: Local Area Network)
b) Redes de Area Metropolitana (*MAN*: Metropolitan Area Network)
c) Redes de Area Amplia (*WAN*: Wide Area Network)

En la tabla 3 vemos un comparativo de los tres diferentes tipos de redes:

	LAN	*MAN*	*WAN*
Alcance	< 5 Km	10 - 150 Km	< 100,000 Km
Velocidad	4-155 Mbps	50-622 Mbps	< 2 Mbps
Información	Datos, imágenes, voz, audio, video	Datos, imágenes, voz, audio, video	Datos, imágenes, voz, audio, video
Propiedad	El usuario	Servicio Público	Servicio Público

Tabla 3. Comparación de los tipos de red

a) Red de área local (LAN)

Una red de área local puede definirse como "*un sistema de comunicaciones que proporciona interconexión a una variedad de dispositivos en un área restringida como un edificio, campus, etc.*"

El elemento fundamental que define una red de área local es la utilización de medios privados de comunicación dentro de un recinto, edificio o campus. En consecuencia, tienen una serie de características que son:

- Propiedad: utilización de medios privados de comunicación
- Alcance: las distancias abarcan desde metros hasta pocos kilómetros
- Velocidad: elevadas velocidades de transmisión, que pueden cubrir un rango desde 10 hasta 100 Mbps e incluso mas altas como 1 Gbps
- Conectividad: permite la comunicación transparente, esto es, se puede conectar un gran equipo de procesamiento como un servidor, hasta una computadora personal.

- Interconexión: ofrece la posibilidad de conexión con otras redes mediante la utilización de puentes o ruteadores

Las LANs más conocidas y extendidas son la *Ethernet* a 10 Mbps, la *IEEE 802.5* o *Token Ring* a 4 y 16 Mbps, y la *FDDI* a 100 Mbps. Estos tres tipos de LAN han permanecido prácticamente sin cambios desde finales de los ochenta.

De tal forma que se describirán de forma breve los 3 tipos de redes locales más significativas.

Ethernet e IEEE 802.3

En los años setenta el PARC (Centro de Investigación de Palo Alto de Xerox Corporation) desarrolló Ethernet, que fue la base tecnológica para la especificación IEEE 802.3 lanzada inicialmente en 1980. Un poco después Digital Equipment Corporation, Intel Corporation y Xerox Corporation desarrollaron y lanzaron de manera conjunta una especificación de Ethernet (versión 2.0) que es sustancialmente compatible con la IEEE 802.3. Juntos, *Ethernet* e *IEEE 802.3*, comparten en la actualidad la mayor parte del mercado de los protocolos LAN.

Cuando *Ethernet* se desarrolló, se diseño para satisfacer la necesidad de conectividad entre las redes de larga distancia y baja velocidad y las redes especializadas de centros de cómputo que transportan datos a altas velocidades y distancias muy cortas. Ethernet está diseñado para aplicaciones en donde el medio de comunicación local debe transportar tráfico elevado y picos de alto flujo de datos en forma esporádica.

Explicando el funcionamiento de forma breve las estaciones de una LAN pueden accesar a la red en cualquier momento. Antes de enviar datos, las estaciones "escuchan" la red para ver si está en uso. De ser así, la estación que desea transmitir espera. Si la red no está en uso la estación transmite. Si dos estaciones escuchan el medio en busca de tráfico en la red y no "escuchan" nada, transmiten de manera simultánea, con lo cual ocurre una colisión. En este caso ambas transmisiones de dañan y las estaciones deben volver a transmitir en un momento posterior.

Las LANs *Ethernet* e *IEEE 802.3* son redes de difusión (*broadcast*). En otras palabras, todas las estaciones ven todas las tramas en circulación en el medio sin importar el destino. Cada estación debe examinar las tramas recibidas para determinar si dicha estación es el destino final. Si lo es, la trama se pasa hacia una capa de protocolo superior para continuar su procesamiento.

Las tramas *Ethernet* e *IEEE 802.3* comienzan con un patrón alternado de unos y ceros llamado *preámbulo*. Este le indica a las estaciones receptoras que está llegando una trama. Este byte termina con dos bits 1 consecutivos, que sirven para sincronizar los elementos de recepción de tramas de todas las estaciones en la LAN.

Después del preámbulo están los campos de dirección del destino y del origen de la información. Ambas direcciones son de 6 bytes de longitud y están contenidas en el hardware de las tarjetas de interfaz *Ethernet* e *IEEE 802.3* especifica los primeros 3 bytes de la dirección con base en el fabricante de la tarjeta. La dirección de origen siempre corresponde a un solo nodo (unicast), en cambio, la dirección del destino puede ser a un solo nodo (unicast), a un grupo de nodos (multicast) o a todos los nodos de la red (broadcast).

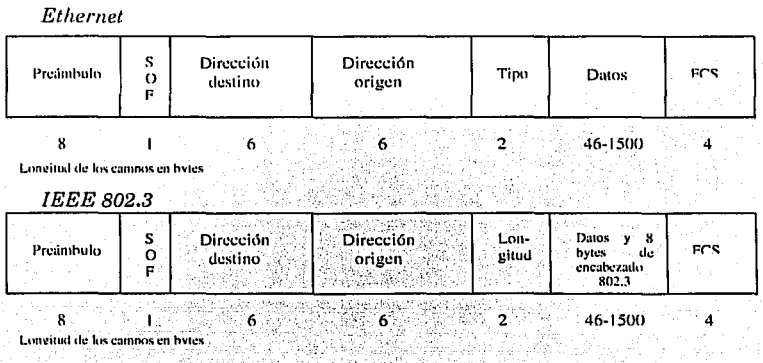

Figura 25. Tramas *Ethernet* e *IEEE 802.3*.

Como se ve en la figura 25, en las tramas *Ethernet* el campo de 2 bytes que sigue a la dirección del origen es un campo que indica el tipo. Este campo especifica el protocolo de capa superior que debe recibir los datos después de que termine el procesamiento *Ethernet*.

En las tramas *IEEE 802.3*, el campo de 2 bytes que está a continuación de la dirección del origen es el de longitud e indica la cantidad de bytes de datos que están después de él y hasta el byte anterior al campo FCS de la trama.

A continuación del campo de tipo/longitud están los datos reales contenidos en la trama. Después de que se haya terminado el procesamiento en las capas física y de enlace, estos datos se enviarán eventualmente a un protocolo de capa superior. En el caso de *Ethernet*, dicho protocolo está identificado en el campo de tipo. Para *IEEE 802.3*, ese protocolo debe estar definido dentro de la parte de datos de la trama, en caso de haberla. Si los datos de la trama son insuficientes para llenar el tamaño mínimo de 64 bytes de la trama, se insertan bytes de relleno para asegurar una trama con al menos 64 bytes.

Después del campo de datos esta un campo FCS de 4 bytes que contiene un valor de CRC. El dispositivo transmisor genera el valor CRC y el dispositivo receptor lo recalcula para revisar si hubo errores en la trama.

Token Ring e IEEE 802.5

La red *Token Ring* fue desarrollada originalmente por IBM en los años setenta. Todavía es la tecnología principal de LAN de IBM y se encuentra después de *Ethernet*. La especificación *IEEE 802.5* es casi idéntica y completamente compatible con la red *Token Ring* de IBM.

Si hacemos una comparación entre *Token Ring* e *IEEE 802.5* veremos que difieren en forma relativamente pequeña. La red *Token Ring* especifica una topología en estrella, con todas las estaciones terminales conectadas a un dispositivo llamado *MAU* (Unidad de Acceso Multiestaciones) y, en cambio, la *IEEE 802.5* no especifica una topología (aunque virtualmente todas las implementaciones *IEEE 802.5* están basadas en una topología en estrella). Existen otras diferencias, entre ellas el tipo de medio (*IEEE 802.5* no especifica un tipo de medio, en cambio, las redes *Token Ring* de IBM utilizan cable de par trenzado) y el tamaño de campo de la información de enrutamiento. La figura 26 muestra un diagrama físico de la red *Token Ring*.

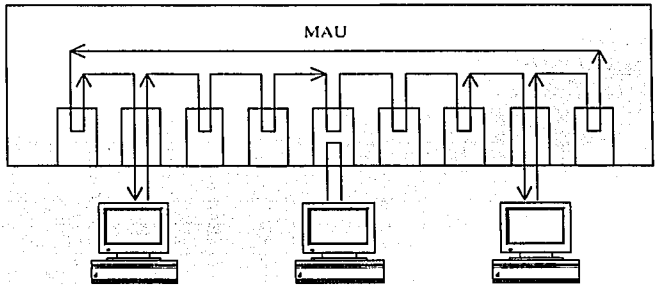

Figura 26. MAU de una red *Token Ring*.

El MAU es un dispositivo de red que actúa como el nodo central. Explicando el funcionamiento de las redes *token ring*, mueven una pequeña trama llamada *token*, alrededor de la red. La posesión del *token* otorga el derecho a transmitir. Si el nodo que recibe el *token* no tiene información para enviar, simplemente pasa el *token* a la siguiente estación terminal. Cada estación puede conservar el *token* por un período máximo.

Si la estación que posee el *token* tiene información por transmitir, toma el *token*, altera un bit de este, le añade información que desea transmitir y, por último, envía esta información a la siguiente estación. Mientras la trama de la información está circulando por el anillo no hay *token* en la red y, por tanto, las

demás estaciones que desean transmitir deben esperar. Por lo tanto, no pueden suceder colisiones.

Esta trama de información circula por el anillo hasta que llega a la estación de destino, la cual copia la información para continuar procesándola. La trama de información continua circulando por el anillo y, por último, se elimina cuando llega a la estación que le envío. Esta puede revisar la trama que regresa para ver si el destinatario vio dicha trama y si la copió.

A diferencia de las redes Ethernet, es posible calcular el tiempo máximo que transcurrirá antes de que cualquier estación terminal sea capaz de transmitir.

Las redes *Token Ring* emplean un sistema de prioridades refinado que permite que determinadas estaciones de alta prioridad designadas por el usuario utilicen la red con más frecuencia. Las tramas Token Ring tienen dos campos que controlan la prioridad: el campo de prioridad y el campo de reservación. En la figura 27 veremos los dos tipos de tramas: *tramas de datos/comandos* y *tokens.*

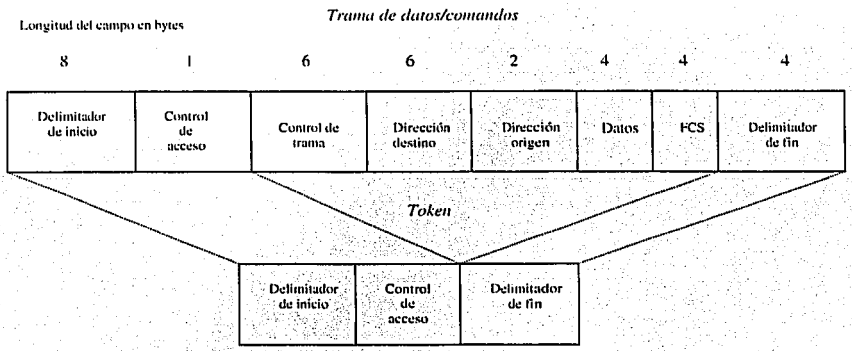

Figura 27. Formatos de trama IEEE 802.5 y Token Ring.

Cada *token* tiene 3 bytes de longitud, y consiste de un delimitador de inicio, un byte de control de acceso y de un delimitador de fin.

El delimitador de inicio sirve para alertar a cada estación de la llegada de un token (o de una trama de datos/comandos). El byte de control de acceso contiene los campos de prioridad y reservación, así como un bit de token y un bit de monitoreo. Por último, el delimitador de fin indica el final del *token* o de *la trama de datos/comandos.*

FDDI (Interfaz de Datos Distribuidos por Fibra)

El comité de estándares ANSI X3T9.5 produjo el estándar *FDDI* a mediados de los años ochenta. Durante este período, las estaciones de trabajo de alta velocidad comenzaban a agotar la capacidad de las LANs existentes – principalmente *Ethernet* y *Token Ring*. Era necesaria una nueva LAN que pudiera soportar a estas estaciones de trabajo y nuevas aplicaciones. Al mismo tiempo, la confiabilidad de la red se convertía en un aspecto cada vez más importante, a medida que los administradores de sistemas comenzaron a migrar las aplicaciones de misión crítica desde las grandes computadoras a las redes. *FDDI* se desarrollo para cubrir estas necesidades.

Aunque opera a velocidades más rápidas, *FDDI* es similar en muchas formas a *Token Ring*. Los dos tipos de redes comparten muchas características, incluyendo la topología (anillo), la técnica de acceso al medio (paso de token) y las características de confiabilidad (por ejemplo, anillos redundantes).

FDDI está definida por cuatro especificaciones por separado:

- *MAC* (Control de Acceso al Medio) – define cómo acceder al medio, incluyendo el formato de trama, el manejo de tokens, el direccionamiento, un algoritmo para calcular un valor de verificación de redundancia cíclica y mecanismos de recuperación de errores.
- *PHY* (Protocolo de la capa física) – define los procedimientos de codificación/decodificación de datos, los requerimientos de reloj, las tramas y otras funciones.
- *PMD* (Medio de la Capa Física) –define las características del medio de transmisión incluyendo el enlace de fibra óptica, los niveles de potencia, la tasa de bits de error, los componentes ópticos y los conectores.
- *SMT* (Administración de Estaciones) –define las configuraciones de estaciones *FDDI*, del anillo y las características de control de anillo, incluyendo la inserción y eliminación de estaciones, la inicialización, el aislamiento y la recuperación de fallas, la programación y el acopio de estadísticas.

FDDI especifica el uso de anillos duales. El tráfico en esos anillos viaja en direcciones opuestas. Físicamente, los anillos consisten de dos o más conexiones punto a punto entre estaciones adyacentes. Uno de los anillos *FDDI* se denomina *anillo primario* y el otro *anillo secundario*. El *primario* se utiliza para la transmisión de datos y el *secundario*, por lo general, se emplea como respaldo.

Los componentes básicos de *FDDI* son concentradores, estaciones, fibra óptica y componentes ópticos. Existen dos tipos de estaciones: las estaciones clase *B* o *SAS* (estaciones de conexión sencilla) se conectan a un anillo y las estaciones clase *A* o *DAS* (estaciones de conexión dual) se conectan a ambos

anillos. Las *SAS* se conectan al anillo primario a través de un concentrador, el cual proporciona conexiones para varias *SAS*. Dicho concentrador asegura que una falla o la falta de corriente de cualquier *SAS* dada no interrumpa el anillo.

En la figura 28 se muestra una configuración típica que comprende ambos tipos de estaciones.

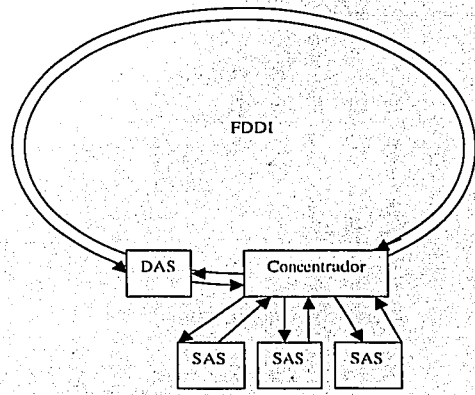

Figura 28. Nodos FDDI: DAS, SAS y concentrador.

Los formatos de la trama FDDI se muestran en la figura 29 y son similares a los de Token Ring.

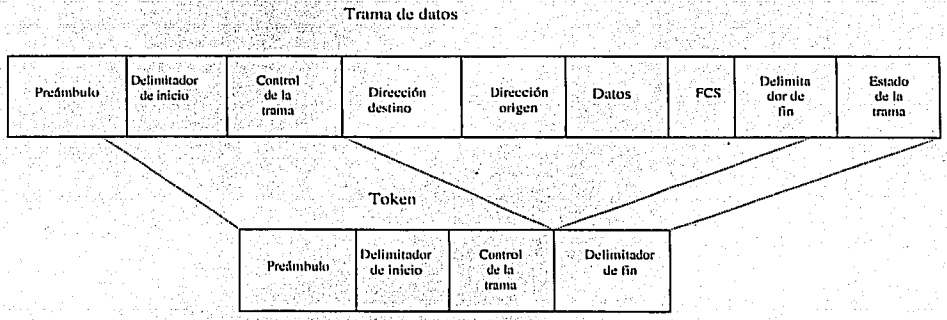

Figura 29. Formato de trama *FDDI*.

Los campos de una trama FDDI son los siguientes:

- Preámbulo: prepara cada estación para la trama futura
- Delimitador de inicio: indica el principio de la trama.
- Control de la trama: indica el tamaño de los campos de direcciones, si contiene datos síncronos o asíncronos y otra información de control
- Dirección destino: contiene una dirección de destino simple (unicast), de difusión restringida (multicast) o de difusión (broadcast) y son de 6 bytes
- Dirección origen: indica la estación individual que envío la trama y son de 6 bytes.
- Datos: contiene información destinada a un protocolo de la capa superior o información de control
- FCS: la estación origen lo llena con un calor calculado CRC que depende del contenido de la trama. La estación destina calcula de nuevo el valor para determinar si la trama se daño en el camino. Si se daño la descarta.
- Delimitador de fin: contiene símbolos que indican el final de la trama
- Estado de la trama: permite que la estación de origen determine si ocurrió un error y si la trama fue reconocida y copiada por una estación de destino.

b) Red de área metropolitana y red de área amplia (MAN / WAN)

La distinción entre una red *MAN* y una *WAN* básicamente radica en la distancia que entre una y otra puede existir. Si damos una definición de cada una de estas redes, podemos decir lo siguiente:

MAN: es la interconexión de redes locales ubicadas en diferentes lugares que abarcan una ciudad y/o su área metropolitana, esté tipo de red puede ser pública o privada, y utiliza enlaces de tipo serial como los DS0, E1, nx64 E1 fracción, etc.

WAN: cubre un área geográfica relativamente grande y frecuentemente usa enlaces de comunicación proporcionados por compañías telefónicas, las redes WAN se utilizan cuando no es factible por la distancia y el costo de la infraestructura invertir en la propiedad de estas redes.

Por las definiciones anteriores, podemos decir que, no hay una línea exacta que diferencie a una *MAN* de una *WAN*, depende en gran medida de la cobertura geográfica, pero sí podemos hablar de elementos comunes entre ellas, de los cuales mencionaremos algunos de los más importantes:

- Cobertura geográfica extensa
- Uso de enlaces de comunicaciones de tipo serial

- Los servicios están basados en diferentes tipos de conexiones como: permanentes o conmutadas.
- Usan diferentes tecnologías: conmutación de circuitos, conmutación de paquetes, conmutación de mensajes
- Usan circuitos virtuales: circuitos virtuales permanentes (PVC) y circuitos virtuales conmutados (SVC)
- Dispositivos como: servidores de acceso, modems, conmutadores, CSU/DSU (NTU), multiplexores, ruteadores, etc.
- Interconectan varias redes LAN y miles de equipos de computo.

Las principales redes *WAN* que explicaremos son las más representativas de la actualidad, de tal forma que daremos una breve explicación de X.25, Frame Relay, y ATM.

X.25

En los años setenta se requería un conjunto de protocolos para proporcionar a los usuarios conectividad mediante WAN (redes de área amplia), a través de PDNs (redes de datos públicos). Las PDSs habían alcanzado un gran éxito, pero se presentía que la estandarización de protocolos incrementaría las subscripciones a las PDNs al proporcionar una mejor compatibilidad entre equipos y un menor costo. El resultado de este esfuerzo fue un grupo de protocolos, y el más popular fue *X.25*.

X.25 fue desarrollado por los proveedores tradicionales de servicios de comunicaciones (básicamente las compañías telefónicas) en vez de una única empresa comercial. Por lo tanto, la especificación está diseñada para que funcione bien sin tomar en cuenta el tipo de sistema del usuario o fabricante. Los usuarios contratan con los proveedores de comunicaciones los servicios de PSN (red de conmutación de paquetes) y se les cobra en base en el uso de la PSN.

X. 25 define una red telefónica para la comunicación de datos. Para iniciar un intercambio, una computadora llama a otra para solicitar una sesión de comunicaciones. La computadora llamada puede aceptar o rechazar la conexión. Si se acepta la llamada los dos sistemas pueden comenzar una transferencia de información full-dúplex. Cualquier lado puede terminar la conexión en cualquier momento.

La especificación *X.25* define una interacción punto a punto entre el *DTE* (equipo terminal de datos) y el *DCE* (equipo de comunicación de datos). El *DTE* se conecta con el DCE y otros puertos en la PDN, que por lo general, se encuentran en las instalaciones del proveedor del servicio, el cual se conecta a su vez con *PSEs* (equipos de conmutación de paquetes o simplemente conmutadores) y otros *DCE* dentro de una PSN y, al final de la comunicación,

con otro *DTE* remoto. En la figura 30 se muestra la relación entre los elementos de una red X.25.

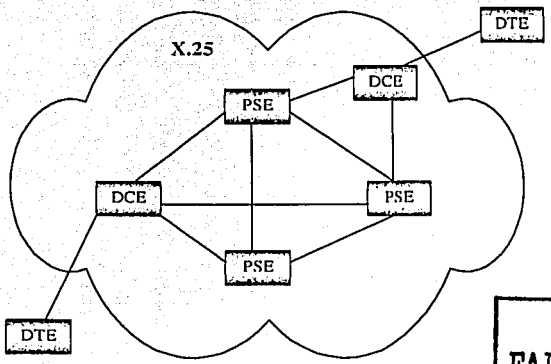

Figura 30. Red *X.25*.

La especificación *X.25* corresponde a las capas 1 a 3 del modelo de referencia OSI. La capa 3 describe los formatos de paquete y los procedimientos de intercambio de paquetes entre elementos iguales de la capa 3. El protocolo utilizado al nivel de red se conoce como PLP (Protocolo de Capa de Paquetes) que realiza las funciones de control de flujo, confirmación y direccionamiento. Las redes *X.25* usan para su direccionamiento la recomendación *X.121* que típicamente tienen entre 9 y 15 dígitos.

La capa 2 está implementada por el LAPB (Procedimiento de Acceso Balanceado al Enlace) que define el formato de trama de paquetes en el enlace *DTE/DCE* y permite que cada uno *DTE* o *DCE* inicie la comunicación con el otro, además de encargarse de revisar que las tramas lleguen al receptor en la secuencia correcta y libre de errores.

La capa 1 define los procedimientos eléctricos y mecánicos para la activación y desactivación del medio físico que está conectado al *DTE* y al *DCE*. En este nivel existen dos interfases la *X.21* cuando se usa señalización digital (poco usual) y la *X.21 bis* cuando es analógica y soporta conexiones punto a punto con velocidades de 19.2 Kbps.

La comunicación de extremo a extremo entre *DTEs* se logra por medio de una asociación bidireccional denominada *circuito virtual*. Los *circuitos virtuales* permiten la comunicación entre distintos elementos a través de cualquier cantidad de nodos intermedios sin la necesidad de dedicar partes del medio físico que caracteriza a los circuitos físicos. Los *circuitos virtuales* pueden

ser permanentes o conmutados (temporales). Por lo general, los *PVCs* (*Circuitos Virtuales Permanentes*) son usados para la transferencia frecuente de datos, mientras que los *SVCs* (*Circuitos Virtuales Conmutados*) se usan para transferencia esporádica de datos.

Una trama *X.25* está compuesta de una serie de campos, como se muestra en la figura 31. Los campos de la capa 3 conforman un paquete *X.25*, e incluye un encabezado y datos de usuario. Los campos de la capa 2 (LAPB) incluyen campos de control y direccionamiento a nivel trama a nivel trama, el paquete de capa 3 incrustado y un FCS (secuencia de verificación de trama).

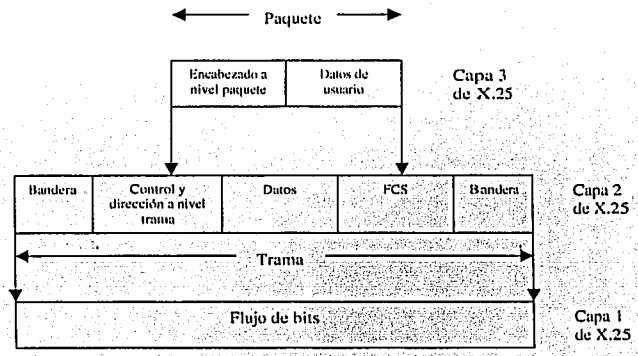

Figura 31. Una trama X.25.

Retransmisión de tramas (Frame Relay)

Frame relay, nació a partir de los trabajos de estandarización de *RDSI* (*Red Digital de Servicios Integrados*), como un intento de crear una versión de *X.25* mas rápida, que permitiera aprovechar las ventajas de poder definir *circuitos virtuales* pero sin la baja eficiencia que tenían los protocolos de *X.25*. Mientras que *X.25* la capa de enlace y la capa de red eran sumamente complejas en frame relay ambas se intentaron reducir a su mínima expresión, dejando en manos de los equipos finales toda la labor de acuse de recibo, retransmisión de tramas erróneas y control de flujo; de esta forma frame relay se convertiría en el complemento perfecto a otros protocolos, como TCP/IP.

El servicio que suministra *frame relay* consiste básicamente en identificar el principio y final de cada trama y detectar errores de transmisión. Si se recibe una trama errónea simplemente se descarta, confiando en que el protocolo de nivel superior de los equipos finales averigüe por sí mismo que se

ha perdido una trama y decida si quiere recuperarla. A diferencia de *X.25*, *Frame Relay* no tiene control de flujo ni genera acuse de recibo de los paquetes.

En la figura 32 se muestra la trama de *Frame Relay*, los campos de bandera delimitan el inicio y el final de la trama. A continuación del campo de bandera inicial se tienen dos bytes de información de dirección. Diez bits de esos dos bytes conforman el ID del circuito actual (llamado *DLCI* por identificador del circuito de enlace de datos).

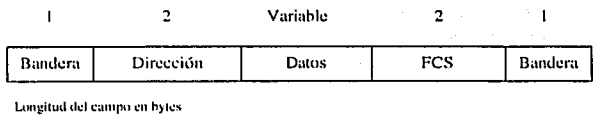

Figura 32. La trama de *Frame Relay*.

El valor *DLCI* de 10 bits es el corazón del encabezado de *Frame Relay*, identifica la conexión lógica que está multiplexada en el canal físico. Los *DLCIs* tiene significado local, esto es, los dispositivos finales de dos extremos diferentes de una conexión pueden usar un *DLCI* diferente para referirse a la misma conexión. La figura 33 proporciona un ejemplo del uso de los *DLCIs* en un direccionamiento de *Frame Relay*.

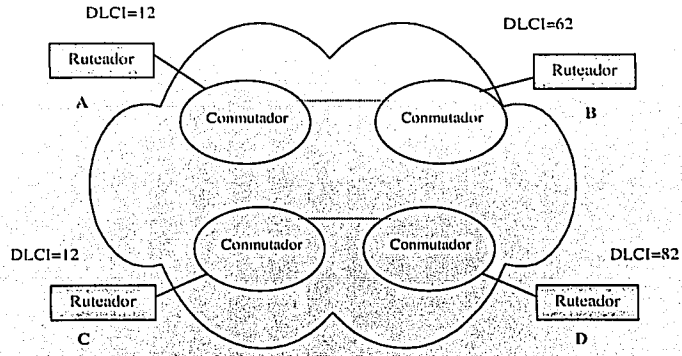

Figura 33. Direccionamiento *Frame Relay*.

En la figura 33 supongamos que hay dos *PVCs*, uno entre C y D, y otro entre A y B. C usa el *DLCI* 12 para referirse a su *PVC* con D, mientras que D se refiere al mismo *PVC* como *DLCI* 82. En forma similar, A usa el *DLCI* 12 para

referirse a su *PVC* con B. La red usa mecanismos internos propios para mantener localmente los dos identificadores *PVC* distintos.

Una novedad importante de *Frame Relay* es que define un ancho de banda asegurado para cada *circuito virtual* mediante un parámetro conocido como *CIR* (Commited Information Rate). Un segundo parámetro, conocido como *EIR* (Excess Information Rate) define el margen de tolerancia que se dará al usuario, es decir, cuanto se le va a dejar pasar del *CIR* contratado. Cuando un usuario hace uso del EIR, es decir, genera un tráfico superior al *CIR* contratado en un circuito virtual, el conmutador frame relay pone a 1 en las tramas excedentes un bit especial denominado *DE* (Discard Elegibility). Si se produce congestión en algún punto de la red el conmutador descartará en primera instancia las tramas con el bit *DE* marcado en 1, intentando resolver así el problema. Este mecanismo permite a un usuario aprovechar la capacidad sobrante de la red en horas sin tráfico excesivo.

Modo de Transferencia Asíncrono (ATM)

Las compañías telefónicas vienen trabajando desde hace bastante tiempo en el diseño de una red adecuada al tráfico multimedia que permita aprovechar las ventajas de la conmutación de paquetes, para así utilizar de forma más eficiente las infraestructuras y ofrecer servicios nuevos, tales como la video conferencia o el vídeo sobre demanda. La tecnología que permite todo esto se denomina *ATM* (*Modo de Transferencia Asincrona*) y sus orígenes se remontan a 1968 cuando los laboratorios Bell concibieron el primer sistema de transmisión de celdas. En cierto modo *ATM* puede verse como una evolución de *frame relay*. La principal diferencia es que los paquetes *ATM* tienen una longitud fija de 53 bytes (5 de cabecera y 48 de datos) frente al tamaño variable y mucho mayor de las tramas *frame relay*. Debido a su tamaño pequeño y constante los paquetes *ATM* se denominan celdas. Manejar celdas de un tamaño reducido tiene la ventaja de que permite responder con mucha mayor rapidez a tráfico de alta prioridad que puede llegar inesperadamente mientras se están transmitiendo otros menos urgente. El hecho de que todas las celdas sean del mismo tamaño simplifica el proceso en los nodos intermedios haciendo que dicho proceso sea lo más rápido posible. Por otro lado la eficiencia de una conexión ATM nunca puede superar el 90% (48/53) debido a la información de cabecera que viaja en cada celda.

ATM tiene su propio modelo de referencia, constituido por tres capas denominadas *capa física*, *capa ATM* y *capa de adaptación ATM*, o *capa AAL* (ATM Adaptation Layer).

La *capa física* está formada por dos subcapas: la *PMD* (Physical Media Dependent) y la *TC* (Transmission Convergence). La subcapa *PMD*, describe la interfaz física con el medio de transmisión, y equivale a la capa física del

modelo OSI. La subcapa *TC* se ocupa de deshacer las celdas en bits para pasarlos a la subcapa *PMD* en el envío, y de recibir los bits de la subcapa *PMD* para reconstruir las celdas en la recepción. Si consideramos la celda como equivalente a la trama en el modelo OSI esta subcapa haría la función de la capa de enlace.

La *capa ATM* trata de la estructura de las celdas y su transporte. También realiza las tareas de señalización, es decir, establece y termina los circuitos virtuales, y realiza el control de la congestión. Sus funciones son una mezcla de la capa de enlace y la capa de red en el modelo OSI.

La *capa de adaptación ATM (capa AAL)* se divide también en dos subcapas; la inferior se denomina subcapa *SAR* (Segmentation And Reassembly) se ocupa de fragmentar el paquete que recibe desde arriba (normalmente mayor de 48 bytes) en celdas para su envío, y de reemsamblarlo en la recepción cuando se lo pasa la capa *ATM*. La subcapa *CS* (Convergence Sublayer) se ocupa de suministrar distintos tipos de servicios adecuados al tipo de tráfico (audio, datos, vídeo, etc.). La capa *AAL* corresponde en sus funciones a la capa de transporte del modelo OSI.

Una celda *ATM* contiene dos tipos principales de información: la carga útil y el encabezado. La carga útil es la información que debe transferirse por medio de una red *ATM*. El encabezado es la información que se emplea para enrutar la celda a través de la red y para asegurarse de que se reenvíe a su destino.

En la figura 34 vemos una celda ATM que tiene 53 bytes de longitud.

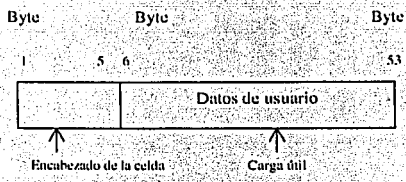

Figura 34. Una celda ATM

El encabezado de 5 bytes, se muestra en la figura 35, contiene varios campos. Los 48 bytes que están a continuación del encabezado (la carga útil) contienen datos del usuario. Describiremos brevemente cada unos de los campos del formato:

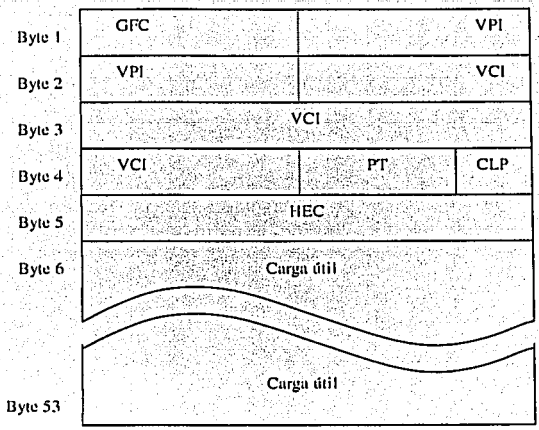

Figura 35. Formato del encabezado de la celda *ATM*.

- GFC(control de flujo genérico): controla el flujo de tráfico a través del interfaz de red del usuario y, por lo tanto, hacia la red ATM.

- VPI(identificador de ruta virtual): identifica un VPC particular. Un VPC es un grupo de conexiones virtuales llevadas a cabo entre dos puntos, y puede involucrar varios enlaces ATM. Los VPIs proporcionan una forma de agrupar tráfico que está dirigido hacia el mismo destino.

- VCI(identificador de canal virtual): identifica un VCC particular. Una VCC es una conexión entre dos entidades ATM activas que se comunican. El VCI consiste de una concatenación de varios enlaces ATM.

- PT(tipo de carga útil): indica el tipo de información que hay en el campo de carga útil. Las celdas ATM transportan diferentes tipos de información que pueden requerir un manejo diferente por parte de la red o el equipo terminal de datos.

- CLP(prioridad de pérdida de celda): indica la prioridad de pérdida de la celda establecida por el usuario. Si el bit está establecido a 1, la red puede descartar la celda cuando ocurre congestión.

- HEC(control de error del encabezado): contiene un código de corrección de errores calculado sobre los cuatro bytes anteriores del encabezado y puede emplearse para corregir errores de un solo bit.

Un *VCC* (conexión por canal virtual) es una serie de *VCLs* (enlaces de canal virtual) entre dos puntos *ATM*. Un *VCL* es un medio de transporte bidireccinal de celdas *ATM* entre el punto en donde se asigna un valor *VCI* (identificador de canal virtual) y el punto en donde es reasignado dicho valor o donde es terminado. El *VCI* identifica al *VCL* a quien pertenece la celda y determina hacia donde debe ir la celda. Como se muestra en la figura 36.

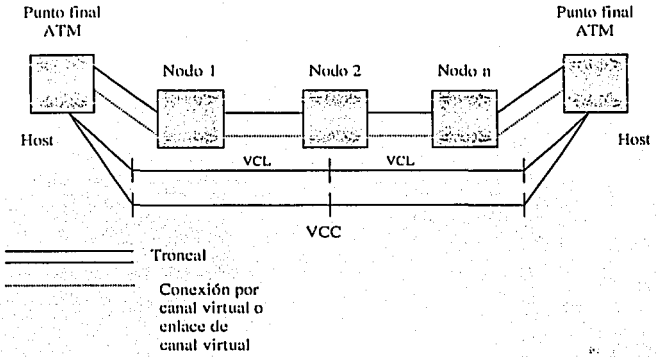

Figura 36. La relación entre *VCLs* y *VCCs* en una red *ATM*.

Los *VCCs* a veces son transportados dentro de *VPs* (rutas virtuales). Una *VP* está identificada por su *VPI* (identificador de ruta virtual). Las *VPs* proporcionan una manera conveniente para encapsular el tráfico que está dirigido hacia el mismo destino o el que requiere la misma *QoS* (calidad de servicio) en la red. Como se muestra en la figura 37.

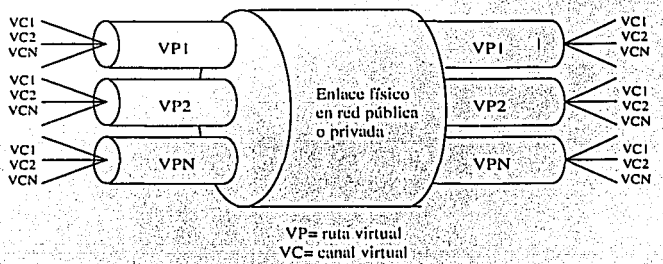

Figura 37. VCCs transportados dentro de VPs.

I.III.3 Topologías

La topología de una red define la distribución de cada estación en relación con la red y a las demás estaciones. Se trata de uno de los parámetros básicos que condicionan fuertemente los recursos de la red.

Dadas las características y funciones de una red, los criterios a considerar en la elección de su topología difieren en gran medida de la expansión de la red y su alcance. En este sentido, en las topologías de redes, son criterios determinantes:

- La complejidad de instalación y mantenimiento del cableado.
- La vulnerabilidad a fallas y averías.
- La gestión del medio y la facilidad de localización de fallas.
- La capacidad de expansión y reconfiguración
- El costo de la infraestructura de la red.

Existen cuatro topologías básicas: *bus, anillo, estrella y árbol.* Que se describen a continuación:

Topología de medio común o bus

En esta topología todas las estaciones se conectan a un único medio bidireccional lineal o *bus*, como se muestra en la figura 38. Cuando una estación transmite, su señal se propaga a ambos lados del emisor hacía todas las estaciones conectadas al *bus* hasta llegar a donde la señal es absorbida; de aquí también reciba el nombre de canal de difusión. En esta topología se permite la transmisión full-duplex y circula en todas direcciones a lo largo del *bus*, y cada estación recibe o transmite.

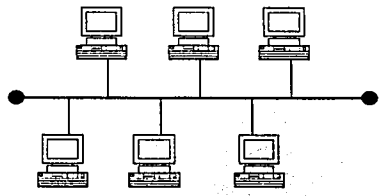

Figura 38. Topología bus.

Topología de anillo

El anillo consiste de una serie de repetidores *R's* conectados entre sí mediante un único enlace de transmisión unidireccional formando un camino

cerrado; véase figura 39. La información se transmite secuencialmente, bit a bit, de un repetidor al siguiente a lo largo del anillo. Cada repetidor regenera y retransmite cada bit. Cuando una estación recibe información destinada a ella, la incorpora a su memoria; en caso contrario se encarga de hacerla circular hasta la próxima estación.

La principal desventaja del anillo es que cada estación está involucrada en la transferencia de datos, por lo que la falla de un elemento inutiliza por completo la red. Por otra parte, la topología en anillo requiere mecanismos de control sofisticados para detectar y anular las informaciones defectuosas e impedir la circulación indefinida de una información por fallo de la estación responsable de su emisión. Algunas redes dedican una estación monitora a estas tareas de control, mientras que otras reparten esta responsabilidad entre todas las estaciones.

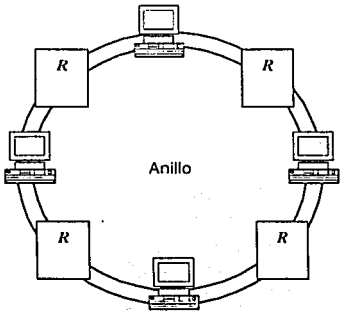

Figura 39. Topología anillo.

Al circular la información por todas las estaciones, se puede repartir equitativamente la capacidad de transmisión entre los usuarios y es posible identificar que estación o enlace ha producido una falla, pues la señal se detiene en una estación determinada y no llega a la siguiente.

Topología de estrella

En la topología en estrella todas las estaciones están conectadas mediante enlaces bidireccionales a un nodo central, que asume las funciones de gestión y control de las comunicaciones proporcionando un camino entre dos estaciones que deseen comunicarse; como se muestra en la figura 40.

La principal ventaja de la topología en estrella es el acceso a la red, es decir, la decisión de cuando una estación puede o no transmitir. Además, la flexibilidad en cuanto a configuración y localización de fallas es aceptable al

estar toda la funcionalidad localizada en un nodo central. La desventaja es que el nodo central es una fuente potencial de falla.

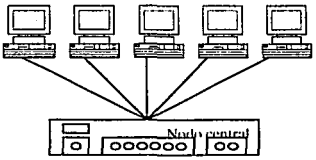

Figura 40. Topología estrella.

Un ejemplo de esta topología son las centrales telefónicas.

Topología de árbol

La topología en árbol es una generalización de la topología en bus en la que el cable se desdobla en varios ramales mediante el empleo de dispositivos de derivación; véase figura 41. Al igual que la topología en bus, las transmisiones se propagan por cada ramal de la red y llegan a todas las estaciones.

Esta topología es especialmente interesante para las redes de banda ancha. Se puede utilizar, por ejemplo, para conectar estaciones de un edificio de varios pisos, de la misma forma que se distribuye la señal en una instalación de antena colectiva.

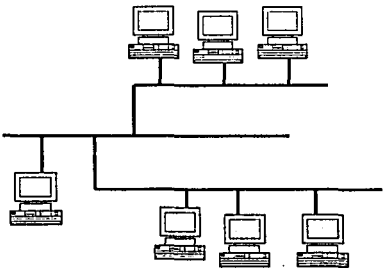

Figura 41. Topología *árbol.*

I.III.4 Sistemas operativos de redes.

El sistema operativo de la red se engloba en dos componentes básicos. El sistema operativo de red del servidor mismo y el sistema de la estación de trabajo. El sistema operativo del servidor del servidor de red se ejecuta dentro de la máquina del servidor y procesa todos los servicios. Los componentes de la estación de trabajo se ejecutan en ésta, y establecen la conexión con la red y el servidor, y controlan el flujo de las comunicaciones.

El sistema operativo del servidor de red se puede dividir en cinco subsistemas: el núcleo de control (control kernel), la interfaz de red, los sistemas de archivo, las extensiones del sistema y los servicios del sistema.

El control kernel o el núcleo de control es el corazón del sistema operativo, el cual coordina los diferentes procesos de los otros subsistemas. De una manera central, en el diseño del kernel están los procesos que optimizan el acceso a los servicios para la actividad del usuario. El kernel puede distribuir la actividad del usuario tan uniformemente como sea posible a través de los servicios de disco y de cualquier dispositivo de entrada/salida, de tal manera que no se favorece a un usuario o grupo de usuarios obteniendo un mejor funcionamiento, con esto, el rendimiento percibido en general es consistente.

La interfaz de red apoya la tecnología que es la implantación real del medio de la red. Los componentes de la interface de red también manejan los protocolos de bajo nivel de la red y proporcionan el traslado básico entre estos protocolos cuando se requieren servicios de puenteo.

Los sistemas de archivo son los mecanismos mediante los cuales, se organizan, almacenan y recuperan los datos, a partir de los subsistemas de almacenamiento disponibles para el Sistema Operativo de Red.

Las extensiones del sistema operativo de red definen lo abierto del sistema. Las extensiones que comúnmente se ofrecen en los sistemas operativos de red, por lo general son controladores de productos de alto nivel que efectúan operaciones, tales como el traslado entre protocolos de acceso de archivos que requieren los diferentes sistemas operativos de usuarios o estaciones.

Las características de seguridad y confiabilidad con frecuencia se implantan en los servicios del sistema de red para asegurar que proporcionan un nivel de sistema verdadero. Por consiguiente, las condiciones de error y las violaciones de acceso, pueden ubicarse antes de que puedan comprometer la integridad del subsistema.

En la estación de trabajo, los servicios de sistema operativo de red atrapan o capturan las llamadas desde la estación de trabajo y luego las

dirigen hacia un recurso de la red. Estas llamadas pueden ser dirigidas por el sistema operativo sí en el sistema están dados de alta los servicios de archivos remotos.

El servidor de archivos es el punto de desarrollo para los protocolos de cliente-servidor. En esencia, estos protocolos llevan un nivel de información más alto, y muchas operaciones de nivel bajo pueden iniciarse por una solicitud para efectuar una operación de nivel alto. Los asuntos tales como acceso y resolución de conflictos, en muchos casos ya no representan un problema, debido a que la solicitud de alto nivel es con frecuencia una transacción por su propio derecho. Las aplicaciones pueden solicitar una acción con poco o ningún conocimiento del estado del resto de la red, y todavía llevar a cabo las operaciones requeridas por una confiabilidad total.

Un *NOS* (Network Operation System) es un programa que trabaja en ambientes cliente-servidor, donde el cliente solicita servicios o recursos al servidor el cual deberá responder a la petición con la información solicitada.

El *NOS* se encarga de administrar los recursos que se van a compartir en la red. Los sistemas operativos de red se clasifican de acuerdo con la forma en que operan, existen dos tipos de *NOS*:

- Sistemas Operativos basados en servidor. Netware y LAN Manager.
- Sistemas Operativos para redes punto a punto. Personal Netware, UNIX, Windows NT.

De tal forma que se explicaran solamente *Novell Netware* y *Windows NT* por ser los más representativos del mercado de *NOS*:

a) Novell Netware

Introducido al mercado a principios de los ochentas. En ese entonces las redes eran pequeñas y predominantemente homogéneas, la comunicación entre grupos de trabajo LAN era nueva y la idea de la PC estaba comenzando a ser popular. Gran parte de la tecnología de conectividad de *Netware* se derivó de XNS (Sistema de Red Xerox), el cual fue creado por la corporación Xerox a finales de los setentas.

A principios de los noventas la participación en el mercado del *NOS* de *Netware* se elevó entre el 50 y 75 por ciento. Con más de 500,000 redes *Netware* instaladas a nivel mundial y un movimiento acelerado para conectar redes a otras redes, *Netware* y sus protocolos de soporte coexisten frecuentemente en el mismo canal físico con otros protocolos populares como *TCP/IP*.

Netware especifica las cinco capas superiores del modelo de referencia OSI. Proporciona mecanismos para compartir archivos e impresoras, soporte para diversas aplicaciones como la transferencia de correo electrónico, acceso a bases de datos y otros servicios. *Netware* esta basado en una arquitectura cliente/servidor. En tal arquitectura, los clientes solicitan determinados servicios a los servidores, como el acceso a archivos e impresoras.

Una característica primordial de un sistema cliente/servidor es que el acceso remoto es transparente para el usuario. Esto se logra por medio de llamadas a procedimientos remotos, un proceso mediante el cual un programa cliente que se ejecuta en una computadora local hace una llamada a un procedimiento en un servidor remoto. El servidor ejecuta la llamada al procedimiento remoto y envía la información solicitada al cliente en la computadora local.

La figura 42 muestra una vista simplificada de los protocolos más conocidos de *Netware* y sus relaciones con el modelo de referencia *OSI*. Con controladores adecuados, *Netware* puede ejecutarse sobre cualquier otro protocolo de acceso al medio.

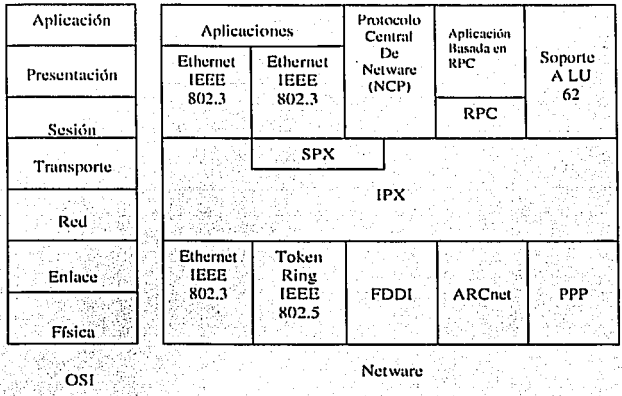

Figura 42. *Netware* y el modelo de referencia *OSI*.

Netware se ejecuta sobre Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, Interfaz de Datos Distribuidos por Fibra (FDDI), y ARCnet. *Netware* funciona también a través de enlaces WAN síncronos usando el Protocolo Punto a Punto (PPP). La capa de red donde trabaja *IPX* (Intercambio de Paquetes de Interred) funciona de tal forma que cuando un dispositivo con el que se va a comunicar se encuentra en una red diferente, *IPX* enruta la información hacia el destino a

través de cualquier red intermedia. La figura 43 muestra el formato de los paquetes *IPX*.

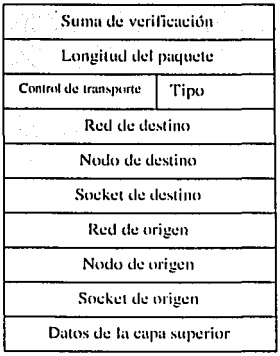

Figura 43. Formato de los paquetes IPX.

Los campos de los paquetes IPX son los siguientes:

- Suma de verificación: es un campo de 16 bits con valor de 1's lógico.
- Longitud del paquete: es un campo de 16 bits que especifica la longitud en bytes del datagrama IPX completo. Los paquetes IPX pueden ser de cualquier longitud hasta el limite del tamaño MTU (unidad máxima de transmisión) del medio. No hay fragmentación de paquetes.
- Control de transporte: es un campo de 8 bits que indica la cantidad de ruteadores por los que ha pasado el paquete. Cuando el valor de este campo llega a 00001111 (15) se descarte el paquete, bajo el supuesto que pudiese haber ocurrido un ciclo en el ruteador.
- Tipo de paquete: es un campo de 8 bits que especifica el protocolo de capa superior que va a recibir la información del paquete.
- Red de destino, nodo de destino y socket de destino: especifican la información del destino
- Red de origen, nodo de origen y socket de origen: especifican la información del origen
- Datos de la capa superior: contiene información para los procesos de capas superiores.

b) Windows NT

El sistema operativo *NT* fue desarrollado por *Microsoft* para superar los obstáculos impuestos por la vieja arquitectura de sus sistemas operativos como

MS-DOS. Como se muestra en la figura 44, *Microsoft* diseño *Windows NT* para que fuera modular y portátil. Está compuesto por un kernel o núcleo, así como diferentes subsistemas. El kernel es el responsable de las operaciones básicas de *NT*. Un I/O Manager (administrador de entrada y salida) maneja las solicitudes de salida y entrada independientes del dispositivo. La capa de abstracción de hardware (HAL) es especifica del sistema y traduce los comandos de *NT* a una forma que pueda ser entendida por el hardware que se encuentra en la plataforma física en la que se ejecuta *NT*.

Windows NT emplea el sistema de archivos *NT* (NTFS). Este sistema de archivos soporta nombres de hasta 256 caracteres. Los vínculos de datos de *Windows NT* incluyen soporte para las especificaciones IEEE 802.2 (Token Ring y Ethernet), el protocolo de Control síncrono de vínculo de datos (SDLC), los protocolos X.25 y la especificación de terminal de función distribuida (DFT).

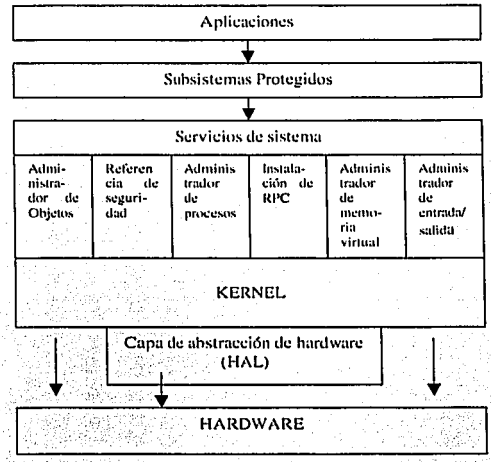

Figura 44. Arquitectura de *Windows NT*.

Windows NT ofrece compartir archivos de forma integrada, capacidad de compartir impresoras para grupos de trabajo y una interfaz de red abierta que incluye soporte para la mayoría de los protocolos como TCP/IP, IPX/SPX, NetBEUI y otros. También es compatible con redes existentes como UNIX, Novell Netware y Windows para Trabajo en Grupo.

Windows NT incluye interfaz de programación de aplicación (API) que permite que los fabricantes de sistemas operativos de red (*NOS*) escriban

software de cliente para que sus productos puedan ejecutarse en *NT*. También da soporte al protocolo de administración de red simple (SNMP) de manera que las actividades del servidor pueden ser manejadas por cualquier programa de administración de red que cumpla con SNMP.

Para ver el funcionamiento hay que distinguir dos partes:

- La parte física de la red. El funcionamiento básico de la red, basado en el protocolo Netbeui, supone que todos los miembros de la red están interconectados entre sí. Esto implica que no hay barreras del tipo conmutador (switch) o encaminadores (gateway) de red entre las diversas partes de la red. Cuando aparece este tipo de elementos se utilizan otros protocolos, como el *TCP/IP* o el *IPX*, que encapsulan al protocolo Netbeui, permitiendo la integración de la red local dentro de una red más compleja.

- Para la parte lógica de la red, el esquema de red permite trabajar de dos modos diferentes: como *grupos de trabajo* y como *dominios*.

I.III.5 Modelo OSI (Open System Interconnect)

Este modelo, conocido por las siglas *OSI*, y cuya actividad fue a principios de 1977, obtuvo el grado definitivo de estándar internacional en 1983; trata de establecer las bases para la definición de protocolos de comunicación entre sistemas informáticos. Su principal objetivo es la interconexión de sistemas de diferentes fabricantes, es decir, de sistemas abiertos. Por ello *OSI* constituye un marco para la coordinación de las actividades de normalización en los sistemas de telecomunicaciones e información.

Diagrama a bloques

La base de la normalización es el Modelo de Referencia. Cada sistema abierto está lógicamente formado por un conjunto ordenado de subsistemas que junto con el medio físico proporcionan un conjunto completo de servicios de comunicación. La funcionalidad de cada nivel viene definida por los servicios OSI. La comunicación entre niveles de distintos sistemas se realiza mediante la definición de un protocolo, siendo éste independiente de los protocolos de los demás niveles. En la figura 45 se muestran los siete niveles del modelo de capas OSI.

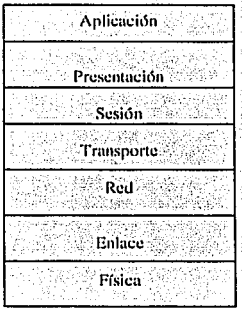

Figura 45. Niveles *OSI*.

El modelo de referencia OSI es el modelo que se ha estructurado más recientemente, por lo que, a pesar de no existir muchas implementaciones OSI, sí puede afirmarse que se trata del modelo que proporciona un nivel de formalización más abstracto. Por este motivo es el que se emplea habitualmente en la literatura y en el mundo académico como marco e hilo conductor para desarrollar los conceptos de redes y sistemas.

Está compuesto por los siguientes niveles de abstracción:

- La *arquitectura OSI*. Define los elementos básicos de los sistemas abiertos abstractos, es decir, de qué manera debe verse un sistema desde el exterior.
- Las *especificaciones* de *servicio OSI*. Definen los servicios proporcionados a los usuarios en cada nivel, es decir, los servicios proporcionados por un nivel al nivel superior.
- Las *especificaciones* de *protocolos OSI*. Definen la información de control transmitida entre los distintos sistemas, así como los procedimientos para la interpretación de dicha información de control.

El modelo de referencia OSI es un modelo de redes estructuradas en capas o niveles. El objetivo es tratar de manera estructurada la totalidad de un sistema. El conjunto de funciones del sistema se divide en niveles, facilitando su estudio y desarrollo, que sean fácilmente controlables de forma individual y que en conjunto resuelvan satisfactoriamente las necesidades de comunicación.

Cada nivel se desarrollo sobre el anterior, de tal forma que recibe una serie de servicios sin conocer los detalles de cómo se realizan dichos servicios. Las diferentes funciones de la arquitectura OSI han sido estructuradas en siete niveles, siendo las funciones asignadas a cada uno de ellos

complementarias. La figura 46 muestra la arquitectura de una red que utiliza el modelo OSI.

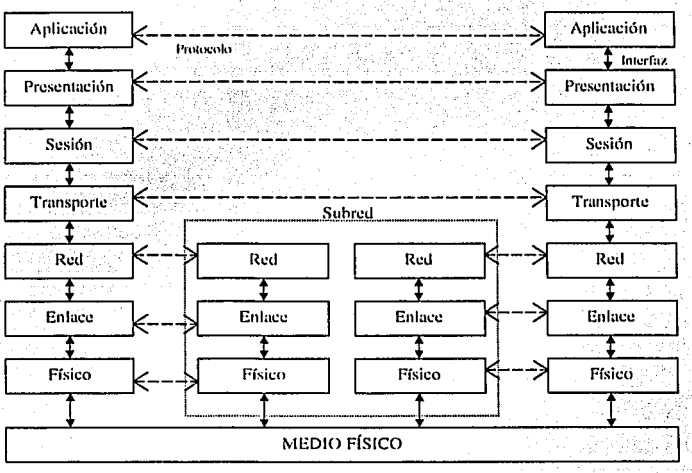

Figura 46. Arquitectura de una red basada en el modelo *OSI*.

La estructura de una red de comunicaciones se compone de una serie de nodos que pueden estar formados por el sistema central, una unidad de control de comunicaciones o una terminal.

En ella se define el término usuario final como el elemento que da origen o es receptor de la información. Este usuario puede ser tanto una aplicación como un dispositivo de entrada/salida.

Cada nivel se relaciona con el nivel inmediatamente superior e inferior a través del concepto interfaz, que representa el conjunto de elementos lógicos y físicos existentes entre dos niveles adyacentes.

Los procesos que una unidad funcional realiza y cuyos resultados son ofrecidos o empleados por el nivel superior se denominan servicios de nivel. Estos servicios se proporcionan a través de los puntos de acceso al servicio (SAP, *Service Acces Points*) de la interfaz.

Por otra parte, se define *protocolo* como el conjunto de reglas o convenciones que controlan el intercambio de información entre unidades funcionales del mismo nivel, tanto en la transmisión como en el control y recuperación de errores. Los *protocolos* de niveles diferentes son

independientes, es decir, sólo tienen que conocer la definición de servicios de su interfaz, y no tienen nada que ver con los protocolos de los restantes niveles ni con los servicios de sus interfaces. La figura 47 muestra la estructura interna de un nivel y su relación con los niveles adyacentes.

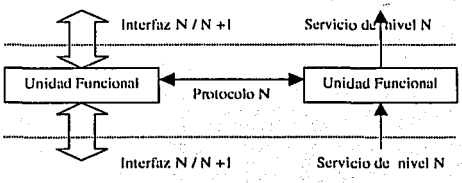

Figura 47. Estructura interna de un nivel.

Transmisión de datos en OSI.

La transmisión de datos a través de una red que sigue el Modelo de Referencia OSI, la vamos a suponer entre dos nodos, uno emisor y otro receptor. El nodo emisor pone a disposición de su nivel de aplicación los datos que desea transmitir. El nivel de aplicación incorpora a los datos pasados por el nodo información propia del nivel mediante datos de cabecera y cola (datos situados al principio y al final del mensaje respectivamente); la totalidad de la información, la cabecera mas datos de cola es entregados al nivel de presentación, quien a su vez, añade una nueva cabecera y colas propias del nivel, transfiriendo el resultado al nivel de sesión. Este proceso se repite en el resto de los niveles por los cuales va pasando el mensaje hasta llegar al nivel físico. En el nivel físico es en donde se realiza realmente la transmisión de la información. En el nodo receptor el mensaje recibido sufre el proceso inverso al que se vio sometido en el emisor. A medida que el mensaje asciende por los niveles de la torre OSI del nodo receptor, se le quita la información de cabecera y cola correspondiente a cada nivel. De esta forma, finalmente, los datos llegan al nodo receptor idénticos a como fueron enviados por el nodo emisor.

La figura 48 ilustra la transmisión de datos en una red con arquitectura OSI. Además se ilustra la clasificación de los niveles en dos grupos. Los niveles de control son los relacionados con las necesidades de comunicación entre los usuarios finales, es decir, si dos usuarios no tuviesen necesidad de utilizar una red de comunicación para comunicarse, sólo utilizarían estos niveles. Los niveles de transporte son los encargados de transferir los mensajes a través de la red.

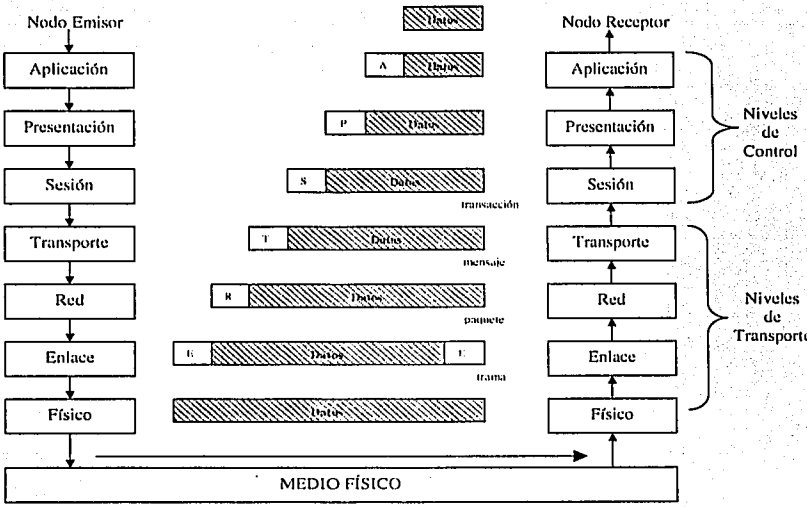

Figura 48. Transmisión de datos en el Modelo OSI.

Nivel físico

El nivel físico es el responsable de la definición de las características mecánicas, eléctricas y funcionales de la transmisión y recepción de la información utilizando un medio de comunicación específico. Entre sus funciones básicas se encuentran la identificación de los circuitos de datos, el secuenciamiento de los mismos y la administración del nivel, también podemos resumir en la siguiente forma sus funciones:

- Se ocupa de la transmisión de los bits sin estructura sobre el medio físico.
- Describe la interfaz en el ámbito eléctrico, electromagnético o luminoso, tanto en lo mecánico como en lo funcional. Por ejemplo: EIA RS-232-C, EIA RS-449, CCITT X.21/X.21bis y CCITT V.35
- Equipo terminal: adaptador o tarjeta y puerto.
- Equipo intermedio: repetidor, amplificador, estrella pasiva, multiplexor, concentrador de terminales, modem, codec, CSU, DSU, transceiver, transductor, balún, filtro.

Nivel enlace

Es el nivel responsable de mantener la integridad de los datos de una transmisión sobre un canal de comunicaciones. Es decir, proporcionar un canal fiable para la transmisión y recepción de la información utilizando un medio de comunicación específico. Entre sus funciones básicas se encuentran las de detección y corrección de errores de transmisión que pudieran ocurrir en el nivel físico. También podemos resumir en la siguiente forma sus funciones:

- Proporciona transmisión confiable entre dos puntos adyacentes de la red.
- Forma las tramas (PDU de la capa 2) basándose en los paquetes (PDU de la capa 3), añadiéndole direcciones físicas, chequeo de integridad, inserción de información de control, banderas de sincronía y delimitadores.
- Equipo terminal: adaptador o tarjeta y protocolo.
- Equipo intermedio: puente o switch.
- Protocolos de nivel de enlace: HDLC, LAP-B, X.25 nivel 2 y LLC (Logical Link Control).
- Para redes WAN es una capa monolítica, para redes LAN y MAN está formada por dos subcapas:
  - LLC (Logical Link Control): subcapa homogeneizadora para permitir la interconectividad entre diferentes tipos de redes.
  - MAC (Media Acces Control): subcapa más relacionada con el medio físico y que maneja el método de acceso para la transmisión confiable y que realiza la microfragmentación.

Nivel red

Este nivel es el responsable de asegurar que la información se transmite correctamente a través de la red. Esta es la capa que tiene conciencia de la topología de la red y se ocupa de decidir por que ruta va a ser enviada la información; la decisión de la ruta a seguir puede hacerse de forma estática, o de forma dinámica en base a información obtenida de otros nodos sobre el estado de la red. Maneja los bits en grupos discretos que aquí reciben el nombre de paquetes. Los paquetes tienen tamaños variables, desde 64 KBytes hasta 4 GBytes dependiendo el estándar que se ocupe. También podemos resumir sus funciones:

- Selecciona la ruta que deben tomar los paquetes (PDU de la capa 3) dentro de las redes.
- Forma los paquetes basándose en los mensajes (PDU de las capas superiores añadiéndole direcciones lógicas, realizando la macrofragmentación.
- Equipo terminal: protocolo ruteado.
- Equipo intermedio: ruteador y protocolos.

- Protocolos utilizados: CCITT X.25 y X.75, IP, CCITT/ITU-T Q.931, Q.933, Q.2931.

Nivel transporte

La principal función de la capa de transporte es fragmentar de forma adecuada los datos recibidos de la capa superior (sesión) para transferirlos a la capa de red, y asegurar que los fragmentos llegan y son recompuestos correctamente en su destino. Establece el tipo de servicio que recibe la capa de sesión y en último extremo los usuarios. El nivel de transporte puede, además, ofrecer servicios de detección y corrección ofrecido para asegurar la integridad de los datos, así como niveles de calidad de servicio. En resumen podemos decir también del nivel de transporte:

- Primer capa que solo reside en los equipos finales (emisor y receptor).
- Garantiza que el conjunto de paquetes que conforma el mensaje (PDU de esta capa) estén formados en secuencia, sin omisiones o duplicaciones.
- Equipo terminal: protocolo de transporte.
- Equipo intermedio: ninguno o gateway (pasarela).
- Protocolos de transporte: CCITT X.224, TCP (Protocolo de Control de Transmisión), UDP (Protocolo de Datagrama de Usuario).

Nivel sesión

El propósito de este nivel es proporcionar los medios necesarios para controlar el diálogo entre entidades de presentación. Este diálogo se realiza a través del establecimiento y uso de una conexión, denominada sesión. Este nivel es el primero que es accesible al usuario y es su interfaz más básica con la red. En resumen podemos decir del nivel de sesión que:

- Permite establecer sesiones entre emisor y receptor
- Establece el dialogo entre programas de los equipos terminales
- Sincroniza la operación entre las tareas de dichos programas.
- Libera la conexión de sesión. Una vez finalizado el intercambio de datos se procede a la desconexión
- Equipo terminal: protocolo de sesión.
- Equipo intermedio: ninguno o gateway (pasarela).

Nivel presentación

Es el nivel encargado de la transferencia de los datos contenidos en los protocolos de aplicación. Se ocupa de realizar las conversiones necesarias para asegurar que los bits se presenten al usuario de la forma esperada, por ejemplo, sí se envía la información alfanumérica de un formato *ASCII* a otro *EBCDIC* será necesario efectuar una conversión, o de lo contrario los datos no serán interpretados correctamente. Otras funciones de este nivel son:

- Formatea los datos para la capa de aplicación
- Traduce los códigos y funciones de diferentes equipos finales para brindar funcionalidad y presentación similares.
- Encripta y desencripta la información que se transmite para evitar que sea utilizada por usuarios no autorizados.
- Equipo terminal: protocolo de presentación.
- Equipo intermedio: ninguno o gateway (pasarela).

Nivel aplicación

Tiene como función controlar y coordinar las funciones a realizar por los programas de usuarios de manera que les permita el acceso al entorno OSI. Comprende los servicios que el usuario final está acostumbrado a utilizar en una red, por lo que a menudo los protocolos de la capa de aplicación se denominan servicios. Dado que se crean continuamente nuevos servicios, existen muchos protocolos para la capa de aplicación, uno o más por cada tipo de servicio. En resumen podemos decir que:

- Interfaz con el usuario final (persona o programa), ofreciendo los servicios de la red:
  - Emulación de terminal
  - Transferencia de archivos
  - Correo electrónico
  - Directorio de usuarios
  - Administración de la red
- Equipo terminal: protocolo de aplicación.
- Equipo intermedio: ninguno o gateway (pasarela).
- Protocolos: CCITT X.400, X.420, X.500, SMTP, FTP, Telnet, HTTP, etc.

A continuación se hace un breve resumen de las características del modelo de referencia OSI:

Capas de comunicaciones:

- Capa 3 (red)
- Capa 2 (enlace)
- Capa 1 (física)

Protocolos de bajo y alto nivel:

- Se les llama protocolos de bajo nivel a los correspondientes de la capa 2 (enlace)
- Se les conoce como protocolos de alto nivel a los protocolos de ruteo (capa 3 -red)

Capas de servicios:

- Capa 7 (aplicación)
- Capa 6 (presentación)
- Capa 5 (sesión)
- Capa 4 (transporte).

Equipos intermedios:

- Capa 1:
  - *Repetidores* (repeaters): trabaja en el nivel físico y puede conectar dos o más segmentos LAN, su función básica es retransmitir cada bit de una trama a otro segmento de red.
- Capa 2:
  - *Puentes* (brigdes): direcciona tramas basadas en la dirección física destino y origen, aprenden las direcciones de la red y las almacenan en una tabla, usa esta de referencia para decidir hacia donde la trama es dirigida. Los puentes son independientes del protocolo.
  - *Conmutadores* (switches): su función es aprender la posición de los nodos en la red para dirigir o filtrar los paquetes dependiendo de la dirección destino, proporcionando ancho de banda dedicado a cada nodo de la red, reduciendo la congestión y colisiones de la red.
- Capa 3: *ruteadores*: un dispositivo que dirige paquetes entre redes basado en la dirección de red localizada en la cabecera del paquete, ya sea *IP*, *IPX*, etc., utiliza tablas de ruteo que pueden ser configuradas, Muchos ruteadores tienen la habilidad de ajustar sus tablas de ruteo. Los ruteadores son dependientes del protocolo.
- Capa 4-7: *pasarela* (gateway): pueden operar hasta el nivel de aplicación y convertir de un protocolo a otro protocolo cuando dos aplicaciones necesitan comunicarse y usar diferentes protocolos.

Capitulo II

La red de datos TCP/IP

II.I Modelo general

A finales de los años sesenta, el Departamento de Defensa de los Estados Unidos creó la red ***ARPANET*** para poder investigar la comunicación de paquetes, esta red llegó a interconectar, en 1972, bases militares, centros de investigación, universidades y laboratorios gubernamentales. A mediados de los años setenta, la ***DARPA*** (Agencia de proyectos de Investigación Avanzada para la Defensa) y otras organizaciones del gobierno comprendieron el potencial de la tecnología de redes y financiaron una investigación hecha por la Universidad de Stanford, para crear una serie de protocolos de comunicaciones. El resultado de este esfuerzo de desarrollo, fue el conjunto de Protocolos de Internet, del cual los dos protocolos más conocidos son ***TCP*** *(Protocolo de Control de Transmisión)* e **IP** *(Protocolo Internet)*. Estos protocolos pueden usarse para establecer una comunicación a través de cualquier conjunto de interredes. También están bien adaptados para las comunicaciones en LANs y en WANs. El conjunto de Protocolos de Internet incluye no solo especificaciones de las capas más bajas (como TCP e IP), sino también especificaciones para aplicaciones tan comunes como el correo electrónico, emulación de terminales y la transferencia de archivos.

Actualmente **TCP/IP** se considera como el conjunto de protocolos abiertos, no específicos de un fabricante determinado, más extendido, con lo que se ha convertido en un estándar de facto, soportado por la mayoría de los fabricantes en los sistemas operativos más extendidos.

La creación y documentación del conjunto de Protocolos de Internet se asemeja mucho a un proyecto de investigación académica. Los protocolos se especifican en documentos denominados Solicitudes de Comentarios (RFC – Request For Comments). Estos documentos se publican y luego son revisados y analizados por la comunidad. Las mejoras a los protocolos se publican en nuevos RFC´s.

Así como el modelo de referencia OSI posee siete niveles, la arquitectura TCP/IP esta definida por 4 niveles: *Aplicación, Transporte, Internet e Interfaz de Red.* Cada nivel corresponde a uno o más niveles del modelo OSI.

En la figura 49 vemos el modelo general de los niveles de TCP/IP.

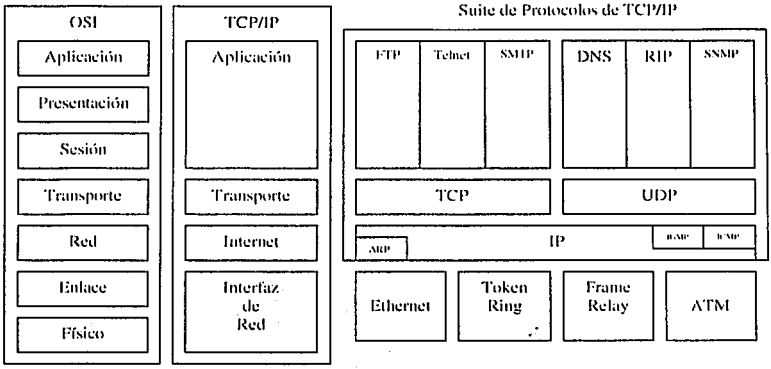

Figura 49. Modelo *TCP/IP*.

TCP/IP es una familia de protocolos desarrollados para la comunicación entre cualquier par de computadoras de cualquier red o fabricante, respetando los protocolos de cada red individual. Los protocolos TCP/IP proporcionan a los usuarios servicios de comunicación universales tales como:

- Transferencia de archivos
- Login remoto o Terminal virtual
- Correo electrónico, etc.

La figura 50 muestra los protocolos de cada nivel indicando los datos manejados por cada uno de ellos.

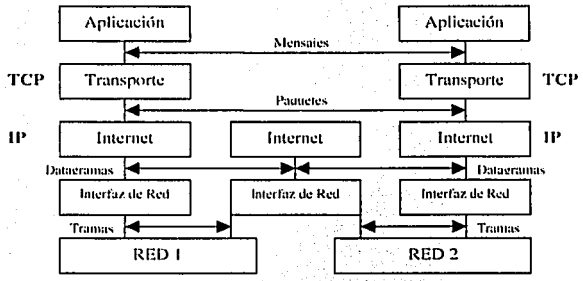

Figura 50. Protocolos de TCP/IP con sus mensajes.

TCP/IP tenía que contemplar realidades operativas de sistemas de producción, como la seguridad, la interoperación de redes, la fiabilidad y la administración de red. Conceptualmente existen diferencias notables entre *OSI* y *TCP/IP*, como son:

- El concepto de jerarquía en relación con el de niveles o capas.
- La interoperación de redes
- La fiabilidad extremo a extremo
- Los servicios no orientados a conexión
- La administración de red

II.II Nivel Internet

El protocolo *IP* es el principal del modelo *TCP/IP*. Las tareas principales de *IP* son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas. El datagrama es la unidad de transferencia que *IP* utiliza, algunas veces identificada en forma más especifica como datagrama Internet o datagrama *IP*. Las características de este protocolo son:

- No orientado a conexión.
- Transmisión en unidades denominadas datagramas.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

En la figura 51 se muestra el formato del paquete IP:

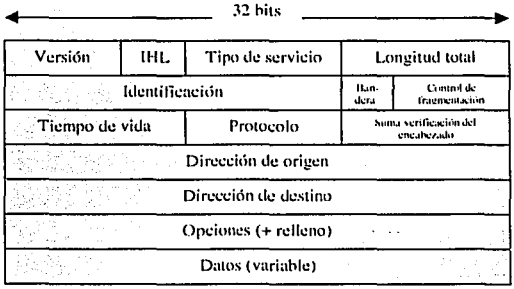

Figura 51. El formato del paquete IP.

Los campos del paquete IP se describen a continuación:

- Versión: indica la versión de IP usada actualmente.
- Longitud del encabezado IP (IHL): indica la longitud del encabezado del datagrama en palabras de 32 bits.
- Tipo de servicio: especifica la manera en que un protocolo de capa superior determinado requeriría que se manejara el datagrama actual. A través de este campo se pueden asignar varios niveles de importancia a los datagramas.
- Longitud total: especifica, en bytes, la longitud de todo el paquete IP, incluyendo datos y encabezado.
- Identificación: contiene un entro que identifica al datagrama actual. Este campo se usa para ayudar a unir los fragmentos de datagramas.
- Banderas: un campo de 3 bits, de los cuales, los dos bits menos significativos controlan la fragmentación. El primer bit especifica sí puede fragmentarse el paquete y el segundo indica si el paquete es el último de una serie de paquetes fragmentados.
- Tiempo de vida: lleva un contador que se disminuye en forma gradual hasta cero, punto en el cual el datagrama se descarta. Esto evita que los paquetes se queden indefinidamente en un ciclo.
- Protocolo: indica cuál de los protocolos de capa superior recibe los paquetes entrantes después de que termina el procesamiento de IP:
- Suma de verificación del encabezado: ayuda a asegurar la integridad del encabezado IP.
- Dirección de origen: especifica el nodo que envía.
- Dirección de destino: especifica el nodo que recibe.
- Opciones: permite que el IP soporte varias opciones, como la seguridad.
- Datos: contiene información de las capas superiores.

Direccionamiento

Al igual que con todos los protocolos de la capa de red, el proceso de enrutamiento de datagramas *IP* a través de una interred depende del esquema de direccionamiento. Una dirección *IP* tiene una longitud de 32 bits, dividida ya sea en dos o tres partes. La primera parte designa la dirección de red, la segunda parte (si la hay) indica la dirección de subred y la última parte designa la dirección del host. Las direcciones de subred sólo se presentan si se decidió dividirse en subredes. La longitud de los campos de red, subred y host es variable.

Hay cuatro formatos para la dirección *IP*, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase *A* hasta Clase *D*, aparecen en la figura 52:

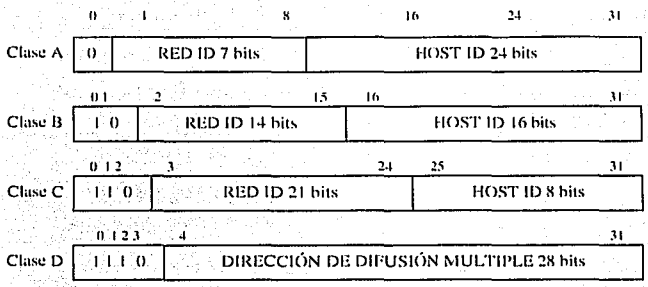

Figura 52. Clases de direcciones IP.

- Las redes *Clase A* corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son *0.1.0.0* hasta la *126.0.0.0* (lo que permite hasta 1.6 millones de direcciones).

- Las redes *Clase B* sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el *128.0.0.0* hasta el *191.255.0.0*. Esto permite tener 16320 redes con 65024 direcciones para estaciones en cada una.

- Las redes *Clase C* tiene sólo 8 bits para la dirección de estación y 21 bits para la dirección de red. Las direcciones de esta clase están comprendidas entre *192.0.1.0* y *223.255.255.0*, lo que permite cerca de 2 millones de redes con 254 estaciones cada una.

- Las direcciones de *Clase D* se usan con fines de multidifusión, cuando se requiere una difusión general a más de un dispositivo. El rango es desde *224.0.0.0* has *239.255.235.255*.

Las redes IP también pueden dividirse en unidades más pequeñas, denominadas *subredes*. Las *subredes* proporcionan flexibilidad adicional a los administradores de redes, al particionar la red lógica en redes menores. Las subredes tienen existencia propia dentro de la red original, pero no respecto al mundo exterior que ve una única red.

Para conseguir incrementar el número de estaciones conectadas en una red, se emplea una *mascara* en la *dirección IP* que se aplica a la *subred*. La *mascara* es un mecanismo compuesto de "*ceros*" y de "*unos*" mediante el cual los "*unos*" indican la parte de dirección de red y subred, y los "ceros " corresponden con las direcciones de estaciones.

Por ejemplo: si una red que contiene una subred de 600 estaciones, serían necesarios 10 bits para poder direccionar todas las estaciones que contiene esa subred. Una máscara válida para este caso sería la que se muestra en la figura 53:

255 • 255 • 252 • 0

11111111 • 11111111 • 11111100 • 00000000

Figura 53. *Máscara de subred.*

Fragmentación y reensamblado

El tamaño máximo de los *datagramas IP* puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño se le denomina *MTU* (*Unidad Máxima de Transmisión*). Una red no puede transmitir ningún paquete cuya longitud exceda el *MTU* de dicha red. Por ejemplo, en *Ethernet* los paquetes no pueden exceder los 1500 bytes.

Debido a esto es necesario algún mecanismo que permita reconvertir los *datagramas IP* en el formato requerido por cada una de las redes que va atravesando. Esto es lo que se denomina *fragmentación* y *reensamblado*. La *fragmentación* divide los paquetes en varios fragmentos de menor longitud, mientras que el *reensamblado* realiza el proceso inverso.

El protocolo *ICMP* (*Protocolo de Control de Mensajes de Internet*) se emplea para informar de errores o de control de la red, aunque *ICMP* se emplea para estos fines, no hace fiable al protocolo *IP*. La fiabilidad debe ser proporcionada por los niveles superiores que utilicen *IP*.

Una de las herramientas de diagnóstico de *ICMP* es el *ping*, que es una herramienta para diagnosticar si una estación está conectada a la red.

En la figura 54 vemos la estructura del mensaje *ICMP*:

Tipo	código	Suma de verificación
Datos ICMP (Dependerán del Tipo de Mensaje)		

Figura 54. Formato del mensaje *ICMP*

Donde:

- *Tipo*: especifica el tipo de mensaje.
- *Código*: contiene el código del error que afecta al datagrama al que se refiere el mensaje *IP*
- *Suma de verificación*: consta de 16 bits que son el resultado de realizar el complemento a uno del resultado obtenido al realizar la suma en complementos a uno del mensaje *ICMP* comenzando desde el campo "Tipo".
- *Datos ICMP*: normalmente el campo datos contiene una parte del mensaje IP original (mensaje causante de generar el mensaje *ICMP*).

Existen los siguientes tipos de mensajes ICMP:

- *Mensajes de destino no alcanzable*: estos mensajes los utilizan los dispositivos de ruteo y en algunas ocasiones los host de destino.
- *Mensajes de control de congestión*: cuando un host destino tiene el buffer lleno, envía este mensaje al host origen indicándole este suceso.
- *Mensajes de redireccionamiento*: estos mensajes los envían los dispositivos de ruteo al host emisor. Indican si el datagrama IP se enviará a través de otro ruteador diferente. La nueva ruta será más óptima.
- *Mensaje de tiempo excedido*: es el mensaje que se envían los equipos de ruteo cuando el campo TTL del datagrama IP es cero, o si el temporizador de reensamblado expira antes de que se hayan recibido todos los fragmentos del datagrama inicial.

El protocolo *ARP* (*Protocolo de Resolución de Direcciones*), se utiliza para convertir las direcciones IP en direcciones de la red física, por ejemplo, direcciones MAC (Control de Acceso al Medio). Las especificaciones de *ARP* están descritas en el *RFC 826*. Para poder realizar esta conversión se utiliza una tabla denominada *Tabla de direcciones ARP*.

Cuando se envía un datagrama *IP* a una estación destino, *ARP* busca en la tabla de direcciones la correspondencia entre la dirección *IP* y la dirección física MAC. Si existe en la tabla se procede a la transmisión.

Si por el contrario, la dirección *IP* de la estación destino no se encuentra en la tabla de direcciones, se genera una petición *ARP* que se difunde a través de toda la red. El paquete que engloba esta petición se compone, entre otros, de los campos que muestra la figura 55:

Dirección IP del host origen
Dirección IP del host destino
Dirección Física del host origen

Figura 55. Petición *ARP*.

Si alguna de las máquinas de la red reconoce su propia dirección IP en el paquete de petición, envía un mensaje de respuesta a la estación origen. A su vez, la respuesta se compone de los campos que muestra la figura 56:

Dirección IP del host destino
Dirección Física IP del host destino

Figura 56. Respuesta *ARP*.

II.III Nivel TCP

TCP (*Protocolo de Control de Transmisión*) y *UDP* (*Protocolo de Datagrama de Usuario*) implementan el nivel de transporte. *TCP* proporciona el transporte de datos orientado a la conexión, mientras que la operación de *UDP* es orientado a la no-conexión.

El protocolo *TCP* proporciona a los protocolos de capas superiores un servicio dúplex total, con confirmación de envío y control de flujo. Los datos son transportados en una flujo de bytes continuo no estructurado en el que los bytes se identifican mediante números de secuencia. *TCP* también soporta diversas conversaciones de capa superior a la vez. En la figura 57 se muestra el formato del paquete *TCP*.

Puerto de origen			Puerto de destino
Número de secuencia			
Número de confirmación de recepción			
Contr	Reservado	Ba	Ventana de transmisión
Suma de verificación			Apuntador urgente
Opciones (+ relleno)			
Datos (variable)			

Figura 57. Formato del paquete *TCP*.

Los campos del paquete *TCP* son como sigue:

- *Puertos de origen y destino*: identifican los puntos en los cuales los procesos de las capas superiores de origen y destino reciben servicios de *TCP*.
- *Número de secuencia*: por lo regular especifica el número asignado al primer byte de datos en el mensaje actual. Bajo ciertas circunstancias, también puede usarse para identificar un número de secuencia inicial que se utiliza en la transmisión futura.
- *Número de confirmación de recepción*: contiene el número de secuencia del siguiente byte de datos que se espera recibir por parte de la otra entidad remota emisora de paquetes.
- *Control de datos*: indica el número de palabras de 32 bits del encabezado *TCP*.
- *Reservado*: reservado para uso futuro.
- *Banderas*: llevan diversa información de control.
- *Ventana de transmisión*: especifica el tamaño de la ventana de recepción del emisor (es decir, el espacio de búfer disponible para datos entrantes).
- *Suma de verificación*: indica si se daño el encabezado en el camino.
- *Apuntador urgente*: apunta al primer byte de datos urgentes en el paquete.
- *Opciones*: especifica las diversas opciones de *TCP*.
- *Datos*: contiene información de la capa superior.

La transmisión que ofrece *TCP* es fiable, permite la recuperación de datos perdidos, erróneos o duplicados, y garantiza la secuencia de entrega, para lo que se asigna al segmento de datos un número de secuencia (información de control) y un checksum (código de control). La fiabilidad de la transmisión se consigue mediante tres mecanismos diferentes:

- Confirmación de recepción
- Temporizadores de espera de confirmación
- Retransmisión de segmentos

Para disponer de control de flujo, el receptor mantiene una ventana que indica al emisor la cantidad de datos que puede enviar a partir de cada confirmación recibida.

TCP utiliza dos conceptos que se explicarán brevemente, pero que son muy usuales en este protocolo. El primero es *socket* y el segundo es *puerto*.

El *socket* es un par de números que identifican de manera única cada aplicación. Cada *socket* se compone de dos campos:

- La dirección IP de la estación en el que la aplicación está corriendo.

- El puerto a través del cual la aplicación se comunica con *TCP/IP*. Este número de puerto identifica el proceso.

Lo más normal es que en un momento dado haya más de un proceso de usuario o aplicación utilizando *TCP* simultáneamente. Por ello es necesario un método que identifique los datos asociados a cada proceso.

Un *puerto* es una palabra de 16 bits que identifica hacia qué aplicación o proceso deben dirigirse los datos. Se trata de un mecanismo a través del cual las distintas aplicaciones contactan con *TCP/IP*.

TCP utiliza un mecanismo de ventanas para controlar el flujo de la información. La idea del mecanismo de ventana deslizante es que el emisor pueda transmitir tantos paquetes de información sin recibir la confirmación de recepción como tenga en la ventana. El rendimiento de este mecanismo depende del tamaño de la ventana y de la velocidad a la que la red transmite los paquetes.

Para el establecimiento de una *sesión*, *TCP* utiliza un mecanismo en el que se intercambian tres mensajes, tal y como se muestra en la figura 58:

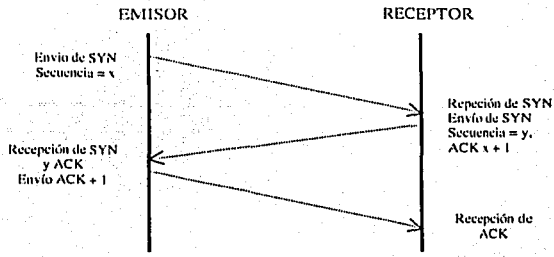

Figura 58. Establecimiento de una *sesión TCP*.

El primer segmento se identifica por que lleva activo el bit de SYNC en el campo de control. El segundo mensaje lleva activo tanto el bit SYN como el bit ACK. El último mensaje se usa para informar al destino que la conexión se ha establecido.

Dos programas que empleen el *protocolo TCP* pueden finalizar su comunicación mediante la operación *close* (cerrar). Internamente, *TCP* emplea un mecanismo similar al de establecimiento de una sesión *TCP* para finalizar

la conexión. Cuando un programa de aplicación comunica a *TCP* que no tiene más datos que transmitir, *TCP* finaliza la conexión en una dirección. Para cerrar esta semi-conexión, el emisor *TCP* transmite los datos restantes y espera a que el receptor tenga conocimiento de que haya recibido estos datos, y entonces envía un segmento con el bit FIN activo. El receptor *TCP* recibe el segmento con el bit FIN e informa al programa de aplicación de que no hay más datos disponibles. Como se describe en la figura 59:

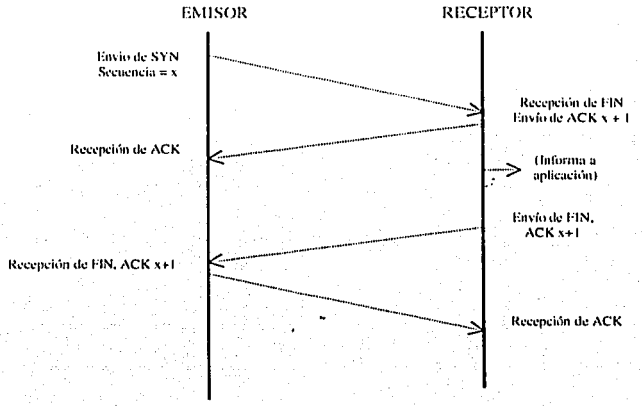

Figura 59. Cierre de una sesión TCP.

Normalmente un programa de usuario emplea la operación cerrar para terminar una conexión cuando deja de utilizarla. En algunas ocasiones, condiciones anormales forzan a que un programa de aplicación rompa la conexión, por lo que TCP suministra una utilidad para estas conexiones anormales.

Para interrumpir una conexión, uno de los procesos envía un segmento con el bit RST activo. El otro responde inmediatamente abortando la conexión TCP también informa al programa de usuario de que se ha producido esta situación. Un *Reset* es la manera de terminar una sesión en la que cesa la transferencia de información inmediatamente y los recursos, como *buffers*, son liberados.

Protocolo de Datagrama de Usuario (UDP)

El *protocolo UDP* es un protocolo del nivel de transporte que se basa en el intercambio de datagramas. *UDP* permite el envío de datagramas a través sin que se haya establecido previamente una conexión (ofrece un servicio no orientado a conexión), para lo que el propio datagrama incorpora la suficiente información de direccionamiento. Esto simplifica notablemente el protocolo, pero a cambio no se confirman los datagramas recibidos ni se garantiza su orden, debiendo ser la aplicación la que se encargue de su control.

El protocolo *UDP* maneja también los conceptos de *puertos* y *sockets*, ya que este protocolo es utilizado simultáneamente por varias aplicaciones (al igual que *TCP*). *UDP* básicamente proporciona acceso a los servicios del nivel *IP*, incorporando mulitplexación/demultiplexación. No proporciona control de flujo ni fiabilidad en las transmisiones o recuperación de algunos tipos de errores. En la figura 60 vemos el formato de los *datagramas UDP*.

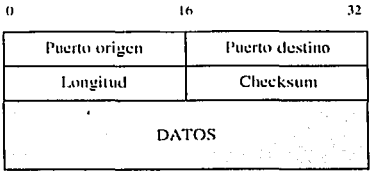

Figura 60. Formato de los *datagramas UDP*.

Donde:

- *Puerto origen*: puerto del proceso emisor u origen (a este puerto deben dirigirse las respuestas requeridas)
- *Puerto destino*: especifica el puerto del proceso destino (en el equipo destino).
- *Longitud*: es la longitud en bytes del datagrama *UDP* (incluida la cabecera).
- *Checksum*: es el complemento a 1 de la suma (en complemento a 1) de todos los bits que forman el datagrama *UDP*, más unos bits adicionales constituidos a partir de la cabecera *IP*.

El software de *UDP* acepta datagramas *UDP* de múltiples programas del nivel aplicación y los pasa al nivel *IP* para su transmisión, a la vez que acepta datagramas de *IP* y se los pasa a los correspondientes programas de aplicación.

Conceptualmente, toda la multiplexación y demultiplexación entre el software *UDP* y los programas de aplicación se realiza mediante puertos. En la práctica cada programa de aplicación debe negociar con el sistema operativo para obtener un puerto de protocolo y un número de puerto antes de que pueda enviar datagramas *UDP*. Una vez que el puerto ha sido asignado, cualquier datagrama que envíe la aplicación pondrá ese número en el campo *número de puerto UDP*.

II.IV Nivel Aplicación

Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La capa de aplicación de TCP/IP ha demostrado ser mas acertada, pues contiene todos los protocolos de alto nivel que se utilizan para ofrecer servicios.

En este nivel trabajan diversas aplicaciones que proporcionan servicio a usuarios, programas, dispositivos o equipos de comunicaciones. Existen diversos protocolos en este nivel y muy variados en cuanto a su función, como la transferencia de archivos, la administración de la red, servicios de archivos distribuidos, emulación de terminal, de correo electrónico y resolución de nombres, por mencionar algunos, pero la mayoría se apega al esquema de trabajo cliente/servidor y RPC (procedimiento a llamadas remotas). En la tabla 4 se muestran diversas aplicaciones con sus respectivos protocolos.

Aplicación	Protocolo
Transferencia de archivos	FTP
Emulación de terminal	Telnet
Correo electrónico	SMTP
Administración de red	SNMP
Servicios de archivos distribuidos	NFS, RPC, X-Windows
Paginas WEB	HTTP
Resolución de nombres	DNS
Asignación de direcciones IP	DHCP

Tabla 4. Protocolos del nivel de Aplicación.

Un RPC es una llamada a un procedimiento que se ejecuta en un sistema diferente del que realiza la llamada, esta es la razón por la que el procedimiento se denomina "remoto". En un RCP el código de programa que realiza la llamada y el procedimiento llamado se comunican a través de una "interfaz RPC", que consiste en un conjunto de operaciones y datos que sirven de "contrato" para un conjunto de procedimientos remotos.

RPC sigue el esquema cliente/servidor. El proceso llamante (cliente) envía un mensajes al proceso servidor y espera una respuesta. Por otra parte el proceso servidor se encuentra en un estado de espera de peticiones y, al recibir un mensaje de un cliente, estudia los parámetros del procedimiento llamado, obtiene los resultados y los envía de regreso al proceso cliente mediante un mensaje de respuesta. Como se ve en la figura 61:

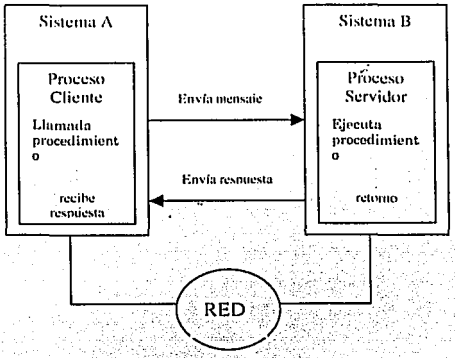

Figura 61. Procedimiento RPC.

Como son muy variados los protocolos utilizados en este nivel de *TCP/IP*, solo describiremos brevemente algunos de los más usuales:

Telnet

Es un protocolo para que dos computadoras remotas se puedan conectar y trabajar uno con el otro, tal como si estuvieran conectados directamente, uno de ellos es el usuario y el otro el servidor. TCP se encarga del intercambio de información.

FTP

Protocolo de transferencia de archivos, permite el envío y recepción de archivos de cualquier tipo de o hacia otra computadora. Cuando se desea el envío, se realiza una conexión TCP con el receptor y se le pasa información sobre el tipo y acciones sobre el archivo, así como los accesos y usuarios que pueden acceder a ese archivo, una vez realizado esto, se envía el archivo, finalmente se puede cortar la conexión.

NFS

Sistema de archivo remoto, autoriza a los usuarios el acceso en línea a los sistemas de archivos que se encuentran en sistemas remotos, de esta forma el usuario accede a un sistema de archivo remoto como si esta fuera un archivo local, desde la perspectiva del usuario es casi transparente.

DNS

Sistema de nombres por domino, es una base de datos de información de las computadoras alojadas en Internet, es un sistema jerárquico distribuido que permite obtener una dirección IP dado un nombre de una estación o computadora. Cada unidad de datos en la base de datos del *DNS* es indexada por un nombre. Estos nombres son caminos completos a través de un gran árbol invertido llamado "espacio de nombres de dominios". El árbol tiene una sola raíz en el tope, llamado directorio raíz y en *DNS* solo se le llama "la raíz" o "dominio raíz"; el árbol del *DNS* puede seccionar algún número de caminos en puntos de intersección llamados "nodos".

SMTP

Es un *protocolo de transferencia simple de correo electrónico*, y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante *TCP/IP*.

SNMP

Es el *protocolo de administración de redes simple*, es un modelo *cliente/servidor* compuesto de estaciones gestoras y agentes actuando, los gestores como clientes (pidiendo información a los agentes) y los agentes como servidores (suministrando información a los gestores), utilizando para este diálogo el protocolo *SNMP*.

Capitulo III

Correo electrónico.

III.I Breve Historia

Hace una década, se pensaba que el *correo electrónico* iba a hacer de la computadora personal un instrumento esencial para todo el mundo. Ahora con la llegada de las redes de área local, de *Internet* y los sistemas de *correo electrónico*, se volvió a descubrir su valor.

Las raíces del *correo electrónico* se encuentran en el *télex*, un sistema mundial para enviar mensajes entre teletipos que ha ido creciendo en importancia a lo largo de un siglo. El *télex* transmite texto a la desesperante velocidad de 10 caracteres por segundo, y frecuentemente envía caracteres incomprensibles debido a errores de transmisión. Sin embargo, el *télex* sigue siendo una vía de comunicación importante para los negocios en muchas de las zonas menos desarrolladas, e incluso se utiliza para transmitir *correo electrónico* en algunos servicios internacionales. El *correo electrónico* creció en los años setenta con sistemas basados en grandes computadoras y minicomputadoras.

La mayor virtud del *correo electrónico* es su conveniencia. El receptor no necesita estar en la computadora cuando se envía el mensaje. La capacidad de almacenar y enviar mensajes del *correo electrónico* permite comunicarse con facilidad con cualquier lugar del mundo.

Existen dos grupos principales de servicios de *correo electrónico*: *privados* y *públicos*. Los servicios privados de *correo electrónico* atienden las necesidades internas de una empresa y se basan en un sistema de computadoras multiusuario, como una gran computadora o una red local. Los servicios públicos de *correo electrónico* están al alcance de personas u organismos mediante suscripción y generalmente tienen un ámbito nacional o internacional.

III.II Funcionamiento

El *correo electrónico* difiere de las otras aplicaciones porque no es un servicio de usuario a usuario: no es necesario que las maquina emisora y receptora del *correo electrónico* se comuniquen directamente entre sí. Al *correo*

electrónico se le conoce como un servicio de *almacenaje y reenvío*. El correo pasa de una maquina a otra hasta que llega a su destino final. Esto es similar a la forma en que el Servicio Postal entrega el correo.

El Servicio Postal opera como una red de *almacenaje y reenvío*. Se escribe el domicilio en el sobre y se deposita en el buzón. La carta es recogida para llevarla a otro lugar y almacenarla. Ahí se clasifica y se reenvía a otro lugar. Este paso se repite hasta que llega a su buzón destino. Si el buzón destino no está en el área de cobertura del Servicio Postal, el mensaje se envía al servicio postal del país destino.

Tanto el *correo electrónico* como el *correo tradicional* son asíncronos; el emisor envía el mensaje cuando lo considera necesario y el receptor lo lee cuando desea. Esto se vuelve muy cómodo cuando se trata de establecer una comunicación con alguien que se encuentra a una gran distancia o cuando los horarios son muy distintos.

El tiempo que toma entregar un mensaje de correo electrónico consta de dos partes: el tiempo que lleva entregar el mensaje en la computadora destino y el tiempo que toma la lectura del mensaje una vez que se encuentra ahí. La primera parte es una función de cómo esta conectada a la red la máquina donde se maneja su correo. La segunda parte esta bajo el control del usuario. Si el *correo electrónico* no se revisa con regularidad, la entrega inmediata de los mensajes carece de sentido. Los mensajes sólo esperan a ser leídos por el usuario. El *correo electrónico* se hace más útil cuando se reduce el tiempo de entrega de los mensajes entre la máquina y el usuario. El *correo electrónico* no es interactivo. Como puede observarse en la figura 62.

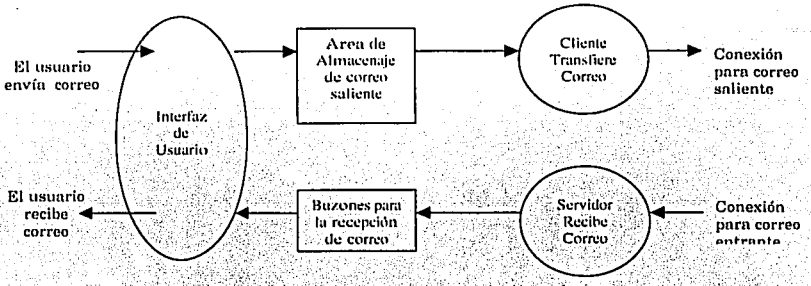

Figura 62. Esquema conceptual de los componentes del sistema de *correo electrónico*.

Cuando un usuario tiene que enviar un mensaje a otro usuario que no está conectado, el sistema de *correo electrónico* debe tomar ese mensaje y

guardarlo, por lo tanto, existen dos partes conceptualmente distintas en la transmisión de correo: por un lado, un *proceso de usuario (front-end)* que acepta correo del usuario y lo coloca en un *área de almacenaje*, mientras que, por otro, existe un proceso que *extrae* esos mensajes y los envía al destino.

De esta forma, un usuario puede comunicarse con otros aunque éstos no estén activos. El área en donde se depositan los mensajes recibidos hasta que el destinatario los recibe se denomina buzón.

Las funciones básicas de un *correo electrónico* son las siguientes:

- *Creación*: el usuario crea y edita un mensaje, generalmente utilizando medios locales de edición.
- *Emisión*: se envíe el mensaje a los destinatarios y se almacena en los correspondientes buzones.
- *Recepción*: el destinatario toma el mensaje almacenado para efectuar su lectura.
- *Almacenamiento*: tanto el emisor como el destinatario pueden almacenar el mensaje en un archivo.

Si el mensaje llega o no a su destino, esto dependerá únicamente de que la dirección destino haya sido escrita correctamente. A veces, el *correo electrónico* falla porque alguna parte de la red no funciona, pero normalmente intenta entregar todos los mensajes durante varios días, antes de darse por vencido. Las direcciones de *correo electrónico* se componen de varias reglas, de hecho, la base para todo el correo es el *nombre del dominio* de la máquina que actúa como agente de correo (la máquina que pone la dirección del destinatario en el mensaje). Una vez que se ha entregado el mensaje a la máquina designada, ha concluido el trabajo de la red. Ahora depende únicamente de esta computadora que el mensaje llegue a su destino, pero la máquina requiere de más información para continuar enrutando el mensaje: *el nombre del usuario*.

Una dirección de correo identifica al sistema de correo a quien va dirigido el mensaje. A pesar de que algunos sistemas de correo poseen direcciones complicadas, las direcciones empleadas por *Internet* son bastantes simples.

Estas tienen el formato definido en el documento *RFC-822*; el cual es:

Parte-local@nombre-dominio =
parte-local@dominio(n).dominio(n-1)....dominio1

Donde la *parte local* es el nombre del buzón situado en el nombre del dominio. Por ejemplo:

Usuario1@dominio2.dominio1.com

III.III Ventajas y desventajas

El *correo electrónico* tiene sus ventajas y sus desventajas. Visto superficialmente, pareciera que sólo sirve como una manera rápida de enviar mensajes o algo equivalente. Para saber cuando es útil el *correo electrónico*, sólo hay que pensar cómo difiere de otros medios de comunicación. De alguna forma el *correo electrónico* es muy similar al teléfono; desde otro punto de vista, es similar al correo tradicional. En la tabla 5 se hace una comparación rápida.

Característica	*Teléfono*	*Correo electrónico*	*Correo tradicional*
Velocidad	Alta	Moderada	Baja
Sincronización	Si	No	No
Formalidad	Varía	Moderada	Varía
Responsabilidad	Baja	Moderada	Alta
Facilidades de conferencia	Grupos pequeños	Algunos a muchos	Solo en un sentido
Seguridad	Moderada	Baja a moderada	Alta

Tabla 5. Comparación de *técnicas de comunicación*.

Primero hay que pensar qué tan rápido es posible enviar un mensaje de un punto a otro por cada uno de los medios. El teléfono ofrece una entrega inmediata y trabaja en un medio de comunicación relativamente rápido. El tiempo que tarda el *correo electrónico* en entregar mensajes va de segundos a un día y el correo tradicional puede ser entregado de uno a varios días, inclusive semanas. El inconveniente de la comunicación telefónica es la sincronización de las personas que van a llamar, esto es que ambas deben estar en el teléfono al mismo tiempo. Como se menciono anteriormente tanto el *correo electrónico* como el *correo tradicional* son *asíncronos* y esto se vuelve muy cómodo cuando se trata de establecer una comunicación con alguien a una gran distancia y en otros horarios.

Ahora examinando las comunicaciones en grupo. El teléfono es un buen medio, pero sólo para grupos pequeños. Las llamadas de conferencias permiten que grupos de personas puedan hablar entre sí, pero cuando el grupo se hace más grande, tratar de programar una conferencia y el establecimiento de la misma, se vuelve muy difícil. Por otro lado, mandar correo a miles de personas es relativamente sencillo con el correo electrónico, además que permite formar grupos de cualquier tamaño y cualquier miembro del grupo puede enviar mensajes a todos en cualquier momento. Esta cualidad del correo electrónico lo hace muy útil para diseminar información y pedir opinión a todo un grupo.

La seguridad, que es otro aspecto importante, que ya esta siendo mejorado en el *correo electrónico*, actualmente existen diversas opciones, como lo son la encripción de mensajes, los filtros para evitar cadenas (spam) y por supuesto *antivirus* para *correo electrónico*.

Podemos decir que el *correo electrónico* tiene sus correspondientes desventajas, pero conociendo estas podemos tener un eficiente *sistema de correo electrónico*. Por mencionar las más significativas:

Probabilidad de mala interpretación: una de las razones de esta desventaja es la ausencia de señales visuales y verbales del receptor del mensaje.

Baja velocidad ocasionalmente: esto es, la entrega de los mensajes puede ser en un lapso de minutos o hasta horas, y en algunas ocasiones el tipo de velocidad no es suficiente para lo que necesitamos, ya que antes que termine el día llegue necesitamos recibir el correo electrónico que esperamos.

Limite de tamaño: los sistemas de correo electrónico frecuentemente limitan el tamaño de los mensajes transmitidos debido principalmente a las limitaciones de espacio en los servidores que almacenan el correo de los usuarios, por lo que el uso de archivos anexos en los correos electrónicos se ve limitado.

III.IV Protocolos

El *correo electrónico* se encuentra estandarizado en diferentes *protocolos*, y cada uno tiene características y funciones particulares, para este trabajo se estudiaran los más representativos. Aunque cabe resaltar que día a día se encuentran mejorías a cada *protocolo* o sistema de *correo electrónico*, y también surgen nuevos protocolos que amplían las facilidades de los anteriores, enriqueciéndolos para que interactuen con otras aplicaciones como

procesadores de texto, aplicaciones multimedia y aplicaciones de reconocimiento de la voz y de servicios de directorios corporativos.

Algunos de los organismos y foros encargados de emitir los protocolos para el correo electrónico, son los siguientes:

- IETF (The Internet Engineer Task Force)
- IMA (International Messaging Associates)

III.IV.1 X.400

El consejo consultivo CCITT ha creado el protocolo X.400 para los sistemas que manejan mensajes (Message Handling Systems).

La *serie X.400* está relacionada principalmente con la interconexión de sistemas de correo electrónico. Estos estándares son referidos como estándares de correo electrónico. El correo electrónico usa facilidades de telecomunicaciones para entregar correspondencia para satisfacer necesidades diarias de la gente. Esa es la más visible aplicación electrónica.

Hay dos versiones del estándard *X.400.* La especificación de 1984 y la de 1988, esta ultima actualizada en 1992 con mayores facilidades como permitir el uso de líneas asincronas, herramientas para conectar usuarios de PC y LAPTOP no conectados a una red *X.400,* además de servicios de directorio y facilidades de seguridad.

X.400 divide un sistema de *correo electrónico* dentro de un cliente, llamado *UA* (User Agent) y un servidor, llamado *MTA* (Message Transfer Agent). Esencialmente el *UA* es un buzón de correo, ese interactua directamente con el usuario, como edición de texto, presentación de servicio, seguridad, prioridad de mensaje, y notificación de entrega.
El *UA* es una interfaz, no una aplicación de usuario final, por lo tanto no define las especificaciones de cómo interactua con el usuario. Los fabricantes de productos deciden estos temas.

El *MTA* dirige y transmite los mensajes, su responsabilidad incluye establecer la ruta de almacenaje-y-envio (store-and-forward), asegurando la seguridad del canal, y dirigiendo los mensajes a través del medio. El *UA* envía su mensaje al *MTA* local y este revisa el mensaje que no tenga errores de sintaxis, luego entrega el mensaje a un *UA* local, o si el mensaje no es local lo dirige al siguiente *MTA*. Ese *MTA* repite el proceso hasta que el mensaje es entregado exitosamente.

Un conjunto de *MTA's* es conocido como *MTS* (Message Transfer System). El *MTS* es usualmente especial para un particular fabricante de producto.

El modelo funcional de *X.400* (MHS) se muestra en la figura 63. Donde un usuario puede ser un originador o un receptor de un mensaje electrónico. Un originador prepara un mensaje con la asistencia de un proceso de aplicación llamado *UA* (User Agent). La responsabilidad de un *UA* incluye interactuar con el *MTS* (Message Transfer System) o un *MS* (Message Store), y enviar los mensajes de un usuario al que pertenece.

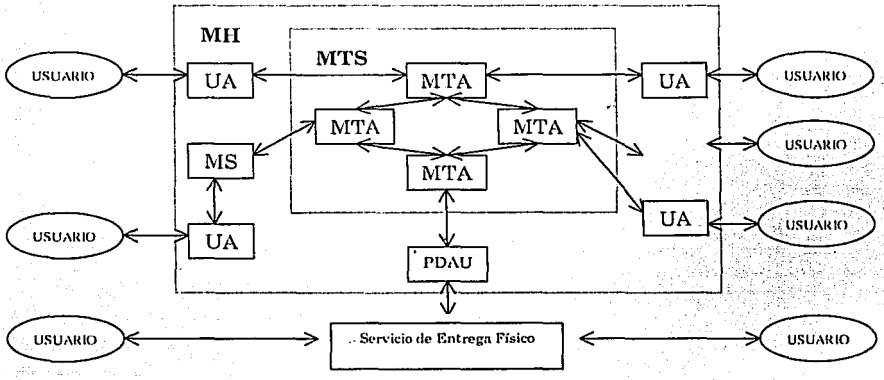

Figura 63. Modelo Funcional *X.400* (MHS).

Si un mensaje es enviado para el *MTS*, el *MTS* lo entrega a una o más unidades *UAs* (Access Units) o *MSs*. El *MTS* puede también regresar al originador una notificación. Hay un numero de *MTAs* (Message Transfer Agents) en el *MTS*. Estos agentes operan juntos para entregar los mensajes a los recipientes.

El *PDUA* (Physical Delivery Access Unit) maneja la entrega física y negocia el acceso para usuarios indirectos de *MHS*.

El *MS* (Message Store) provee la facilidad para almacenar mensajes, enviar y recuperar, también complementa a los *UA* para dispositivos que no están siempre disponibles, así como PC's o terminales

X.400 define varios protocolos para maneja mensajes entre los diferentes componentes del sistema. Dos *MTA's* pueden comunicarse directamente, sin la

intervención de un *UA*, usando el protocolo *P1*. Si un *UA* quiere comunicarse con un servicio fuera del dominio de la red *X.400*, este usara el protocolo *P2*, el protocolo de mensajería interpersonal.

La implementación de 1988 define para *P2* adicionales tipos de cuerpos de mensaje, así además de soportar Teletex y Group III Fax, también soporta formatos de procesadores de palabras. P3 define las convenciones para transferir un mensaje desde el *UA* al *MTA*, inicialmente definido en 1984, *P3* asumía que el *UA* estaba en línea y listo para aceptar mensajes desde su *MTA*, pero *X.400* no previa que los *UA* podrían estar en línea de forma intermitente.

En la practica muchos *UA* son implementados en computadoras personales y por lo tanto no siempre estaban en línea, para remediar esta situación, el *MS* (Message Store) fue agregado en 1988 y p7 fue definido para la comunicación entre el *UA* y el *MS*. El *MS* siempre esta conectado al *MTS* (Message Transfer System), almacenando mensajes para los *UA*. Los *UA* envían a través del *MS*, también como los recupera, lista, resume y borra mensajes desde la base de datos del *MS*.

La recomendación *X.400* de 1988 recomienda el uso de *X.500* servicio de directorio para nombres, almacenar listas de distribución, almacenar perfiles de *UA*'s y autentificacion de usuarios.

X.400 es solo una opción para construir el backbone de una red de mensajes empresarial, como quiera, X.400 tiene aceptación internacional e independencia del fabricante.

III.IV.2 Protocolo de Transferencia de Correo Simple SMTP

El *protocolo de transferencia de correo simple SMTP* fue desarrollado para el Departamento de Defensa de Estados Unidos como un sistema de correo electrónico simple y fácil de usar para el Internet. *SMTP* forma parte del conjunto de protocolos de TCP/IP.

El *SMTP* se usa con frecuencia para transferir correo entre dos estaciones de trabajo en red con conexión remota. Lo que hace que *SMTP* sea tan fácil de usar es que no hay que escribir muchos comandos. Aunque primero describiremos su modelo.

El modelo SMTP

El intercambio de correo usando *TCP/IP* es ejecutado por un *MTA* (Message Transfer Agent). El protocolo *SMTP* describe como dos *MTAs* se comunican usando una conexión simple de *TCP*. *SMTP* usa el concepto de almacenamiento (spooling), esto es permitir al correo ser enviado desde una aplicación local a la aplicación de *SMTP*, que almacena el correo dentro de algún dispositivo o memoria. Una vez que el correo ha arribado al área de selección es formado. Un servidor verifica para ver sí algún mensaje esta disponible y luego intenta entregarlo. Si el usuario no está disponible para la entrega, el Servidor puede intentarlo después.

Eventualmente, si el correo no puede ser entregado, ese va a ser descartado o regresado al remitente. Esto es conocido como un Sistema de Entrega Extremo-Extremo (End-to-End Delivery System), por que el Servidor esta intentando contactar al destinatario para entregar el correo, manteniéndolo en el área de selección por un periodo de tiempo hasta que ha sido entregado.

SMTP se encuentra en dos *RFC's* (Request For Comments). El *RFC 822* que describe la estructura para los mensajes, y el *RFC821* que especifica el protocolo que controla el intercambio de correo entre dos maquinas. La figura 64 ilustra el modelo *SMTP*.

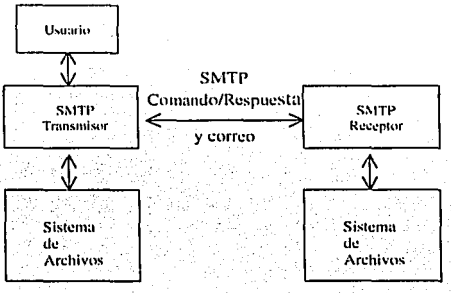

Figura 64. El modelo *SMTP*.

1. Como resultado de la petición de un usuario de correo, el *SMTP-transmisor* establece un canal de transmisión de dos vías hacia un *SMTP-receptor*, algunos comandos son generados por el *SMTP-transmisor* y enviados al *SMTP-receptor*, y sus respuestas son enviadas del *SMTP-receptor* al *SMTP-transmisor* en respuesta a los comandos.

2. Una vez establecido el canal de transmisión, el *SMTP-transmisor* envía un comando *MAIL* indicando el remitente del correo. Si el *SMTP-receptor* puede aceptar correo este responde con un comando *OK*. Luego el *SMTP-transmisor* envía un comando *RCPT* identificando un destinatario del correo. Si el *SMTP-receptor* puede aceptar correo para ese destinatario este responde con un comando *OK*, si no, este responde con una respuesta de rechazo a ese destinatario, pero no la sesión de correo completamente. El *SMTP-transmisor* y el *SMTP-receptor* pueden negociar varios destinatarios (recipientes). Cuando los destinatarios (recipientes) se han negociado, el *SMTP-transmisor* envía los datos de correo, terminando con una secuencia especial. Si el *SMTP-receptor* procesa exitosamente los datos de correo este responde con un comando *OK*. El dialogo es resuelto y se cierra uno los recipientes de los destinatarios

3. *MAIL*: este comando es una ruta inversa, esto es una ruta de regreso

4. *RCPT*: es una ruta de reenvío, esto es una ruta fuente (origen)

El procedimiento SMTP

Los pasos para las transacciones de correo de *SMTP* son:

La transacción es iniciada con un comando *MAIL*, que da la identificación del remitente. Una serie de unos o comando *RCPT* sigue dando la información del receptor. Luego un comando *DATA* da los datos del correo. Finalmente, al terminar los datos del correo indica que confirma la transacción.

Los comandos que actualmente son implementados para la capa *SMTP* son:

HELO

Este comando debe ser el primero que enviamos cuando se abre una conexión *SMTP*, en respuesta al mensaje de bienvenida del servidor. Requiere un parámetro, que será el nombre jerárquico que identifica nuestra máquina.

EHLO

Este comando es equivalente al anterior (y con el mismo parámetro), pero comprueba si el servidor es un servidor *SMTP* de segunda generación. Ello da pie a utilizar servicios extendidos. Para más información consultar [*RFC1869*]. Si se trata de un servidor de primera generación, el comando

"*EHLO*" no será reconocido y tendremos que identificarnos mediante "*HELO*".

220 READY FOR MAIL

es la respuesta de un servidor a cualquiera de los dos comandos anteriores

MAIL

Este comando contiene el buzón fuente-origen, la sintaxis es la siguiente:

MAIL <SP> *FROM*:<reverse-path> <CRLF>

Si es aceptado por el *SMTP-recepetor*, este responde con un comando *OK*. La <reverse-path> puede contener más de un buzón.

RCPT

Este comando da una ruta de envío identificando un recipiente, si es aceptado el *SMTP-receptor* responde con el parámetro *250 OK* y almacena la ruta de envío. Si el recipiente es desconocido responde con *550 Failure*. La sintaxis es la siguiente:

RCPT <SP> TO:<forward-path> <CRLF>

La <forward-path> puede contener más de un buzón

DATA

Si este comando es aceptado, el *SMTP-receptor* regresa el parámetro *354 START MAIL*, y considera todas las subsiguientes líneas el texto del mensaje, cuando concluye el texto es recibido y almacenado, el *SMTP-receptor* envía el parámetro *250 OK*. Los datos del correo incluyen *cabecera, fecha, tema, para, con copia, de, etc.*

SEND

Este comando hace que el correo sea enviado de inmediato y con frecuencia se emplea cuando alguien desea enviar una pagina de datos a la vez.

SOML

Este comando es, de hecho, dos comandos: *send* y *mail*, es decir, enviar de inmediato o entregar los datos a un buzón. Si un usuario esta conectado, el mensaje se envía a su pantalla, si no lo esta, el mensaje se envía como correo al buzón del usuario.

RSET

El comando *RESET* sirve para cancelar una transacción de correo.

VRFY

El comando *VERIFY* revisa para asegurarse de que el usuario cuenta con un buzón en el sistema receptor.

EXPN

El comando *EXPAND* indica que el mensaje se enviara a una lista de correos y no a un usuario individual.

HELP

Este comando da como resultado el despliegue de un mensaje.

NOOP

El comando *NO OPERATION* en realidad no hace nada: solo ocasiona que el servidor de correo envíe un mensaje *OK* como respuesta. Esto es útil para verificar la conexión.

QUIT

El comando *QUIT* le indica al servidor de correos que emita una respuesta *OK* y cierre el canal.

TURN

El comando *TURN AROUND* invierte las comunicaciones de manera que el emisor se convierte en receptor y viceversa.

Ejemplo de un procedimiento SMTP

En este ejemplo se envía correo del usuario Smith (transmisor) del host Alpha.ARPA, para Jones, Green y Brown (receptores) del host Beta.ARPA. Asumimos que el host Alpha se comunica directamente con Beta.

S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

El correo tiene que ser aceptado para Jones y Brown. Green no tiene buzón en el host BETA.ARPA.

Los tres componentes principales del correo electrónico son: *sobre*, *cabecera*, y *cuerpo*.

1. El *sobre* (*envelope*) es usado por el *MTA* para la entrega, como ejemplo se especifican sus dos comandos: *MAIL* y *RCPT*

   MAIL from: <usuario1@domino1.edu>

   RCPT to: <usuario@domino1.edu>

2. La *cabecera* (*headers*) es usada por los *UA's*. Los siguientes campos de cabecera: Received, Message-ID, From, Date, Reply-to, X-Phone, X-Mailer, To, y Subject; contienen un nombre, seguido por una coma y seguido por el valor del campo. El *RFC 822* especifica el formato e interpretación de los campos de cabeceras, donde las cabeceras que empiezan con *X* son campos definidos por el usuario.

3. El *cuerpo* (*body*) es el contenido del mensaje enviado por el usuario origen hasta el usuario destino. El *RFC 822* especifica el cuerpo como

líneas de texto del código NVT *ASCII* (variación de código *ASCII* de 7 bits usado en *TCP/IP*). Cuando se transfiere usando el comando *DATA*, la cabecera se envía primero, seguido por una línea en blanco, seguido por el cuerpo del mensaje. Cada línea transmitida usando el comando *DATA* debe ser menor que 1000 bytes.

III.IV.3 Protocolo de Oficina Postal POP3

Mientras que el protocolo *SMTP* se dedica a la retransmisión de mensajes desde el remitente hasta el buzón del destinatario, el *Protocolo de Oficina Postal* (Post Office Protocol), versión 3, llamado *POP3* definido en el *RFC-1939*, es el protocolo que debe controlar el software de correo electrónico y transferirlo a la maquina local. Y también el servidor de correo electrónico en cuestión tiene que dar soporte a *POP3* para poder dar respuesta al software de correo electrónico solicitante y que ambos utilicen el mismo idioma.

La estructura del protocolo POP3

En lo referente a la comunicación entre *cliente POP3* (software de correo electrónico en el lado del usuario) y *servidor POP3* (servidor de correo con buzones), *POP3* se parece un poco a *SMTP*. En *POP3*, el intercambio de datos entre ambas partes de la comunicación también se realiza a través de *TCP*, y todo se da en el formato *ASCII*, como es usual con el *correo electrónico* se usa el formato *US-ASCII de 7 bits*. Por tanto, se trata de comandos y respuestas de texto no cifrado, que viajan de un lado a otro, y no de estructuras binarias. Para los comandos dirigidos al servidor, no importa la escritura en mayúsculas o minúsculas.

El punto para el establecimiento de la conexión es el *puerto 110*, en el que espera un *servidor POP3* para recibir la solicitud de un cliente.

Presentarse al servidor POP3 (Fase de autorización)

Al igual que en el caso de un cliente *SMTP*, también el *cliente POP3* tiene que presentarse primero al entrar en contacto con un servidor. Para dicha presentación precisa dos comandos ya que, a diferencia de *SMTP*, el protocolo *POP3* prevé la identificación del cliente mediante *nombre* y *contraseña*. Mientras que no se precisa una *contraseña* determinada para introducir

mensajes en el sistema de correo electrónico de un servidor SMTP, no tiene este que disponer de una legitimación determinada para retransmitir un mensaje, sin embargo, esto no es válido para traer mensajes mediante *POP3*. Para no permitir que cualquiera pueda ver el correo del buzón, *POP3* exige la *autenticación* mediante una *contraseña*.

Si se divide la comunicación entre *cliente POP3* y *servidor* en diferentes fases, la conexión entraría en la *fase de autorización* (*authorization state*). Después del establecimiento de la conexión, el *servidor* envía en primer lugar una línea de saludo, que siempre debería comenzar por la identificación *+OK*, por ejemplo:

+OK POP3 server ServidorMX ready<administrador@dominio1.com><CRLF>

Desde el otro lado, el cliente envía como primer comando *USER* e indica también, el nombre del usuario o del que se desea comprobar. Si todo funciona, el servidor responde con *+OK* por que el buzón indicado existe realmente. Se recibe un *–ERR* el buzón indicado no existe o ya esta abierto. En este caso, otro usuario está ocupando el buzón en una sesión *POP3*.

En el caso de un mensaje de error, se puede volver a intentar presentarse a través de *USER* (quizá para otro buzón). No obstante, es posible que el cliente desee despedirse inmediatamente, para lo que en cualquier momento puede emplearse el comando *QUIT*.

Con *+OK* o *–ERR* se suele recibir un texto adicional, y se presenta al usuario pero no está estandarizado. Las respuestas pueden ser, por tanto, diferentes, por ejemplo:

+OK El usuario especificado existe <CRLF>
-ERR Usuario desconocido <CRLF>

Cuando el servidor ha confirmado el comando *USER*, el paso siguiente es el empleo del comando *PASS*, acompañado por la *contraseña* del propietario del buzón. Si la *contraseña* es correcta se recibe una respuesta *+OK*, junto con el texto de acompañamiento adecuado y es posible acceder con otros comandos al contenido del buzón. En caso de que se produzca un error, se recibe *–ERR* más un mensaje de error. Se puede intentar de nuevo pero, después de varios intentos fallidos, el servidor cancelará la conexión como medida de seguridad, ya que teme que se trata de algún intento no permitido o malicioso.

Si el servidor ha aceptado la *contraseña* y ha respondido de forma positiva, se accede a la *segunda fase* de una conexión *POP3*, o fase de *transacción* (*transaction state*). Durante esta fase, el servidor asegura el buzón

en cuestión, para que no puedan modificarse o eliminarse mensajes desde otro lugar o desde otra sesión.

Ver y cargar mensajes (Fase de transacción)

En la fase de transacción, el cliente dispone de toda una serie de comandos para traer los mensajes existentes en su buzón desde el servidor o para obtener de momento una visión global de todo el contenido del buzón. Además, también pueden eliminarse mensajes una vez leídos o incluso antes de bajarlos.

Dos de estos comandos, *STAT* y *LIST*, sirven para obtener información global acerca de los mensajes que esperan, mientras que con *RETR* se pueden traer mensajes del buzón. Veamos estos comandos más detalladamente.

STAT, LIST (Información acerca de los mensajes en espera)

Con *STAT*, el software de cliente obtiene una visión global sobre el número de mensajes en espera y su tamaño total. Puede ser una información muy útil ya que, por supuesto, en el disco duro del cliente tiene que haber suficiente espacio no sólo para recibir los nuevos mensajes, sino también para poder guardarlos. Como respuesta a *STAT* se obtiene una línea *+OK* y, después del *+OK*, consta como primer parámetro el *número de mensajes* y después, como segundo parámetro, su *tamaño total* en bytes. Ambas indicaciones están, como siempre, en formato *ASCII* tal y como muestra el siguiente extracto de una comunicación entre cliente y servidor. En esta caso, hay 5 mensajes en el buzón abierto, con un tamaño total de 1,284 bytes.

Cliente: STAT <CRLF>

Server: +OK 5 1284<CRLF>

Server: 1 420<CRLF>

Server: 2 64377<CRLF>

Server: 3 230 <CRLF>

Server: 4 512 <CRLF>

Server: 5 1067 <CRLF>

Server: . <CRLF>

A pesar de que el servidor ya ofrece en la respuesta *+OK* la información sobre el número de mensajes en espera, esta información no suele ser tan precisa en las líneas que le siguen a continuación ya que el texto no está estandarizado. Pero, de alguna manera el software del cliente tiene que poder reconocer que la lista ha finalizado; por ello el servidor envía al final una línea, que sólo contiene *un punto* con el siguiente salto de línea, de manera idéntica a como lo hace el protocolo *SMTP* durante la transmisión de respuestas de varías líneas. De este modo, el protocolo *POP3* recurre también a este procedimiento y no sólo lo hace con el comando *LIST*, sino que también lo empleará con otros comandos, como veremos a continuación.

Si el cliente indica, después de *LIST*, el parámetro opcional *MSG*, el servidor no enviará una lista completa de todos los mensajes que hay en espera, sino que interpreta el valor contenido en *MSG* como el número del mensaje acerca del cual se debe obtener información. Si el mensaje con el número indicado está disponible, se obtiene en primer lugar una línea *+OK* y, a continuación, una línea con el listado (*Scan Listing)* del mensaje indicado. Si no existe mensaje alguno con ese número, se obtiene una respuesta *–ERR* del servidor. Como se muestra en el siguiente ejemplo:

Cliente: LIST 5 <CRLF> //el usuario tiene 5 mensajes//

Servidor: +OK message avialiable <CRLF> //el servidor responde que esta disponible//

Servidor: 5 1067 <CRLF> //lista el mensaje 5 y el tamaño//

Cliente: LIST 6 <CRLF> //el cliente quiere ver el mensaje 6//

Servidor: -ERR no such message <CRLF> //no existe mensaje 6//

RETR (Traer mensajes)

Una vez se averiguado mediante *LIST*, los números de los mensajes que hay en espera, pueden procederse a traer dichos mensajes, sin importar el orden y varias veces un mensaje. Cada mensaje se solicita individualmente, enviando un comando *RETR* al servidor *POP3* y debe indicarse como parámetro el número del mensaje deseado. Si el mensaje está disponible, el servidor envía en primer lugar una respuesta *+OK* y, a continuación, presenta el contenido del mensaje en las siguientes líneas. De este modo, se obtiene línea a línea la cabecera del mensaje, después la obligada línea de separación y, finalmente, el contenido del mensaje, tal y como el *RFC 822* define el formato de un mensaje. Como se muestra en el siguiente ejemplo:

Cliente: RETR 1

Servidor: +OK 1270 octets

Servidor: From: Víctor Gómez <vgomez@dominio_externo.com>

Servidor: To: administrador@dominio_interno.com.mx

Servidor: Date: Mon, 3 Mar 2001 12:34:10 +0300

Servidor: Subject: Nuevo Proceso Informativo

Servidor: MIME-Version: 1.0

Servidor: Content-Type: test/plain; charset=ISO-8859-1

Servidor: el resto del texto del mensaje

Servidor: .

También en esta caso, el servidor indica el final del contenido del mensaje mediante una línea, que sólo contiene un punto y la combinación de caracteres <CR/LF>. Al igual que en *SMTP*, aquí debe crearse un mecanismo Escape, para que las líneas del mensaje que sólo contengan .<CR/LF> no sean interpretadas por el cliente erróneamente como final del mensaje. *POP3* trata este problema igual que *SMTP*, agregando el servidor simplemente un punto adicional adelante y suprimiendo el cliente el primer punto de cada línea que comience por dos puntos consecutivos.

DELE (Eliminar mensajes)

La transmisión de un mensaje al cliente mediante *RETR* no elimina automáticamente el mensaje del buzón. Mientras el cliente no envíe explícitamente un comando *DELE* para solicitar al servidor que elimine el mensaje, continuara mostrándose en el comando *LIST* y puede volver a ser solicitado mediante *RETR*. Para que el servidor pueda reconocer que mensaje debe eliminarse, tiene que indicarse el número del mensaje después de *DELE*. Como se muestra a continuación:

Cliente: DELE 3 <CRLF>

Servidor: +OK message deleted <CRLF>

Servidor: LIST 3 <CRLF>

Cliente: -ERR message 3 deleted <CRLF>

UPDATE (Fase de actualización)

Pero, en realidad, los mensajes marcados para ser suprimidos no se eliminan hasta llegar a la llamada *fase de actualización*, *UPDATE* de una conexión *POP3* (*UPDATE STATE*) y que es introducida por el cliente al enviar un comando *QUIT*. A la vez que marca el final de una conexión, consigue que el servidor, tras enviar una respuesta *+OK*, cierre la conexión. En la próxima sesión entre el cliente y servidor, los mensajes eliminados ya no estarán disponibles. Como se ve el siguiente ejemplo:

Cliente: *QUIT*<CRLF>

Servidor: *+OK POP3* server terminating connection<CRLF>

Capitulo IV

Requerimientos y desarrollo de un sistema de correo electrónico en una red TCP/IP.

IV.I Introducción

En este capitulo hablaremos de los requerimientos básicos que todo sistema de correo electrónico necesita, para cumplir con un funcionamiento adecuado, principalmente cuando se tiene una red ya establecida y se tienen que analizar varios factores que permitirán hacer la mejor elección del sistema de correo electrónico y de la configuración que se requiera.

Se iniciara con presentar una red que no cuenta con un sistema de correo electrónico, de tal forma que en este punto ser realizara una cuantificación detallada de los requerimientos identificados de esa red (Etapa de Análisis), después la etapa de factibilidad permitirá hacer una estimación inicial de los anchos de banda requeridos y por medio de estos hacer una primera aproximación de los costos, ya teniendo estas dos etapas documentadas se pasara a la etapa de estrategia, donde se obtendrá la Arquitectura de Procesamiento de la información de la organización, la cual incluye la localización del procesamiento y de almacenamiento de la información en relación con la infraestructura de la organización.

En esta primer parte podemos identificar las necesidades reales que los usuarios de una red pueden tener, además del flujo de información que se establece entre ellos, es decir, los mensajes que viajen por la red pueden llevar un destino en común o pasar por un punto de la red que se vuelve critico, ya sea por el tipo de mensaje, tamaño o cantidad de información que un dispositivo de la red tenga que procesar.

Partiendo del hecho que la red ya fue analizada, y se llegaron a ciertas conclusiones del estado actual de la red, se pasara a la segunda parte de este capitulo que se enfoca al desarrollo del sistema de correo electrónico, donde identificamos tres etapas principalmente que son: Diseño, Implementación y Administración.

La etapa de diseño tendrá por objetivo lograr alcanzar el mejor desempeño con un costo/beneficio obtenido del sistema de correo electrónico. La siguiente etapa de Implementación corresponderá con los planes de trabajo, instalaciones y modificaciones que sean necesarios para cumplir con esta etapa y por ultimo la etapa de Administración, mostrara las tareas mínimas

necesarias para tener en funcionamiento el sistema de correo electrónico implementado en una red.

IV.II Análisis

En esta sección se presentara la infraestructura que analizaremos, esto es, tomaremos un caso real de una empresa de tamaño mediano como muchas que existen en México que requiere tener un sistema de correo electrónico, de tal forma que se pueda identificar la información necesaria de la red de esta empresa.

Presentación

La empresa que se esta analizando, se ha desarrollado en los últimos años, teniendo un rápido crecimiento, y se ha colocado en su ramo como la empresa líder y constantemente busca de nuevas tecnologías para ampliar su desarrollo.

Panorama

El director de la empresa esta buscando una solución a las necesidades de comunicación entre los diferentes departamentos y los empleados, también requiere comunicación con otras compañías a través de Internet usando un sistema de correo electrónico.

Red actual

La empresa, tiene una red WAN porque conecta sus 3 diferentes oficinas (redes LAN), que se encuentran una en la ciudad de México y las otras 2 en otras localidades. La oficina principal tiene una red LAN con 100 usuarios, y las otras dos oficinas tienen una red LAN de 50 usuarios cada una.

Objetivos de la empresa

- Como objetivo principal es tener un sistema de correo electrónico, que permita una eficiente comunicación de los usuarios a través de este, usando la infraestructura con la que cuenta la empresa.

- Mejorar la comunicación con clientes y socios.

- Ahorrar costos de llamadas de larga distancia y de envío de documentos de forma tradicional como es el caso del fax.

Documentar la red actual

En esta parte se documentara la información técnica que nos ayude a entender la red actual y a identificar rápidamente los elementos que conforma dicha red.

La primera actividad a desarrollar será identificar las aplicaciones que en la red se estén utilizando, para lo cual se obtendrá la información y se vaciara en la siguiente tabla.

ítem	Nombre de Aplicación	Tipo de Aplicación	Número de Usuarios	Número de Servidores	Comentario
1	Inventarios	Base de datos	10	1	
2	Ventas	Base de datos	10	1	
3	Transferencias	FTP	5	1	
4					

Tabla 6. Identificación de Aplicaciones

Para usar la anterior tabla se necesita la siguiente información:

- En el campo "Nombre de Aplicación", se debe anotar el nombre de cada aplicación que este funcionando sobre la red.
- En el campo "Tipo de Aplicación", se escribe la información que ayude a definir el tipo de aplicación que se trate, por ejemplo, base de datos, multimedia, contabilidad, etc.
- El campo "Numero de usuarios", se llena con la cantidad de usuarios que tienen acceso a cada aplicación.
- En el campo "Numero de Servidores", se anota la cantidad de servidores que provean cada aplicación.
- En el campo "Comentario", se escribe cualquier información relevante acerca de cada una de las aplicaciones listadas.

Como siguiente tarea, se listaran los protocolos en uso de la red actual de la empresa, como se muestra en la tabla 7.

	Nombre del Protocolo	Tipo de Protocolo	Numero de usuarios	Numero de Servidores	Comentario
1	TCP/IP	LAN/WAN	100	-	
2	NetBEUI/NetBIOS	LAN	100	3	
3	IPX	LAN	150	3	
4					

Tabla 7. Protocolos

Para llenar la anterior tabla, utilizamos las siguientes instrucciones:

- El campo "Nombre de Protocolo", se llena con el nombre de cada uno de los protocolos utilizados en la red.
- En el campo "Tipo de Protocolo", se escribe la información que nos ayude a identificar el protocolo, por ejemplo, protocolo LAN, WAN, protocolo de capa de sesión, protocolo cliente/servidor, etc.
- En el campo "Numero de usuarios", se anota la cantidad de usuarios correspondiente a cada protocolo, independientemente si un usuario utiliza dos o más protocolos.
- En el campo "Numero de Servidores", se llena con la cantidad de servidores que usan cada uno de los protocolos listados.
- En el campo "Comentario", se escribe cualquier información relevante acerca de cada protocolo listado, por ejemplo, el tipo de escalabilidad.

La siguiente actividad será Documentar la topología de red y sus dispositivos, además del esquema de direcciones que utiliza la actual red, siguiendo las instrucciones descritas a continuación:

- ***Topología de red y dispositivos:*** dibujar la topología de la red, incluyendo el tipo y velocidad de cada segmento, además de incluir los nombres de cada dispositivo, como se muestra en la figura 65.
- ***Esquema de direcciones:*** documentar el actual esquema de direcciones, por ejemplo las direcciones IP de cada segmento y si existe algún criterio para asignar direcciones a estaciones de trabajo, equipos y servidores, como se muestra en la figura 65.

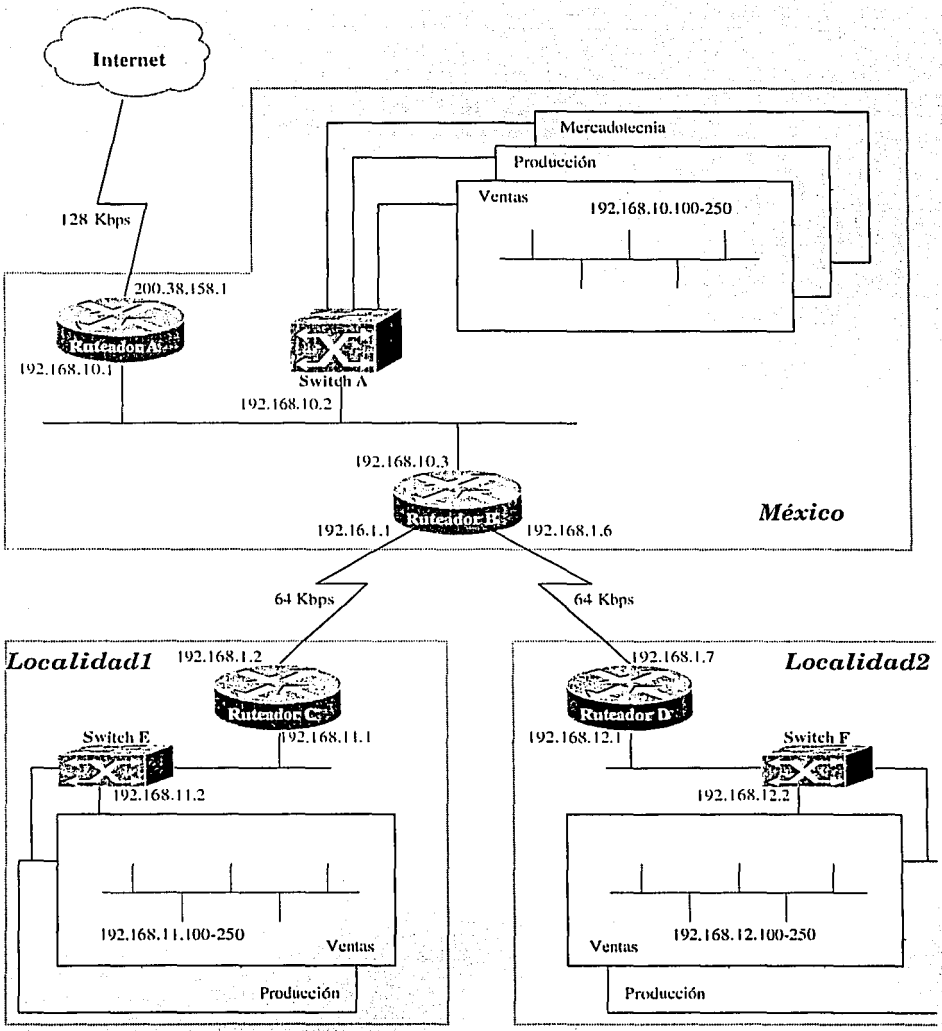

Figura 65. Topología de Red y dispositivos.

Después de completar las anteriores actividades podemos tener nuestro análisis de la red, lo cual, nos permite identificar los puntos críticos y entender la red actual.

IV.III Factibilidad

En esta etapa, a partir de los requerimientos cualitativos de comunicación identificados en la etapa de Análisis, se hace una cuantificación inicial de estos, lo cual permitirá hacer una estimación inicial de los anchos de banda requeridos, y por medio de estos hacer una primera aproximación de los costos.

Los objetivos de esta etapa son cuantificar el gasto de recursos en el desarrollo de la red, y examinar la factibilidad técnica, organizacional y financiera.

La factibilidad organizacional determina los requerimientos asociados con la implementación y la administración de los recursos de la red, lo que incluye los procedimientos de administración, las herramientas y los conocimientos necesarios para manejar la red a diario.

Para nuestro caso la organización se encuentra de esta manera:

- De acuerdo al organigrama de la figura 66 no se encontró ningún inconveniente de la organización para la implementacion del sistema de correo electrónico.

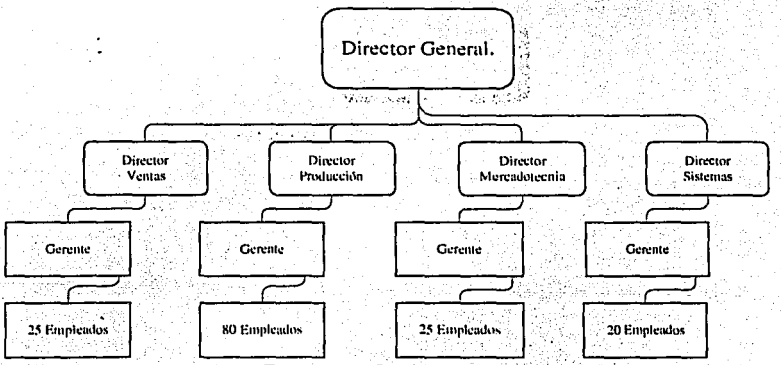

Figura 66. Organigrama

- En cada red LAN existe un Administrador de red y 5 ingenieros, que tienen los conocimientos para implementar nuevos sistemas, como este de correo electrónico, por consiguiente no es necesario aumentar el personal para este nuevo sistema.
- Se definieron los procedimientos de cotizaciones y adquisiciones de equipos, hardware, software, accesorios y capacitación que se requieren para la implementación del sistema de correo electrónico.

La Factibilidad técnica involucra estimar el tráfico de la red y evaluar las opciones existentes a la luz de estos estimativos. Las fuentes importantes para realizar estos estimativos son:

- Los usuarios: número de usuarios y el número de transacciones por cada uno.
- Por cada departamento existe un Director y Gerente, que tendrán acceso al sistema de correo electrónico.
- Los departamentos de Ventas y Mercadotecnia determinaron que solo 25 usuarios de cada área tendrán acceso al correo electrónico.

Para realizar la estimación del tráfico se parte de los siguientes supuestos:

- Por cada localidad se tendría un numero máximo de usuarios, distribuidos de la siguiente manera: para la localidad de México son 100 usuarios, para las otras dos localidades son 50 usuarios, en total son 200 usuarios de correo electrónico.
- Se permitirá enviar documentos anexos en el correo electrónico hasta un máximo de 2000 KB.
- Se estima un promedio de 15 mensajes por usuario diario.
- El flujo de información debe de ser de cada localidad hacia México y de México hacia Internet.
- No todos los usuarios se les permitirá enviar correos por Internet, estos solo podrán enviar mensajes por la red interna, con el fin de reducir la cantidad de mensajes y evitar saturación del enlace hacia Internet.

Estimación del tráfico de acuerdo a los nuevos requerimientos de la red:

Para determinar el tráfico, se han realizado entrevistas con los usuarios, lo que ha permitido establecer un promedio de uso del correo electrónico de 15 mensajes diarios, durante las horas hábiles (8 horas de trabajo al día).

De acuerdo a lo anterior se realizara el calculo por cada uno de los circuitos, por lo que tenemos lo siguiente:

Circuito 1.-

Localidad1 – México:

50 usuarios X 15 mensajes X día = 750 mensajes en 8 horas

Necesitamos saber cuantos mensajes por segundo se estarían enviando por lo que hacemos el siguiente calculo:

750 mensajes / 8 horas X 3600 segundos = 0.02604 mensajes por segundo.

Considerando que el tamaño mínimo de un mensaje es de 1 KByte

1Kbyte=1024 bytes
1Byte= 8 bits

0.02604 * 1 KByte = 0.02604 * 1024 * 8 = ***213.33 bits por segundo.***

Entonces ***213.33 bps*** es el ancho de banda mínimo necesario para soportar la cantidad de mensajes de tamaño de 1Kbyte que de acuerdo al promedio de los usuarios se requiere.

Considerando ahora que el tamaño máximo permitido de los mensajes sea 2000 KBytes.

0.02604 * 2000 KByte = 0.2604 * 2000 *1024 * 8 = ***426,667 bps o 426.667 Kbps.***

Ahora ***426,667 bps*** es el ancho de banda mínimo necesario para soportar la cantidad de mensajes considerando el tamaño máximo de 2000 KBytes.

Recordando que este circuito tiene un enlace de 64 Kbps, se pueden iniciar operaciones con este enlace, ya que cubre el ancho de banda mínimo para iniciar operaciones, pero se recomienda ampliar en un futuro el enlace a 512 Kbps de acuerdo al incremento del uso del correo electrónico.

Circuito 2.-

Localidad2 – México:

50 usuarios X 15 mensajes X día = 750 mensajes en 8 horas

Necesitamos saber cuantos mensajes por segundo se estarían enviando por lo que hacemos el siguiente calculo:

750 mensajes / 8 horas X 3600 segundos = 0.02604 mensajes por segundo.

Considerando que el tamaño mínimo de un mensaje es de 1 KByte

1Kbyte=1024 bytes
1Byte= 8 bits

0.02604 * 1 KByte = 0.02604 * 1024 * 8 = ***213.33 bits por segundo.***

Entonces ***213.33 bps*** es el ancho de banda mínimo necesario para soportar la cantidad de mensajes de tamaño de 1Kbyte que de acuerdo al promedio de los usuarios se requiere.

Considerando ahora que el tamaño máximo permitido de los mensajes sea 2000 Kbytes.

0.02604 * 2000 Kbyte = 0.2604 * 2000 *1024 * 8 = ***426,667 bps o 426.667 Kbps.***

Ahora ***426,667 bps*** es el ancho de banda mínimo necesario para soportar la cantidad de mensajes considerando el tamaño máximo de 2000 KBytes.

Recordando que este circuito tiene un enlace de 64 Kbps, se pueden iniciar operaciones con este enlace, ya que cubre el ancho de banda mínimo para iniciar operaciones, pero se recomienda ampliar en un futuro el enlace a 512 Kbps de acuerdo al incremento del uso del correo electrónico.

Circuito 3.-

México – Internet:

100 usuarios X 15 mensajes X día = 1500 mensajes en 8 horas

Necesitamos saber cuantos mensajes por segundo se estarían enviando por lo que hacemos el siguiente calculo:

1500 mensajes / 8 horas X 3600 segundos = 0.05208 mensajes por segundo.

Considerando que el tamaño mínimo de un mensaje es de 1 KByte

1Kbyte=1024 bytes
1Byte= 8 bits

0.05208 * 1 KByte = 0.05208 * 1024 * 8 = ***427.67 bits por segundo.***

Entonces ***427.67 bps*** es el ancho de banda mínimo necesario para soportar la cantidad de mensajes de tamaño de 1Kbyte que de acuerdo al promedio de los usuarios se requiere.

Considerando ahora que el tamaño máximo permitido de los mensajes sea 2000 KBytes.

0.05208 * 2000 KByte = 0.05208 * 2000 *1024 * 8 = ***853,333 bps o 853.333 Kbps.***

Ahora ***853,333 bps*** es el ancho de banda mínimo necesario para soportar la cantidad de mensajes considerando el tamaño máximo de 2000 KBytes.

Recordando que este circuito tiene un enlace de 128 Kbps, se pueden iniciar operaciones con este enlace, ya que cubre el ancho de banda mínimo para iniciar operaciones, pero se recomienda ampliar en un futuro el enlace a 1.0 Mbps de acuerdo al incremento del uso del correo electrónico.

La factibilidad financiera es uno de los principales objetivos para reducir el costo de las comunicaciones, por que el aspecto financiero es de gran importancia.

Para comenzar se determinaran los costos totales y la inversión inicial, cuya base son los estudios realizados anteriormente, ya que tanto los costos como la inversión inicial dependen de la tecnología seleccionada.

De acuerdo con las consultas hechas sobre cada equipo y sistema de correo electrónico que ofrecen los proveedores de los bienes y servicios que se desean adquirir, tenemos los siguientes costos:

Cantidad	Descripción	Costo Unitario M.N.	Costo Total M.N.	Comentario
1	Software de correo electrónico con licencia para 200 usuarios y 3 años de actualizaciones	$30,000	$30,000	
3	Servidor con las siguientes características: CPU P-IV a 900 MHz, 512 MB RAM, arreglo de discos duros con capacidad de 10 discos de 36 GB, tarjeta red 10/100 Mbps, Monitor 17", Sistema Operativo Windows NT.	$25,000	$75,000	
1	Servicio de capacitación de uso del correo electrónico para 200 usuarios	$25,000	$25,000	
2	Ampliación de enlace a 512 Kbps	$30,000	$60,000	
1	Ampliación de enlace a 1.0 Mbps	$45,000	$45,000	
1	Servicio de Acondicionamiento de Servidores en Cuarto de Telecomunicaciones	$15,000	$15,000	
1	Adquisición de nombre de Domino de la organización en Internet.	$2,000	$2,000	
1	Gastos varios e imprevistos del 20% del subtotal	$50,400	$50,400	
		Total	$302,400	

Como inversión total inicial se tendría la cantidad de $ 302,400 M.N., pero debemos dividir esta en dos: la inversión fija y la diferida.

La inversión fija es aquella que se tiene que pagar para iniciar el proyecto como es el software de correo electrónico, los servidores, etc., y la inversión diferida es aquella que se tiene proyecta para un corto, mediano o largo plazo, como son los costos de ampliación de los enlaces.

Por consiguiente y para tener más en claro cual será el desembolso monetario para este proyecto, se desglosa la inversión total inicial de la siguiente manera:

Inversión *inicial fija*:	$ 197,400 M.N.
Inversión *inicial diferida*:	$ 105,000 M.N.
Inversión ***inicial Total***:	**$ 302,400 M.N.**

De esta forma se pueden tener previstos los montos de inversión necesarios a presupuestar por la organización y cubrir el aspecto monetario de la inversión necesario de este proyecto.

IV.IV Seguridad

Los mecanismos de seguridad deben "insertarse" dentro del marco de las actuales redes de área local, debiendo satisfacer lo siguientes requisitos:

- Proporcionar servicios criptográficos de seguridad
- No interferir con el funcionamiento de sistemas no protegidos
- Soportar modos de operación transparentes en los sistemas protegidos
- Proporcionar comunicación opcional con sistemas no protegidos

La arquitectura de seguridad del modelo de referencia para interconexión de sistemas abiertos ISO 7498/2 define cinco servicios de seguridad: autenticación, control de acceso, confidencialidad de los datos, integridad de los datos y no-repudiación. Estos servicios se proporcionan por un determinado nivel (N) a través de la apropiada aplicación de uno o más mecanismos de seguridad. Se identifican ocho mecanismos de seguridad específicos: cifrado, firma digital, control de acceso, integridad de los datos, intercambio de autenticación, protección del tráfico, control de encaminamiento y notarización; y cinco mecanismo de seguridad generales: funcionalidad fiable, etiquetas de seguridad, detección de eventos, auditoría de seguridad y recuperación de la seguridad.

Como se observa la seguridad actualmente en las redes y sistemas es de gran importancia de tal forma que se deben implementar o por lo menos señalar las políticas, procedimientos o reglas a seguir en el buen uso de las redes y sistemas, ya que de este correcto uso, se puede tener un sistema de correo electrónico confiable y seguro, que cumpla con los preceptos antes mencionados.

Las siguientes políticas son una guía de lo que se debe hacer para mantener un sistema seguro, por lo que se describen las más importantes.

Política de Passwords:

La identificación y autenticación (I&A) es el proceso de reconocer y verificar a los usuarios y procesos válidos. La información de I&A es generalmente utilizada para determinar que recursos del sistema pueden accesar un proceso o un usuario. La determinación de quién puede accesar que recurso es decisión de cada director de área y debe ser notificada al administrador de la red para que se proporcionen los privilegios adecuados para accesar los recursos deseados.

Para lograr este propósito, las claves de usuario, así como sus Passwords deben cumplir con los siguientes requisitos:

- Las claves de usuario y los passwords son únicos para cada persona autorizada a accesar el sistema.
- Deben ser alfanuméricos de 8 caracteres, sin utilizar nombres o palabras comunes y fáciles de adivinar. Debe haber listas controladas por el sistema de reglas para passwords proscritas y pruebas periódicas (por ejemplo, Secuencias de letras y números, repetición de caracteres, iniciales, palabras y nombres comunes) para poder identificar la posible debilidad de un password.
- Los passwords deben mantenerse privados, no deben compartirse, codificados en programas o escritos.
- Deben cambiarse cada 90 días (o cuando sea necesario).
- Deben bloquearse a los 3 intentos de acceso erróneo. Todos los intentos fallidos de acceso de un usuario serán registrados en una bitácora de auditoría para su posterior revisión, y si es necesario para tomar acción.
- En caso de tener un password violado se debe acudir al administrador de la red para que sea desbloqueado.
- La única persona que puede pedir que se desbloquee un password es el dueño del mismo.
- Las sesiones inactivas deben ser suspendidas después de 30 minutos (o cualquier otro periodo de tiempo según se considere adecuado) y se requiere que la autenticación del usuario sea hecha nuevamente.
- Los usuarios y las claves van a ser suspendidos después de un periodo

de tiempo de no ser utilizados.

Política de Respaldos

- Los respaldos se deben hacer de acuerdo a la importancia de la información que contenga cada servidor, mientras más importante sea la información, más seguido deberá de programarse el respaldo. Se recomienda comenzar con respaldos semanales para los servidores con la información más importante y mensual para aquellos que no tengan información tan importante.

- La frecuencia de los respaldos puede variar, y en algunos casos puede llegar a ser más frecuente que lo mencionado aquí (como sería el caso de hacer respaldos diarios para información de bases de datos con datos muy importantes para la operación diaria).

Los respaldos deben guardarse en lugar seguro y con acceso restringido, preferentemente en un lugar alterno al centro de datos.

Política de Seguridad Física

- El acceso al centro de trabajo debe estar restringido.

- El acceso al centro de datos debe estar restringido a aquellas personas encargadas de dar servicio y mantenimiento a los equipos.

- El acceso al centro de datos debe ser controlado, llevando registro de quién entra, y la hora de entrada y de salida.

- Las personas que manejen información confidencial deben dejar sus lugares limpios y la información en lugar seguro (preferentemente bajo llave) y sus computadoras o terminales bloqueadas o apagadas para evitar el acceso a información confidencial.

- Al final del día los escritorios deberán quedar limpios, esto es sin ningún papel que contenga información confidencial sobre ellos, las computadoras o terminales apagadas y los cajones cerrados con llave.

Política de uso de Internet.

El acceso a Internet es una fuente muy valiosa y útil de información, pero a su vez es una puerta muy utilizada para tener accesos ilegales a las redes que no están bien protegidas. Las personas que hacen accesos no

autorizados pueden estar motivados por varias cosas, bien sea por curiosidad o bien por malicia con el fin de realizar algún daño (desde cambiar la página principal de un sitio por otra con algún mensaje) hasta el realizar un ataque para deshabilitar el servicio de la red sujeta al ataque. Aunque en una minoría también hay quienes lo hacen con fines de lucro, buscando obtener alguna ganancia de la información que puedan obtener de su acceso.

Es por eso que es importante el tener políticas bien definidas conocidas por todos aquellos con acceso a Internet para poder establecer las responsabilidades, y la forma adecuada de actuar cuando se tenga acceso a este medio de información.

Con tal fin se tiene las siguientes políticas.

- Los sistemas y redes de la red son proporcionados para uso en los asuntos de la Organización solamente. Un uso personal, ocasional y razonable de los mismos es permitido siempre y cuando sea fuera de horario de trabajo. Cualquier uso que se pueda considerar como ilegal, ofensivo, intimidatorio, en violación directa a políticas de la Organización u otras compañías, o cualquier uso que pueda reflejar en forma adversa a la Organización puede ser base para una acción disciplinaria que puede ser desde una llamada de atención hasta la terminación del contrato o acción legal en contra del responsable de la falta.

- Los passwords de acceso a los recursos de la red son proporcionados con el fin de proteger información sensitiva y mensajes de usos no autorizados o que sean vistos por personas no autorizadas.

- La conexión a Internet es un recurso de la Organización. Todas las actividades en la red pueden ser sujetas de monitoreo, registro y auditoria periódicas para asegurar que están funcionando en forma apropiada y para proteger a la Organización de uso no autorizado. Además la Organización puede accesar cualquier cuenta o computadora de los empleados así como su comunicación.

- Los administradores de la red son responsables de implantar la seguridad de la red. Si hay más de un administrador de red, es importante que los roles sean coordinados.

- La Organización debe nombrar específicamente a una o más personas o puesto responsable de la seguridad diaria de la conexión a Internet. Esta responsabilidad puede ser asignada al administrador de la red, pero también puede ser otorgada a un área separada y especializada. En este caso es imperativo que el administrador de la red y el administrador de la Seguridad se coordinen cuidadosamente y que el

administrador de Seguridad tenga un muy buen conocimiento de protocolos de Internet.

- Herramientas de Hardware o Software tales como firewall (equipo de seguridad) o filtros serán utilizados para bloquear el acceso a todos los sitios de Internet, excepto aquellos que sean aprobados por la Dirección General.

- El administrador de la red puede suspender temporalmente los privilegios de acceso a cualquier usuario si se considera necesario para mantener la integridad de la red.

- El acceso a las paginas de Internet queda restringido por los filtros puestos por las herramientas destinadas para ello y solamente por usuarios autorizados para hacer uso de este recurso informativo.

- El acceso a Internet se debe utilizar únicamente como herramienta de trabajo para complementar las actividades diarias con información actualizada.

- No se permite el uso de los recursos de Internet para realizar actividades ilegales o no permitidas (hacking, spam, etc.) No se puede utilizar el acceso a Internet con propósitos comerciales, ni para accesar sitios obscenos o pornográficos, y no se puede utilizar o accesar información que pueda considerarse como inapropiada.

- Todos los accesos a sitios no autorizados por la Organización serán auditados, registrados y notificados a los directores de cada área.

Política de Grupos de trabajo.

- Los grupos de trabajo deben hacerse en forma adecuada, para que todos aquellos usuarios que vayan a estar dentro de ellos puedan accesar los recursos y la información adecuada para el desarrollo de su trabajo diario.

- Los grupos de trabajo deben estar diferenciados en base en las funciones genéricas que desempeñen los empleados, por ejemplo por área y después por funciones. En todo caso los grupos de trabajo deben de estar formados de tal manera que los usuarios que estén dentro de ellos tengan los privilegios necesarios para poder trabajar, pero sin permitirle el acceso a los recursos que no debe de ver por seguridad.

- Se debe tener registro de qué usuario tiene acceso a qué recursos, así como los accesos extras que se den para poder hacer auditorías de las transacciones que haga un usuario en la red.

Política de uso del correo electrónico:

El correo electrónico, al igual que el teléfono o el fax, es muy difícil de controlar para uso personal. Es por ello que se permitirá un uso limitado y razonable del correo electrónico para uso personal siempre y cuando no afecte a la Organización.

Para lograr esto se tienen estas políticas.

- El correo electrónico es provisto por la Organización a los empleados que lo requieran para conducir los asuntos de la Organización. No se permite el uso del correo electrónico para negocios personales o para actividades que quiten el tiempo a otras personas.

- La Organización se reserva el derecho de accesar el correo electrónico de los empleados si se tienen motivos justificados para hacerlo. El contenido del correo electrónico no va a ser accesado o revelado a menos que sea por motivos de seguridad o requerido por la ley.

- Los usuarios no deben permitir que nadie envíe correo electrónico utilizando sus cuentas.

- Los directorios de correo electrónico internos no deben hacerse públicos.

- Si información confidencial es enviada por correo electrónico, esta debe ser encriptada para que solo pueda ser leída por el destinatario, utilizando software y algoritmos aprobados por la Dirección General.

- Ningún visitante, contratista o empleados eventuales pueden hacer uso del correo electrónico de la Organización.

- Los mensajes entrantes serán revisados contra virus o contenido malicioso.

- Los servidores de correo electrónico deben ser configurados para rechazar correo remitido por sistemas que no sean confiables.

- Las bitácoras de los servidores de correo serán revisadas para detectar versiones no aprobadas de clientes de correo para notificar al administrador.

En términos generales con estas políticas se incrementa la seguridad de

la red y del sistema de correo electrónico, permitiendo optimizar los recursos con los que cuenta la Organización. De hecho se pueden o deben diseñar políticas a la medida de cada necesidad para hacer de los sistemas y redes una herramienta útil, para que no suceda al contrario si por el mal uso de cierto sistema o recurso se provoque congestionamiento de trafico en la red, falla en algún sistema, como el correo electrónico o la total perdida de los servicios de la red.

IV.V Desarrollo del sistema de correo electrónico

IV.V.1 Diseño

En esta fase se obtiene la configuración del sistema de correo electrónico, a partir de los resultados cuantitativos obtenidos de las fases anteriores. Se establecen datos tales como los enlaces a emplear y una estimación del desempeño de la red.

Esta fase consta de los siguientes pasos:

1. Elaboración de un modelo del sistema de correo electrónico.

2. Evaluar el modelo para varias combinaciones de comunicación y formas de acceso, empleando los niveles de servicio como base para los objetivos.

3. Seleccionar el modelo más deseable entre los considerados, tomando en cuenta los niveles de servicio, requerimientos de entrenamiento y administración, requerimientos de migración, requerimientos de seguridad y control.

4. Obtener la aprobación del Director de la Organización

Los factores que deben ser tomados en cuenta, son el tiempo de respuesta y el costo. Otros parámetros de diseño son la confiabilidad, disponibilidad, seguridad y control.

Las decisiones más importantes que deben ser tomadas al diseñar son:

- El tipo, localización y capacidad de los servicios y de los enlaces de transmisión que son empleados para construir la topología de la red

- El tipo, localización y capacidad de los enlaces de transmisión que conectaran los equipos terminales (los equipos clientes) a los nodos de entrada a la red.

El objetivo de la fase de diseño es obtener un sistema de correo electrónico que cumpla con los requerimientos de nivel de servicio con una inversión de capital y costos de operación aceptables.

Como modelo se propone el siguiente:

De acuerdo a la figura 65, observamos las siguientes características de este diseño:

- Hay un servidor de correo electrónico por cada localidad: ***Servidor MX***, ***Servidor LOC1***, ***Servidor LOC2***, donde se almacenara el correo electrónico de los usuarios.

- El tráfico generado será principalmente en cada red local, haciendo que cada uno de los servidores proporcione el servicio a los usuarios de cada red local.

- El intercambio de correo electrónico entre servidores se hará por medio del protocolo ***SMTP***, ***protocolo de transferencia de correo simple.***

- Los usuarios obtendrán su correo electrónico de cada servidor por medio del protocolo **POP 3**, ***protocolo de oficina postal versión 3.***

- Unicamente el servidor de la localidad de México, el ***Servidor MX***, intercambiara correo electrónico hacia el exterior, es decir, hacia **Internet**, de tal forma que este será el único punto de contacto al exterior para intercambiar correo electrónico con proveedores, clientes o socios de la organización, lo que permite aumentar la seguridad del sistema de correo.

- En caso de que algún servidor de correo electrónico presente alguna falla, sé deberá habilitar a cualquiera de los otros dos servidores para soportar el servicio y continuar con la misma funcionalidad del sistema de correo electrónico.

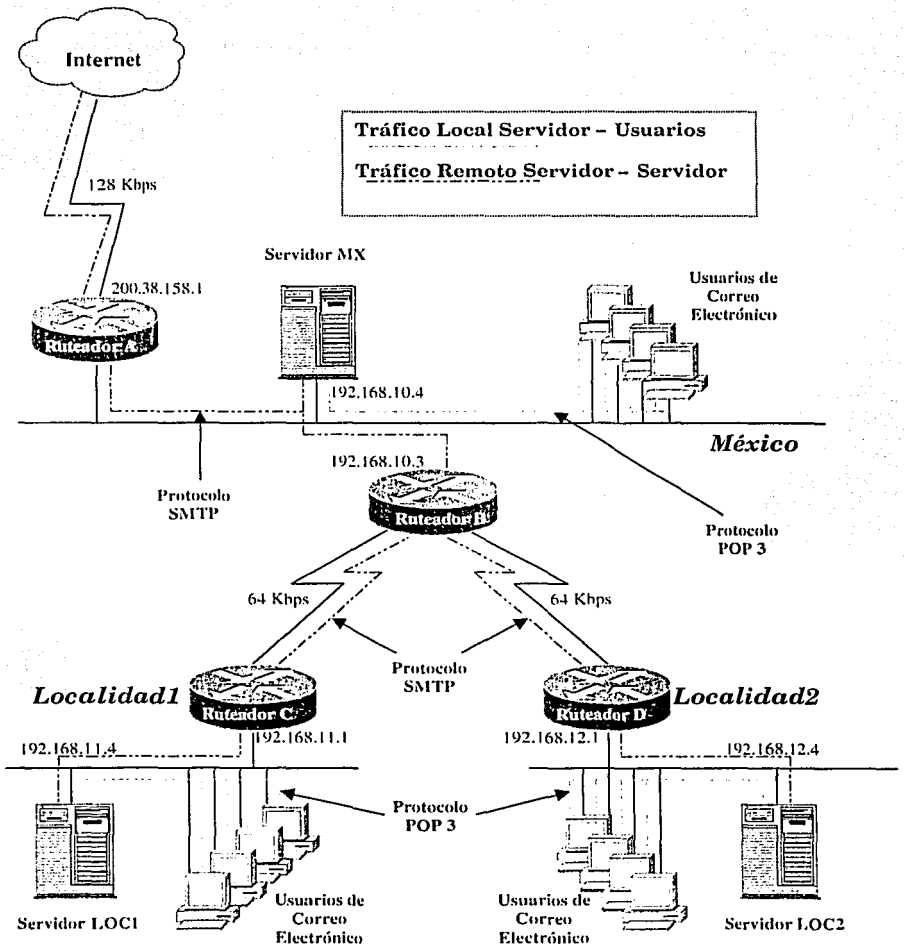

Figura 65. Modelo del Sistema de Correo Electrónico.

Una combinación que se podría tener del modelo es que el sistema de correo electrónico sea únicamente con un servidor central ubicado en la localidad de México, y no uno en cada localidad, la combinación de esta propuesta representa un mayor tiempo de respuesta para los usuarios de las localidades 1 y 2, que tendrían que consultar sus buzones de correo electrónico en el servidor central, además de ser un punto de mayor vulnerabilidad del sistema, ya que en caso de falla no existiría otro servidor que tomara la función de este, por lo que tener un modelo con estas características representaría un riesgo mayor de operabilidad y no cumpliría con el nivel de servicio en cuanto al tiempo de respuesta esperado por los usuarios del sistema de correo electrónico. Por lo anterior se selecciono el modelo inicial.

Para tener la aprobación del Director General de la organización se presento el modelo inicial, explicándole las características técnicas y la factibilidad financiera.

IV.V.2 Implementación

En esta fase se ejecuta la estrategia de comunicación, realizando una planeación del desarrollo de la red de comunicaciones ayudado por un cronograma.

El termino implementación se refiere a la adquisición, instalación y operación satisfactoria de la nueva infraestructura creada por el sistema de correo electrónico.

Los resultados que se deben obtener de esta fase son:

- Un *plan de implementación*, identificando que tareas deben llevarse a cabo y cuando (cronograma).
- Un *plan de administración*, identificando la estructura organizacional, habilidades y recursos requeridos para implementar y administrar la red.
- Un *plan de contingencia*, identificando las fuentes potenciales de fallas y acciones a tomar para restaurar el servicio de correo electrónico.

Plan de Implementación.

Actividad	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7
Cotización de equipos, software de correo electrónico.	✓						
Adquisición de equipos, software de correo electrónico		✓	✓				
Instalación de equipos y software de correo electrónico.				✓			
Pruebas del diseño y puesta a punto del sistema de correo electrónico.					✓		
Capacitación del personal administrador del sistema de correo electrónico.						✓	
Capacitación de los usuarios del sistema de correo electrónico.							✓

Tabla 7. Cronograma de Actividades.

Las tareas o actividades que se deben realizar por semana se muestran en el Cronograma de la tabla 7, donde la duración será de 7 semanas.

Plan de administración

Este plan muestra como los recursos materiales y humanos se coordinaran para llevar a cabo la implementación, como tal el plan de administración se propone de la siguiente manera:

1. Se designara un Líder del proyecto, cuya principal función es mantener el control desde el inicio hasta el final de la implementación del sistema de correo electrónico.
2. Por cada actividad deberá existir un responsable para llevar a buen termino dicha actividad.
3. La revisión del hardware y el software de este proyecto no deberá pasar del tiempo estipulado por los proveedores para en su caso hacer

las devoluciones correspondientes.

4. Toda la documentación financiera y técnica de este proyecto deberá archivarse en una carpeta especial que incluya los documentos, manuales, facturas y memorias técnicas del proyecto, para su consulta en cualquier momento.

Plan de contingencia

Este plan permitirá establecer los procedimientos necesarios para tomar las acciones correspondientes en caso de que algún tipo de falla del sistema de correo electrónico se presente, de esta manera el *plan de contingencia* propuesto es el siguiente:

1. Identificación de diferentes tipos de fallas y prioridades, por ejemplo:

   - Un usuario no puede enviar y recibir correo electrónico, prioridad baja
   - Varios usuarios no pueden enviar y recibir correo electrónico, prioridad media
   - Todos los usuarios no pueden enviar y recibir correo electrónico, prioridad alta.

2. Asignación de la falla al personal correspondiente para su resolución de acuerdo al siguiente ejemplo:

   - Falla de prioridad baja, responsable: Ingeniero de Soporte telefónico.
   - Falla de prioridad media, responsable: Ingeniero de Soporte en sitio.
   - Falla de prioridad alta, responsable: Ingeniero especialista en correo electrónico.

3. Recuperación de mensajes de correo electrónico y bloqueo de mensajes sospechos de virus o actividad maliciosa, utilizar las siguientes herramientas:

   - Software de respaldo para la recuperación de mensajes.
   - Software de inspección de virus para correo electrónico.
   - Software de bloqueo de mensajes en cadena.

IV.V.3 Administración

En esta fase se realiza la definición de estándares, herramientas y procedimientos que aseguren una correcta utilización y mantenimiento del sistema de correo electrónico.

El objetivo de esta fase es proporcionar herramientas que permitan tener todos los elementos de la red bajo control.

La administración de la red se puede definir como el conjunto de actividades requeridas para planear, instalar, supervisar y mantener todos los componentes del sistema de correo electrónico con el fin de lograr los niveles de servicio requerido de manera confiable, a un costo aceptable.

Las funciones del administrador del sistema de correo electrónico pueden dividirse en dos grupos:

1. Funciones diarias: están relacionadas con el control diario del sistema de correo electrónico, incluyendo:

   - Supervisión y mantenimiento del nivel del servicio
   - Manejo de las fallas (identificación, diagnostico y reparación de las fallas en los componentes del sistema)
   - Administración de los cambios en el sistema de correo electrónico (esta actividad incluye la administración de inventarios de todos los componentes del sistema y de la red, además de la configuración de ambos. También comprende control de las adiciones, movimientos y otros cambios en los sistemas de los usuarios).
   - Supervisión del desempeño del sistema de correo electrónico (esta función esta relacionada con la supervisión y el mantenimiento del nivel de servicio, y con la planeación del crecimiento del mismo).
   - Soporte a los usuarios (incluyendo entrenamiento y soporte en todos los aspectos relacionados con el acceso y uso de los servicios y facilidades de la red).
   - Seguridad (es necesaria para garantizar que el acceso a los servicios del sistema de correo electrónico sea realizado únicamente por usuarios autorizados y que se encuentra bajo control).

- Contabilizar los costos de operación del sistema de correo electrónico.

2. Funciones de Planeación: cubren las actividades de largo plazo, que se encuentran relacionadas con la operación del sistema de correo electrónico en el futuro. Estas actividades incluyen las siguientes:

   - Planeación y diseño (es la planeación que asegurara que el sistema de correo electrónico será capaz de responder al crecimiento y será capaz de soportar la implementación de nuevas versiones).

   - Relaciones con los proveedores (el objetivo de esta función es supervisar las políticas de los proveedores, en aspectos como son las políticas de ventas y las políticas de mantenimiento del sistema de correo electrónico).

Conclusiones.

Como resultado de los cambios tecnológicos suscitados por Internet en prácticamente todas las formas de comunicación, dentro de las más importantes destaca el intercambio de mensajes, es decir, el correo electrónico. Por supuesto existen otras aplicaciones de igual importancia como es la enseñanza por Internet, las transacciones electrónicas de tipo bancarias, el comercio electrónico, la telefonía por Internet, etc., es seguro que se desarrollen nuevas aplicaciones y tecnologías para ser implementadas en las organizaciones que así lo requieran.

El presente trabajo permitió establecer objetivos relacionados con el correo electrónico, con los requerimientos que un sistema de esta naturaleza genera y con la metodología necesaria para implementar en una organización un sistema de correo electrónico.

Durante el desarrollo de los capítulos de este trabajo la información contenida en cada uno representa un concepto, teoría, modelo, o sistema, explicados con la mejor intención para que permita al lector llevar una secuencia lógica de la información, pero sin dejar de profundizar en temas cuya relevancia lo requerían, tal es caso de los protocolos de correo electrónico, donde podemos encontrar los conceptos, modelos, comandos y procesos que interactuan para que un sistema de correo electrónico funcione, pues a simple vista pareciera que es muy sencillo su uso, y si lo es, pues del lado del usuario de estos sistemas, solo se tiene una interfaz, por lo regular gráfica de un programa de computación, que es la punta de la pirámide tecnológica de los sistemas de mensajería.

Ahí en la parte tecnológica es donde se encuentra el conocimiento que como Ingeniero se puede desarrollar, en el aprendizaje de nuevas teorías, protocolos y sistemas, pero que se deben complementar con metodologías, procedimientos, análisis, diseño y administración de recursos, para construir por medio de la tecnología sistemas lo suficientemente robustos que cumplan con los requerimientos actuales de comunicación mundial, impulsados principalmente por el uso de Internet.

Podemos concluir que el correo electrónico, ya no es simplemente una forma novedosa y rara de enviar mensajes a alguien en otra red, en otra localidad, en otro país o continente, pues ahora representa en muchas organizaciones el medio oficial de comunicación entre los usuarios, pues se han dejado atrás los memorándums, los escritos de fax, e inclusive las cartas tradicionales, claro mencionando que no en todos los casos se puede sustituir con un mensaje de correo electrónico una decisión importante. Además otra conclusión que de este trabajo se desprende es el hecho que cada vez mas se reúnen en una red de comunicaciones, diferentes sistemas para convivir como si fueran uno solo, pues el desarrollo de las redes locales (LAN) y de las tecnologías para redes amplias/extendidas (WAN-MAN), ha permitido que los programadores amplíen las opciones de sus aplicaciones, sobre todo de las que se están empleando en Internet.

Con toda esta información se puede tener el criterio de selección de tecnologías para implementar un sistema de correo electrónico, incluyendo las tareas administrativas y de mantenimiento, además de los procedimientos que son necesarias para que el ciclo de vida de este tipo de sistemas sea eficiente.

Como conclusión final podemos decir que las necesidades de intercambiar información por medio de mensajes electrónicos es cada día mas demandante de velocidad, seguridad, privacidad, facilidad, administración, tecnología, recursos y sobre todo de Ingenieros capacitados para implementar sistemas de correo electrónico, y mantenerlos en operación las 24 horas del día y disponibles durante su ciclo de vida útil.

Bibliografía

Libros:

- "REDES PARA PROCESO DISTRIBUIDO"
  Jesús García Tomas, Santiago Ferrando, Mario Piattini
  Alfa-Omega Grupo Editor, 1997.

- "SISTEMAS DE COMUNICACIONES ELECTRÓNICAS"
  Wayne Tomasi
  Prentice Hall Hispanoamericana, 1997.

- "TRANSMISIÓN DE INFORMACIÓN, MODULACIÓN Y RUIDO".
  Schwartz Mischa.
  Limusa, 1990.

- "TELECOMUNICACIONES PARA PC".
  Duorak C. John, Anis Nick.
  Mc Graw Hill, 1992.

- "REDES DE COMPUTADORAS, PROTOCOLOS, NORMAS E INTERFACES".
  Uyless Black.
  Macro Bit, 1990.

- "REDES DE COMUNICACIONES".
  Huidrobo José.
  Paraninfo, 1996.

- "COMUNICACIONES Y REDES DE PROCESAMIENTO DE DATOS".
  González Sainz Nestor.
  McGraw-Hill, 1997.

- "DATA AND COMPUTER COMMUNICATIONS".
  Stalling Williams.
  Mac Millan, 1992.

- "EVALUACIÓN DE PROYECTOS"
  Urbina Baca Gabriel, 3er. Edición
  McGraw-Hill, 1995.

- "INTERCONECTIVIDAD, MANUAL PARA RESOLUCIÓN DE PROBLEMAS"
  Lew, H. Kim y colaboradores
  Pearson Educación, 2000.

- "DESIGNING CISCO NETWORKS"
  Cisco Systems, Inc. 2000.

- "INTERNET E-MAIL"
  Wood, David
  O´Reilly. 1999.

- "NETWORKING SECURITY AND STANDARDS"
  Weidong, Kou
  Kluwer, 1997.

- "INTERNET TÉCNICA Y PROGRAMACIÓN"
  Tischer Jennrich
  Marcombo, 1997.

- "THE EUDORA USER'S GUIDE"
  Levi Reiss
  AP Profesional, 1996.

- "CONTACTE AL MUNDO DE INTERNET"
  Krol Ed
  McGrwa-Hill, 1995.

- "USING INTERNET E-MAIL"
  Sadler Will
  QUE, 1997.

- "EVALUACIÓN DE METODOLOGÍAS DE DISEÑO DE REDES"
  Cuellar Miranda, Iván Fernando.

RFC´s

- RFC821: "SIMPLE MAIL TRANSFER PROTOCOL"
  Jonathan B. Postel, 1982.

- RFC822: "STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES"
  David H. Crocker, 1992.

- RFC1725 POP3: "POST OFFICE PROTOCOL VER. 3"
  John G. Myers, 1994

Direcciones electrónicas:

- www.cisco.com
- www.microsoft.com
- www.novell.com
- www.ietf.org
- www.ima.com
- www.lotus.com
- www.rad.com
- www.itu.org