UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGON

"ANÁLISIS Y DESARROLLO DE LA INTRANET UTILIZADA EN LA DIRECCIÓN GENERAL DE CONSERVACIÓN DE CARRETERAS (DGCC), ADSCRITA A LA SECRETARIA DE COMUNICACIONES Y TRANSPORTES (SCT); PARA LA PRESENTACIÓN Y ADMINISTRACIÓN DE LOS PROGRAMAS DE OBRA DE LA RED FEDERAL DE CARRETERAS DE LA REPUBLICA MEXICANA"

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICO
AREA: COMUNICACIONES Y ELECTRONICA
P R E S E N T A :

SALVADOR SUAREZ ESQUIVEL

ASESOR: M . en C. DAVID MOISÉS TERAN PEREZ

MÉXICO 2005.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCIÓN

SALVADOR SUAREZ ESQUIVEL
P R E S E N T E.

En contestación a la solicitud de fecha 3 de septiembre del año en curso, relativa a la autorización que se le debe conceder para que el señor profesor, M. en C. DAVID MOISÉS TERÁN PÉREZ pueda dirigirle el trabajo de tesis denominado "ANÁLISIS Y DESARROLLO DE LA INTRANET UTILIZADA EN LA DIRECCIÓN GENERAL DE CONSERVACIÓN DE CARRETERAS (DGCC), ADSCRITA A LA SECRETARÍA DE COMUNICACIONES Y TRANSPORTES (SCT); PARA LA PRESENTACIÓN Y ADMINISTRACIÓN DE LOS PROGRAMAS DE OBRA DE LA RED FEDERAL DE CARRETERAS DE LA REPÚBLICA MEXICANA", 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, 22 de septiembre de 2003
LA DIRECTORA

ARQ. LILIA TURCOTT GONZÁLEZ

U.N.A.M. ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON
DIRECCION

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

LTG/AIR/

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

SECRETARÍA ACADÉMICA

Ing. RAÚL BARRÓN VERA
Jefe de la Carrera de Ingeniería Mecánica Eléctrica,
Presente.

En atención a la solicitud de fecha 3 de diciembre del año en curso, por la que se comunica que el alumno SALVADOR SUAREZ ESQUIVEL, de la carrera de Ingeniero Mecánico Electricista, ha concluido su trabajo de investigación intitulado "ANÁLISIS Y DESARROLLO DE LA INTRANET UTILIZADA EN LA DIRECCIÓN GENERAL DE CONSERVACIÓN DE CARRETERAS (DGCC), ADSCRITA A LA SECRETARÍA DE COMUNICACIONES Y TRANSPORTES (SCT); PARA LA PRESENTACIÓN Y ADMINISTRACIÓN DE LOS PROGRAMAS DE OBRA DE LA RED FEDERAL DE CARRETERAS DE LA REPÚBLICA MEXICANA", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 8 de diciembre del 2003
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis.
C p Interesado.

AIR/VF

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN – UNAM

JEFATURA DE CARRERA DE INGENIERÍA MECÁNICA ELÉCTRICA

OFICIO: ENAR/JAME/0943/2003.

ASUNTO: Revisión Previa de Tesis antes de autorizar su Impresión.

M. en C. MOISÉS TERÁN PÉREZ (ASESOR)
ING. JUAN GASTALDI PÉREZ
ING. ADRIÁN PAREDES ROMERO
ING. JESÚS NÚÑEZ VALADÉZ
MAT. LUIS RAMÍREZ FLORES

En forma anexa le hago entrega de un ejemplar del proyecto de tesis titulado "**ANÁLISIS Y DESARROLLO DE LA INTREANET UTILIZADA EN LA DIRECCIÓN GENERAL DE CONSERVACIÓN DE CARRETERAS (DGCC), ADSCRITA A LA SECRETARÍA DE cOMUNICACIONES Y TRANSPORTES (SCT); PARA LA PRESENTACIÓN Y aDMINISTRACIÓN DE LOS PROGRAMAS DE OBRA DE LA RED FEDERAL DE CARRETERAS DE LA REPÚBLICA MEXICANA"**, del alumno: **SALVADOR SUÁREZ ESQUIVEL,** con Número de Cuenta: **08503158-8.**

Esto con el fin de que sea revisada por usted, y nos dé su evaluación y comentarios por escrito, mismos que le pido me haga llegar a la brevedad posible.

Agradezco de antemano su colaboración y aprovecho la oportunidad para enviarle un cordial saludo.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Bosques de Aragón, Estado de México, 21 de octubre de 2003.
EL SECRETARIO TÉCNICO

ING. JOSÉ LUIS GARCÍA ESPINOSA

C.c.p. Alumnos.
JLGE/amce

A mis padres :

Salvador Suárez Valladolid
Socorro Esquivel Velásquez

Porque gracias a ellos con su apoyo, logre una de las metas mas importantes de mi vida.

Gracias por todo el amor y comprensión, por haberme dado la vida y sobre todo, por su herencia mas preciada que me dejan.

A mis hermanos :

Adriana, José Luis y Edith

Quienes siempre me alentaron a llegar al lugar en donde estoy.

A mis Jefes :

Julio, Joel y Ricardo

Por todo el apoyo brindado para poder realizar esta Tesis.

A ustedes mis amigos :

Por tu forma de presionarme y apoyarme para lograr el objetivo de la terminación de esta Tesis.

INTRODUCCIÓN

Muchas organizaciones tienen una cantidad importante de ordenadores en operación, con frecuencia alejadas entre sí. Por ejemplo, una compañía con muchas fábricas puede tener un ordenador en cada localidad para llevar el control de los inventarios, vigilar la productividad y pagar la nómina local. Inicialmente, cada uno de estos ordenadores puede haber trabajado aislado de los otros, pero en algún momento, la Gerencia decidió conectarlos para poder extraer y correlacionar información acerca de toda la compañía. (Stallings, 1995a).

En términos más generales, la cuestión aquí es compartir los recursos y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios. En otras palabras, el hecho de que un usuario esté a 1 000 kilómetros de distancia de sus datos no deberá impedirle usar los datos como si fueran locales. Este objetivo puede resumirse diciendo que es un intento por acabar con la "tiranía de la geografía".

Una segunda meta es lograr una alta confiabilidad al contar con fuentes alternativas de suministro. Por ejemplo, todos los archivos podrían replicarse en dos o tres máquinas; así, si una de ellas no está disponible (debido a una falla de la arquitectura), podrán usarse las otras copias. Además, la existencia de múltiples equipos significa que si uno de ellos falla, los otros serán capaces de hacer su trabajo, aunque se reduzca el rendimiento. En aplicaciones militares, bancarias, de control de tráfico aéreo, seguridad de reactores nucleares y muchas otras, la capacidad para continuar operando pese a problemas de arquitectura, es de suma importancia.

Otra meta es ahorrar dinero. Los ordenadores pequeños tienen una relación costo/beneficio mucho mejor que los grandes equipos. Los llamados *"mainframes"* (ordenadores del tamaño de un cuarto) son aproximadamente 10 veces más rápidos que los ordenadores personales, pero cuestan mil veces más que éstos. Este desequilibrio ha ocasionado que muchos diseñadores construyan sistemas compuestos por ordenadores personales, uno por usuario, con los datos guardados en uno o más equipos llamados servidores de archivos compartidos. En este modelo, los usuarios se denominan clientes, y el arreglo completo se llama Modelo Cliente-Servidor.

En el Modelo Cliente –Servidor, la comunicación generalmente adopta la forma de un mensaje de solicitud del cliente al servidor pidiendo que se efectúe algún trabajo. A continuación, el servidor hace el trabajo y devuelve la respuesta. Por lo regular, muchos clientes utilizan un número pequeño de servidores.

Otra meta al establecer redes, es la escalabilidad: la capacidad para incrementar el rendimiento del sistema gradualmente cuando la carga de trabajo crece, añadiendo solamente más procesadores. En el caso de *"maiframes"* centralizados, cuando el sistema esté lleno hay que reemplazarlo por uno mayor, usualmente más caro, lo que implica largas interrupciones para los usuarios. Con el Modelo Cliente-Servidor se pueden añadir nuevos clientes y nuevos servidores cuando es necesario.

Un objetivo más del establecimiento de una Red de ordenadores tiene poco que ver con la tecnología. Una Red de ordenadores puede proporcionar un potente medio de comunicación entre empleados o clientes que están muy distantes. Al usar una red, es fácil para dos o más personas que viven lejos escribir un informe de manera conjunta. (Stallings, 1995b).

Cuando un trabajador hace un cambio a un documento en línea, los demás pueden ver el cambio inmediatamente, sin tener que esperar varios días la llegada de una carta. Tal rapidez hace fácil la cooperación entre grupos de gente muy apartada, cosa que previamente era imposible. A largo

plazo, el uso de redes para mejorar la comunicación entre las personas probablemente resultará más importante que las metas técnicas tales como la mejora de la confiabilidad.

Todas las innovaciones arriba citadas para construir redes de computadoras son de naturaleza esencialmente económica y tecnológica. Si *"mainframes"* suficientemente grandes y potentes estuvieran disponibles a precios aceptables, muchas compañías hubieran optado por guardar todos sus datos en ellas y proporcionar a sus empleados terminales conectadas a estas máquinas. En la década de los 70 y a principios de los 80, casi todas las compañías operaban de esta forma. Las redes de ordenadores llegaron a ser populares únicamente cuando los ordenadores personales ofrecieron una descomunal ventaja precio/rendimiento (costo/beneficio), sobre los llamados *"mainframes"*.

Al iniciar la década de los 90, las redes de ordenadores comenzaron a prestar servicios a particulares en su hogar. Estos servicios y la motivación para usarlos son muy diferentes del modelo de "Eficiencia Corporativa" descrito anteriormente. A continuación se esbozan tres de los más estimulantes aspectos de esta evolución:

1.- Acceso a información remota.
2.- Comunicación de persona a persona.
3.- Entretenimiento interactivo.

El acceso a la información remota vendrá de muchas formas. Un área en la cual ya está sucediendo es el acceso a las instituciones financieras. Mucha gente paga sus facturas, administra sus cuentas bancarias y maneja sus inversiones en forma electrónica. Las compras desde el hogar se están haciendo populares, con la facilidad de inspeccionar los catálogos en línea de miles de compañías.

Algunos de estos catálogos pronto ofrecerán un video instantáneo de cualquier producto que se pueda ver sólo con hacer *"clic"* con el puntero del ratón en el nombre del archivo.

Los periódicos de publicarán en línea y serán personalizados. Se podrá decirle al periódico que se quiere saber todo lo que haya acerca de los políticos corruptos, los grandes incendios, los escándalos de las celebridades y las epidemias, etcétera. En la noche mientras se duerme, el periódico se bajará al disco del ordenador o quedará impreso en documento. A pequeña escala, este servicio ya existe. El siguiente paso más allá de los periódicos (y de las revistas y publicaciones científicas) es la biblioteca digital en línea. Dependiendo del costo, tamaño, peso de los ordenadores portátiles, los libros impresos quizá lleguen a ser obsoletos. (Stallings, 1999).

Otra aplicación en esta categoría es el acceso a sistemas de información como la actual red mundial *("World Wide Web")*, la cual contiene información sobre arte, negocios, cocina, gobierno, salud, historia, aficiones, recreación, ciencia, deportes, viajes y muchos otros temas, demasiado diversos y numerosos para mencionarlos en este trabajo de tesis.

Todas las aplicaciones antes mencionadas implican la limitación entre una persona y una Base de Datos remota. La segunda categoría extensa de redes que se utilizará implica la interacción persona a persona; básicamente, la respuesta del Siglo XXI al teléfono del Siglo XIX. Millones de personas ya utilizan el Correo Electrónico *(e-mail)* y pronto contendrá en forma rutinaria audio, video y texto.

El correo electrónico de tiempo real permitirá a los usuarios remotos comunicarse sin retraso, posiblemente viéndose y escuchándose. Esta tecnología hace posible realizar reuniones virtuales llamadas videoconferencias, entre gente muy alejada. A veces se dice que el transporte y la comunicación están en competencia, y cualquiera que gane hará al otro obsoleto.

Las reuniones virtuales podrán servir para recibir enseñanza remota, obtener opiniones médicas de especialistas distantes, y muchas otras aplicaciones.

Los grupos de noticias a nivel mundial, con discusiones sobre todos los temas concebibles, son ya comunes entre un grupo selecto de personas, y esto crecerá para incluir a la población en general. Estas discusiones en las cuales una persona pone un mensaje y los demás suscriptores al grupo de noticias pueden leerlo, van desde lo humorístico hasta lo apasionado.

La tercera categoría es el entretenimiento, que es una industria enorme y en crecimiento. La aplicación irresistible aquí (y que puede impulsar a todas las demás) es el video por solicitud. Dentro de algunos años, será posible seleccionar cualquier película o programa de televisión creado en cualquier país y exhibirlo en la pantalla en forma instantánea.

Algunas películas nuevas llegarán a ser interactivas, preguntándose al usuario ocasionalmente que dirección debe seguir la historia, con argumentos alternativos para todos los casos. La televisión en vivo también puede llegar a ser interactiva, con el auditorio participando en concursos, escogiendo entre los concursantes, etcétera.

Por otro lado, tal vez la aplicación irresistible no sea la petición de videos, sino los juegos. Se tienen ya, juegos de simulación en tiempo real multipersonales, como las aventuras en calabozos virtuales, y simuladores de vuelo en que los jugadores en equipo tratan de derribar a los del equipo contrario. Si esto se hace con anteojos que muestren imágenes en movimiento con calidad fotográfica en tiempo real tridimensional, se tendrá una especie de realidad virtual compartida mundial. En pocas palabras, la capacidad para combinar información, comunicación, audio, video, datos y entretenimiento, seguramente hará surgir una nueva y enorme industria basada en las redes de ordenadores. (Stallings, 1995c).

La introducción ampliamente difundida de redes significará nuevos problemas sociales, éticos y políticos (Laudon, 1995). Sólo se mencionará en forma breve algunos de ellos: un estudio minucioso requiere un libro completo, por lo menos. Una característica popular de muchas redes son los grupos de noticias o quioscos de anuncios en los que la gente puede intercambiar mensajes con individuos de gustos muy parecidos. Mientras los temas estén restringidos a asuntos técnicos o aficiones como la jardinería, no se presentarán muchos problemas.

El problema surge cuando los grupos de noticias tratan temas que a la gente de verdad le importan como la política, la religión o el sexo. Las opiniones expresadas en tales grupos pueden ser profundamente ofensivas para algunas personas de criterio muy cerrado. Además, los mensajes no necesariamente están limitados al texto. Fotografías a color de alta definición e incluso pequeños *"videoclips"* pueden transmitirse ahora con facilidad por las redes de ordenadores. Algunas personas adoptan una postura de vive y deja vivir, pero otras sienten que enviar cierto material (por ejemplo; pornografía infantil) es simplemente inaceptable. Así pues, el debate sigue causando furor.

Hay gente que ha demandado a los operadores de redes, reclamando que son responsables por el contenido de lo que aquéllas acarrean, como los periódicos y revistas. La respuesta inevitable es que una red es como una compañía de teléfonos o como la oficina de correos y no puede esperarse que los operadores vigilen lo que los usuarios dicen. Por otro lado, si se obligara a los operadores a censurar los mensajes, probablemente optarían por eliminar cualquier cosa que tuviera la más leve posibilidad de causar una demanda en su contra y por lo tanto, violarían el derecho de los usuarios a hablar con libertad. Lo más seguro es que este debate continuará durante un tiempo.

Otra área divertida es el conflicto entre los derechos de los empleados y los derechos de los patrones. Muchas personas leen y escriben correo electrónico en su trabajo.

Algunos patrones han reclamado el derecho a leer y posiblemente censurar los mensajes de los empleados, incluidos los mensajes enviados desde una terminal casera después de las horas de trabajo. No todos los empleados están de acuerdo con esto. (Sipior y Ward, 1995).

Aun si los patrones tienen poder sobre los empleados, ¿esta relación también gobierna a las universidades y estudiantes? En 1994, la Universidad Carnegie-Mellon decidió bloquear la entrada de mensajes de algunos grupos de noticias que trataban el sexo porque la Universidad (sus autoridades) sintió que el material era inapropiado para los pocos alumnos aún menores de edad. Las repercusiones de este suceso tardarán años en disiparse.

Las redes de ordenadores ofrecen la posibilidad de enviar mensajes anónimos. En algunas situaciones, esta capacidad puede ser deseable. Por ejemplo, proporciona un mecanismo para que estudiantes, empleados, ciudadanos y militares, llamen la atención sobre comportamientos ilegales por parte de profesores, oficiales, superiores y políticos, sin miedo a represalias. Por otro lado, en los Estados Unidos de América la Ley otorga específicamente a una persona acusada, el derecho de enfrentar y recusar a su acusador en los tribunales. Las acusaciones anónimas, no pueden aceptarse como pruebas.

En pocas palabras, las redes de ordenadores, igual que la imprenta hace 500 años, permiten a los ciudadanos comunes distribuir sus puntos de vista en diferentes formas y a diferentes públicos que antes estaban fuera de su alcance. Esta nueva libertad trae consigo muchos problemas sociales, políticos y morales aún no resueltos.

JUSTIFICACIÓN

A manera de *Justificación* del presente trabajo de Tesis se menciona la tendencia actual a que los Sistemas de ordenadores, se configuren a modo de Red, para obtener un alto índice de rendimiento y rentabilidad de los equipos así configurados y operados.

El almacenamiento y análisis de Información ha sido uno de los grandes problemas a que se ha enfrentado el hombre desde que inventó la Escritura. No fue sino hasta la segunda mitad del Siglo XX que el hombre ha podido resolver en parte este problema gracias a la invención del ordenador.

En la década de los años cincuenta, el hombre dio un gran salto en este problema al inventar el ordenador. Ahora la Información podía ser enviada en grandes cantidades a una localidad central donde se realizaba el procesamiento de la misma. El problema era que esta Información (que se encontraba en grandes cajas repletas de tarjetas) tenía que ser *acarreada* al Departamento de Procesamiento de Datos.

Con la aparición de la Terminales o Estaciones de Trabajo en la década de los sesenta, se logró la comunicación directa entre los usuarios y la Unidad Central de Proceso, logrando con esto una comunicación más rápida y eficiente, pero se encontró con un problema, entre más terminales y periféricos se agregaban a los ordenadores, la velocidad de respuesta de las mismas comenzó a decaer.

Hacia la mitad de la década de los años setenta, la refinada Tecnología del Silicón e integración en miniatura permitió a los fabricantes de ordenadores construir más *"Inteligencia"* en máquinas más pequeñas.

Estas máquinas llamadas *micro-ordenadores*, descongestionaron a las viejas máquinas centrales y ahora cada usuario tenía su propio *micro-ordenador* en su escritorio.

A principio de la década de los años ochenta, los *micro-ordenadores* habían revolucionado por completo el concepto de la computación electrónica, así como sus aplicaciones y mercados. Los Gerentes de los Departamentos de Informática fueron perdiendo el Control de la Información ya que ahora el proceso de la Información no estaba centralizada.

Como la mayoría de los Proyectos de Ingeniería; independientemente de la disciplina, las Redes de ordenadores cuentan con una serie de Estándares o Normas que definen su funcionamiento en todos los aspectos. Por ello se establecen los Modelos de Referencia cuya finalidad se divide en dos puntos básicos:

1.- Flexibilizar la implantación de una Red dividiéndola en Capas o Niveles de Programas y Paquetes *("Software")* interactuando jerárquicamente.

2.- Estandarización de los diversos fabricantes tanto de Arquitectura de Sistemas ("Hardware") como de Programas y Paquetes ("*Software*") del Modelo de Referencia más utilizado en la actualidad.

Además, el desarrollo de las Redes de Área Local (LAN) a mediados de la década de 1980, ayudó a cambiar la forma de *"pensar"* de los ordenadores, como ordenadores; a la forma en que nos comunicamos entre ordenadores y usuarios y por qué se hace de ese modo (Rosenthal, 1982).

Las Redes de Área Local (LAN) son particularmente importantes, ya que puede ser conectada a muchas Estaciones de Trabajo como la primera fase de un entorno distribuido de Redes y Operaciones de ordenadores de mayor magnitud.

Así mismo, las Redes de Área Local (LAN) son importantes para muchas Organizaciones de menor tamaño porque son la ruta a seguir hacia un Entorno de ordenadores Multi-usuarios, distribuido y capaz de comenzar en forma modesta, pero también de extenderse a medida que aumenten las necesidades de la Organización.

Como se puede apreciar, una de las influencias más profundas en el desarrollo de las Redes de Área Local (LAN)[1], ha sido la adopción de *"Estándares"* Nacionales e Internacionales ("Estándares" que incluso los gigantes de la Industria encuentran difícil de pasar por alto).

Las Redes que transmiten Información pueden organizarse en diversas formas. Al comienzo de la década de 1980, era imposible distinguir entre lo que se ha llamado *"Redes Locales"* y lo que se denominara *"Redes Globales"*. En muchas Redes Locales, todos los nodos son ordenadores; aunque no hay nada inherente en la *Tecnología* que requiera tal condición, pese a que la existencia de grandes números de ordenadores ha sido probablemente un factor importante en el desarrollo de las Redes de Área Local (LAN).

Las Redes de Área Local (LAN) fueron estructuradas con el aspecto de la conectividad en mente. Las Redes Locales pueden servir a usuarios locales, se pueden interconectar o bien pueden ser nodos de una Red Global.

Las Redes Locales pueden tener radios que varían de algunos cientos de metros a cerca de 50 kilómetros. Las Redes Globales se pueden extender por todo el mundo, de ser necesario.

Las Redes de Área Local (LAN), se describen a veces, como aquellas que: **"Cubren una área geográfica limitada, donde todo nodo de la Red puede comunicarse con todos los demás y no requiere un nodo ó procesador central".**

Además, una Red de Área Local (LAN) es una Red de Comunicación que puede ofrecer intercambio interno entre Medios de Voz, Datos de ordenador, Procesamiento de Palabras, Facsímil, Videoconferencias, Transmisión Televisiva de Vídeo, Telemetría y otras formas de Transmisión Electrónica de Mensajes. Una Red de Área Local (LAN) puede clasificarse además como:

1. Intrainstitucionales, de propiedad privada, administradas por el usuario y no sujetas a la regulación de la FCC. De esta categoría se excluyen a Empresas de servicios comunes, tales como Sistemas Telefónicos Públicos y Sistemas Comerciales de Televisión por Cable.

2. Integradas a través de la interconexión vía un medio estructural continuo; pueden operar múltiples servicios en un mismo juego de cables.

3. Capaces de ofrecer conectividad global.

4. Que soportan Comunicaciones de Datos a baja y alta velocidad. Las Redes de Área Local (LAN) no están sujetas a las limitaciones de velocidad impuestas por Empresas de servicios comunes tradicionales y pueden ser diseñadas para soportar dispositivos cuya velocidad va de 75 Baudios con base en casi cualquier Tecnología, a cerca de 140 Mbaudios en el caso de una Red de Área Local (LAN) de Fibra Óptica disponibles en el Mercado.

5. Disponibles en el Mercado (al alcance de el Comprador). El Mercado de las Redes de Área Local (LAN) sigue siendo volátil, sin menospreciar los productos que ofrece IBM, muchos sistemas siguen siendo diseñados por pedido. Incluso, los productos ya anunciados pueden encontrarse aún en la fase de prueba.

[1] LAN (Local Area Network). Red de Área Local.

Como la Red de Área Local (LAN) es más un concepto que un producto, el término "disponibles en el mercado", debe interpretarse de la manera siguiente: Los componentes de las Redes de Área Local (LAN) que ofrecen conexiones de dispositivos a un medio físico, como un Sistema de Televisión por Cable (CATV), son las que se pueden conseguir realmente en el Mercado.

La *Justificación* más importante para este trabajo es que las Redes de Área Local (LAN) son únicas porque simplifican procesos sociales. Las Redes Globales se implantan para hacer un uso más efectivo en costo de *"Mainframes"* o Macro-ordenadores costosos. Las Redes de Área Local (LAN) se implantan para hacer un uso más efectivo en costo de las personas (Tanenbaum, 1981).

La Conectividad es el concepto impulsor de las Redes de Área Local (LAN) en una forma desconocida para las Redes Globales. Las Redes de Área Local (LAN) son un reconocimiento de la necesidad que tienen las personas de utilizar datos y, como un producto secundario, de transmitir datos de una persona a otra.

Una clave de interés en las Redes de Área Local (LAN), es que aquellos que dirigen grandes Organizaciones han reconocido que *"Organización"* implica interacción social.

Los ordenadores no dirigen Organizaciones, lo hacen las personas. Los ordenadores no toman decisiones, sino las personas. Los ordenadores, no importa cuán *"Inteligentes"* sean; sólo ayudan a las personas a dirigir las Organizaciones.

Como una Organización es principalmente un Proceso Social, operar en forma más eficiente cuando las personas que las constituyen dispongan de herramientas que les ayuden en la *"Toma de Decisiones"*.

Esto significa que las personas que utilizan ordenadores en las Organizaciones no lo hacen en forma aislada, sino como seres sociales comprometidos en actividades de comercio y conversación.

En el entorno organizacional, se han introducido muchos recursos de ordenadores: ordenadores, Terminales, Copiadoras Inteligentes, y ordenadores grandes y pequeños.

No obstante, un ordenador vacío, es como una mente también vacía; de poca o ninguna utilidad para nadie, incluyendo a su propietario. Si cada ordenador debe ser llenado en forma diferente, y a mano, entonces el trabajo se vuelve menos (no más) eficiente.

En el desarrollo de la era de la Informática es importante, que la Tecnología ayude a las personas a reducir la cantidad de información a niveles manejables y a mejorar la calidad de dicha información.

En un contexto Organizacional, las Redes ofrecen el medio para permitir que el poder de Ordenación disponible, sea utilizado a su máximo alcance.

Así mismo, otros aspectos han sido importantes para generar interés en las Redes de Área Local (LAN), incluyendo el deseo de las personas de tener independencia en las operaciones del ordenador, la necesidad de contar con ordenadores en todos y cada uno de los Departamentos de una Organización y la economía de las Redes de Área Local (LAN).

ANTECEDENTES AL TRABAJO

La unión de ordenadores y Comunicaciones ha tenido una influencia profunda en las formas en que se organizan los Sistemas de Información bajo ordenadores. Estas áreas convergen y las diferencias entre Coleccionar, Transportar, Almacenar y Procesar Información, están desapareciendo rápidamente con lo que la demanda de tecnología que procese Información crece a pasos agigantados.

Así el viejo Modelo de un sólo ordenador sirviendo a las necesidades de toda la Organización está cambiando; por otro lado, en que un gran número de ordenadores separados pero interconectadas hacen el trabajo; estos *"nuevos"* Sistemas Interconectados de ordenadores son las Redes.

Hasta hace unos años los Sistemas Transaccionales eran los encargados de soportar la Información de un negocio, pero éstos sólo manejan las operaciones a un nivel muy detallado; lo cual no era muy bueno para los gerentes o personas encargadas del análisis de los datos de una Empresa, ya que tenían que esperar a que el Departamento de Sistemas elaborara el reporte que ellos necesitaban para el análisis de su Empresa, lo cual podía llevarse de días hasta semanas para que el reporte se recibiera en la forma requerida por el Gerente.

Por otra parte, el área de Sistemas tenía que "sufrir" tratando de dar formato, hacer consultas e imprimir los archivos que se generaran para poder entregar los reportes con todos los requerimientos que el Gerente había solicitado.

Las personas encargadas de la Toma de Decisiones eran dependientes de el Área de Sistemas, en lo que a información se refiere, ya que para poder adquirir Información de las Operaciones de la Empresa debían recurrir a esta área.

Y en ocasiones, el Área de Sistemas no podía proporcionar los reportes requeridos por la Gerencia porque existían ciertas circunstancias que no permitían elaborar los reportes con los formatos especificados por la Gerencia, Schwartz, 1999).

Por otra parte, los Sistemas Transaccionales sólo podían dar respuesta a preguntas como: ¿Cuántos Productos se han vendido en el presente mes? ¿Cuál es el Producto más caro? ¿Cuántos Productos se tienen en existencia? En cambio a la Gerencia le interesaba contestar preguntas como: ¿Qué pasaría si se incrementa el precio a un Producto "X"?

¿Se puede reducir el precio de un Producto sin afectar el consumo de otros? ¿Qué pasaría si se reduce la existencia de un Producto "X" en el Almacén?

Este tipo de cuestiones no podían ser contestadas por los Sistemas Transaccionales, así como el Gerente tenía que ingeniárselas para poder realizar análisis de su Negocio tomando los datos que sus Sistemas Transaccionales le otorgaban. Hasta que se desarrolló la idea del Data Warehouse, el cual vino a cambiar la forma de manejo de la Información.

En el Siglo XX, creció aún más la necesidad de producir más Información, que esté disponible para un mayor número de usuarios. Como ejemplos de aplicación, se puede decir que los Inversionistas de una Empresa, necesitan información, acerca de su Estado Financiero y sus perspectivas futuras. Los banqueros y los proveedores necesitan información para evaluar el desempeño y la solidez de un negocio antes de proceder a un préstamo o concederle un crédito.

Las Agencias de el Gobierno necesitan varios reportes que les muestren las actividades financieras y operativas para efectos de impuestos y reglamentación. Los Sindicatos están interesados en las utilidades de las Organizaciones en las que trabajan sus afiliados.

Sin embargo, los individuos que están más involucrados con la información y dependen de ella, son los que tienen a su cargo la responsabilidad de Administrar y operar las Organizaciones, es decir; la Gerencia y los Empleados; sus necesidades van desde el mantenimiento de las Cuentas por Pagar hasta la información estratégica para la adquisición de otra Compañía.

Sin Información de Calidad, las Organizaciones se encuentran a la deriva, flotando con dificultad en un mar de incertidumbre. *La Información de Calidad* es, de hecho, un recurso crítico y se obtiene siguiendo varias etapas y asegurándose que la información producida sea exacta, oportuna y relevante.

Todas las Organizaciones están formadas por factores organizacionales, clave que ayuda a describir la *"Organización"*. Sin embargo, la esencia de todas las Organizaciones está compuesta del lugar de trabajo, la cultura, la base de los activos y los interesados, y los afectados. El ingrediente principal que aglutina a estos componentes para obtener una Organización coordinada y que funcione fluidamente es la Información de Calidad (SNA, 1995).

El receptor principal de la información es la Gerencia, que la necesita para planear, controlar y tomar decisiones. Sin embargo, los Gerentes que se encuentran en los niveles táctico y estratégico, aún no están recibiendo suficiente información para satisfacer sus necesidades.

En un mundo competitivo, el arma más poderosa es la *Información.* ésta ayuda a los Gerentes a desempeñarse mejor, a combatir a los competidores, a innovar, a reducir el conflicto y a adaptarse a las vicisitudes de el Mercado.

La Información mejora la diferenciación de Productos y Servicios, ofreciendo a los Clientes Productos y Servicios actualizados y más baratos, un mejor y más fácil acceso a los Productos y Servicios, mejor Calidad, respuesta y servicio más rápidos, mayor información de seguimiento y estado del proceso, y una gama más amplia de Productos y Servicios.

Gran parte de la mejora en la dimensión de Productos y Servicios, se logra insertando el *"Sistema de la Organización"* en el *"Sistema del Cliente"* para obtener un acoplamiento interactivo y coordinado. Igualmente, la Información de Calidad mejora la productividad, derribando las barreras de comunicación entre las oficinas y las operaciones.

Además, la Información y la Tecnología Informática (en este caso las Redes de Área Local (LAN)), pueden mejorar de manera significativa la productividad, tanto de los Trabajadores de la Información, como los de las Operaciones.

PLAN PROPUESTO

Para obtener un buen aprovechamiento de este Trabajo de Tesis, se recomienda asumirlo y asimilarlo de la siguiente manera:

En el Capítulo I, se establecen los Conceptos Fundamentales de los *Sistemas de Comunicación.* Dentro de éstos se desarrollan los referentes a los Antecedentes Históricos de los Sistemas basados en Redes, los Tipos de Redes en función de su Topología y su Alcance Geográfico.

En el Capítulo II, se dan los Fundamentos de los conceptos sobre *Redes de ordenadores de Área Local.*

En el Capítulo III, se analiza lo referente a los *Protocolos* utilizados para *Redes de Área Local.*

En el Capítulo IV, se establece todo lo concerniente a la *Conectividad para Redes de Área Local.*

Finalmente, en el Capítulo V se establece la Aplicación de una *Intranet* dentro de una Empresa Estatal Mexicana, como una herramienta para la Toma de Decisiones.

OBJETIVO GENERAL

Presentar los conceptos generales de las Redes de Área Local (LAN) y de una Intranet, así como los elementos referentes a la Transmisión de Datos sobre Tecnología IP, aplicados en una Intranet perteneciente a una Empresa Estatal en México.

OBJETIVOS PARTICULARES

1. Presentar y analizar los conceptos básicos de los Sistemas de Comunicación.
2. Analizar los conceptos y elementos inherentes a los fundamentos de las Redes de Área Local.
3. Analizar los conceptos y elementos inherentes a los fundamentos de los Protocolos para Redes de Área Local.
4. Analizar los conceptos y elementos inherentes a los fundamentos de la Conectividad para Redes de Área Local.
5. Establecer los criterios y especificaciones para una Intranet dentro de una Empresa Estatal Mexicana.

CAPÍTULO I

SISTEMAS DE INFORMACIÓN

I.1.- Introducción

Uno de los principales problemas del ser humano desde que se inventó la escritura, ha sido el manejo eficiente de la información. Este problema ha sido resuelto en gran parte gracias a la invención del ordenador. Los agigantados avances de la tecnología actual, han permitido que el ordenador se integre de manera sencilla y eficiente a las actividades cotidianas del ser humano. Hasta ahora, no existe campo alguno de la Ciencia, que no se haya visto beneficiado con los múltiples servicios que ofrece un ordenador Digital.

Así mismo, gracias a la popularidad que los ordenadores personales han adquirido en los últimos años, su costo ha disminuido notablemente, pero su poderío y su versatilidad se siguen incrementando día a día. Este hecho ha provocado que corporaciones de todo tipo, adquieran ordenadores buscando incrementar la productividad de la Empresa u Organización, con sistemas de información más rápidos y confiables.

Actualmente, el volumen de información a procesar se ha incrementado considerablemente, y los sistemas de información tienden a ser más complejos. Esto ha dado pie a que los trabajos que antes realizaba un solo ordenador, se distribuya ahora entre varios ordenadores que deben ser capaces de comunicarse entre sí y trabajar de manera conjunta, para satisfacer los actuales requerimientos de información.

Esta comunicación puede darse entre ordenadores que estén físicamente cercanos (dentro de un mismo edificio, un campus educativo o un complejo industrial), o geográficamente distantes (ubicados en países e incluso continentes distintos); las primeras dan origen a redes locales y las segundas, a redes de área global.

I.2.- Antecedentes Históricos de las Redes de ordenadores.

Hace más de treinta años, surgieron las primeras Redes de ordenadores, y su aparición ha aportado elementos valiosos a las Redes que hoy se conocen y operan. A continuación se citan algunas de ellas como mera referencia histórica, (Tanenbaum, 2000):

1.- En Diciembre de 1969, surgió la primera Red Experimental llamada ARPANET, desarrollada por la Agencia de Proyectos e Investigaciones Avanzadas (ARPA), de el Departamento de Defensa de los Estados Unidos de América. Esta red contaba con 4 nodos y conectaba hasta ordenadores conectados en varios estados de ese país. Muchos de los conocimientos actuales sobre redes, son el resultado directo del *"Proyecto ARPANET"*. Por ello, la terminología actual de las Redes de ordenadores, conserva algunos conceptos ideados para esta Red primigenia.

2.- En 1973, la Compañía XEROX desarrolló una Red de Gestión de Archivos en base a sus equipos instalados en los Estados Unidos de América. Esta red fue pionera de las Redes Ethernet que hoy se conocen.

3.- En 1974, comenzó a funcionar la Red pública TRANSPAC de Francia; la cual conectó algunos cientos de equipos en ese país. TRANSPAC fue la primera Red Pública en operación.

4.- En 1981, México puso en marcha su Red Pública TELEPAC para ofrecer servicios de trasnmisión de datos en todo el país.

5.- Finalmente, en 1982, la aparición de los primeros ordenadores personales de escritorio marcó un cambió definitivo en la informática y, comenzaron a desarrollarse las primeras redes de micro-ordenadores.

I.3.- Red de Transmisión de Datos.

Existen diversos sistemas de comunicación utilizados en la transmisión de datos. Tradicionalmente, la Red Telefónica y la Red de Microondas han sido un excelente soporte de la comunicación de datos, pero debido a la demanda de información se han saturado rápidamente. Es por ello, que los satélites de comunicación se están utilizando en todo el mundo. A diferencia de las redes de ordenadores, las Redes de Transmisión de Datos sólo se encargan de garantizar que la información llegue íntegramente de un punto a otro, para lo cual utilizan métodos de detección de errores, de aprovechamiento máximo del canal de transmisión, repetidores, amplificadores y multicanalizadores.

I.3.1.- Red Telefónica.

En comunicaciones telefónicas se utilizan con frecuencia los términos *"pares"* y *"cuadretes"*, para describir el circuito que compone el canal. Los circuitos de *"pares"* suelen conocerse como circuitos *"semi-dúplex"*. Uno de los hilos sirve para transmitir los datos y el otro, es la línea de retorno eléctrico. Los circuitos de 4 hilos o circuitos de *"cuadretes"* suelen conocerse como circuitos *"full-dúplex"*. Incluyen dos pares de hilos cada uno; dos de los hilos transmiten datos y los otros dos cierran el circuito eléctrico. (Para las compañías telefónicas, un enlace de dos hilos suele corresponder a un circuito telefónico conmutado normal; mientras que un circuito de 4 hilos, suele ser una línea privada no conmutada).

I.3.2.- Red de Microondas.

En una Red de Microondas, se utilizan antenas de transmisión y recepción, repetidores y el espacio atmosférico como medio físico de transmisión. La información se transmite en forma digital a través de ondas de radio de muy alta frecuencia y por lo tanto, de una longitud de onda mínima (microondas). Pueden direccionarse múltiples canales a múltiples estaciones dentro de un enlace dado, o pueden establecerse enlaces punto a punto. Las estaciones consisten de una antena de tipo parábola y de circuito que interconectan la antena con la terminal del usuario.

Cuando el sistema de microondas pertenece a la compañía de teléfonos, se utilizan parte de los circuitos telefónicos disponibles. Dependidendo del País y de su legislación, a veces es necesario, obtener una licencia especial para uso privado y esto puede constituirse en un contratiempo. También puede decirse que por el momento, los componentes resultan bastante costosos y no está disponible fácilmente.

En redes de microondas, la transmisión es en línea recta (lo que está a la vista), y por lo tanto, se ve afectada por accidentes geográficos (edificios, bosques, cerros, mal tiempo, etcétera), los cuales provocan que la señal transmitida esté sujeta a los fenómenos de reflexión, refracción y difracción. El

alcance promedio entre dos antenas es de 40 Kms. Estos fenómenos, provocan que se presenten interferencias instructivas y destructivas.

En el sitio receptor se presentan puntos ubicados en diferentes alturas, en los cuales se tendrán interferencias constructivas y destructivas. Al patrón resultante de interferencias destructivas y constructivas se le conoce como "Zonas de Fresnel". Este concepto, es muy importante ya que la antena receptora debe estar a una altura que corresponda a una zona de Fresnel, con interferencia constructiva. Una de las ventajas importantes de usar, los enlaces de microondas es la capacidad de poder transportar miles de canales de voz a grandes distacias a través de repetidoras, a la vez, que permite la transmisión de datos en su forma natural (digital).

I.3.3.- Red Satelital.

Actualmente es muy común, el uso de satélites en Redes de Procesamiento de Datos, y se espera, además un futuro muy promisorio en lo que concierne a una cobertura total en la Tierra; que elimine definitivamente la barrera de los océanos y las montañas.

El satélite de comunicaciones es un dispositivo que actúa principalmente como "reflector" en las emisiones terrenas. Se puede decir, que es la extensión al espacio del concepto de "torre de microondas". Al igual que éstas, los satélites "reflejan" un haz de microondas que transporta información codificada. Realmente la función, de la reflexión se compone de un receptor y un emisor, que operan a diferentes frecuencias: Recibe a 6 GHz y envía (refleja) a 4 GHz.

Físicamente, los satélites giran alrededor de la tierra, descubriendo una órbita circular en un arco ubicado sobre el ecuador, a una distancia de 35 680 Kms, y de manera síncrona, es decir, conservándose fijos con respecto a un punto específico de la tierra. La distancia a la que se encuentran es la requerida para que un satélite gire alrededor de la tierra en 24 horas, coincidiendo entonces en la vuelta completa de un punto en el ecuador. Esta es la característica que definitivamente determina el objetivo geoestacionario que tienen los satélites de comunicación.

El espaciamiento o separación entre dos satélites de comunicación, es de 2880 Kms, equivalente a un ángulo de 4°, visto desde la tierra. La consecuencia inmediata, es que el número de satélites posibles a conectar de esta forma es finito.

I.3.4.- Estaciones Terrenas.

Las primeras estaciones terrenas (a principios de los años 70) usaban una antena-parábola de más de 10 metros de diámetro y actualmente llegan a medir hasta 5 metros. Sin embargo hoy en día se pueden encontrar "Micro-estaciones terrenas", de hasta 60 cms. de diámetro y unos 7 Kgs de peso, provocando con esto el abaratamiento de costos además que facilitan su instalación y mantenimiento. Algunas de las características de estas micro-estaciones son:

- De fácil ubicación en la oficina o el hogar.
- Eliminan las cargas de la conexión telefónica.
- Uso de LAN como inteligencia de control.
- Permite el acceso "local" a archivos centralizados, sin demoras producidas por compartir recursos.

CAPÍTULO II

CONCEPTOS SOBRE REDES DE ÁREA LOCAL

II.1.- Introducción.

Las Redes de ordenadores (locales o remotas) surgieron para hacer posible compartir de forma eficiente los recursos informáticos (Arquitectura de Sistemas, Paquetes y Programas, y finalmente los Datos), de los usuarios. En general, esos recursos son sistemas heterogéneos: los equipos de fabricantes tienen características diferentes, utilizan y ejecutan Programas con características específicas y distintas para las aplicaciones deseadas por los usuarios, y manipulan y producen datos con formatos incompatibles. Así mismo, equipos idénticos de un único fabricante, que se integran en aplicaciones distintas, pueden presentar características heterogéneas.

Esa heterogeneidad de los sistemas beneficia al usuario, que no está limitado a un único tipo de sistemas para sus distintas aplicaciones. Así, se puede seleccionar el sistema que mejor se adapte a las condiciones de aplicación que interesen y el presupuesto disponible. Por otro lado, tal heterogeneidad dificulta considerablemente la interconexión de equipos de fabricantes diferentes, según Menascé, (1994).

La interconexión de "redes", a su vez, contribuye a hacer más difícil el problema, ya que puede haber redes diferentes con servicios de transmisión diferentes, que requieran interfases diferentes. En necesario, pues, una manera por la cual, el problema de las heterogeneidades no haga inviable la interconexión de sistemas distintos. En otras palabras, ¿cómo diseñar e implantar una red para la interconexión de sistemas heterogéneos? La incompatibilidad de equipos y/o redes fue inicialmente resuelta a través del uso de convertidores.

El almacenamiento y análisis de Información ha sido uno de los grandes problemas a que se ha enfrentado el Hombre desde que inventó la Escritura. No fue sino hasta la segunda mitad del Siglo XX que el Hombre ha podido resolver en parte este problema gracias a la invención del ordenador.

En la Década de los años cincuenta, el Hombre dio un gran salto en este problema al inventar el ordenador Personal. Ahora, la Información podía ser enviada en grandes cantidades a una localidad central donde se realizaba el procesamiento de la misma.

El problema era que esta información (que se encontraba en grandes cajas repletas de tarjetas) tenía que ser *"acarreada"* al Departamento de Proceso de Datos).

Con la aparición de las terminales en la década de los sesenta se logró la comunicación directa entre los usuarios y la Unidad Central de Proceso, logrando con esto una comunicación más rápida y eficiente, pero se encontró con un problema, entre más terminales y periféricos se agregaban a los ordenadores, la velocidad de respuesta de las mismas comenzó a decaer.

Hacia la mitad de la década de los setenta la refinada tecnología del silicón e integración en miniatura permitió a los fabricantes de ordenadores construir más inteligencia en máquinas más pequeñas.

Estas máquinas llamadas micro-ordenadores, descongestionaron a las viejas máquinas centrales y ahora cada usuario tenía su propio micro-ordenador en su escritorio.

Al principio de la década de los ochenta los micro-ordenadores habían evolucionado por completo el concepto de la Computación Electrónica así como sus aplicaciones y mercados. Los Gerentes de los Departamentos de Informática fueron perdiendo el control de la Información ya que ahora el proceso de la Información no estaba centralizada.

Esta época se podría denominar como la era del *"Disco Flexible"* (Floppy Disk). Los Vendedores de micro-ordenadores proclamaban *"en estos 30 discos el usuario puede almacenar la información de todos sus archivos"*.

Sin embargo, de alguna manera se había retrocedido en la forma de procesar la Información, ya que ahora había que *"acarrear"* la Información almacenada de los discos de un micro-ordenador hacia el otro, y también la relativa poca capacidad de los discos hacía difícil el manejo de grandes cantidades de Información.

Con la llegada de la *"Tecnología Winchester"* (almacenamiento de Información en Disco Duro) se lograron dispositivos que podían almacenar grandes cantidades de Información que iban desde 5 hasta 100 Megabytes. Una desventaja de esta tecnología era el alto costo que significaría la adquisición de un disco duro de tipo Winchester.

Fue entonces cuando nació la idea que permitiría a múltiples usuarios compartir los costos y beneficios de un disco de tipo Winchester. Las primeras Redes Locales estaban basadas en *"Disk Server's"*. Estos permitían a cada usuario el mismo acceso a todas las partes del disco. Esto causaba obvios problemas de la seguridad y de integridad en los datos.

La Compañía *Novel Inc.* fue la primera en introducir un *"File Server"* en el cual todos los usuarios pueden tener acceso a la misma Información, compartiendo archivos pero con niveles de seguridad, lo cual permitía que la seguridad e integridad de la Información no se violara.

Novel basó su investigación y desarrollo en la idea de que son los *"Programas y Paquetes"* de la Red y no de la *"Arquitectura"* que hacía la diferencia en la operación de la Red. Esto se ha podido constatar y en la actualidad Novel soporta más de 20 tipos diferentes de Redes en base a la variedad de sus Sistemas Operativos, (Novel, 1995).

El mundo de las Redes de Área Local (LAN) nació de la necesidad de compartir recursos entre los ordenadores y los usuarios para hacer más eficiente, económico y administrable un sistema de ordenadores.

La expansión de la Industria de las Redes Locales durante los últimos seis años ha sido explosiva. Se estima que sólo en los Estados Unidos de América existen más de 100 Fabricantes de Sistemas Completos, otras Empresas ofrecen componentes de Red individuales. Son más de 250 las Empresas dedicadas al negocio de Redes Locales y sus componentes.

La idea básica de una Red de Área Local (LAN) es facilitar el acceso a todos y desde todos los Equipos Terminales de Datos (ETD) de la Oficina, entre los que se encuentran no sólo los ordenadores, sino también otros dispositivos presentes en casi todas las Oficinas: Impresoras, Trazadores Gráficos, Archivos Electrónicos, Bases de Datos, así como compartir recursos disponibles dentro de la Red.

La Red de Área Local (LAN) se configura de modo que proporcione los Canales y Protocolos de Comunicación necesarios para el intercambio de datos entre ordenadores y Terminales.

Una Red Local de micro-ordenadores según Green (1992), es la interconexión de Estaciones de Trabajo que permite la comunicación entre ellas y compartir recursos en forma coordinada e integral, aprovechando la base instalada de ordenadores. Las ventajas que ofrece este tipo de Red de ordenadores son las siguientes:

1.- Compartir recursos *("Hardware y Software")*. Se tiene información y dispositivos a los cuales se puede acceder.

2.- Intercambiar información.

3.- Respaldar datos.

4.-Tener flexibilidad en el manejo de la información.

5.- Crecimiento modular (se puede empezar con una Red pequeña).

6.- Facilidad de adquisición (principalmente por el Sector Público, ya que los ordenadores se arman en México).

7.- Son sistemas que permiten cambiar de recursos sin muchas dificultades.

8.- Servicios de Correo Electrónico y Mensajería.

II.2.- Elementos de una Red.

Los elementos básicos de una Red de Área Local (LAN) son, según Tanenbaum, (1991):

1.- Las Estaciones de Trabajo (ordenadores).

2.- El Servidor de la Red (ordenador tipo AT).

3.- Los Cables de Comunicación.

4.- Las Tarjetas de Interfase.

5.- El Sistema Operativo.

1.- Las Estaciones de Trabajo.- Son micro-ordenadores que utiliza el usuario para Procesar su información. Estos micro-ordenadores pueden ser de tipo AT, con o sin Disco Duro. Para procesar la información, el usuario puede hacer uso de los recursos de su micro-ordenador o acceder a la Red para utilizar unidades de memoria, impresoras, graficadores y Módems.

2.- El Servidor de la Red.- Es un micro-ordenador de alto rendimiento que tiene uno o varios discos duros de alta velocidad, gran capacidad de memoria y varios puertos para conectar periféricos. Este micro-ordenador ofrece sus recursos a los demás usuarios.

Puede haber uno o varios Servidores en la misma Red, y dependiendo del tamaño de la Red, el Servidor puede ser un ordenador con un Microprocesador PENTIUM® de alta capacidad.

Se tienen los siguientes tipos de servidores para una Red de Área Local (LAN):

a). Dedicado o no Dedicado.

b). Centralizado o distribuido.

Las funciones del servidor dedicado son exclusivamente administrar los recursos de la Red y controlar el acceso a datos y programas de aplicación por parte de los usuarios de la Red.

Por otra parte, un servidor no dedicado es aquel que además, se utiliza también como una Estación de Trabajo de la Red. Es poco recomendable utilizar el Servidor en modo no dedicado, ya que hace más lento el funcionamiento de la Red.

Las Redes con Servidor centralizado, utilizan una sólo ordenador como Servidor de Archivos, Servidor de Impresoras y Administrador de la Red.

Las Redes con varias Estaciones de Trabajo, y gran tráfico de información, utilizan como Servidor Distribuido dos o más ordenadores en donde alguna de ellas, se encarga de Administrar el uso de Impresoras, otra para Administrar Archivos y proporcionar Programas de Aplicación y posiblemente una tercera, para Comunicación con otras Redes o *"Mainframes"*.

Una de las ventajas de las Redes de ordenadores, es que se puede aumentar la capacidad de almacenamiento con sólo agregar más equipos y que la ubicación de éstos, se puede ajustar a la distribución física de los Departamentos de la Empresa que utilice la Red.

3.- El Cable de Comunicación.- Es el Medio Físico que se utiliza para enviar o recibir mensajes de un ordenador a otro. Son tres los medios de Comunicación para Redes Locales de ordenadores y son:

a). Cable Trenzado o Telefónico.

b). Cable Coaxial.

c). Fibra Óptica.

4.- Tarjetas de Interfase.- Las tarjetas de interfase de Red *NIC (Network Interface Card)*, son una pieza de la Arquitectura *("Hardware")* que va dentro del ordenador y que provee la conexión física a la Red.

La tarjeta de interfase toma los datos del ordenador, los convierte a un formato apropiado para poder ser transportados y los envía por el cable, a otra tarjeta de interfase. Esta tarjeta los convierte nuevamente al formato original y los envía al ordenador. Las funciones de la tarjeta de interfase son las siguientes:

a). Comunicaciones de la Tarjeta de Interfase hacia el ordenador.

b). Almacenamiento en Memoria.

La mayoría de las tarjetas de interfase utilizan un *"Buffer"*[2]. Este *"Buffer"* compensa los retrasos inherentes a la transmisión. Para hacer esto, el *"Buffer"* almacena temporalmente los datos que serán transmitidos a la Red o al ordenador.

Usualmente, los datos vienen a la tarjeta más rápido de lo que pueden ser convertidos a serie o paralelo *"Despaquetizados"*, leídos y enviados; por lo cual, se debe contar con un *"Buffer"* que los almacene temporalmente.

[2] "Buffer".- Se define como un canal de retención momentáneo de información.

Algunas tarjetas de interfase no cuentan con *"Buffer"* de memoria, sino que utilizan la Memoria tipo RAM del ordenador, lo cual es más barato, pero también más lento.

c). Construcción de Paquetes.- La tarjeta de interfase funciona como un Dispositivo de Entrada/Salida en el que la memoria de su Microprocesador, es compartida tanto por la *UPC* (Unidad de Procesamiento Central), como por la tarjeta y es ahí donde se *"Parte"* el mensaje en pequeños paquetes de información que son enviados a la tarjeta de interfase receptora, la cual reconstruye el mensaje original.

d). Conversión Serie/Paralelo.- La tarjeta de interfase posee un controlador que toma los bits que recibe el ordenador en paralelo, y los envía en serie por el cable de la Red. En el lado receptor, se repite el proceso en forma inversa.

e). Codificación y Decodificación.- Esta tarea consiste en convertir los datos que envía el ordenador, en señales eléctricas que representan *"0" y "1" lógicos,* para poder ser transmitidos por el cable de comunicación.

f). Acceder al Cable.- Todas las tarjetas de Interfase, cuentan con un conjunto de circuitos que definen el método para acceder a la red: *TOKEN BUS, TOKEN RING Y CSMA/CD.*

g). *"Handshaking".-* Es un proceso de señalización entre la tarjeta transmisora y la tarjeta receptora, para ponerse de acuerdo en la forma de transmitir. La negociación consiste en establecer el tamaño máximo de los paquetes a ser enviados, los tiempos de espera, el tamaño del *"Buffer"* de memoria, etcétera.

La complejidad de la tarjeta de interfase, es la que define las características de la transmisión, pero cuando se enlazan dos tarjetas de características diferentes, se transmite en la forma en que puede hacerlo la tarjeta menos compleja.

h). Transmisión - Recepción.

5.- Sistema Operativo de la Red.- Es un conjunto de programas que residen en el Servidor, y que se encargan de comunicar a las Estaciones de Trabajo entre sí, garantizar la integridad de la información y controlar el uso de los recursos de la Red.

Hay muchos Sistemas Operativos, cada uno con características propias, que los diferencian de otros. Los más populares son: *Sistema Operativo Novel® Network, IBM PC LAN® y el LAN MANAGER®, WINDOWS NT®, UNIX®, LINUX®, SUN SOLARIS®, etcétera.*

II.3.- Topologías y Métodos para Acceder a las Redes.

Según Madron (1997): *"La Topología de una Red, es la forma física de conectar las Estaciones de Trabajo, adoptada por la persona que diseña la Red, así mismo, las Estaciones de Trabajo se comunican a la Red por un Método de Acceso Específico que depende del tipo de Red de que se trate".*

Los Métodos para Acceder son técnicas utilizadas por las Estaciones de Trabajo, para compartir el canal de comunicación. Los tipos de Redes más importantes de acuerdo a la Topología son:

1.- Red Tipo Anillo.

2.- Red Tipo Bus ó Lineal.

3.- Red Tipo Árbol ó Estrella.

La elección de uno u otro tipo de Red influye en algunas características de la Red, tales como:

1.- La flexibilidad de la Red para aceptar más Estaciones de Trabajo.

2.- El tráfico máximo de información que acepta la Red, sin que se produzcan interferencias continuas.

3.- Los tiempos máximos de Transmisión - Recepción.

4.- El precio de la Red.- Una Topología mal elegida, eleva los costos de la Red.

II.4.- Características de las Topologías de una Red.

II.4.1.- Red Tipo Anillo.

"En esta Topología, las Estaciones de Trabajo y el Servidor están conectados a través de un sólo Cable de Comunicación de trayectoria cerrada, en donde la información fluye en un sólo sentido.

El Método para Acceder al Cable se llama TOKEN-RING, en el cual, si una Estación de Trabajo quiere transmitir datos, envía un arreglo de bits de información (TOKEN) que son recibidos por el ordenador más cercano, la cual los retransmite y los envía al siguiente ordenador; y así sucesivamente hasta que el mensaje llega a su destinatario". (Giozza; De Araújo; Moura, 1996).

Con este Método para Acceder se tienen las siguientes ventajas:

1.- Los tiempos máximos de espera están definidos.

2.- Como el Servidor sondea primero cuál Estación de Trabajo quiere transmitir, no existen interferencias entre las Estaciones de Trabajo.

3.- Es un Método de Acceso útil en Redes con gran carga de trabajo.

4.- Los nodos se conectan en forma circular.

5.- Cada uno de los nodos retransmite a su vecino.

6.- Se necesita que una máquina sea *"MONITOR"* y esto se decide según criterios.

Desventajas:

1.- Si un nodo falla, afecta el funcionamiento de la Red.

2.- La ruptura de un cable afecta a toda la Red.

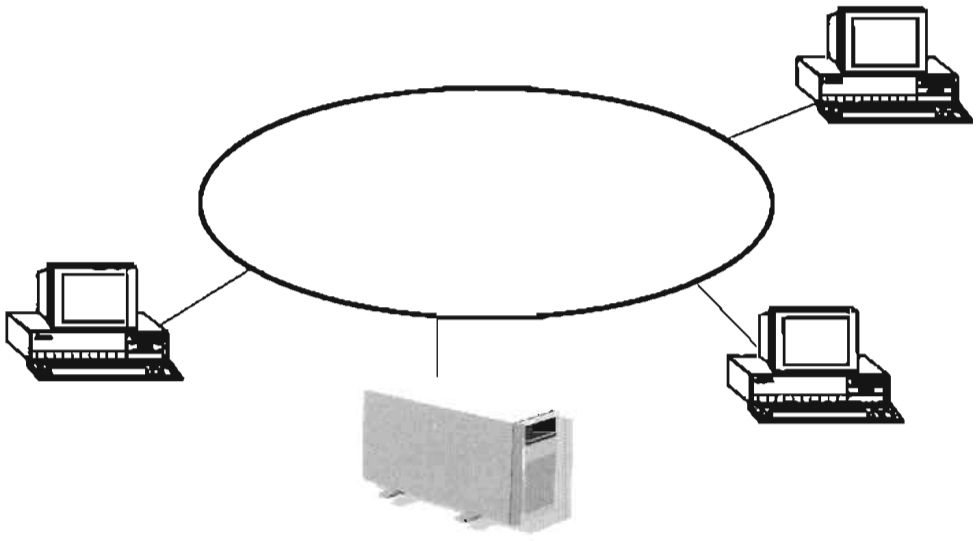


Figura II.1.- Topología de Anillo.

II.4.2.- Red Tipo Bus o Lineal.

"Este tipo de Redes tienen un sólo bus ó Cable Común de Comunicación, que transporta la información de todas las Estaciones de Trabajo conectadas a él. Estas Redes pueden utilizar el Método para Acceder CSMA/CD (Carrier Sense Multiple Access With / Colision Detection) ó el "TOKEN PASSING".

En el Método para Acceder de Forma Múltiple en el Sentido del Portador con Detección de Colisión, las Estaciones de Trabajo que desean transmitir compiten entre sí para utilizar el Cable de Comunicación". (Conant, 1996).

Cuando una Estación de Trabajo transmite, espera una confirmación de que su mensaje fue recibido correctamente, pero si esto no sucede, quiere decir que hubo una *"Colisión"* en el cable debido a que dos ó más Estaciones de Trabajo, transmitieron al mismo tiempo.

Una vez detectada la *"Colisión"* de datos de los ordenadores involucrados, esperan un tiempo aleatorio y diferente en cada una para retransmitir el mensaje, con lo que se garantiza el que no exista otra colisión.

La principal desventaja de este Método de Transferir Información, es que los tiempos de espera pueden llegar a ser muy grandes en condiciones de alto tráfico de información. Las características principales de esta Topología son:

1.- Es la Topología más simple. Un cable lineal con varios dispositivos conectados a lo largo de él.

2.- Las transmisiones de un nodo viajan en ambos sentidos.

3.- Los nodos no retransmiten la información.

4.- Si un nodo falla, no afecta el funcionamiento de la Red.

5.- La ruptura en el cable afecta a toda la Red.

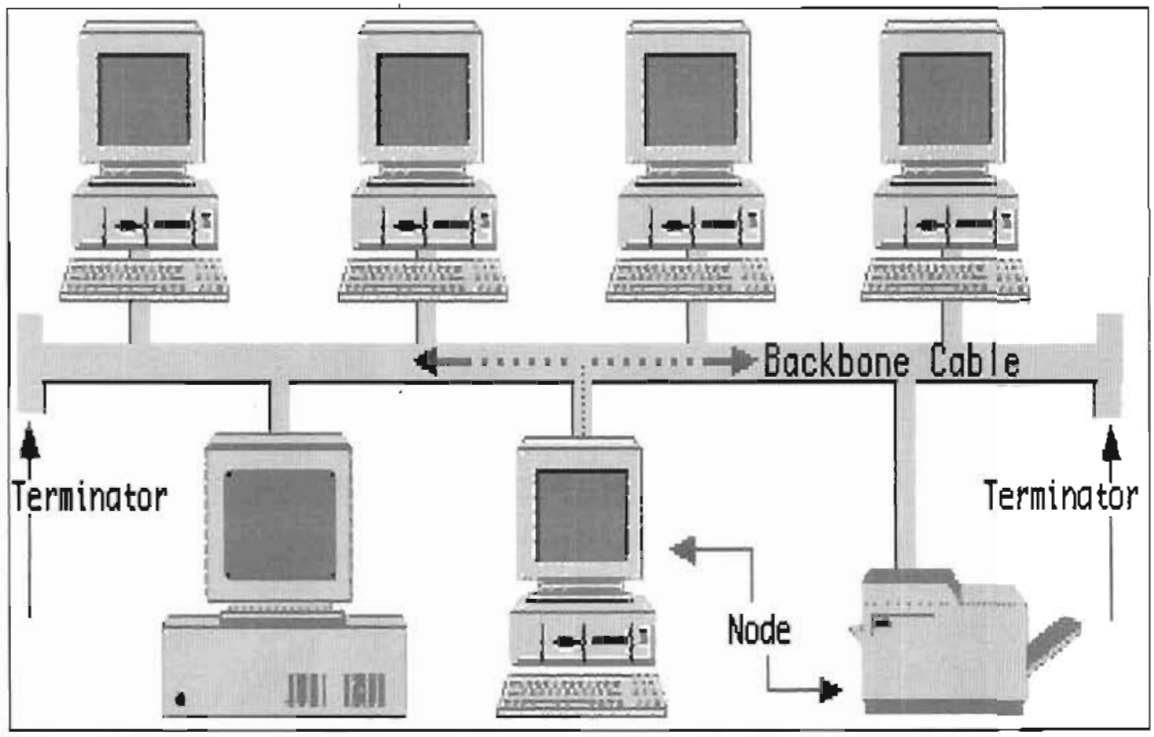


Figura II.2.- Topología de Bus.

II.4.3.- Red Tipo Árbol o Estrella.

"La Red tipo Árbol se conoce también como Anillo Modificado, lo cual se debe a que esta Red es una combinación de la Red de Anillo y la Red tipo Lineal. Se dice que físicamente es una Red Lineal, porque tiene un bus central de comunicaciones al que se conectan las Estaciones de Trabajo en forma directa o a través de ramificaciones.

Por otra parte, su Método para Acceder, llamado TOKEN PASSING, hace que lógicamente funcione como si fuera una Red tipo Anillo". (Bates, 1994).

El Método para Acceder llamado *"TOKEN PASSING"*, consiste en la transmisión de tramos de bits *(TOKEN's)* de una Estación de Trabajo a otra; pero a diferencia de la Red Anillo, a cada Estación de Trabajo se le asigna un turno para transmitir que puede ser diferente al de su ubicación física dentro de la Red. Las características más importantes de esta Topología son:

1.- Los nodos se conectan a un Concentrador Central.

2.- La falla de un nodo no afecta la Red.

3.- La ruptura de un cable afecta sólo al nodo conectado a él.

4.- El tráfico de información aumenta conforme se incrementan los puertos.

5.- El repetidor Reenvía la información n-1 veces a través del repetidor.

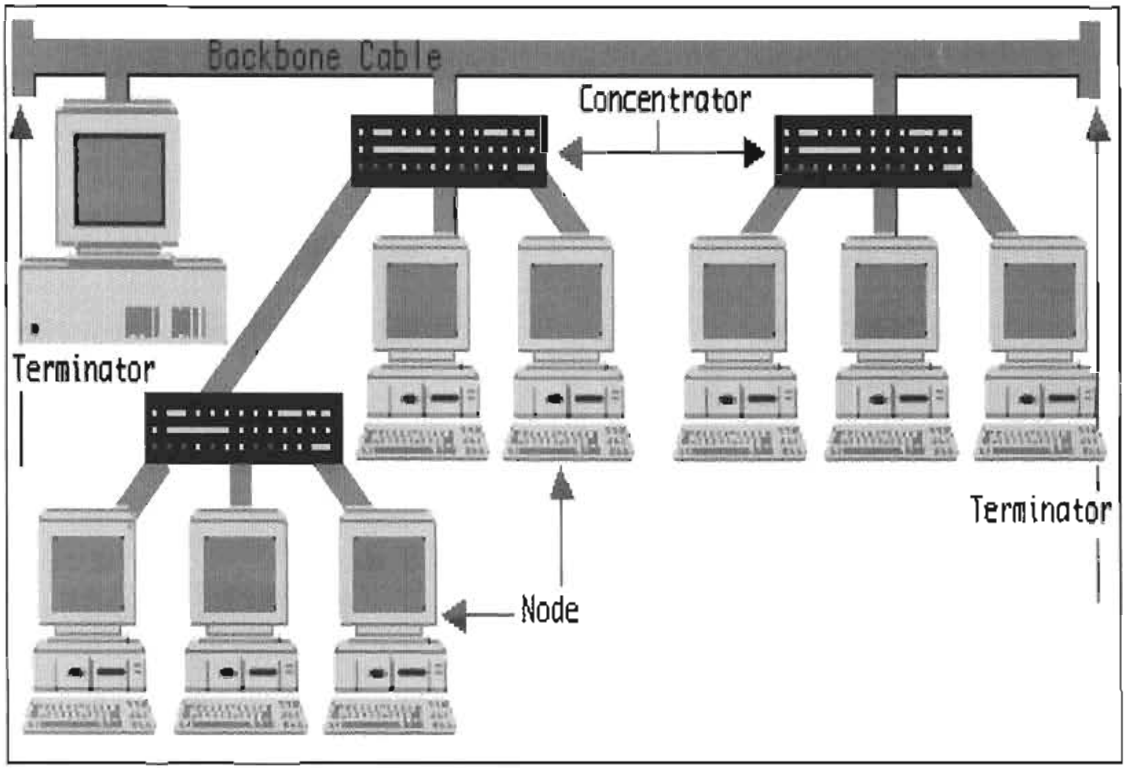


Figura II.3.- Topología de Árbol.

Aunque las diferencias entre las Redes de Área Local (LAN) son grandes, todas ellas comparten varias características comunes, según (Black, 1994), son las siguientes:

1.- Una Red de Área Local (LAN) proporciona la facilidad mediante la cual se interconectan los Microprocesadores, el almacenamiento auxiliar, los dispositivos de facsímil, las impresoras, las copiadoras inteligentes, los equipos de fotocomposición, los teléfonos y los dispositivos de video para comunicarse entre sí. Algunas Redes de Área Local (LAN) interconectan cientos de dispositivos.

2.- El objetivo supuesto de todas las Redes de Área Local (LAN), es permitir a las Organizaciones tener grandes ganancias en productividad y ahorros en costos mediante las eficiencias inherentes de la compartición de recursos.

Una Red de Área Local (LAN) es una Red de Comunicaciones entre elementos al mismo nivel debido a que todos los dispositivos de la Red tienen iguales condiciones para acceder a todos los servicios de la Red.

3.- Debido a que son de propiedad privada y se instalan de manera que no interfieran con las comunicaciones de otras Redes, las Redes de Área Local (LAN) no están sujetas a la Jurisdicción de las Agencias Reguladoras Federales o Estatales.

4.- Las Redes de Área Local (LAN) generalmente están limitadas a un sólo edificio o a un complejo de edificios, aunque algunos dispositivos de la Red pueden extenderse hasta 80 kilometros. Esto significa que una Red de Área Local (LAN) puede conectar dispositivos de comunicación ubicados en diferentes pisos de un edificio, en edificios adyacentes o en la misma Ciudad.

5.- Las velocidades de transmisión típicamente se encuentran entre 1 y 10 MBits/seg. Sin embargo, algunas Redes de Área Local (LAN) emplean velocidades de transmisión que superan bastante a los 10 Mbits/seg. Como podría sospecharse, entre mayor sea la velocidad de datos, mayor será el costo de la Red de Área Local (LAN).

6.- Las Topologías de Bus y de Anillo emplean un cable compartido. Esto significa que no puede haber dos mensajes en el cable en el mismo lugar, y al mismo tiempo, sin que se presente una colisión entre ellos, ocasionando la destrucción de ambos mensajes.

Los dispositivos de alguna manera, deben transmitir mensajes de acuerdo a un esquema de acceso, tomando turnos para el uso del cable. El principal esquema para acceder para el cable en el caso de un Bus es la contención. Para un Anillo es el pase de *(TOKEN's)*. Una Estrella utiliza un *Concentrador Central* para controlar la entrada.

II.5.- Técnicas de Comunicación.

La transmisión de bits de información a través del Cable de Comunicación, se realiza en dos formas: *En Banda Base y en Banda Ancha.* (De Prycker, 1993).

La mayor parte de las Redes Locales trabajan en Banda Base; es decir, utilizan Señales Digitales para transmitir su información a lo largo del cable. La ventaja de utilizar Señales Digitales es que el costo y la complejidad de la Red disminuyen, porque dado que el ordenador también trabaja con Señales Digitales, los módulos de conexión al cable son sencillos.

En las Redes de Banda Ancha, las Señales Digitales del ordenador se tienen que convertir en Señales Analógicas usando un Módem para poder ser transmitidas a través del cable.

El ritmo de frecuencia que ocupan estas Señales al ser transmitidas por el cable, es pequeño comparado con el rango de frecuencias (ancho de banda), que puede manejar el Cable de Comunicaciones, lo cual permite que otras Señales Analógicas (Voz, TV, Fax), de frecuencias distintas puedan ser transmitidas simultáneamente por el mismo cable.

Algunos Bancos prefieren gastar en una Red de Banda Ancha, para poder conectar sus ordenadores, Teléfonos y Cámaras de TV por un mismo cable, y reducir así los costos de instalación.

Las características de las Redes que operan en Banda Base son:

1.- Son de fácil mantenimiento e instalación, ya que no se requieren Módems.

2.- El número máximo de ordenadores conectadas a la Red es reducido.

3.- Las distancias máximas entre elementos de la Red son más pequeñas que las de Redes en Banda Ancha.

4.- Aceptan sólo Señales Digitales.

Las características de las Redes que operan en Banda Ancha son:

1.- Permite conectar más elementos a la Red y utilizar cables de conexión de longitudes mayores.

2.- Se pueden transmitir varias señales (Voz, Datos, TV, Fax), por el mismo cable simultáneamente.

3.- Las velocidades globales de comunicación son altas.

4.- Utilizan un cable para transmitir y uno para recibir, ó un sólo cable con un rango de frecuencia para transmitir y otro para recibir, ya que las Señales de Información viajan en un sólo sentido.

5.- Debido a la utilización de equipos para Modular y Demodular la Señal, filtros de frecuencia y amplificadores, la instalación y mantenimiento de estas Redes es más costoso y complejo.

II.6.- Redes Locales en el Mercado.

Cuando se desea contar con una Red Local de ordenadores, se puede elegir entre tres opciones establecidas y por los Estándares Internacionales. Cada tipo de Red se diferencia, no sólo por su Topología y Método de Acceso, sino también por características especiales que las hacen más apropiadas en ciertos casos. Los tipos más comunes son:

II.6.1.- Red Local ARCNET.

La Red ARCNET (ATTACHED RESOURCE COMPUTER NETWORK), es una Red Local tipo Árbol capaz de interconectar hasta 255 nodos. Por nodo se refiere a cualquier dispositivo conectado a la Red como Periféricos y Estaciones de Trabajo. (Black, 1999).

Las principales características de esta Red son:

1.- Topología: Estructura de Árbol.

2.- Velocidad: 2.5 Mbits/segundo.

3.- Tiempo de Respuesta: Determinístico.

4.- Método de Acceso: Token Passing.

5.- Medio de Transmisión: Cable Coaxial de 93 Ohms.

6.- Modo de Transmisión: Banda Base.

Las unidades repetidoras de *ARCNET* se clasifican en pasivas y en activas; las activas a su vez se clasifican en internas y externas.

a). Unidades repetidoras pasivas.- Cuando la distancia que debe cubrirse entre los nodos más lejanos de una Red, no sobrepasa los 60 metros, y además el número de nodos no excede a cuatro, es posible conectar una unidad repetidora pasiva, la cual tiene cuatro puertos con un alcance de 30 metros en cada uno de ellos.

Esta unidad debe ser conectada directamente a las tarjetas de Red o a un puerto de un repetidor activo; esto significa, que no se pueden conectar dos pasivos entre sí, ni tampoco dos o más activos por medio de un pasivo.

b). Unidades repetidoras activas.- Tienen un alcance por puerto de 600 metros, lo cual las hace ideales para instalaciones donde la distancia sea un factor importante.

Por otro lado, tienen la capacidad de ser interconectados entre ellos y con repetidores pasivos, lo cual brinda la posibilidad de contar con el crecimiento que se requiera en cualquier tipo de instalación. Estos alimentadores pueden ser internos o externos y requieren alimentación eléctrica.

Regularmente los repetidores activos, poseen ocho puertos y los pasivos cuatro. Mientras el activo amplifica la señal a sus niveles óptimos, el pasivo sólo divide la señal (técnicamente hace un acoplamiento de impedancias en un sencillo circuito de 4 resistencias).

Principales ventajas de la *Red Local ARCNET:*

1.- Es una Red de uso general.

2.- Tiempo de respuesta estable bajo carga de trabajo.

3.- Flexibilidad en crecimiento.

4.- Excelente costo-beneficio.

II.6.2.- Red Local ETHERNET.

La Red Local ETHERNET es una Red tipo Bus o Lineal, y recibe este nombre en analogía a la Teoría del Éter de la transmisión de la luz, para Black (1999), las principales características de este tipo de red son:

1.- Topología: Bus o Lineal.

2.- Medio Físico: Cable Coaxial de 50 Ohms.

3.- Modo de Transmisión: Banda Base.

4.- Método de Acceso: CSMA/CD.

5.- Velocidad de Transmisión: 10 Mbits/segundo.

El crecimiento total de la Red es de 86 nodos repartidos en tres segmentos de una distancia no mayor a 200 metros cada uno, unidos por dos repetidores, siendo éste el número máximo de ellos.

Un segmento es un cierto tramo de cable, al que se agregan elementos de conexión hacia los ordenadores *(Transceiver's),* y que en los extremos se les colocan dispositivos terminadores.

Un segmento está limitado a soportar un máximo de 30 nodos; sin embargo, este número puede duplicarse o triplicarse al colocar uno o dos repetidores; estos elementos están considerados como un nodo más entre cada segmento al que están conectados, por lo tanto, al agregar dos repetidores, se tienen 4 nodos, menos del total de 90, así que el número máximo es 86.

Esta Red puede trabajar a una velocidad promedio de 10 Mbits/segundo, lo cual la hace ideal para cargas pesadas de acceso a la Red; sin embargo, debido a que utiliza el Método de Acceso

CSMA/CD, su funcionalidad va decayendo rápidamente a medida que el número de usuarios en la Red se incrementa, es por esto que esta Topología se recomienda cuando la carga de trabajo es pesada, pero el número de Estaciones de Trabajo activas no es mayor de 10 a 15.

El Cable de Comunicación utilizado es el cable coaxial de 50 Ω, que viene en dos versiones:

1.- Cable grueso: Hasta 500 metros/Segmento. Mínimo 2.5 metros de distancia entre estaciones de trabajo. Requiere un "Transceiver" por estación, y dos terminadores por segmento.

2.- Cable delgado: Hasta 300 metros/Segmento. Mínimo 3 metros de distancia entre estaciones. Requiere un conector tipo "T" por Estación y dos terminadores por segmento.

Para un cableado *ETHERNET*, se recomienda lo siguiente:

1.- Un segmento no debe exceder los 185 metros.

2.- Se puede tener un total de 5 segmentos conectados por repetidores, tres segmentos activos y dos pasivos.

3.- La distancia total de la Red, no debe exceder de 555 metros.

4.- La mínima distancia de cable entre dos nodos, debe ser de 0.5 metros.

5.- El número máximo de nodos por segmento es 30.

6.- El número total de nodos por Red es de 86.

Principales ventajas de la *Red Ethernet:*

1.- Garantiza conectividad a otros ambientes (uso específico).

2.- Excelente rendimiento con pocos nodos.

3.- Está apoyado por varias Empresas Transnacionales de importancia.

Principales desventajas:

1.- Tiempo de respuesta decreciente bajo carga de trabajo.

2.- Es necesario anticipar y dejar cableado el crecimiento de la Red.

II.6.3.- Red TOKEN-RING.

Esta Red fue patrocinada por IBM y apareció a finales de 1985. Sus principales características son las siguientes: (Latif: Rowlance: y Adams, 1992).

1.- Topología: Anillo.

2.- Modo de Transmisión: Banda Base.

3.- Número Máximo de Nodos: 72.

4.- Velocidad de Transmisión: 4 Mbits/Segundo.

El dispositivo básico de la Red es conocido como *MUA* (Multi Acces Unit) cuya finalidad es la de mantener el Anillo cerrado pese a que algunas Estaciones de Trabajo no estén prendidas o estén fallando. Esta Red es altamente recomendada cuando se tiene la necesidad de que la Red se comunique con un Mini-ordenador o un *"Mainframe"* IBM.

Los *MAU's* que se ofrecen en el mercado son de 4 puertos, lo cual significa que únicamente se pueden tener cuatro máquinas conectadas a éste; sin embargo, si se requiere de más equipo en la Red, es necesario que se coloquen más unidades de este tipo.

Para que siga respetando la estructura de Anillo, es necesario que se sigan conectando las Unidades Centralizadoras entre sí, para ello cada unidad posee dos puertos adicionales mediante los cuales es posible la interconexión.

Las características del cableado para una *Red Token-Ring* son:

1.- Cable tipo 3 (AWG 22/24) de dos pares trenzados (Telefónico).

2.- El máximo número de nodos es 72.

3.- El máximo número de *MAU's* conectados en cascada es de 18.

4.- La distancia máxima de cableado entre el *MAU* y la Estación de Trabajo es de 150 metros.

5.- La distancia máxima entre *MAU's* es de 150 metros.

Las principales ventajas de la *Red Token-Ring* son:

1.- Tiempo de respuesta estable.

2.- Conecta gran cantidad de nodos.

3.- Conectividad a otros productos IBM.

4.- El Sistema Operativo *IBM PC LAN*, está diseñado específicamente para esta Red.

5.- Su principal desventaja es el alto costo de la Red.

CAPÍTULO III

PROTOCOLOS PARA REDES DE ÁREA LOCAL

III.1.- Orígenes y Evolución del Protocolo TCP/IP.

Esta tecnología tiene su origen en el Gobierno de los Estados Unidos de Norte América, concretamente en su Departamento de Defensa (DoD). La DARPA (Defense Advanced Research Projects) comenzó a trabajar con una internet[3] (red de redes) a mediados de los años 70.

Las dos razones principales por las que el departamento de defensa creó el estándar de los protocolos de comunicación para una arquitectura fueron las siguientes:

- Una rápida proliferación de las computadoras y otros elementos de procesamiento de señales dentro de la milicia y la necesidad de conectar equipos de diferentes fabricantes.
- El creciente uso de redes de comunicaciones en la milicia y la necesidad de una variedad de tecnologías de interconexión.

El decremento del costo del *"hardware"* de las computadoras y su creciente poder había provocado un aumento en el uso de las minicomputadoras y microcomputadoras para manejar una amplia variedad de tareas. El reforzar esto provocó la superioridad del procesamiento distribuido de datos sobre los "Mainframes" tradicionales y su proceso centralizado de datos. Las principales ventajas que el procesamiento distribuido ofrecía en ése momento son: alto rendimiento y la disponibilidad de aplicaciones. Así pues, se pensó en comunicar los equipos de procesamiento de datos de varios fabricantes entre sí; tradicionalmente el software de comunicaciones desarrollado por un fabricante no era compatible con el de los demás. Al mismo tiempo, hubo un rápido incremento en el uso de redes de comunicaciones de datos dentro del DoD.

Para enfrentar estas necesidades, el DoD, a través de la Agencia de Comunicaciones de la Defensa (DCA - Defense Communications Agency) desarrolló un conjunto de protocolos militares estándares que ofrecen las siguientes ventajas:

Interoperabilidad. Es el resultado de implantar el mismo conjunto de protocolos en todos los equipos de procesamiento de datos que se desee interconectar en una Internet.

Eficiencia y productividad del fabricante. El deseo de vender del fabricante lo obliga a concentrarse en el desarrollo de protocolos estándares.

Competitividad. Sin un conjunto de protocolos estándares, los clientes tendrían que adquirir equipo nuevo del mismo fabricante para preservar la interoperabilidad.

---

3 A partir de este momento se hará la distinción entre internet (con minúscula) e Internet (con mayúscula). Propiamente, la primera se refiere a cualquier red de redes. La segunda se refiere a la red originada por ARPANET tal como la conocemos ahora, la red de computadoras más grande del mundo.

III.1.1.- Uso de los Protocolos del Departamento de Defensa (DoD) por Instalaciones No Militares.

Un desarrollo interesante e inesperado ha incrementado el uso de TCP/IP en aplicaciones no militares. Esto se debe a la introducción de la Arquitectura de Sistemas de Redes (SNA - System Network Architecture) por parte de IBM en 1974 o a la introducción de otras arquitecturas propietarias de comunicaciones creadas por otros fabricantes que obligan al cliente a permanecer ligado al hardware del mismo.

Este tipo de arquitecturas propietarias ha forzado a los fabricantes y a sus clientes a usar estándares internacionales basados en la arquitectura del modelo OSI. Sin embargo, para sorpresa de muchos observadores, una gran cantidad de clientes se ha optado por la familia de protocolos TCP/IP.

En **1969** el DoD construyó una red de Área Amplia de 4 nodos; la de la corporación de desarrollo de sistemas, las Universidades de California en Santa Bárbara, y en los Ángeles e ISR Internacional. Esta red fue llamada ARPANET[4] y se trataba de un experimento para demostrar la factibilidad de la tecnología de intercambio de paquetes. Este experimento fue todo un éxito y fue demostrado al público en **1972**, para estas fechas la red incluía varias universidades y centros de investigación cuyos hosts[5] contaban con la implantación de varios protocolos experimentales (se trataba de 50 hosts en 20 redes). ARPANET se usó varios años para proyectos de investigación científicos y del ejército.

En el año en que se demostró ARPANET, comenzaron los trabajos para el desarrollo de una segunda generación de protocolos para usar la experiencia obtenida con el primer experimento. En **1980** la Universidad de California en Berkeley recibió el patrocinio del DoD para el mejoramiento del sistema operativo UNIX con capacidades de cómputo distribuido, éste sistema operativo había sido desarrollado originalmente en los Laboratorios Bell y posteriormente esta Universidad lo adoptó.

El resultado fue el desarrollo de sistema UNIX 4.1 BSD, el cual corría en máquinas VAX de DEC. Este sistema operativo entre otras mejoras incluía soporte para redes locales a través de NCP y TCP.

Así, para **1982** se especificó una familia de nuevos protocolos, sujetos a exhaustivos experimentos. Los dos principales miembros de esta familia fueron el Protocolo de Control de Transmisiones (TCP - Transmission Control Protocol) y el Protocolo Internet (IP - Internet Protocol). Actualmente a estos protocolos se les conoce como la familia de protocolos TCP/IP.

Para **1983** se comenzó a utilizar el protocolo TCP/IP en la red ARPANET del DoD como el protocolo estándar al mismo tiempo se derivaba MILNET, una segunda red surgida de la ARPANET. MILNET se encargaba de las tareas relacionadas con la investigación militar y, junto con ARPANET y otras redes clasificadas, se conocieron como la Red de Datos de la Defensa (DDN - Defense Data Network). Existen gateways (compuertas) entre ARPANET y MILNET para facilitar el intercambio de información entre ellas.

Las oficinas del ARPA se responsabilizaron de las actividades de investigación y desarrollo de varios grupos académicos y comerciales, entre los que se encontraban SRI Internacional, de la

---

4 ARPA - Advanced Research Projects Agency. ARPANET es la red que esta organización construyó.

5 Dentro de la nomenclatura TCP/IP un host es una computadora de la red.

Universidad de Stanford, la UCLA, el MIT, la corporación RAND, la Universidad de California en Santa Bárbara, la Universidad de Utah y otros.

Estos grupos desarrollaron gran parte de los conceptos que actualmente permiten la comunicación en redes locales y remotas. En realidad, TCP/IP es la segunda generación de protocolos desarrollada por la comunidad ARPA. La primera generación fueron aquéllos protocolos creados en diferentes ordenadores *"hosts"* independientes, tales como los protocolos punto a punto (Network Control Protocol, precursor de TCP/IP) y el de punto a multipunto (IMP, precursor de X.25).

III.2.- ¿Qué es la Familia ("Stack") de Protocolos TCP/IP?

TCP/IP es una colección de protocolos. Debe su nombre a sus dos protocolos más conocidos; TCP o Transmission Control Protocol, corresponde a la capa 4 del modelo de OSI (la capa de transporte) y ofrece transmisión confiable de datos. IP o Internet Protocol trabaja en la capa 3 del Modelo OSI (capa de enlace de red) y ofrece el servicio de datagramas sin conexión.

III.2.1.- TCP/IP y la Internet.

Las redes se han convertido en una parte fundamental, (se puede decir la más importante), de los sistemas de información de hoy. Forman la espina dorsal *("Backbone")* para compartir información dentro de empresas, grupos empresariales y científicos.

La mayoría de estas redes fueron instaladas en la década de los 60 y 70, cuando el diseño de red era el asunto de investigación más importante relacionado a la computación. Dio lugar a múltiples modelos de *"Networking"* tales como tecnología de conmutación de paquetes, detección colisiones en redes de área local, redes jerárquicas de la empresa, y muchas otras tecnologías excelentes.

Desde el inicio de los 70's, otro aspecto de *"Networking"* tendió a ser importante: protocolo en capas, que permite que las aplicaciones se comuniquen una con otra. Un rango completo de arquitecturas de modelos fue propuesto e implementados por varios equipos de investigadores y fabricantes de computadoras.

El resultado de todos estos grandes conocimientos técnicos es que cualquier grupo de usuarios puede encontrar hoy una red física y una conveniente arquitectura de modelo para sus necesidades específicas. Esto se extiende desde líneas asíncronas baratas sin otra recuperación de error que una función de la paridad de bit por bit, hasta amplias funciones de las redes de área amplia (públicas o privadas) con protocolos confiables tales como redes públicas de conmutación de paquetes o redes privadas SNA, para redes de área local de alta velocidad pero distancia limitada.

El problema de compartir esta información es una situación algo complicada cuando un grupo de usuarios desea extender su sistema de información a otro grupo de usuarios quienes tienen una tecnología diferente de red y diferentes protocolos de red. Consecuentemente, si pudieran acordar en un tipo de tecnología de red para interconectar físicamente las dos localidades, sus aplicaciones (tales como sistemas de correo) todavía no podrían comunicarse una con otra porque tienen diferentes protocolos.

Esta situación fue reconocida a principios de los 70's por un grupo de investigadores en los Estados Unidos de América que llegaron con un nuevo principio: *"Internetworking"*. Otras organizaciones oficiales llegaron a estar implicadas en esta área de interconectar redes, tales como ITU-T (antes CCITT) e ISO. Todos estuvieron tratando de definir un conjunto de protocolos, distribuidos en una suite bien definida de modo que la aplicación pudieran comunicarse con otras

aplicaciones, sin importar la tecnología de red subyacente y el sistema operativo donde estas aplicaciones corren.

Hoy, el Internet, el World Wide Web (www), y la supercarretera de la información son términos familiares para millones de gente en todo el mundo. Transmisión Control Protocol (TCP/IP) es la familia de protocolos desarrollada para el **Internet**.

III.3.- Asociación de la Familia de Protocolos ("Stack") de Protocolos TCP/IP con el Modelo de Referencia OSI.

Todos los protocolos de comunicación de datos tienen el mismo objetivo: mover datos entre aplicaciones sobre diferentes dispositivos. Diferentes métodos han sido desarrollados para cumplir con este objetivo, cada protocolo debe proveer la funcionalidad marcada en las capas del modelo de referencia OSI.

TCP ofrece servicios de la capa de transporte e IP los de la capa de red. Fueron desarrollados para propósitos de la IFIP (International Federation for Information Processing), el Technical Committee Working Group y la DARPA, la cual originalmente había combinado las funciones de conexión entre redes y las de transporte confiable dentro de un solo protocolo. El subsecuente desarrollo de otros protocolos de transporte separó estas funciones para que el IP se encargara de la función de interconexión entre redes donde TCP proporcionaría los circuitos virtuales confiables.

En la figura III.1se puede observar el Modelo de referencia OSI contra la familia de protocolos TCP/IP.

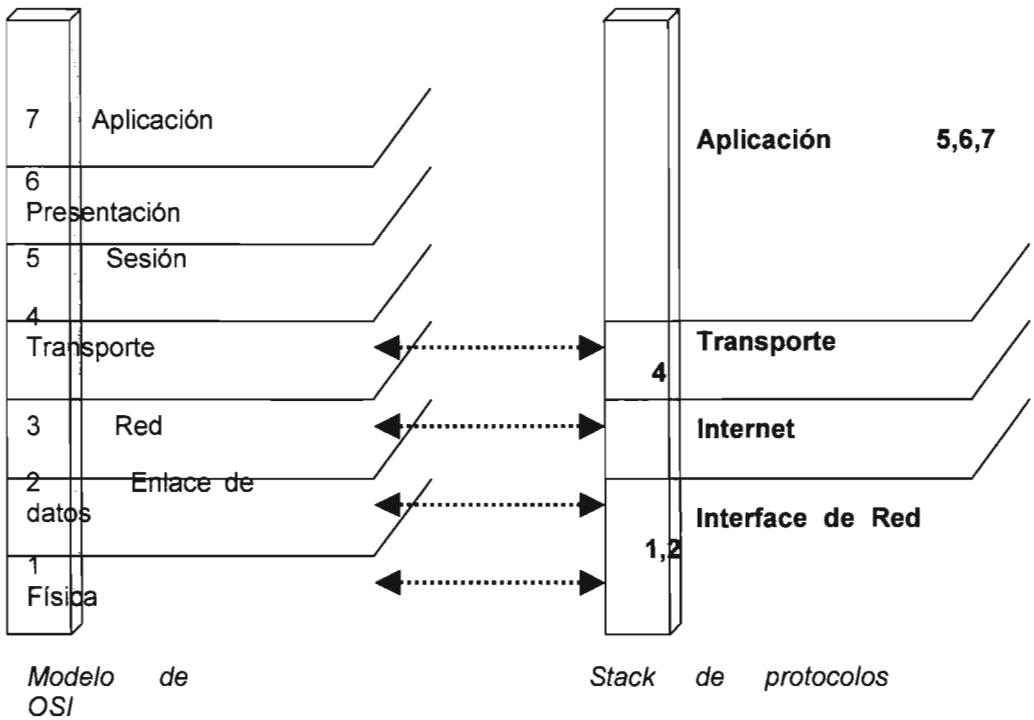


Figura III.1.- Modelo de Referencia OSI y *"Stack"* de Protocolos TCP/IP.

TCP/IP es un protocolo definido principalmente por las siguientes capas:

- Capa de Acceso a Red.
- Capa de *"Internetwork"*.
- Capa de Transporte.
- Capa de Aplicación.

III.4.- Componentes de Redes TCP/IP.

La Capa de Acceso a Red es la capa más baja en el modelo de referencia. Los servicios de los dos principales protocolos (TCP e IP) son aumentados por las aplicaciones de los niveles superiores.

Tal como se había explicado, TCP/IP se refiere a una gran familia de servicios y protocolos. Estos protocolos aparecen en la siguiente figura, la cual muestra que IP y los protocolos de los niveles superiores se pueden implantar en diversos tipos de redes. Ethernet, ARPANET y PDN (X.25) aparecen ilustradas de manera individual, mientras que Milnet e IEEE 802 se incluyen dentro de "Otras".

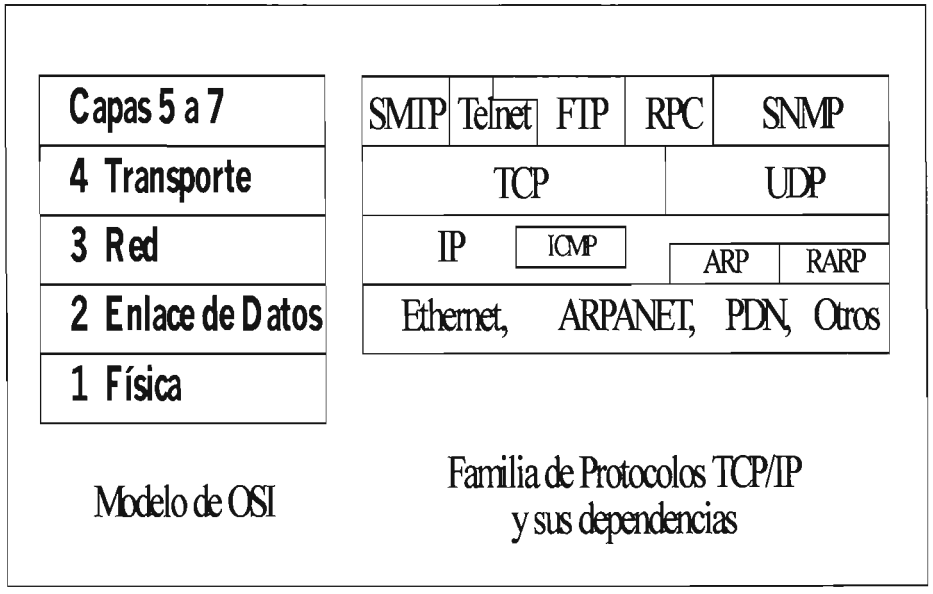


Figura III.2.- Familia de Servicios y Protocolos.

A continuación se muestra una lista con los nombres de los protocolos cuyos acrónimos aparecen en la figura siguiente y el servicio que ofrecen.

III.4.1.- Capa de Red: Nivel 3.

IP (Internet Protocol)
Entrega de datagramas sin conexión.

ICMP (Internet Control Message Protocol)
Usado por los *"gateways"* y *"hosts"* para evaluar las condiciones de funcionamiento de los servicios IP.

ARP (Address Resolution Protocol)
Mapea una dirección IP a su dirección Ethernet asociada.

RARP (Reverse ARP)
Mapea una dirección Ethernet a su dirección IP asociada.

III.4.2.- Capa de Transporte: Nivel 4.

TCP (Transmission Control Protocol)
Protocolo orientado a la Conexión con acuse de recibo.

UDP (User Datagram Protocol)
Protocolo sin conexión no confiable.

III.4.3.- Capas de Sesión, Presentación y Aplicación: Niveles 5 a 7.

SMTP (Simple Mail Transfer Protocol)
Envío y recepción de correo.

FTP (File Transfer Protocol)
Intercambio de archivos completos.

TELNET (Telecommunications Network)
Terminal virtual para acceso interactivo a servidores remotos.

NFS (Network File System)
Sistemas de Archivos Distribuidos.

SNMP (Simple Network Management Protocol)
Servicios de Administración Centralizada de Sistemas Remotos.

III.5.- Capa de INTERNET PROTOCOL (IP).

La relación de IP con el Modelo de OSI se representa de la siguiente manera:

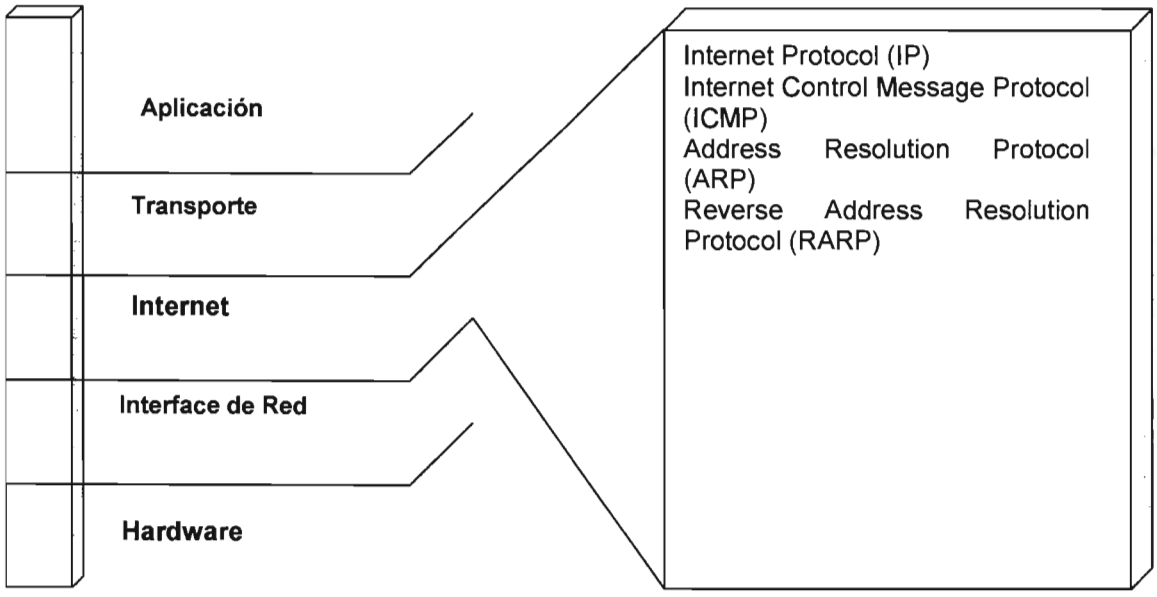


Figura III.3.- Relación IP y OSI.

Capa de Internet Protocol

El Internet Protocol (**IP**), esta definido por el RFC 791, y es el corazón de la capa de Internet. IP provee un esquema de direccionamiento conocido como IP *"Address"* o dirección lógica. Tiene el propósito de conocer la dirección a la cual se desea enviar u obtener información.

El Datagrama Internet, unidad básica de información.

La analogía entre una red física y una Internet TCP/IP es muy fuerte. En una red física, la unidad de transferencia es un *"Frame"* que contiene un encabezado y datos, donde el encabezado proporciona información tal como las direcciones fuente y destino (físicas).

La Internet le llama *datagrama de Internet* a su unidad básica de transferencia, a la que frecuentemente se le llama *datagrama IP* o simplemente *datagrama*. Al igual que un *"Frame"* típico de una red física, un datagrama se divide en áreas del encabezado y de datos.

El encabezado del datagrama contiene las direcciones fuente y destino y un campo de tipo que identifica el contenido del datagrama. La diferencia, por supuesto, es que el encabezado del datagrama contiene direcciones IP mientras que el encabezado de un *"Frame"* contiene direcciones físicas. La figura muestra la forma general de un datagrama.

Ahora que se ha descrito el formato general de un datagrama IP, se explorará su contenido con mayor detalle. La figura muestra la disposición de los campos del datagrama.

Bit 0 Bit 31

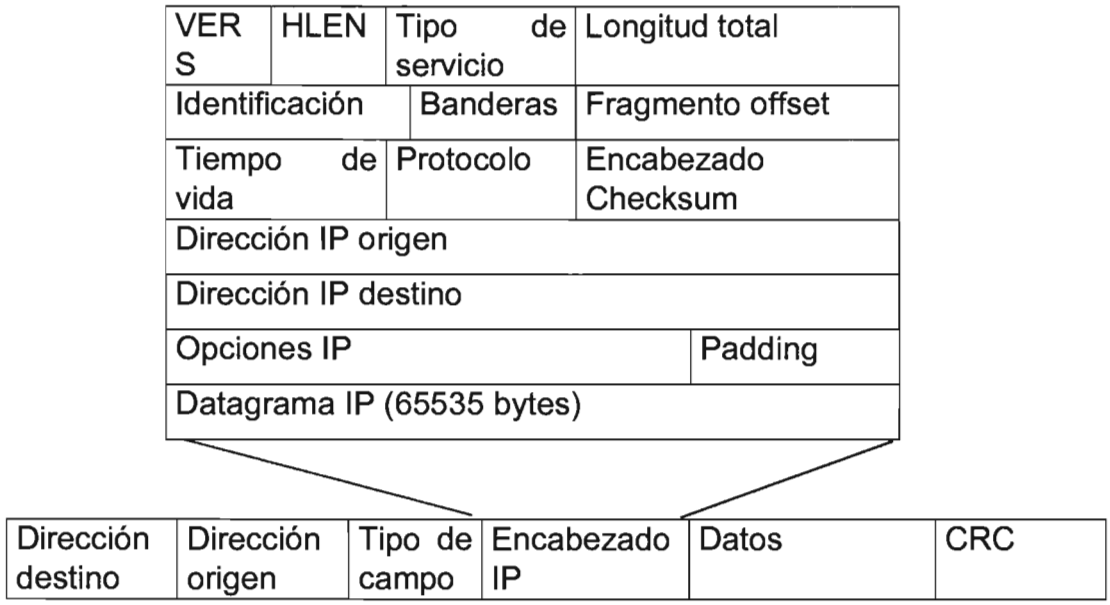


Figura III.4.- Campos del Datagrama.

III.5.1.- "Frame" de INTERNET PROTOCOL (IP).

Los campos relevantes de la porción de la cabecera de IP son:

Versión, se está utilizando la versión 4 lo que indica que el direccionamiento de IP es de 32 bits.

Identificación, en caso de ser fragmentado algún paquete entre los puntos intermedios el mismo debe ser reensamblado y se usa este campo para identificar información del mismo.

Protocolo, tipo de protocolo que usaran las capas superiores.

Checksum, método de verificar la integridad de la cabecera.

Dirección IP fuente y destino, dirección IP de 4 bytes o su equivalente en bits (32).

Tamaño del Datagrama, MTU de la Red y Fragmentación.

En el mejor de los casos, el datagrama IP entero cabría en un *"Frame"* del servicio que se esta utilizando, es decir ETHERNET, TOKEN RING, por citar algunos, haciendo la transmisión a través de la red eficiente.[6]

Para lograr tal eficiencia, los diseñadores de IP tuvieron que seleccionar un tamaño máximo de datagrama que le permitiera siempre caber en un *"Frame"*. Pero, ¿qué tamaño hubiera sido ése?

6 Un campo en el header del frame identifica el tipo de dato que se está transportando. Ethernet usa el valor 0800_{16} para especificar que el área de datos contiene un datagrama IP encapsulado.

Después de todo, un datagrama puede viajar a través de muchos tipos de redes a medida que se mueve en una Internet para llegar a su destino final.

Para entender el problema, se necesita un hecho acerca del hardware de red: cada tecnología de intercambio de paquetes pone un límite en la cantidad de datos que se pueden transportar en un *"Frame"* físico. Por ejemplo, Ethernet limita las transferencias a 1500 octetos[7] de datos mientras que proNET permite 2044 octetos por Frame. A este límite se le llama MTU (Maximum Transfer Unit) de la red. Los MTUs pueden ser pequeños: algunas tecnologías limitan las transferencias a 128 octetos o menos. El limitar los datagramas para que quepan en el MTU más pequeño de la Internet, haría las transferencias ineficientes cuando esos datagramas pasaran por redes que pudieran llevar *"frames"* de mayor tamaño. Sin embargo, permitir que los datagramas sean más grandes que el MTU mínimo en una Internet significa que un datagrama no siempre cabrá en un solo *"Frame"* de la red.

La elección debería ser obvia: el objetivo en el diseño de Internet es ocultar las tecnologías de red subyacentes y hacer la comunicación conveniente para el usuario. Así, en lugar de diseñar datagramas que se adhieran a las restricciones de las redes físicas, el software de TCP/IP escoge un tamaño inicial de datagrama conveniente y busca la manera de dividir los datagramas más grandes en piezas más pequeñas cuando el datagrama necesite atravesar una red que tenga un MTU pequeño. Las pequeñas piezas en las que se divide un datagrama se llaman *fragmentos*, y el proceso de dividir un datagrama se conoce como *fragmentación*.

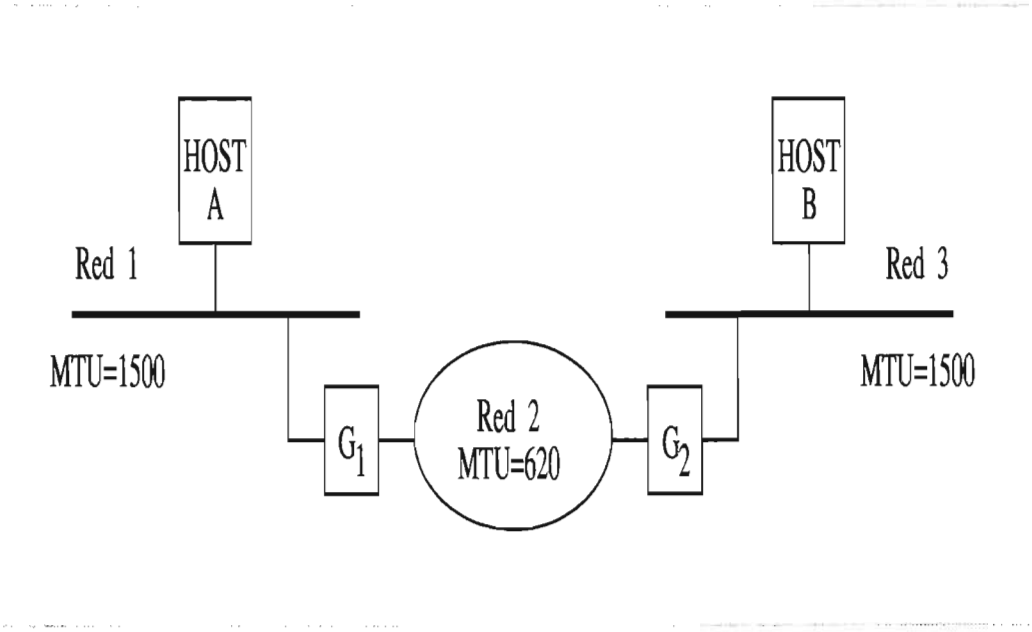


Figura III.5.- Fragmentación.

7 El límite de 1500 viene de la especificación Ethernet. Cuando el estándar IEEE 802.3 se usa con un header SNAP, limita los datos a 1492 octetos. Existe cierto hardware que permite transferencias ligeramente mayores.

Reensamblado de Fragmentos

¿Debe reensamblarse un datagrama después de pasar a través de una red? O deberán transportarse los fragmentos hasta el *"host"* final antes de reensamblarlos. En una internet TCP/IP, una vez que un datagrama se ha fragmentado, los fragmentos viajan como datagramas separados todo el camino hasta el destino final donde son reensamblados. Este procedimiento es posible por el campo que identifica al datagrama.

Tiempo de Vida (TTL)

El campo "Tiempo de Vida" especifica qué tanto, en segundos, podrá permanecer un datagrama en la Internet. La idea es muy simple: siempre que una máquina inyecta un datagrama a la Internet, le da un tiempo de vida máximo para que el datagrama pueda sobrevivir. Los *"gateways"* y *"hosts"* que procesan los datagramas deben decrementar este valor a medida que el tiempo pasa y eliminar el datagrama de la Internet cuando su tiempo de vida expira. El TTL original por omisión es 255 segundos.

III.5.2.- Direccionamiento IP (INTERNET PROTOCOL).

Las redes interconectadas no tienen ninguna razón para disponer del mismo mecanismo de direccionamiento de los nodos. Por lo tanto, es necesario dar una **dirección lógica** (dirección IP) a cada nodo.

Una dirección IP esta compuesta de 4 bytes (32 bits) y esta dividida en dos partes, los bits más significativos (MSB) identifican una **RED** en particular y los demás bits especifican un **NODO** perteneciente a esa red.

Todos los nodos que se localizan en la misma red, deben coincidir en la parte correspondiente a la dirección de Red, sin embargo la parte que identifica a la dirección de Nodo debe ser diferente.

Estos 32 bits de dirección IP se escriben normalmente como cuatro números decimales, en el rango de 0 a 255, separados por un punto, uno para cada byte de dirección:

- Se expresa en formato X.X.X.X
- El máximo valor para cada octeto es de 255
- Por ejemplo 192.100.180.15

Para aprovechar de manera más eficiente el espacio de direccionamiento IP y ajustar el tamaño de las redes a las necesidades individuales de cada entidad, el InterNIC clasificó las redes de Internet en cinco clases de direccionamiento, Clase A, Clase B, Clase C, Clase D, Clase E.

Cada red Clase A agrupa alrededor de 16,000,000 direcciones únicas, la clase B agrupa aproximadamente 65,000, y la clase C solo agrupa 254 direcciones diferentes.

Sin embargo las redes de clase A, han sido asignadas en su totalidad a alguna corporación como IBM, ATT, HP, el Pentágono o la NASA y el InterNIC impone muchas restricciones para asignar alguna de las pocas redes clase B restantes. Lo más usual es que el InterNIC asigne una clase C, a menos que se argumente de manera sólida la necesidad de una clase B.

La Clase a la que pertenece una dirección de IP define cuantos de los 32 bits deberán ser interpretados como dirección de Red y cuantos como dirección de Nodo.

- ✓ Clase A R.N.N.N 8 bits red - 24 bits nodo
- ✓ Clase B R.R.N.N 16 bits red - 16 bits nodo
- ✓ Clase C R.R.R.N 24 bits red - 8 bits nodo

Los bits más significativos de la porción de red determinan la clase de dirección, como se muestra en la siguiente tabla:

Clase	Primer octeto
A	0XXXXXXX
B	10XXXXXX
C	110XXXXX

Tabla III.1.- Clase de Dirección.

III.5.2.1.- Redes Clase A.

Para las redes clase A, el primer bit siempre es 0, los siguientes 7 bits, determinan el número de RED, y los siguientes 24 bits, determinan el número de nodo.

De este modo el direccionamiento de la clase A debe de tener un rango de números de dirección de 1.0.0.0 hasta 126.0.0.0, la primera y la última dirección (0.x.x.x y 127.x.x.x) están reservadas. Esto es 126 posibles redes clase A.

El número de direcciones por red clase A es de 16,777,214, esto es dos menos que dos elevado a la potencia 24, debido a que los números de host 0.0.0 y 255.255.255 (La primera y la última dirección de cada red), están reservadas.

III.5.2.2.- Redes Clase B.

Para una dirección clase B los primeros dos bits son 10, mientras que los siguientes 14 bits identifican el número de red y los 16 restantes el número de *"host"*. La clase B incluye los números de red en el rango de 128.1.0.0 al 191.254.0.0, la primera y la última dirección (128.0.x.x y 191.255.x.x) están reservadas.

Esto permite un total de 16,382 redes con un total de 65,534 direcciones de *"host"* cada una (La primera y la última dirección de cada red, están reservadas).

III.5.2.3.- Redes Clase C.

Para una red clase C, los tres primeros bits de la dirección son 1, 1 y 0, los siguientes 21 bits identifican la red y los últimos 8 el *"host"*.

Así, el direccionamiento de la clase C incluye los números de red en el rango que va de 192.0.1.0 hasta 223.255.254.0, la primera y la última dirección (192.0.0.x y 223.255.255.x) están reservadas.

Esto permite un total de 2,080,798 redes clase C, con un total de 254 direcciones de *"host"*. (La primera y la última dirección de cada red, están reservadas).

III.5.2.4.- Redes Clase D y E.

Finalmente tenemos las direcciones de la clase D y la clase E. Las de clase D empiezan en 224.0.0.0 y se usa para *"Multicast"*. A diferencia de un *"Unicast"* (mensaje para uno nodo) y de un *"Broadcast"* (mensaje para todos los nodos) un 'multicast' es un mensaje para un grupo de nodos. Las direcciones de la clase E empiezan en 240.0.0.0 y se usan frecuentemente solo para propósitos experimentales.

En la tabla se observan las clases de direcciones IP y el rango para cada una de ellas.

Clase	**Primer Byte de la dirección**
A	1-127
B	128-191
C	192-223

Tabla III.2.- Clases de Direcciones IP.

Ejemplos:

128.128.45.6
-> Clase: B
-> Red: 128.128
-> Nodo: 45.6

204.87.205.129
-> Clase: C
-> Red: 204.87.205
->Nodo: 129

III.6.- Restricciones en Direcciones de INTERNET PROTOCOL (IP).

Los nodos deben tener dirección de nodo diferente a la CERO (puros bits en cero).

La dirección de nodo con puros unos se reserva para *"Broadcasts"*.

En ocasiones tenemos que dividir una red grande en varias pequeñas para:

- Reducción de tráfico.
- Optimizar prestaciones *("performance")*.
- Simplificar la administración.

Para esto recurrimos al uso de subredes, que no son otra cosa más que una extensión a la dirección de Red. Para hacer la extensión se utilizan la máscara de red *("Netmask")*.

Una dirección de IP es de 32 bits, escritos como 4 octetos separados con un punto.

Una máscara de red también es de 32 bits, escritos como 4 octetos. La máscara de red se construye de la siguiente forma:

1 binario en posiciones de dirección de Red
0 binario en posiciones de dirección de nodo.

La máscara de red indica que bits de la dirección de Nodo se deberán de interpretar como dirección de red.

Las máscaras de red por default son:

CLASE	DIRECCION	MASCARILLA
A	R.N.N.N	255.0.0.0
B	R.R.N.N	255.255.0.0
C	R.R.R.N	255.255.255.0

Tabla III.3.- Máscaras de Red.

Para la interpretación de las direcciones de IP por un Ruteador *("Router")*, se aplica un AND lógico entre la dirección de IP y la máscara de red, con esto lo que se hace es eliminar la dirección de Nodo y solo dejar la dirección de Red.

Operación del AND lógico:

0&0=0
0&1=0
1&0=0
1&1=1

Ejemplo.

131.108.66.160	10000011	01101100	01000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
AND	10000011	01101100	00000000	00000000
	131	**108**	**0**	**0**
	Red	**Red**	**Nodo**	**Nodo**

Tabla III.4.- Interpretación de las Direcciones IP.

III.6.1.- Direcciones IP Especiales o Reservadas.

Existen dos direcciones IP que tienen una interpretación particular, cualquiera que sea el tamaño de la red.

La dirección donde todos los bits son 0's permite hacer referencia a la red o a la máquina actual (0.0.0.0).

La dirección donde todos los bits son iguales a 1 se utiliza para direccionar un mensaje a todas las máquinas de la red *("Broadcast")*, esto es: 255.255.255.255, el *"Broadcast"* se puede decir que es una dirección en la que todos los integrantes del segmento de red al que se pertenece deben de prestar atención, con la finalidad de procesar los datos que se están enviando, y al mismo tiempo saber si un nodo, que podría ser mi equipo es el que debe responder a tal solicitud.

III.7.1.- "Address Resolution Protocol" (**ARP**).

Tomando como referencia al paquete de ETHERNET versión 2, y prestando atención en el encapsulamiento de la porción de las direcciones destino y origen del mismo.

Dirección de destino	Dirección de origen	Tipo de servicio	Datos, incluyendo IP	CRC
6 bytes, MAC Address	6 bytes, MAC Address	2 bytes	MTU, hasta 1500 bytes	4 bytes

Tabla III.5.- Paquete de Ethernet.

La información en el concepto de un datagrama, incluye la porción de IP y la información de capas superiores de transporte o aplicativos ya definidos.

Véase a más a detalle un encapsulamiento total por parte de ethernet, desde la definición de inicio hasta el término del datagrama del mismo, Los datos están incluidos desde que parte final del campo de tipo de servicio, sin embargo para establecer la comunicación, entre dos *"hosts"* es necesaria la dirección MAC tanto del origen como del destino. La dirección MAC del origen, es por razón obvia conocida, ¿pero que hay de la dirección MAC destino?,

Para poder establecer la comunicación entre dos *"hosts"* es indispensable conocer la dirección MAC de destino, por lo que se envía a la red un paquete para obtener la dirección MAC de destino, a este servicio se le llama ARP, Address Resolution Protocol.

De una dirección IP conocida se puede obtener una dirección MAC desconocida.

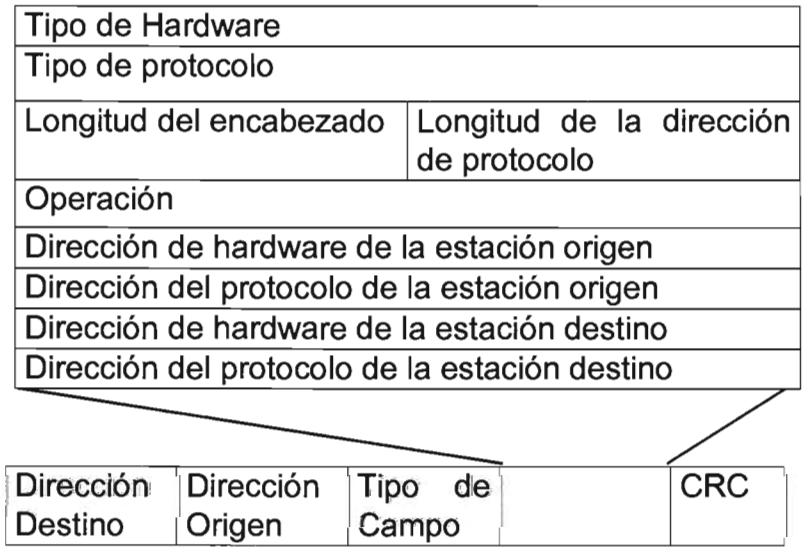


Figura III.6.- Formato de un Mensaje ARP sobre ETHERNET.

Hay que hacer notar que el servicio de solicitud de la red es un servicio de ETHERNET y la dirección de destino también debe llevar un campo, mismo que se llena con una dirección de *"Broadcast".*

ARP permite la designación de tipos específicos de tarjetas de red (Ethernet, Token Ring, etcétera). De esta manera, cuando el *"host"* solicitante recibe un datagrama ARP también puede obtener información del tipo de tarjeta que aquélla máquina esté usando. Sobre el servicio de red que esta utilizando.

III.7.2.- "Reverse Address Resolution Protocol" (**RARP**).

Lo contrario al trabajo realizado por ARP en donde se conoce la dirección física pero no se conoce la dirección IP. Los mensajes de este protocolo tienen el mismo formato que los de ARP. Un ejemplo del uso de RARP es, el caso de una estación de trabajo sin disco duro *("Diskless").*

Cuando la estación es inicializada, leerá su dirección física de ROM pero necesitará conocer su dirección IP, entonces manda un mensaje RARP a todas las máquinas *("Broadcast")* solicitando su dirección IP. En este caso deberá existir un servidor que reconozca el mensaje de la estación, cambie el código del mensaje a Respuesta de Solicitud y que copie la dirección IP de la estación desde sus tablas de mapeo internas hacia el mensaje RARP y lo envíe de regreso.

III.8.- Mensajes de Control.

III.8.1.- "Internet Control Message Protocol" (ICMP).

Un datagrama viaja de un ruteador a otro hasta llegar a un ruteador que pueda enviar al datagrama directamente a su destino final. Si un ruteador no puede rutear o enviar un datagrama, o si el ruteador detecta una condición inusual que impida al ruteador enviar el mensaje (ejemplo, congestión en la red), el ruteador necesita informar al *"host"* origen (*"host"* donde se originó el mensaje), para que el *"host"* ignore esta situación o corrija el problema. Esta sección discute el mecanismo que ruteadores y *"hosts"* usan para comunicar tal información de control. Los ruteadores utilizan tal mecanismo para reportar problemas y los *"hosts"* lo usan para probar si el destino puede ser alcanzado.

III.8.2.- Servicios de ICMP (Internet Control Messaging Protocol).

El Internet Control Messaging Protocol (ICMP), es un protocolo de la capa de Internet (capa 3) que proporciona mensajes de reporte de error y otro tipo de información relevante al ruteo y envío de paquetes IP. ICMP está descrito en el RFC 792 y actualizado en el RFC 950.

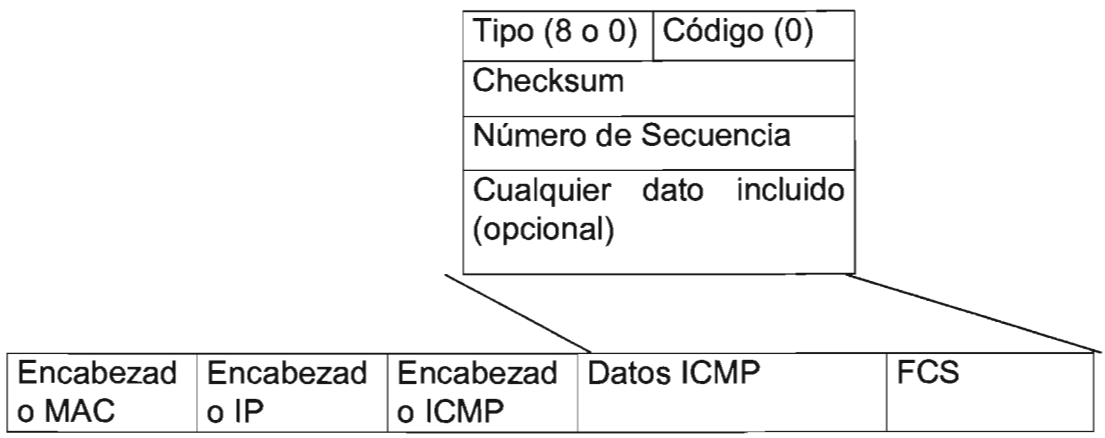


Figura III.7.- Formato del Paquete ICMP para Respuesta a Solicitud.

Cuando un ruteador o un *"host"* destino debe informar al *"host"* fuente sobre los errores en el envío o ruteo del datagrama, usa ICMP y se caracteriza por:

ICMP usa IP como si fuera un protocolo de nivel superior (esto es, los mensajes de ICMP están encapsulados en datagramas IP). Sin embargo ICMP es una parte integral de IP y debe ser implementada por cada modulo de IP.

ICMP es usado para reportar algunos errores, no para hacer confiable a IP. Los datagramas pueden ser no enviados y no existir algún reporte al respecto. La confiabilidad debe ser implementada por protocolos de nivel superior que usa IP.

ICMP puede reportar errores sobre cualquier datagrama IP con excepción de mensajes ICMP, para evitar repeticiones infinitas.

Mensajes ICMP nunca se envían en respuesta a datagramas que tienen una dirección destino *"Broadcast"* o *"Multicast"*.

Mensajes ICMP nunca se envían en respuesta a un datagrama que no contenga una dirección IP fuente, que representa un *"host"* único. Esto es, la dirección fuente no puede ser cero, una dirección *"loopback"*, una dirección *"Broadcast"* o *"Multicast"*.

El RFC 792 establece que los mensajes ICMP pueden ser generados para reportar errores en el procesamiento de datagramas IP. En la práctica, los ruteadores por lo general siempre generaran mensajes ICMP para errores, pero para los *"hosts"*, el número de mensajes ICMP generados es dependiente de la aplicación.

Mensajes de control.

Los mensajes ICMP están descritos en el RFC 792 y el RFC 950. Los mensajes ICMP se envían en datagramas IP. El encabezado de IP siempre tiene el número de protocolo 1, indicando ICMP y el tipo de servicio cero (rutina). El campo de datos de IP contendrá el mensaje actual ICMP en el formato mostrado en la figura III.7.

Donde:

Tipo especifica el tipo de mensaje:

Echo reply
Destination unreachable
Source quench
Redirect
echo
Router advertisement
Router solicitation
Time exceeded
Parameter problem
Time stamp request
Time stamp reply
Information request (obsoleto)
Information reply (obsoleto)
Address mask request
Address mask reply
Traceroute
Datagram conversion error
Mobile host redirect
IPv6 Where-Are-You
IPv6 I-am-Here
Mobile registration request
Mobile registration reply
Domain name request
Domain name reply
SKIP
Photuris

Código contiene el código de error para el datagrama reportado por este mensaje ICMP.

Suma de Control, (Checksum) contiene los 16 bits, control de suma del mensaje entero ICMP. Este algoritmo es el mismo que es usado por UDP y TCP, así como por IP.

Datos, contiene información para este mensaje ICMP. Típicamente contendrá una parte del mensaje IP original para el cual este mensaje ICMP fue generado. La longitud de los datos puede ser determinada desde la longitud del datagrama IP que contiene el mensaje menos la longitud del encabezado de IP.

Mensaje de echo (8) y echo reply (0).

Echo es usado para detectar si otro *"host"* está activo en la red. El *"host"* origen (*"sender"*), inicializa el identificador y número de secuencia (el cual es usado si múltiples **Echo Request** son enviados), agrega algunos datos al campo de datos y envía el echo ICMP al *"host"* destino. El campo code del mensaje ICMP esta en cero. El recipiente cambia el tipo a **Echo Reply** y regresa el datagrama al *"host"* origen. Este mecanismo es usado por el comando **Ping**, comando para determinar si un *"host"* destino está presente en la red, alcanzable.

Mensaje Destination Unreachable (3).

Si este mensaje es recibido desde un ruteador intermedio, significa que el ruteador coloca la dirección IP destino como inalcanzable.

Si este mensaje es recibido desde el *"host"* destino, significa que el protocolo especificado en el campo de número del datagrama original no esta activo, o que el protocolo no esta activo en este *"host"* o el puerto especificado esta inactivo.

El campo de código tendrá alguno de los siguientes valores:

Red inalcanzable
"Host" inalcanzable
Protocolo inalcanzable
Puerto inalcanzable
Fragmentación necesaria, pero el bit de no-fragmentación (Do Not Fragment) fue colocado.
Ruta origen fallada
Red destino desconocida
"Host" destino desconocido
"Host" origen aislado (obsoleto)
Red destino administrativamente prohibida
"Host" destino administrativamente prohibido
Red inalcanzable por este tipo de servicio
"Host" inalcanzable por este tipo de servicio

Si un ruteador implementa el Path MTU Discovery Protocol, el formato del mensaje de destino inalcanzable es cambiado por código 4 para incluir el MTU del enlace que podría no aceptar el datagrama.

Mensaje Source Quench (4).

Si este mensaje es recibido desde un ruteador intermedio, significa que el ruteador no tiene espacio en el buffer, espacio requerido para enfilar los datagramas para la salida a la siguiente red.

Si este mensaje es recibido desde el *"host"* destino, significa que los datagramas entrantes están arribando de manera muy rápida para ser procesados.

El campo de código es siempre cero.

Mensaje Redirect (5).

Si este mensaje es recibido desde un ruteador intermedio, significa que el *"host"* debe enviar futuros datagramas por la red al ruteador cuya dirección IP esta especificada en el mensaje ICMP. Este ruteador preferido estará siempre en la misma subred que el *"host"* que envía el datagrama y el ruteador que regreso el datagrama IP. El ruteador enviará el datagrama a su siguiente salto (*"Hop Destination"*). Si la dirección IP del ruteador iguala la dirección IP del origen en el datagrama original, indica un ciclo de ruteo (*"Routing Loop"*). Este mensaje ICMP no será enviado si el datagrama IP contiene una ruta fuente *("Source Route")*.

El campo del código tendrá uno de los siguientes valores:

redireccionamiento de red
redireccionamiento de host
redireccionamiento de red para este tipo de servicios
redireccionamiento de host para este tipo de servicios

Mensaje Time Exceeded (11).

Si este mensaje es recibido desde un ruteador intermedio, significa que el campo de time-to-live de un datagrama de IP ha expirado.

Si este mensaje es recibido desde el *"host"* destino, significa que el tiempo *"time-to-live"* para reensamblar un fragmento IP ha expirado mientras el *"host"* esta esperando por un fragmento del datagrama. El campo del código puede tener uno de los siguientes valores:

Tránsito TTL excedido
Reensamble TTL excedido
Aplicaciones de ICMP

Existen dos simples aplicaciones usadas ampliamente, basadas en ICMP:

Ping y **Traceruote**. **Ping** usa los mensajes ICMP **Echo** y **Echo Reply** para determinar si un *"host"* es alcanzable. **Traceroute** envía datagramas IP con valores de TTL péquenos que expiren en la ruta hacia un destino. Utiliza el resultante mensaje ICMP **Execeeded Messages** para determinar donde en el Internet expiró el datagrama y obtener la ruta hacia un *"host"*.

Estas aplicaciones se describen a continuación.

III.8.2.1 Ping.

Ping es la aplicación más simple de TCP/IP. Ping envía uno o más datagramas IP hacia un *"host"* destino específico solicitando una respuesta y midiendo el tiempo que tarda el datagrama en llegar al destino y regresar al origen. La palabra **Ping** se toma de la operación del sonar para localizar un objeto bajo el agua. También es una abreviación para *"Packet Internet Gropher"*.

Tradicionalmente, si un *"host"* responde la petición de ping de otro *"host"*, otras aplicaciones tales como Telnet o FTP también podrían comunicarse con ese *"host"*.

Con la implementación de la seguridad en Internet, particularmente los cortafuego (*"Firewalls"*), los cuales controlan el acceso a redes por medio de protocolos de aplicaciones y/o número de puerto. No obstante, la primera prueba para alcanzar un *"host"* es intentar hacer un ping hacia ese *"host"*.

La sintaxis que se usa en diferentes implementaciones del **Ping** cambia dependiendo de la plataforma.

III.8.2.2 Traceroute.

El programa **Traceroute** puede ser de mucha utilidad cuando se usa con el objetivo de depurar (*"debugging"*). **Traceroute** permite determinar la ruta que sigue de *"host"* a *"host"* el datagrama IP. **Traceroute** se basa en ICMP y UDP (protocolo de capa superior, TCP). Traceroute envía un datagrama IP con un valor de TTL igual a "1" al *"host"* destino.

El primer ruteador en recibir el datagrama decrementará el valor de TTL a 0 y regresara un mensaje *"Time Execeeded"* y descartara el datagrama. De esta manera el primer ruteador en la ruta es identificado. Este proceso puede ser repetido, con valores de TTL más grandes, para identificar la serie de ruteadores en la ruta al *"host"* destino. **Traceroute** envía datagramas UDP al *"host"* destino, el cual hace referencia a un número de puerto que esta fuera del rango normalmente usado. Esto permite a **Traceroute** determinar cuando es alcanzado el *"host"* destino, que es, cuando un mensaje ICMP *"Port Unreachable"* es recibido.

III.9.- Panorama General de IPv6.

Esta sección presenta un panorama de la siguiente generación de Protocolo Internet (**Internet Protocol Next Generation, IPnG**). IPnG fue recomendado por el *"IPnG Area Directors del Internet Engineering Task Force"* (IETF) en la reunión de Toronto en Julio 25 de 1994, y documentada en el RFC 1752, "La Recomendación para el IPnG". La recomendación fue aprobada por *"The Internet Engineering Steering Group"* en Noviembre 17 de 1994 y declarada una Norma (estándar).

El nombre formal de este protocolo es IPv6. La actual versión del protocolo Interne es versión 4 (referido como IPv4). El objetivo de esta sección es darle al lector un panorama del protocolo IPnG.

III.9.1.- Limitaciones del Modelo de Direcciones IP.

El Internet a crecido sumamente rápido en años recientes, en 1994 tenia más de 32000 redes conectadas, con más de 3.8 millones de computadoras en más de 90 paises. IPv4 con un campo de direcciones de 32 bits provee más de 4 mil millones de direcciones posibles, parecería que el esquema de direcciones IP es más que adecuado para la tarea de direccionar todos los datagramas de los *"hosts"* en el Internet, desafortunadamente este no es el caso, por varias razones, incluyendo las siguientes:

El direccionamiento IP está dividido en dos partes, número de red y número de *"host"*, el cual es administrado separadamente. Aunque el espacio de direcciones dentro de una red puede ser ocupada esparcidamente, tan lejano como el espacio de direcciones IP le permita, si un número de red es usado entonces todas las direcciones dentro de esa red son ocupadas.

El espacio de direcciones para las redes esta estructurado en clase de redes A, B, C de diferente tamaño, el espacio dentro de cada una de estas clases requiere ser considerado separadamente.

El esquema de direccionamiento IP requiere que a todas las redes IP les sea asignado un número de red único, aunque actualmente estén o no conectadas al Internet.

El crecimiento de TCP/IP (usado en nuevas áreas), podría resultar en una explosión rápida del número requerido de direcciones IP. Por ejemplo, el uso extendido de TCP/IP para conectar terminales electrónicas punto de venta o para recibir cable por televisión podría incrementar enormemente el número de *"hosts"* IP.

El esquema de direccionamiento IPv4 con una única dirección IP por cada *"host"* (no ruteador) podría cambiar en un futuro (RFC 1681).

Estos factores significan que el espacio de direcciones es mucho más restringido de lo que el análisis anterior puede indicar. Este problema es conocido como Agotamiento de las direcciones IP.

III.9.2.- IP la Siguiente Generación (IPnG).

Métodos para resolver el problema de agotamiento de direcciones IP ya se están empleando, pero eventualmente, el espacio de direcciones IP será agotado. El IETF (*"Internet Engineering Task Force"*) tiene un grupo trabajando sobre las expectativas del tiempo de vida del esquema de direcciones IP (*"Address Lifetime Expectetions"*, ALE) con el propósito de proporcionar una fecha estimada cuando las direcciones IP se agoten, actualmente las expectativas son (como lo informo ALE en diciembre de 1994) que el espacio de direcciones IP estará agotado en algún momento entre el 2005 y el 2011.

Existen varios grupos de trabajo relacionados con el funcionamiento de IPng: IPng Requerimientos (IPNGREQ), *"Transition and Co-existence including Testing"* (TACIT) y un grupo propuesto por cada uno de los candidatos propuestos para IPnG, todos estos grupos son temporales y se espera que sean unidos a otros grupos de trabajo en otras areas cuando el proceso de definición de IPnG concluya.

En Julio de 1994 en la reunión del IETF en Toronto, el IPnG *"Area Directors"* del IETF presento el RFC 1752 – la recomendación para el IPnG *"Next Generation Protocol"*. La recomendación fue aprobada por el IETF en Noviembre de 1994 y se hizo una norma (estándar).

Estos eventos fueron la culminación de mucho trabajo y discusión, el cual involucra a muchas partes interesadas. El consejo de administración publicó el RFC 1550-IP, donde se establecen los requerimientos para IPnG. Los requerimientos más importantes son:

Un espacio de direcciones dramáticamente más grande: al menos 10 redes (superscript 9), preferentemente 10 (superscript 12); y al menos 10 *"hosts"* (superscript 12), preferentemente 10 (superscript 15). Al menos 1 billón de redes, preferentemente 1000 billones; y al menos 1000 veces como host. Esto podría permitir incrementar considerablemente el uso de las direcciones IP y al mismo tiempo permite que el espacio de direcciones IP sea extensamente poblado permitiendo a las direcciones IPnG tener más estructura que la posible en IPv4.

- IPnG debe permitir el encapsulamiento de su propio paquete o de otros protocolos.
- IPnG debe permitir agregar clases de servicios para distinguir tipos de datos que están siendo transmitidos, como por ejemplo, tráfico isócrono como real-time audio y vídeo.
- IPnG debe proporcionar direccionamiento *"Multicast"*, de forma que este completamente más integrado con el resto del conjunto (*"suite"*) de protocolos que la implementaron actual.
- IPnG debe proporcionar Autentificación (*"Authentication"*) y Encriptación (*"Encryption"*).
- IPnG debe preservar las virtudes de IPv4: robustez, independencia de las características físicas de la red, alto desempeño, topología flexible, extensibilidad, servicio de datagramas, direccionamiento globalmente único, un protocolo de control internamente construido, estándares libremente disponibles.
- La implementación de IPnG debe comprender un plan de transición sencillo.
- IPnG debe coexistir con IPv4.

Existieron tres propuestas principales para IPnG, Common Architecture for the Internet (CATNIP), TCP and UDP whit Bigger Address (TUBA), Simple Internet Protocol Plus (SIPP).

III.9.3.- IP Versión 6 (**IPv6**).

El Consejo de Administración determinó que las tres propuestas fueron insuficientes para cumplir con la lista de requerimientos aceptada, pero que SIPP, como se definió en RFC1710, era la propuesta más cercana a la lista de requerimientos.

Después de algunos cambios a la propuesta original, por la instancia de usar 128 bits en lugar de 64 bits de direccionamiento, el Consejo de Administración de IPnG dictaminó que SIPP era la base para IPnG y que características de las otras propuestas podrían ser agregadas para cubrir el resto de los requerimientos. La solución propuesta fue llamada ***IP Versión 6(IPv6)***.

Se debe considerar que la definición de IPv6 esta aún en progreso y la información presentada aquí esta basada en documentos Internet-Draft. La definición final de IPv6 será definida en una serie de Standards Track RFCs.

IPv6 usa el término paquete en lugar de datagrama, pero el significado es el mismo, aunque los formatos son diferentes. IPv6 introduce un nuevo término, **nodo**, para un sistema corriendo IPv6,

que puede ser un *"host"* un ruteador. Un *"host"* IPv6 es un nodo que no reenvía paquetes IPv6 los cuales no están explícitamente direccionados hacia él. Un ruteador es un nodo el cual reenvía paquetes IP no direccionadas hacia él. Las características básicas de IPv6 son las siguientes.

*III.9.3.1.- Formato del Encabezado de IP, (**IPv6 Header**).*

IPv6 incrementa la longitud del encabezado (*"header"*) de IP de 20 bytes a 40 bytes. El encabezado de IPv6 contiene dos direcciones de 16-bytes cada una (origen y destino) precedidas por 8 bytes de información de control.

El encabezado de Ipv4 tiene dos direcciones de 4 bytes cada una precedida por 12 bytes de información de control y seguido posiblemente por datos de opción. La reducción del control de información y la eliminación de opciones en el encabezado tiene por objeto optimizar el procesamiento de la mayoría de los datagramas (paquetes). Los campos frecuentemente no usados han sido removidos del encabezado, fueron movidos al encabezado opcional de extensiones.

Campos del encabezado de IPv6

Vers
4-bits número de versión del protocolo Internet: 6

Flow Label
28-bits ver descripción en la sección Flow Label

Payload Length
La longitud del paquete en bytes (no incluido el encabezado) codificado como un entero sin signo de 16 bits, si la longitud es mayor a 64KB este campo es 0 y un encabezado opcional proporcional la longitud real.

Next Header
Indica el tipo de encabezado inmediatamente después de este encabezado. Este encabezado es el mismo que el usado para el número de protocolo en IPv4.

El siguiente encabezado también es usado para indicar la presencia del encabezado de extensión, el cual proporciona el mecanismo para agregar información adicional al paquete de IPv6. Los siguientes valores son importantes:

41	IPv6 Header
43	IPv6 Routing Header
44	IPv6 Fragment Header
51	IPv6 Authentication Header
?	IPv6 End-to-End Options Header
?	IPv6 ICMP Packet

Los valores, a excepción del los últimos dos (los cuales no estaban definidos al momento de escribir este manual) están incluidos en STD 2 –Assigned Internet Numbers, Aunque la edición actual de STD 2 (RFC 1700), en el momento de escribir el manual, menciona como protocolo a SIP o SIPP.

Hop Limit
Este es el campo TTL en IPv4, pero no es medido en saltos ni segundos. Fue cambiado por dos razones:

- IP normalmente envía los datagramas más rápido que un salto por segundo y el valor de TTL es siempre decrementado en cada salto, en la práctica es medido en saltos y no en segundos.

- Muchas implementaciones de IP, no expiran datagramas de salida, sobre la base de tiempo transcurrido.

Source Address
Una dirección de 128-bits. Ver sección Direccionamiento IPv6.

Destination Address
Una dirección de 128-bits. Ver sección Direccionamiento IPv6. Una comparación entre el encabezado de Ipv4 e Ipv6 mostrara que existen campos en el encabezado de IPv4 no tienen campos equivalentes en IPv6.

Type of Service
El tipo de servicio será manipulado usando el concepto de flujo (flow).

Identidication, Fragmentation Flags y Fragment Offset
Los paquetes fragmentados tienen un encabezado de extensión mucho mejor que el de Información de Fragmentación en el encabezado de IPv6. Esto reduce el tamaño del encabezado básico de IPv6.

Los protocolos de alto nivel, particularmente TCP, tienden a evitar la fragmentación de datagramas, esto reduce los *"overhead"* para el caso normal, Ipv6 no fragmenta los paquetes en la ruta hacia sus destinos, únicamente en la fuente (*"source"*).

Header Checksum
Debido a que los protocolos de transporte implementan *"checksum"*, y porque IPv6 incluye un encabezado opcional de autentificación que se puede utilizar para asegurar la integridad, IPv6 no proporciona monitoreo del *"checksum"* de los paquetes de IP.

TCP y UDP incluyen un pseudo encabezado IP en el *"checksum"* que ellos usan, en este caso, el encabezado de IP en IPv4 es verificado dos veces.

TCP y UDP, y cualquier otro protocolo que usa los mecanismos de *"checksum"*, trabajando sobre IPv6 continuarán usando un pseudo encabezado IP aunque, el formato del pseudo encabezado IPv6 será diferente del encabezado de IPv4. ICMP e IGMP y cualquier otro protocolo que no utilice un pseudo encabezado IP sobre IPv4 usara un pseudo encabezado IPv6 en su *"checksum"*.

Options
Todos los valores opcionales asociados con paquetes IPV6 están contenidos en encabezados de extensión asegurando que el encabezado básico IP es siempre del mismo tamaño.

III.9.3.2.- Tamaño del Paquete.

Todos los nodos IPv6 se esperan que dinámicamente determinen la Unidad Máxima de Transferencia (MTU) soportado por todos los enlaces a lo largo de una ruta (como se describe en el RFC 1191 – Path MTU Discovery) y los nodos fuente únicamente enviaran paquetes que no excedan el MTU de la ruta.

De esta forma los ruteadores IPv6 no fragmentaran los paquetes entre en los múltiples saltos de la ruta para alcanzar el destino final, haciendo más eficiente el uso de rutas las cuales cruzan diversos medios físicos de transmisión.

Actualmente se propone que IPv6 requiera que cada enlace soporte un MTU de 576 bytes, pero este valor como muchos otros valores (en el tiempo que se escribió el manual) de IPv6 pueden cambiar.

III.9.3.3.- Encabezados de Extensión.

Los encabezados de extensión se colocan entre el encabezado del paquete de IPv6 y los datos que especifican el protocolo de nivel superior. Forman parte del campo *"payload length"*. Cada encabezado tiene un campo de 8 bits *"Next Header"* como el encabezado IPv6, el cual identifica el tipo de encabezados siguientes. Todas las extensiones definidas en el momento de escribir el manual tienen el campo *"Next Header"* como el primer byte del encabezado.

La longitud de cada encabezado, el cual es siempre múltiplo de 8 bytes, es codificada posteriormente en el encabezado en un formato específico para ese tipo de encabezado. Existe un número limitado de encabezados de extensión.

Alguno de ellos o todos pueden estar presentes una vez (únicamente una vez) en el paquete IPv6. Cuando el campo *"Next Header"* contiene un valor diferente a un *"header"* de extensión, esto indica el fin de los encabezados de IPv6 y el inicio de los datos del protocolo de capa superior.

IPv6 permite encapsular IPv6 con IPv6 (*"tunneling"*). Esto es hecho con un *"Next Header"* de valor 41 (IPv6). El paquete encapsulado de Ipv6 puede tener su propio encabezado de extensión. Ya que el tamaño de un paquete es calculado por el nodo que lo origina para igualar el MTU de la ruta, los ruteadores IPv6 no deben agregar encabezados de extensión a un paquete en lugar de eso deben encapsular el paquete recibido dentro de un paquete Ipv6 que el mismo genere (el cual puede ser fragmentado si es necesario).

Con la excepción del encabezado *"Hop-by-Hop"* (este debe estar inmediatamente después del encabezado IP si existe), los encabezados de extensión no son procesados por ningún ruteador en la ruta del paquete, excepto por el ruteador final.

IPv6 usa un formato común llamado el *"Type-length-Value"* (TLV), formato para campos de longitud variable, estos se pueden encontrar en los encabezados de opción *"Hop-by-Hop"* y *"End-to-End"*. La opción tiene un encabezado de 2 bytes, a continuación datos de la opción.

Type
El tipo de opción. Todos los tipos de opción tienen el mismo formato:

xx
Un número de 2 bits indicando como debe ser tratado un nodo Ipv6 que no reconoce la opción.

0 *Salta la opción y continúa.*

1 *Descarta el paquete silenciosamente.*

2 *Descarta el paquete e informa al dispositivo que lo envío con un mensaje ICMP* "Unrecognized Type".

3 *Descarta el paquete e informa al dispositivo que envío el paquete un mensaje ICMP* "Unrecognized Type" *a menos que la dirección destino sea una dirección de* "Multicast".

Y *Este bit tiene un significado específico solo para el encabezado* "Hop-by-Hop". *Si esta colocado, indica que el valor de la opción puede cambiar en la ruta y por lo tanto debe ser excluido de cualquier calculo de integridad, desarrollado en el paquete. Puesto que los ruteadores intermedios únicamente examinan los encabezados* "Hop-by-Hop", *solo las opciones* "Hop-by-Hop" *pueden ser validamente cambiadas en la ruta.*

zzzzz
Los bits restantes que definen la opción.

Length
La longitud del valor de la opción.

Value
El valor de la opción. Esto depende del tipo.

Para implementar el desempeño de una IPv6, las opciones individuales se alinean de tal forma que valores multi-byte son colocados en sus límites naturales.

En muchos casos, en que los encabezados de la opción son más grandes de lo necesario, pero debe permitir que los nodos procesen datagramas más rápidamente. Para permitir esta alineación, todas las implementaciones IPv6 deben reconocer dos opciones que completan (*"padding"*):

Pad1
Un byte X'00' usado para completar un solo byte. Mayores secuencias de completar deben ser echas con el PadN option.

PadN
Una opción en el formato TLV. Su valor X'01'. La longitud del byte proporciona el número de bytes a completar después de los 2 bytes como mínimo que se requeriré

III.9.3.4.- Direccionamiento IPv6.

IPv6 proporciona un esquema de direcciones de 128 bits de longitud. A diferencia de IPv4 que tiene una forma estrictamente codificada sobre la base de clases de direcciones indicadas por el bit de mayor orden en la dirección, las direcciones IPv6 no están estructuradas de esta forma.

Están diseñadas para ser usadas con *"Classless InterDomain Routing"* (CIDR). El espacio de direcciones IPv6 es suficientemente grande que puede encerrar un rango muy amplio de espacios de direcciones ya existentes y propuestas. En conjunto con CIDR, parte principal del direccionamiento IPv6, por ejemplo, el primer byte indicaría el tipo de direccionamiento. Tales tipos incluirían asociar el espacio de direccionamiento actual IPv4 a IPv6, direcciones OSI NSAPs, Novell IPX. Además el encabezado del ruteo de IPv6 permite a IP encapsular de manera arbitraria información sobre direccionamiento en cada paquete. Esto podría extender el esquema de IPv6 a direcciones de sistemas hipotéticos que no pueden ser asociados al espacio de direcciones IP. Dada la longitud del campo de dirección IPv6, es poco probable que esto sea necesario en un futuro próximo.

Técnicamente las direcciones IPv6 son identificadoras de 128 bits para interfaces y grupo de interfaces. Esto es equivalente a elevar al cuadrado dos veces el espacio de direcciones IPv4; verdaderamente un número muy grande de direcciones. El protocolo IPv6 define tres tipos de direcciones:

Unicast addresses. Una dirección *"unicast"* es un identificador para una sola interfase. Los tres tipos de dirección *"unicast"* son direcciones basadas en proveedores (*"provider-based"*), direcciones de uso local del sitio (site-local-use) y direcciones de uso local del enlace (link-local-use).

Anycast addresses. Un nuevo tipo de dirección la cual es un identificador (un simple valor) asignado a más de una interfaz. El conjunto de interfaces a una dirección de *"anycast"* típicamente pertenecen a más de una computadora.

Cuando un paquete se envía a una dirección de *"anycast"*, el protocolo de ruteo usado en ese momento envía el paquete a la interfase más cercana identificada por esa dirección. La interfaz más cercana es determinada por la medida de distancia del protocolo de ruteo.

Multicast addresses. El formato de la dirección permite la posibilidad de obtener trillones de códigos de grupos de *"multicast"*. Una dirección de *"multicast"* es un identificador para un conjunto de interfases que típicamente pertenecen a diferentes nodos. Cada código de grupo de *"multicast"* identifica dos o más recipientes de paquetes. Además, una dirección de *"multicast"* particular puede ser confinada a un solo sistema, restringido dentro de un sitio específico, asociado con un enlace de red particular o distribuido mundialmente.

Cuando un paquete es enviado a una dirección de *"multicast"*, el protocolo envía el paquete a todas las interfaces identificadas por esa dirección.

La nueva dirección *"multicast"* de IPv6 reemplaza a la dirección *"broadcast"* como es usada en IPv4. IPv6 usa el mismo modelo para subredes como lo hace IPv4:

- Una subred puede ser asociada con solo un enlace
- Múltiples subredes pueden ser asignadas al mismo enlace.

III.9.3.5.- Reglas del Direccionamiento.

Todos los tipos de direcciones IPv6 son asignadas a interfases, no a nodos. Cada interfase pertenece a un solo nodo. Esto significa que puede identificar un nodo por su dirección *"unicast"* de su interfase.

Una dirección *"unicast"* IPv6 hace referencia a una única interfase. Una sola interfase puede tener múltiples direcciones IPv6 de cualquier tipo de las direcciones de IPv6. Las dos excepciones a esta regla son:

Una sola dirección *"unicast"* puede ser asignada a múltiples interfaces físicas bajo las siguientes condiciones:

Cuando compartir carga sobre múltiples interfases físicas es necesario. Cuando las aplicaciones tratan las múltiples interfases físicas como una sola interfase. Los ruteadores pueden obtener interfaces no numeradas sobre enlaces *"Point-to-Point"*. Esto significa que direcciones IPv6 no son asignadas a la interfase. Ruteadores *"Point-to-Point"* ni requieren direcciones si no son fuente o destino de datagramas IPv6.

III.9.3.6.- Representación de Direcciones IPv6.

Las direcciones Ipv4 tradicionalmente eran representadas en notación decimal con puntos; cada dirección de 32-bits esta dividida en cuatro secciones de 8-bits, un número decimal entre 0 y 255 representa cada sección. Por ejemplo 192.168.95.143.

La dirección IPv6 de 128-bits utiliza un método diferente para representar la dirección. Existen tres formas para representar la dirección IPv6.

La Forma Preferida es la dirección IPv6 completa en valores hexadecimales. Como se define en el RFC 1884, la forma preferida es X:X:X:X:X:X:X:X, donde la X representa los valores hexadecimales de cada componente de 16-bits de la dirección. Por ejemplo, una dirección IPv6 podría tener la siguiente forma:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Los dos puntos separan cada sección y cuatro números hexadecimales presentan cada sección de 16-bits. Algunas veces una sección de 16-bits esta formada principalmente por ceros en un

campo individual, pero debe existir al menos un número que representa una dirección como se muestra en el ejemplo:

1080:0:0:0:8:800:200C:417A

La Forma Reducida substituye cadenas de ceros con una sintaxis especial para reducir los ceros Esta forma utiliza dobles dos puntos (::) Para indicar múltiples grupos de ceros de 16-bits El doble dos puntos puede ser usado una vez en una dirección. La dirección puede ser simplificada como sigue:

1080:0:0:0:8:800:200C:417A

según lo descrito anteriormente:

1080::8:800:200C:417A

Los dobles dos puntos pueden ser usados para reducir los primeros y/o últimos ceros en una dirección. La siguiente tabla muestra la simplificación de algunos ceros en una dirección usando dobles dos puntos.

Dirección	*es*	*Puede ser representada como*
1080:0:0:0:8:800:200C:417A	Dirección Unicast	1008::8:800:200C:417A
FF01:0:0:0:0:0:0:43	Dirección Multicast	FF01::43
0:0:0:0:0:0:0:1	Dirección Loopback	::1
0:0:0:0:0:0:0:0	Dirección no Especificada	::

La forma combinada es conveniente usarla para ambientes de nodos combinados de IPv4 e IPv6. Esta forma se puede representar X:X:X:X:X:X:D.D.D.D. Las X's representan los valores hexadecimales de los seis componentes de más alto orden de la dirección. Las D's representan el valor estándar de la representación decimal de los cuatro componentes de 8-bits de la dirección.

La siguiente tabla muestra la representación combinada.

Dirección combinada	*Forma Compuesta*
0:0:0:0:0:0:13.1.68.3	::13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38

Prefijo de Dirección IPv6.

Así como Ipv4, Ipv6 puede tener un prefijo de dirección. Para nuestro propósito, un prefijo de dirección IPv6 esta definido como una dirección IPv6 y alguna indicación de los bits contiguos más significantes dentro de la porción de esta dirección. La representación de un prefijo de dirección Ipv6 es similar a la forma que los prefijos IPv4 son escritos en notación CIDR. Un prefijo de dirección Ipv6 tiene la siguiente forma:

Las direcciones IPv6 pueden ser escritas usando cualquiera de las formas previamente descritas (preferida, compuesta o combinada) con esta diferencia: si la dirección escrita finaliza en dobles dos puntos, los dobles dos puntos finales pueden ser omitidos.

La longitud del prefijo es un valor decimal. Especifica el número de bits contiguos más a la izquierda de la dirección que comprende el prefijo. El siguiente ejemplo muestra la representación legal del prefijo de 60-bits 12AB00000000CD30.

12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30::/60
12AB:0:0:CD30/60

La siguiente tabla muestra algunas representaciones que no son legales para este prefijo de 60 bits.

Prefijo de dirección ilegal	*Razón*
12AB::CD30/60	Se pueden omitir los primeros ceros pero no los últimos, dentro de cualquier porción de 16-bits de la dirección.
12AB::CD30/60	Direcciones a la izquierda del"/" se expanden a 12AB:0000:0000:0000:0000:0000:0000:CD30
12AB::CD3/60	Direcciones a la izquierda del "/" se expanden a 12AB:0000:0000:0000:0000:0000:0000:0CD3

La dirección de un nodo y el prefijo de subred de un nodo pueden ser combinados y escritos como se muestra a continuación.

Dirección del nodo:	12AB:0:0:CD30:123:4567:89AB:CDEF
Número de subred del nodo	12AB:0:0:CD30/60
Dirección combinada y abreviada:	12AB:0:0:CD30:123:4567:89AB:CDEF/60

III.9.3.7.- Tipos de Dirección y Asignación.

Los primeros bits de una dirección IPv6 indican el tipo específico de dirección. El campo de longitud variable comprende estos primeros bits y es llamado el Prefijo de Formato (Formato Perfil, FP). En la siguiente tabla se muestra la asignación inicial de estos prefijos. La dirección del *"loopback"*, la dirección IPv6 con la dirección Ipv4 integrada y la dirección no especificada, son detalladas fuera del espacio del prefijo de formato (FP) 0000 0000. El 15% del espacio de direcciones es inicialmente asignado para soportar la asignación directa de las direcciones del proveedor, direcciones de uso local y direcciones *"multicast"*.

Además como se puede ver en la tabla existen espacios de direcciones reservados para NSAP, direcciones IPX y direcciones geográficas. El resto del espacio de direcciones no esta asignado, para uso futuro. Tal uso puede incluir la expansión de usos existentes y la introducción de nuevos usos, tales como localidades separadas e identificadoras.

El valor del octeto de mayor orden de la dirección diferencia a una dirección *"unicast"* de una dirección *"multicast"*. Un valor de FF (11111111) identifica a una dirección como una dirección de *"multicast"*; cualquier otro valor identifica a una dirección como una dirección de *"unicast"*. Debido a que las direcciones de *"anycast"* derivan del espacio de direcciones *"unicast"*, son sintácticamente idénticas a las direcciones *"unicast"*.

Asignación	**Prefijo (binario)**	**Fracción del espacio de dirección**

Reservado	0000 0000	1/256
No asignado	0000 0001	1/256
Reservado para asignación NSAP	0000 001	1/128
Reservado para asignación IPX	0000 010	1/128
No asignado	0000 011	1/128
No asignado	0000 1	1/32
No asignado	0001	1/16
No asignado	001	1/8
Dirección Unicast	010	1/8
Provider-based no asignada	011	1/8
Reservada para dirección Unicast Geographic-based	100	1/8
No asignada	101	1/8
No asignada	110	1/8
No asignada	1110	1/16
No asignada	1111 0	1/32
No asignada	1111 10	1/64
No asignada	1111 110	1/128
No asignada	1111 1110 0	1/512
Dirección Link-Local-Use	1111 1110 10	1/1024
Dirección Site-Local-Use	1111 1110 11	1/1024
Dirección Multicast	1111 1111	1/256

III.10.- Interconexión de Redes ("Internetworking").

El origen de las subredes ha sido un misterio para muchos administradores de sistemas. Parece que estas son una maraña de bits, bytes y mascaras que no valen la pena. Además, ¿Quién necesita complicaciones cuando se puede hacer lo necesario para mantener la red como está?

Sin embargo, si se proyecta tener acceso a Internet entonces las direcciones IP (*"Internet Protocol"*) y el enmascaramiento de subredes son tópicos con los que se debe estar familiarizado. Mientras la red crece, se incrementa la cantidad de segmentos y se requieren más direcciones de red, ya que cada segmento requiere un rango de direcciones. El InterNIC se encarga de asignar estas direcciones, sin embargo, no pueden otorgar un número de direcciones ilimitadas, ya que el espacio de direccionamiento de Internet esta llegando a su límite.

Un método de fomentar la conservación de direcciones es dividir una red en segmentos o subredes. Esto permite incrementar el número de segmentos independientes sin necesidad de más números de red IP.

III.10.1.- Subredes ("Subnetworking").

En la práctica, no se ponen en red 16 millones de nodos para una red clase A ó 65000 en una red clase B, frecuentemente lo que se hace es dividir este tipo de redes en subredes (la subdivisión de redes es soportada por muchos sistemas operativos).

Para dividir una red en subredes, se utilizan parte de los bits que identifican al *"host"*, para denotar un número de subred. De esta forma la identificación total de un *"host"*, que inicialmente estaba dada por el número de red y el número de *"host"*, ahora queda definida por el número de red, el número de subred y el número de *"host"*.

La cantidad de bits que se utilizan para la subred, determina el número de subredes en los que se dividirá la red original. Este número esta dado por 2 elevado a la cantidad de bits utilizados. Por ejemplo si se toman 3 bits, el número de subredes será 8. El resto de los bits usados inicialmente para el *"host"*, identificarán el número de *"host"* en cada subred.

En el caso especifico de una red clase A los 16,777,216 *"hosts"* se podrían agrupar en varias subredes. Por ejemplo, podemos utilizar los 16 bits de mayor valor (MSBs More Significative Bits) de la porción que le corresponde al *"host"* en una red clase A, para denotar el número de la subred y los 8 más bajos para el *"host"*, como se ve en la siguiente tabla:

RED CLASE A	*SUBRED DE 16 BITS*	*HOST DE 8 BITS*
<---------->	<---------->	<---------->
XXXXXXXX	XXXXXXXX.XXXXXXXX	XXXXXXXX

Tabla III.6.- *"Host"* en una Red Clase A.

Este esquema permitiría hasta 65,534 subredes utilizables (las subredes 0.0 y 255.255 están reservadas) y cada una con 254 *"hosts"* útiles (las direcciones 0 y 255 de cada subred están reservados). Obviamente se podría plantear cualquier otro esquema, para obtener un número diferente de subredes y *"hosts"* por subred.

III.10.1.1.- La Máscara de Subred.

La máscara de subred es usada para determinar el número de bits (de una dirección IP) que se utilizan para la subred y el *"host"*. La máscara tiene un valor de 32 bits (similar a una dirección IP) y esta formada por unos para la porción de red y subred y ceros para la porción de *"host"*.

Por ejemplo, en la dirección IP clase B 191.70.55.130, sin aplicar ningún esquema de subdivisión la mascara de red asociada por default será 255.255.0.0, aplicando el operador AND lógico, entre la dirección del *"host"* y la mascara definida, obtenemos la dirección de la red.

Es decir la máscara retiene los bits de la red y enmascara los bits de *"host"*, como lo ilustra la siguiente gráfica.

191	**70**	**55**	**130**	Dirección IP del host
1011 1111	1000 0110	0011 0111	1000 0010	BITs host IP
1111 1111	**1111 1111**	0000 0000	0000 0000	Mascara por Default clase B
1011 1111	1000 0110	0000 0000	0000 0000	BITS de la red clase B
191	**70**	**0**	**0**	Dirección IP de la red clase B

Tabla III.7.- Máscaras.

Se pueden utilizar distintos esquemas de partición, esto dará diferentes mascaras, que ahora se denominan de mascaras de subred.

En el siguiente ejemplo se subdivide una red clase B en 256 subredes de 256 *"hosts"* cada una. Para lograr esto, se diseñara una nueva mascara que divida la porción de *"host"*, inicialmente de 16 bits, en dos partes, una que denote el número de subred y otra que identifique al *"host"* dentro de cada subred. Cada una de estas partes consta de 8 bits.

Por lo que la máscara ahora incluye 16 "unos" para la parte de la red y 8 "unos" para la parte de la subred, es decir un total de 24 "unos" o sea 255.255.255.0. La siguiente tabla muestra como la mascara aplicada a una dirección cualquiera dentro de esta red, determina el número de red y subred a la que pertenece un *"host"*.

191	**70**	**55**	**130**	Dirección IP del host
1011 1111	1000 0110	0011 0111	1000 0010	BITs host IP
1111 1111	1111 1111	**1111 1111**	0000 0000	Mascara de subred
1011 1111	1000 0110	0011 0111	0000 0000	BITS de la subred
191	**70**	**55**	**0**	Dirección IP de la subred

Tabla III.8.- Máscara Aplicada a una Dirección en una Red.

Esta división, permite determinar fácilmente a partir de una dirección IP en notación punteada el número de subred del penúltimo byte y el número de *"host"* del último byte.

No se tiene que utilizar un byte completo exclusivamente para denotar el número de subred, se pueden utilizar cualquier número de bits, Si la porción inicial de bits para el *"host"* es H, y se utilizan S bits para denotar la subred, entonces queda H - S bits para el número de *"host"* con subred.

En el siguiente ejemplo, se usa una máscara que permite más subredes (512), pero con la desventaja de tener menos *"hosts"* (128) por cada subred:

191	**70**	**55**	**130**	Dirección IP del host
1011 1111	1000 0110	0011 0111	1000 0010	BITs host IP
1111 1111	1111 1111	**1111 1111**	1000 0000	Máscara de subred
1011 1111	1000 0110	0011 0111	1000 0000	BITS de la subred
191	**70**	**55**	**128**	Dirección IP de la subred

Tabla III.9.- Máscara que Permite más Subredes.

III.10.1.2.- Subredes contra Nodos.

El RFC 950 determina que al realizar el *"subnetmasking"* no deberán utilizarse ni la primera subred, ni la última subred al obtener los números de subredes.

La división en subredes permite segmentar el tráfico en diferentes redes, sin embargo una de sus principales desventajas, es que se pierden muchas direcciones dado que se debe recordar dos reglas importantes:

La primera y la última subred no se pueden utilizar (en su totalidad). Esto se debe a que son usadas para situaciones de direccionamiento especial. La última dirección de la red original (todos los bits en unos), corresponde a la última dirección de la última subred, esta se utiliza para mandar una señal de *"broadcast"* a todas las subredes directamente.

La primera dirección de la red original (todos los bits en ceros), corresponde a la primera dirección de la primera subred, ésta se utiliza para identificar a la red original.

La primera y la última dirección de cada subred, están reservadas. La primera dirección de cada subred está reservada para identificar a la subred, mientras que la última se utiliza para mandar un *"broadcast"* a todas los *"hosts"* de la subred.

Por lo que si N es el tamaño de cada subred y S representa el número de subredes, se perderán 2N+ 2(S-2) direcciones.

Por ejemplo si decido partir una red clase B en 256 subredes de 256 direcciones cada una, se pierden todas las direcciones de la primera y la última subred, esto es 512, pero por otra parte también se pierden la primera y la última dirección de las 254 subredes restantes, esto es 254*2=508, por lo que se pierde un total de 512+508=1020 direcciones sacrificadas para realizar la partición.

Esto no es muy crítico en redes clase A o B, pero sí en redes clase C donde el número de direcciones disponibles es crítico.

A continuación se presenta una tabla que permite observar diferentes configuraciones entre el número de subredes y *"hosts"* con diferentes máscaras de subred para las clases de direccionamiento B y C.

En esta tabla, se eliminan en cada caso, las dos subredes reservadas (primera y última) y las dos direcciones reservadas de cada subred (primera y última).

# Bits de mascara	Mascara de subred	# Subredes	# Hosts por subred
18	255.255.192.0	2	16382
19	255.255.224.0	6	8190
20	255.255.240.0	14	4094
21	255.255.248.0	30	2046
22	255.255.252.0	62	1022
23	255.255.254.0	126	510
24	255.255.255.0	254	254
25	255.255.255.128	510	126
26	255.255.255.192	1022	62
27	255.255.255.224	2046	30
28	255.255.255.240	4094	14
29	255.255.255.248	8190	6
30	255.255.255.252	16382	2

Tabla III.10.- Subred Clase A.

# Bits de	**Mascara de subred**	**# Subredes**	**# Hosts por subred**

mascara			
26	255.255.255.192	2	62
27	255.255.255.224	6	30
28	255.255.255.240	14	14
29	255.255.255.248	30	6
30	255.255.255.252	62	2

Tabla III.11. -Subred Clase C.

III.10.1.2.1.- Ventajas de las Subredes.

Al subdividir las redes, se oculta la organización de la red interna a los ruteadores externos y esto simplifica el ruteo. Por ejemplo, una subred de clase B requerirá menos rutas que el número equivalente de direcciones clase C. Las tablas de ruteo mas cortas hacen que la transferencia sea más rápida.

Además de ventajas técnicas, subdividir una red permite la administración descentralizada de las direcciones. Esto puede proporcionar beneficios políticos a la organización. Por ejemplo, un administrador puede asignar una subred a un departamento, y responsabilizar de la administración de su propia subred al encargado, esto es, de la asignación de direcciones, y la vigilancia de la unicidad de las mismas.

El *"subnetworking"*, elimina las limitaciones de distancia entre redes distantes, ya que aunque se encuentren en localidades diferentes, forman una sola red lógica, interconectada mediante ruteadores.

III.10.1.2.2.- Parámetros para Realizar la División.

Una de las principales tareas de un administrador de la red es determinar los requerimientos de la red. Lo más lógico es empezar por considerar cuántos *"host"* estarán conectados a la red.

Conectar el máximo número de *"hosts"* en un segmento Ethernet no es muy práctico debido a que esto crea problemas de desempeño ya que se congestiona la red. Sin embargo si solo se tiene asignada una red de clase C, aparentemente el *"subnetworking"* no tiene sentido, debido al escaso número de direcciones.

Aunque una clase C puede soportar hasta 254 *"hosts"*, en la práctica un segmento Ethernet clásico de una oficina en donde se usa herramientas de automatización, mantiene su eficiencia con 60 a 80 *"hosts"*. Dependiendo del tráfico, el máximo recomendable es 100 hosts por segmento. Por lo que también es recomendable particionar una clase C en varias subredes. Si se usa cableado estructurado, muchas tarjetas de HUB vienen con 12, 16 ó 24 puertos UTP, por lo que se recomienda adquirir concentradores *("hubs")* expandibles o con capacidad de realizar una pila *("snack")* para que las características de estos equipos no sean lo que determine el tamaño de las subredes.

El esquema de división puede ser definido por dos factores:

- Cuantas redes se desean tener
- El máximo número de *"host"* por red.

Usando el primer parámetro, se definiría inmediatamente el esquema de división, El procedimiento es el siguiente: el número de subredes+2, se redondea a la potencia de 2 inmediatamente superior, esto determina el número de bits que se usarán para la máscara de subred, el número de bits restantes de la porción de *"host"*, determinará el número de *"hosts"* por subred.

El segundo parámetro también definiría el esquema de división. El número máximo de *"hosts"* en alguna subred +2, se redondea a la potencia de dos inmediatamente superior, esto determina el número de bits utilizados por los *"hosts"* de cada subred, los bits restantes, determinan la cantidad de subredes con esa cantidad de *"host"*, en las que se podrá partir la subred.

Una configuración posible será dividir la red clase C en 8 subredes, con 32 direcciones IP cada una, debido a que la primera y la última subred no se pueden utilizar y la primera y la última dirección de las subredes restantes tampoco se pueden utilizar, esta configuración permite 6 subredes de 30 *"host"* cada una.

Caso de estudio: subdividiendo una red clase C.

La compañía ACME, posee la red clase C 192.100.180.0, el tráfico en el segmento único, hace que el desempeño de su red, sea poco eficiente. La compañía cuenta con 5 departamentos, con un número de computadoras entre 5 y 14. Determinar el esquema de división y por lo tanto la máscara de subred a utilizar.

Recordamos que para una red clase C, se utilizan 8 bits para el número de *"host"*.

Utilizando como parámetro la cantidad de subredes deseadas, se tienen 5+2=7, redondeando a la potencia de 2 más cercana que es 8, se determina que el número de bits utilizados por el número de subred es 3, para dar una máscara de subred de 27 bits que expresada en la notación punteada es: 255.255.255.224. Entonces los 5 bits restantes se usan para el número de *"host"*, lo que permite 32 direcciones por subred o hasta 30 *"hosts"*, lo que cumple con los requerimientos.

Utilizando como parámetro la máxima cantidad de *"hosts"* por subred, se tienen 14+2= 16, que es una potencia de 2, por lo que no hay que redondear, esto determina que se requieren 4 bits para identificar los *"host"* de cada subred, los 4 bits restantes se usarán para identificar las 16 subredes posibles. Este esquema permite 14 subredes de hasta 14 *"hosts"* cada una, lo que cumple con los requerimientos, la máscara de subred para este esquema es 255.255.255.240.

La siguiente tabla especifica las direcciones de las 8 posibles subredes bajo el esquema de la máscara 255.255.255.224, a partir de los tres bits utilizados por la subred.

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

Tabla III.12.- Direcciones de las 8 posibles Redes.

Entonces para cada subred tendremos las siguientes características:

NÚMERO DE SUBRED	IP SUBRED	IP PRIMER HOST	IP ULTIMO HOST	DEC.MIN	DEC.MAX
1	X.X.X.32	X.X.X.33	X.X.X.62	33	62
2	X.X.X.64	X.X.X.65	X.X.X.94	65	94
3	X.X.X.96	X.X.X.97	X.X.X.126	97	126
4	X.X.X.128	X.X.X.129	X.X.X.158	129	158
5	X.X.X.160	X.X.X.161	X.X.X.190	161	190
6	X.X.X.192	X.X.X.193	X.X.X.222	193	222

Tabla III.13.- Características.

En resumen podemos decir que la división de una red clase C debe ser cuidadosamente planeada y ejecutada. Se debe de instalar un ruteador para dividir la red en un determinado número de subredes, y entonces reenumerar los segmentos y homologar la máscara de subred en cada uno.

III.11.- Ruteo de IP.

Para poder manejar una red, en ocasiones es necesario dividirla en segmentos más sencillos de administrar. La forma de interconectar los segmentos es por medio de los ruteadores. Un ruteador pasara paquetes de datos de una red a otra y determinara la ruta óptima (**ruteo**) hacia la cual el tráfico de datos deberá ser dirigido de acuerdo con su destino final.

Para poder enviar datos se emplean lenguajes entre los ruteadores que se conocen como protocolos de ruteo, ya sea protocolo Interno de ruteo (IGP, *"Internal Gateway Protocol"*) o protocolo externo de ruteo (EGP, *"External Gateway Protocol"*) mismos que veremos más adelante.

III.11.1.- Datos de Ruteo.

Un paquete que es enviado a la red puede ser entregado a un elemento de la red dentro del segmento físico de red, a este tipo de servicio se le conoce como ruteo directo. Si se establece que el paquete debe ser enviado a un segmento diferente de red, distinto a su segmento de red, el paquete deberá ser enviado a través de un ruteador, a este tipo de ruteo se le conoce como ruteo indirecto.

¿Cómo sabe un nodo cuando utilizar un ruteo directo o un ruteo indirecto? El proceso es simple. Cuando un nodo (nodo origen) envía un paquete a otro nodo (nodo destino), el nodo origen verifica la dirección IP de red del nodo destino (recordando que los 4 primeros bits más significativos de la dirección IP son los que definen la clase de la dirección). Si el número de red del nodo destino pertenece al segmento de red local, los paquetes seán enviados de manera local, en caso contrario, el paquete será enviado a los dispositivos que tengan la capacidad de ruteo.

Una vez que se determinó que el paquete debe ser reenviado a otro segmento físico de red, el nodo origen deberá enviar la información necesaria al ruteador para que éste pueda dirigir el paquete hacia el segmento de red adecuado para alcanzar su destino final.

Cuando se alcanza el destino, el ruteador que se encuentra conectado a la red donde esta el nodo destino, manejará la información como si se tratara de un ruteo directo al realizar el proceso de establecer la comunicación local con su dirección MAC.

Cuando el paquete es enviado no se puede determinar cuantos ruteadores debe pasar para alcanzar su destino final, cada ruteador que sea atravesado irá decrementando el campo TTL (*"Time To Live"*) en la cabecera de IP, cuando el campo TTL sea cero, se enviará un mensaje ICMP, el destino no pudo ser alcanzado.

III.11.2.- Información de Ruteo y Tablas de Ruteo.

Una tabla de ruteo es necesaria para hacer más eficiente la decisión de que si el paquete de información que será enviado debe ser dirigido a un ruteador o debe ser manejado de manera local.

La tabla de ruteo es un conjunto de entradas (rutas), las cuales definen el camino por el cual un paquete de información puede ser enviado. La tabla de ruteo está formada por rutas previamente definidas(ruteo estático) o por intercambio de información de ruteo (protocolos de ruteo) entre los ruteadores (ruteo dinámico).

El método de ruteo estático siempre designa las mismas rutas para trayectos equivalentes en la red, siguiendo un esquema básico implementado por el administrador en la configuración del sistema. En el método de ruteo dinámico, los dispositivos ruteadores eligen las rutas para los paquetes de información, calculando en cada ocasión, las rutas más convenientes. El parámetro que se toma como referencia para obtener la mejor ruta se llama métrica.

Existen dos criterios de calcular la métrica, vector distancia (*"Distance Vector"*) y estado del enlace (*"Link State"*).

Cuando el ruteador no cuenta con la información necesaria en su tabla de ruteo para enviar un paquete a su destino hace uso de una entrada en la tabla de ruteo conocida como Rutas por omisión (*"Default Route"*), configurada manualmente por el administrador del sistema como la ruta a tomar cuando no existe ruta hacia el destino.

Una tabla de ruteo típica es la siguiente:

Número de Red	Conocida por algoritmo de ruteo	Métrica	Tiempo para mantener la ruta	Conocido por
134.4.0.0	Directamente conectado	0 hop	_____	Puerto 1
134.3.0.0	Directamente conectado	0 hop	_____	Puerto 2
200.34.234.0	Ruta estática	1	----------	Puerto 1
132.48.0.0	RIP	1 hop	270	134.4.3.56
148.4.0.0	RIP	1 hop	250	134.3.1.100
9.0.0.0	OSPF	Cost = 900	300	134.3.1.101
192.1.1.0	OSPF	Cost = 64	350	134.4.3.90

Tabla III.14.- Tabla de Ruteo Típica.

En la tabla anterior se observan protocolos de ruteo, de los cuales se hablará mas adelante; también se puede ver el ruteo estático y ruteo dinámico.

III.11.3.- Protocolos de Ruteo.

En ocasiones se confunden los términos protocolo ruteable y protocolo de ruteo. Los protocolos ruteables son los protocolos que se rutean entre las redes. Ejemplos de estos protocolos son IP, IPX, DECnet, AppleTalk, NetWare, OSI, Banyan VINES, y Xerox Network.

Los protocolos de ruteo son los que implementan los algoritmos de ruteo, en pocas palabras éstos rutean los protocolos ruteables entre las redes, y son los protocolos mediante los cuales se entienden los ruteadores.

Ejemplos de estos incluyen: Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), OSI Routing, Advanced Peer-to-Peer Networking, Intermediate System to Intermediate System (IS-IS), y Routing Information Protocol (RIP).

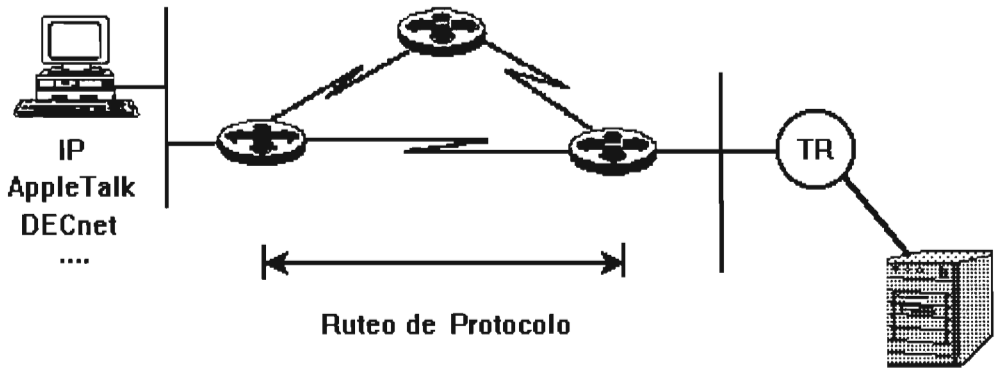


Figura III.8.- Protocolos de Ruteo.

III.11.4.- Algoritmo de Ruteo.

Los algoritmos de ruteo soportan a los protocolos de ruteo proporcionando las siguientes características:

- Construcción y mantenimiento de las tablas de ruteo.
- Escalar un protocolo ya existente a uno mejorado, por ejemplo RIP a IGRP.

La mayoría de los algoritmos de ruteo pueden ser clasificados conforme a cualquiera de dos algoritmos básicos, éstos son:

- Vector Distancia.
- Estado de Enlace.

Los algoritmos de ***Vector Distancia*** hacen llamados a cada ruteador vecino (adyacente) para enviarles su tabla de ruteo completa. Las tablas de ruteo de vector distancia incluyen información correspondiente al costo total de transferencia por cada ruta (el costo queda definido por el tipo de métrica en uso).

Con el algoritmo de vector de distancia se tiene que las tablas de ruteo se envían de manera rutinaria y periódicamente o bien cuando se han incluido cambios a la topología.

El segundo algoritmo básico para el ruteo es el de ***Estado de Enlace***. Este algoritmo realiza una captación total de la información relativa a la topología de la red y crea tablas de distancias mínimas y de caminos de tiempo mínimo de todo el sistema. Las tablas generadas con el uso de este algoritmo podrían compararse con mapas de carreteras, puesto que en éstos se puede localizar la ubicación de cada uno de los puntos de la red.

A diferencia del algoritmo de Vector de Distancia, el algoritmo de Estado de Enlace mantiene una información completa sobre todos los caminos disponibles a cada punto de la red. Los algoritmos de ruteo resultan procesos fundamentales en el método de ruteo dinámico y tienen cuatro características básicas:

- Exactitud

Los algoritmos de ruteo deben utilizar las características de reconocimiento de rutas para darles consistencia y exactitud a las decisiones de ruteo. Las decisiones deben estar basadas en la información más reciente sobre la topología de la red, que debe ser precisa y exacta.

- Sencillez

Los algoritmos de ruteo deben realizar sus funciones con un mínimo de software y de sobrecarga en la utilización del procesador. Los algoritmos de ruteo constantemente realizan las tareas de recálculo de rutas e intercambian información con los puntos en conexión. Si estas actividades no se realizan de manera eficiente pueden añadir un tráfico considerable en la red y con ello afectar el rendimiento de los procesos de ruteo.

- Confiabilidad

Los algoritmos de ruteo deben contar con operaciones continuas y facilidades de recuperación para situaciones poco comunes. Deben ser robustos.

- Adaptabilidad

Los algoritmos y sus protocolos asociados deben negociar con velocidad y eficiencia los cambios que se realicen en la topología.

III.11.5.- Métricas.

Los ruteadores usan distintas métricas para determinar la mejor ruta, algunos algoritmos combinan varias de ellas para obtener una métrica híbrida. Algunas de estas son:

- Longitud de la trayectoria (número de saltos o ruteadores en el trayecto)
- Confiabilidad
- Retardos
- Ancho de banda
- Carga de Tráfico
- Costo de la Comunicación

III.11.6.- Sistemas Autónomos (Autonomus System, AS).

En redes muy grandes que están conectadas a Internet, se tiene una administración local separada llamada Sistema Autónomo (AS-*"Autonomous System"*) que tiene un número único asignado por la DDN del NIC (*"Network Information Center"*). Un Sistema Autónomo (SA) puede estar integrado por varias LAN interconectadas por medio de puertas (*"gateways"*) internas.

En un sistema autónomo, la estructura de la red no es visible para el resto de la Internet. Por lo general una compuerta lleva hacia la red por lo que todo el tráfico correspondiente a esa red debe pasar a través de la compuerta, que oculta la estructura interna de la red local al resto de la red.

III.11.7.- Protocolos de Gateway Interno y Gateway Externo.

Si existe más de un *"gateway"* dentro de la red local y pueden comunicarse con otra, se consideran *"gateways"* vecinos interiores. Si los *"gateways"* pertenecen a diferentes sistemas autónomos, se trata de *"gateways"* exteriores.

III.11.8.- IGP ("Interior Gateway Protocol").

IGP es un protocolo cuya principal función es intercambiar información de tablas de ruteo entre *"gateways"*, *"hosts"* y ruteadores dentro de un esquema autónomo, es decir una red corporativa de redes independientes que desean intercambiar información entre ellas. El esquema de autonomía se define dentro del servicio de ruteo como Sistema Autónomo (*"Autonomous System"*).

Los protocolos de mayor relevancia en IGP son *"Routing Information Protocol"* (RIP) y *"Open Shortest Path First"* (OSPF).

III.11.8.1.- ***RIP*** *("Routing Information Protocol").*

RIP es unos de los protocolos de ruteo más utilizados para manejar la información al interconectar redes de área local LAN, RIP está clasificado como un protocolo de ruteo interno (IGP) por el *"Internet Engineering Task Force"* (IETF). Su base es utilizar el algoritmo de ruteo 80.

Al utilizar RIP como protocolo de ruteo, los *"gateways"* envían toda la información de las rutas que él conoce hacia el vecino más cercano, a este proceso se le conoce como actualización de tablas de ruteo, el vecino que recibe la información pasara al otro vecino la información que le llegó por el vecino original, este procedimiento de enviar las tablas de ruteo se realiza cada 30 segundos. El algoritmo de vector distancia usa como medida (métrica) de decisión para la generación de su tabla de ruteo la cuenta en saltos (*"Hop Count"*).

En caso de ocurrir algún cambio en la red, será reflejado hasta que la actualización de la tabla de ruteo se lleve a cabo, (30 segundos si está directamente conectado al vecino inmediato ó 450 segundos si es que se encuentra en la distancia máxima soportada por RIP, 15 saltos) a este cambio y el reflejo del mismo se le llama tiempo de convergencia.

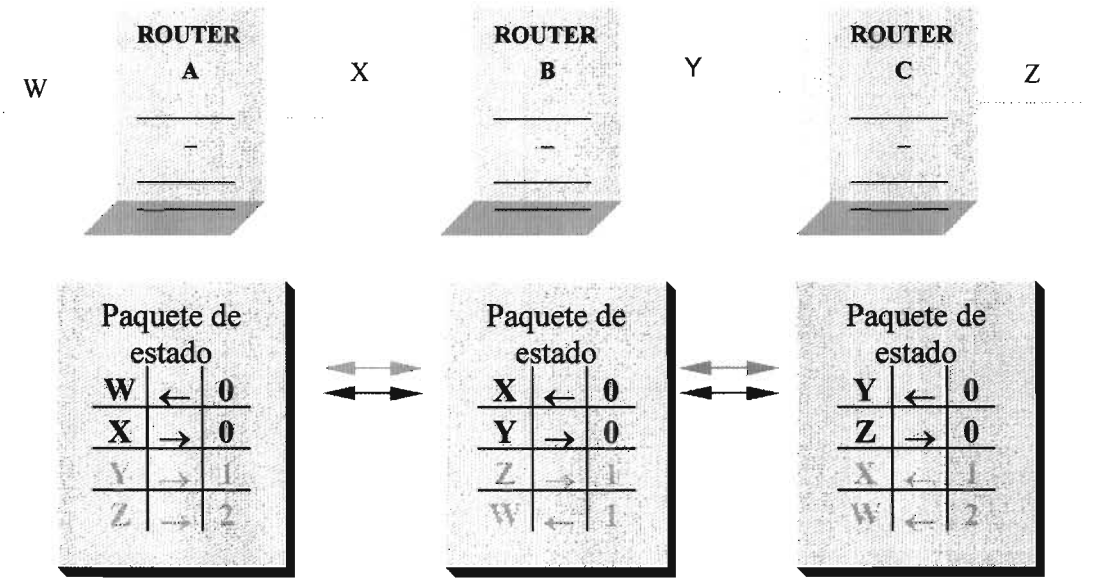


Figura III. 15.- RIP.

RIP es una buena solución para redes pequeñas. Sin embargo, para redes de mayor dimensión la transmisión de toda la tabla de ruteo cada 30 segundos sería una gran cantidad de tráfico innecesario en la red.

*III.11.8.2.- "Open Shortest Path First Protocol" (**OSPF**).*

OSPF es un protocolo de ruteo utilizado para redes más complejas dentro de un sistema autónomo, OSPF es preferido sobre RIP.

En OSPF, cuando se detecta un cambio en la tabla de ruteo o algún cambio en la topología de la red, es reflejado de manera inmediata por medio de *"Multicast"*, enviando la información a todos los nodos de la red. A diferencia de RIP de enviar la actualización cada 30 segundos, OSPF reporta de manera inmediata la actualización sí y sólo sí, ha existido algún cambio.

A diferencia de RIP que utiliza un método simple (número de saltos) para calcular la métrica, OSPF toma la decisión de la ruta basado en el algoritmo de ruteo *"link state"* que usa información adicional de los parámetros del enlace de red para realizar el cálculo de la métrica de su red. OSPF además soporta el concepto de subredes de máscara variable (VLSM, *"Variable Length Subnet Mask"*).

RIP no toma en cuenta la velocidad del enlace, para realizar el cómputo de decisión por donde debe de enviar el paquete de información, observando la figura se aprecia que se llega al mismo destino por dos rutas distintas, una línea es de 64kbps y las otras líneas son de 2.048Mbps, desde el punto de vista de RIP, la mejor ruta es por la línea de 64kbps (un salto), pero para OSPF la misma decisión es incorrecta, ya que la mejor ruta para OSPF es el enlace de 2.048 Mbps, por la capacidad de ancho de banda que tiene el enlace hacia el mismo destino.

Existe un concepto denominado sumarización, el cual surge con el objetivo de agrupar un rango de redes y reportar como si fuera una sola, este termino es mejor conocido como CIDR (*"Classless Interdomain Routing"*), que será tratado mas adelante.

Con OSPF debe existir una conectividad con los ruteadores vecinos, es decir se deben de reconocer para poder establecer el intercambio de información. La conectividad se lleva a cabo por medio de paquetes llamados *"Hello"*, éstos; permiten que los vecinos establezcan el intercambio de comunicación para manejar una comunicación bidireccional.

No se puede decir que todo es mágico en OSPF, si una red es muy grande los *"Multicast´s"* mencionados con anterioridad pueden convertirse en un problema, para evitar este problema se generan áreas.

III.11.9.- **EGP** ("Exterior Gateway Protocol").

Este tipo de protocolo es utilizado para intercambiar información de tablas de ruteo entre los Sistemas Autónomos, es utilizado principalmente por DDN (*"Defense Data Network"*); la tabla de ruteo contiene una lista de los ruteadores con el costo asociado (métrica) para seleccionar la mejor ruta. Cada ruteador solicita actualización de sus tablas de ruteo a los vecinos cada 120 a 480 segundos, EGP-2 es la versión más nueva de EGP.

El administrador de la red decidirá el ruteador que funcionará como ruteador externo para poder anunciar a la red interna las rutas que están recibiendo de otros sistemas autónomos.

"Border Gateway Protocol" (BGP), es más reciente, proporcionando capacidades adicionales.

III.11.10.- Áreas.

La administración se puede hacer compleja por conveniencia, la frase de Julio Cesar "divide y vencerás", aplica perfectamente en este concepto, ya que nos permite dividir nuestra red en regiones que sean más sencillas de administrar. Un área es una administración de equipos que constantemente se están comunicando entre sí.

El nivel óptimo de ruteo es cuando esta porción de información requiere comunicarse con un área con la que nunca perderá comunicación, a esta área se le conoce como el área 0 o área 0.0.0.0 en algunas implementaciones de OSPF, recibe el nombre de *"Backbone"*. Todas las áreas siempre están de manera contigua, todos los ruteadores tienen una ruta hacia otro ruteador.

III.11.11.- Ruteadores de Área Frontera ("Area Border Routers").

Los ruteadores que tienen comunicación con el área 0, (*"backbone"*) en alguna de sus interfases, serán llamados *"Area Border Routers"*. Éstos tienen la capacidad de propagar la información de las redes que están contenidas dentro del área de manera sumarizada, es decir con una *"subnet mask"* diferente a la del sistema autónomo.

III.11.12.- Enlaces Virtuales ("Virtual Links").

Todas las áreas deben tener contacto con el área 0 para poder conservar comunicación con las diferentes áreas, debido a que esto puede ser impráctico o difícil, existe un tipo especial que es conocido como un enlace virtual, virtual porque simula que conecta el área cero sin tener una interfase directamente conectada al *"Backbone"*.

III.11.13.- Interfase OSPF ("OSPF Interface").

Un ruteador tiene al menos dos interfases de red, el *"Area Border Router"* es un ruteador que tiene como característica que una o más de las interfases pertenecerá al área cero y el resto puede pertenecer a otra área. El decir que pertenece a un área es por que las interfases del ruteador están en contacto con los vecinos del área, éste contiene un identificador y posiblemente si se tiene autenticación con el ruteador, se necesitara el envío de una contraseña (*"Password"*). La información de ruteadores mal configurados o funcionando inapropiadamente será descartada.

III.11.14.- Comunicación entre Ruteadores con Protocolo OSPF ("OSPF Pockets").

Como todos los protocolos de ruteo la manera de comunicar información entre los ruteadores es por medio de paquetes, pero a diferencia de RIP que usa un servicio UDP y a diferencia de BGP que utiliza TCP, en el campo de tipo de protocolo de IP, con el servicio 89 asignado, determina que el mismo es un servicio de OSPF. Eliminando la cabecera del Protocolo de Internet (*"Internet Protocol"*), el ruteador sabe que la porción de información de datos de IP es información de OSPF.

In the Internet Protocol (IP) [DDN], [RFC791] there is a field, called Protocol, to identify the next level protocol. This is an 8 bit field.

Assigned Internet Protocol Numbers

Decimal	Keyword	Protocol	References
0	Reserved		[JBP]
1	ICMP	Internet Control Message	[RFC792,JBP]
4	IP	IP in IP (encapsulation)	[RFC1853]
6	TCP	Transmission Control	[RFC793,JBP]
17	UDP	User Datagram	[RFC768,JBP]
89	OSPFIGP	OSPFIGP	[RFC1583,JTM4]

Figura II.16.- Protocolo OSPF.

III.11.15.- Mantenimiento y Descubrimiento de los Vecinos.

Un ruteador con OSPF descubre a sus vecinos mediante paquetes de reconocimiento llamados paquetes de *"Hello"* en sus interfases, estos mensajes son enviados cada 10 segundos, es un parámetro que se puede configurar.

La porción de información que se envía con el protocolo OSPF, es responsable de establecer la comunicación entre los vecinos y detectar una falla en uno de sus vecinos, en caso de existir alguna; el vecino al no detectar información de que es lo que está ocurriendo en el sistema y al no recibir respuesta, inundará (*"flooding"*) con LSA[8] avisando que los ruteadores deberán de hacer el cálculo de la topología de la red. Este proceso se llama convergencia.

El paquete *"Hello"* es responsable de que cada vecino envíe y reciba paquetes en ambos sentidos. Además de manejar el intervalo de actualización, los intervalos sin envío de información y determinar cuando existe algún cambio.

8 Link State Advertisement, paquete de actualización.

Las redes se pueden clasificar en dos tipos de servicios, redes que manejan *"Broadcast"* y redes que no manejan *"Broadcast"*.

III.11.16.- Sincronización de la Base de Datos.

Cuando se realiza una conexión entre dos vecinos, el vecino que está arrancando debe esperar a que los *"link state packets"* para poder sincronizar su propia base de datos antes de empezar a utilizar el servicio de redireccionar tráfico en sus interfases.

El intercambio de LSA (*"Link State Advertisement"*), permite que la base de datos de información de las tablas de ruteo sea conocida y el LSA avisa solo cuando existe un cambio en la estructura de la red.

III.11.17.- Conclusión de IGP's.

RIP	**OSPF**
La topología de la red se ve desde la perspectiva del vecino	La topología de red es desde el punto de vista del propio ruteador
La métrica utilizada para sus tablas de ruteo son saltos sin tomar en cuenta la cantidad de información que puede llevar el enlace (bandwidth).	La métrica para el uso de servicio es un costo, en el cual se toma en cuenta el bandwidth.
Se realizan actualizaciones para saber los cambios en la red.	Se envían LSA para conocer de algún cambio en la red.
Su convergencia es lenta.	La convergencia es más rápida.

Tabla III.15.- IGP´s.

III.11.18.- "Border Gateway Protocol" (**BGP**).

BGP (*"Border Gateway Protocol"*) es un protocolo que intercambia su propia tabla de ruteo entre puertas (*"gateways"*), cada una de ellas con su propio Sistema Autónomo; es el protocolo que se usa actualmente para intercambiar información en Internet, la información es enviada por parte de los ruteadores en su tabla de ruteo.

III.11.18.1.- Figura de Sistemas Autónomos.

Los nodos al comunicarse con BGP utilizan TCP (*"Transmission Control Protocol"*) al puerto 179 y envían la información cuando han detectado algún cambio de información. Una vez establecida la comunicación de TCP el propósito es intercambiar rutas entre los vecinos. BGP-4 es la última versión de BGP.

BGP-4 tiene la capacidad de manipular sumarización, mejor conocido como CIDR (*"Classless Inter-Domain Routing"*). Que es la manera de agrupar un número de redes con *"subnet-mask"* diferente al asignado a las redes internas.

BGP fue desarrollado para poder reemplazar a su predecesor EGP (ya un protocolo obsoleto), mientras la red en Internet empezó a crecer las actualizaciones por parte de EGP, empezaron a tener sus altibajos, BGP los ha ido resolviendo de manera más eficiente, BGP es el protocolo utilizado por los ISP´s.

El RFC 1771 describe a BGP-4. El RFC 1654 describe la primera versión de BGP-4. BGP inicialmente intercambia toda la información posible, posteriormente, envía actualizaciones increméntales, en caso de no existir actualizaciones, se envían mensajes de *"keepalive"*, para monitorear si el vecino está funcionando.

III.11.18.2.- "Classless Inter-Domain Routing" (CIDR).

Las tablas de ruteo de internet han ido creciendo de manera exponencial, en Diciembre de 1990 existían 2190 rutas, 2 años después, eran aproximadamente 8500 rutas. Para Julio de 1995 eran alrededor de 29,000 rutas que requieren aproximadamente 10MB de RAM por ruteador para mantenerlas. Los ruteadores con 64MB podrían mantener en RAM alrededor de 60,000 rutas.

IDR (*"Classless Inter-Domain Routing"*) está generado por los RFC1517, RFC1518, RFC1519, RFC1520. **CIDR** es un método de evitar que la tabla de ruteo se pierda por falta de recursos en el equipo. Sin la implementación CIDR en 1994, Internet actualmente no podría seguir funcionando.

El principio de CIDR elimina el concepto de las redes Clase A, B y C, y lo generaliza en un prefijo de IP, CIDR cubre un espacio de direcciones más amplio al agrupar una cantidad mayor de redes.

Cuando se habla de la dirección 192.1.0.0, es una red clase C, el número de red es 192.1.0.0 y el *"Netmask"* es 255.255.255.0, el formato que maneja CIDR es el siguiente: La red 192.1.0.0/16, es decir el rango de direcciones comprendida entre 192.1.0.0 a 192.255.0.0, este rango se reporta como una sola red, en lugar de guardar 255 redes en la tabla de ruteo solo se conserva una red que agrupa a todo el rango. Es como si el ruteador da a conocer una dirección clase C 192.1.0.0 pero con máscara de red clase B.

III.11.18.3.- Información de las Cabeceras de BGP.

Todos los mensajes de BGP están comprendidos en un solo paquete de información, pueden variar según sea el tipo de información que se está enviando.

Cada paquete de BGP tiene como principal propósito identificar qué servicio será el que se va a utilizar.

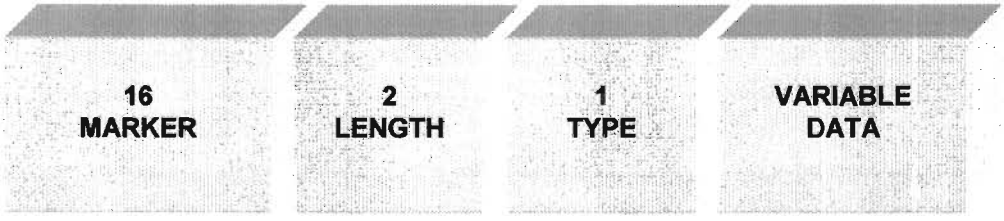


Figura III.17.- Cabeceras de BGP.

BYTES

Marker
Contiene Información de autenticación del mensaje del receptor.

Length
Longitud total del mensaje en bytes.

Type
El tipo de mensaje:

Open
Update
Notification
Keep-alive

Data
Información para las capas superiores. Este campo es opcional

III.11.18.4.- Resumen de BGP-4.

Es considerado un protocolo de ruteo para comunicar sistemas autónomos. Existen dos clases de BGP, interno y externo, (IBGP y EBGP). BGP soporta CIDR.

III.12.- Capa de Transporte.

Esta sección presenta el segundo protocolo más importante y bien conocido de los servicios Internet, el Protocolo de Control de la Transmisión (*"Transmission Control Protocol"*, TCP), aunque aquí se presenta como parte de la familia de protocolos TCP/IP, en realidad se trata de un protocolo independiente, de propósito general que se puede adaptar para usarse sobre otro sistema de entrega. Por ejemplo, debido a que TCP hace muy pocas asunciones acerca de la red subyacente, es posible usarlo sobre una sola red Ethernet o sobre la compleja Internet. De hecho, TCP es tan popular que uno de los protocolos de ISO, el TP-4 se ha derivado de él. El estándar TCP está definido en el RFC 793. [Postel, 1981].

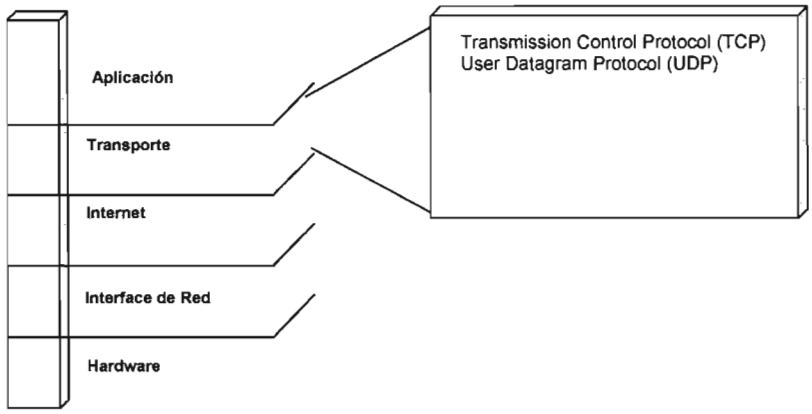


Figura III.18.- TCP.

III.12.1.- La Necesidad de una Entrega Garantizada.

En el nivel más bajo, las redes de comunicaciones ofrecen una entrega no confiable de paquetes. Los paquetes pueden perderse o destruirse cuando ocurren errores en la transmisión de datos, cuando falla la red o cuando la red está demasiado saturada. Las redes que envían dinámicamente los paquetes, los podrían entregar en desorden, retardarlos o entregarlos duplicados. Más aún, las tecnologías de red subyacentes podrían dictar un tamaño óptimo de paquete u otras restricciones necesarias para lograr los niveles óptimos de transferencia.

En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de información de una computadora a otra. El uso de un sistema de entrega no orientado a la conexión, no confiable para la transferencia de grandes cantidades de datos es tedioso y problemático además de que requeriría que los programadores desarrollaran un método de detección y corrección de errores para cada programa de aplicación.

Debido a la dificultad que representa la elaboración de software que ofrezca confiabilidad en cuanto a los conocimientos técnicos que un programador necesitaría, sería difícil contar con tal *software*.

III.12.2.- Propiedades de un Servicio de Entrega Confiable.

La interfase entre los programas de aplicación y el servicio de entrega de TCP/IP debe contar con 5 características:

Orientación a *"Streams"* o Flujos.

Cuando dos aplicaciones transfieren grandes volúmenes de datos nos imaginamos los datos como flujos de bits, divididos en octetos de 8 bits o bytes. El servicio de entrega de un *"stream"* a su destino se realiza en la misma secuencia de octetos en que estaban en la máquina original.

Conexión de Circuitos Virtuales.

La transferencia de un *"stream"* es análoga a una llamada telefónica. Antes de que pueda comenzar la transferencia, la aplicación que envía y la que recibe, interactúan con sus respectivos sistemas operativos, informándoles acerca de su deseo de hacer una transferencia de un *"stream"*.

Conceptualmente, una máquina pone una "llamada", la cual debe aceptarse por la otra. El software del protocolo en los dos sistemas operativos se conecta con el otro enviando mensajes a la red, verificando que la transferencia se ha autorizado y que ambos lados están listos. Una vez que se han establecido todos los detalles, los módulos del protocolo le informan a las aplicaciones que se ha establecido una comunicación y que puede comenzar la transferencia.

Durante la transferencia, el software del protocolo de ambas máquinas continúa comunicándose con el de la otra máquina para verificar que los datos se hayan recibido correctamente. Si la comunicación fallara por alguna razón (ejemplo: Por una falla de hardware en la red), ambas máquinas detectan la falla y la reportan a los programas de aplicación apropiados. Aquí el término *circuito virtual* se usa para describir tales conexiones porque aunque las aplicaciones ven a la conexión como un circuito de hardware dedicado, la confiabilidad es una ilusión provista por el servicio de entrega de *"streams"*.

Transferencia con Buffer.

Las aplicaciones mandan un flujo de datos a través del circuito virtual al pasar octetos de datos repetidamente al software del protocolo. Cuando se están transfiriendo los datos, cada aplicación usa el tamaño de piezas que crea conveniente, que puede ser tan pequeño como un octeto.

En el lado del receptor, el software del protocolo entrega los octetos desde el flujo de datos en el mismo orden en que fueron enviados, poniéndolos a disposición de la aplicación receptora tan pronto como son recibidos y verificados. El software del protocolo es libre de dividir el flujo en paquetes independientes de piezas que la aplicación transferirá. Para hacer más eficiente la transferencia y para minimizar el tráfico de la red, las diferentes implantaciones usualmente colectan suficientes datos de un *"stream"* para llenar un datagrama razonablemente grande antes de transmitirlo a través de la Internet.

Así, cuando las aplicaciones generen el *"stream"* en base de un octeto a la vez, la transferencia a través de la red puede ser muy eficiente. De manera similar, si la aplicación elige generar bloques de datos extremadamente grandes, el software del protocolo podría optar por dividir cada bloque en piezas más pequeñas para su transmisión.

Para aquéllas aplicaciones donde los datos deben entregarse aún cuando el buffer no esté lleno, el servicio de *"stream"* ofrece un mecanismo de *empujar,* mismo que las aplicaciones usan para transferir todos los datos que se hayan generado sin esperar a que se llene el buffer. Cuando llegan al lado del receptor, el mecanismo de *empujar* causa que TCP ponga los datos a disposición de la aplicación sin retardo alguno. Sin embargo esto solo garantiza que todos los datos serán transferidos; no ofrece límites de los registros. Así, aún cuando la entrega sea forzada, el software del protocolo puede optar por dividir el *"stream"* de una manera indeterminada

"Stream" no Estructurado.

Es importante entender que el servicio TCP/IP no reconoce flujos de datos estructurados. Por ejemplo, no hay manera de que una aplicación de nómina haga que el servicio de *"stream"* marque los límites entre los registros de los empleados, o para identificar que el contenido del *"stream"* sean datos de la nómina. Los programas de aplicación que usan el servicio de *"stream"* deben interpretar su contenido y estar de acuerdo en su formato antes de iniciar la conexión.

Conexión Full Dúplex.

Las conexiones que ofrece el servicio de *"stream"* de TCP/IP son concurrentes en ambas direcciones, es decir, full dúplex. La ventaja de una conexión full dúplex es que el software del protocolo subyacente puede enviar información de control de un *"stream"* de regreso a la fuente en los mismos datagramas que llevan los datos en la dirección opuesta. A esta técnica se le llama *"piggybacking"* y reduce el tráfico de la red.

III.12.3.- Proporcionando Confiabilidad.

Un servicio confiable conocido en ingles como envío de *"streams"* garantiza la entrega de los datos de una máquina a otra sin la duplicación o pérdida de datos. Pero, ¿Cómo puede el software del protocolo ofrecer una transferencia confiable si el sistema de comunicación inferior (llámese IP) sólo ofrece entrega no confiable de paquetes? La respuesta es un poco complicada y se llama *acuse de recibo positivo con retransmisión ("positive aknowledgment").* La técnica requiere un recipiente para comunicarse con la fuente, mandando un mensaje de regreso llamado *acuse de recibo o ("acknowledge")* a medida que va recibiendo los datos, el que envía manda un registro con cada paquete que envía y espera el *acuse de recibo* antes de enviar el siguiente paquete.

El que envía también activa un reloj cuando envía un paquete y lo *retransmite* si el tiempo de reloj expira antes de recibir el acuse de recibo. La siguiente figura muestra cómo el protocolo más simple con acuse de recibo transfiere los datos, cada línea diagonal representa la transferencia de un mensaje a través de la red.

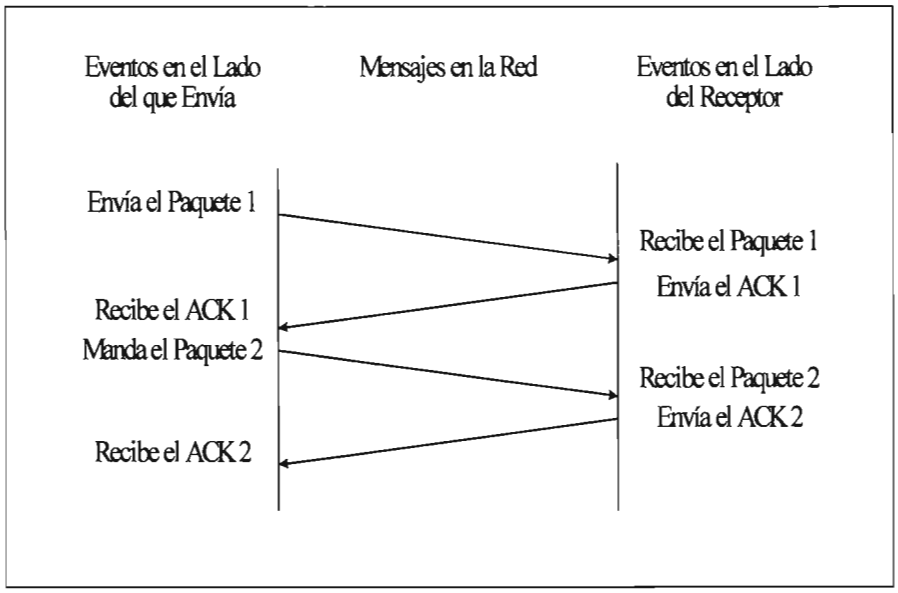


Figura III.19.- Transferencia de un Mensaje.

Un protocolo usando acuse de recibo con retransmisión que envía espera un acuse de recibo para cada paquete enviado. La distancia vertical hacia abajo representa el incremento del tiempo y las líneas diagonales en medio representan la transmisión de paquetes en la red.

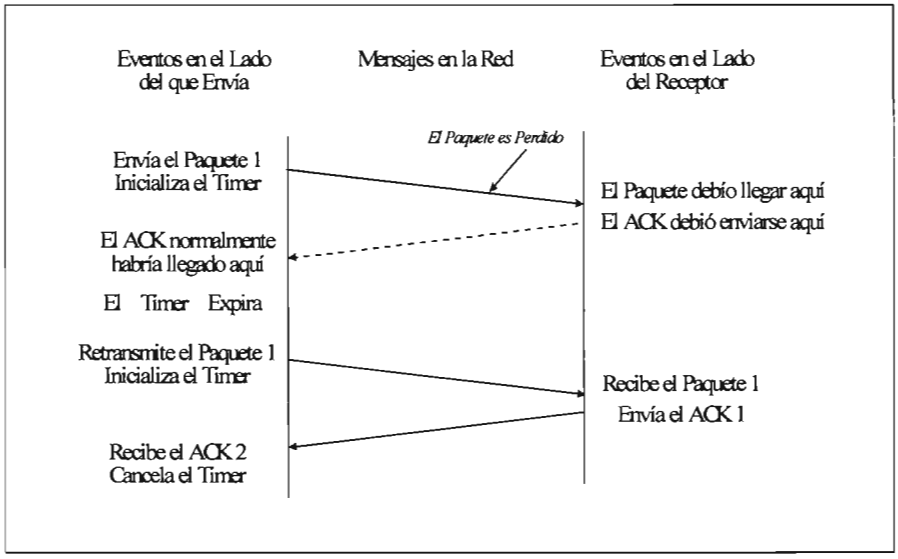


Figura III.20.- Transmisión de Paquetes en Red.

El problema final de confiabilidad surge cuando el sistema de entrega de paquetes subyacente duplica los paquetes. Los duplicados también pueden originarse cuando las redes experimentan retardos largos que causan la retransmisión prematura.

Para resolver la duplicación se requiere especial cuidado porque tanto los paquetes como el acuse de recibo podrían estar duplicados. Usualmente, los protocolos confiables detectan los paquetes duplicados al asignarle a cada paquete un número de secuencia y exigiéndole al receptor que recuerde los números se secuencia que ha recibido.

En la figura III.20, el *"timeout"* y retransmisión ocurre cuando se pierde un paquete. Las líneas punteadas muestran el tiempo que tomaría la transmisión de un paquete y su acuse de recibo si el paquete no se hubiera perdido.

Para evitar confusiones causadas por los acuses de recibo duplicados o retardados, los protocolos con acuse de recibo mandan los números de secuencia de regreso en los acuses de recibo para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes.

III.12.4.- Las Ventanas Deslizantes ("Sliding Windows").

Antes de examinar el servicio de flujo de TCP, se debe explorar un concepto adicional sobre el que trabaja la transmisión de flujos. El concepto, conocido como Ventanas Deslizantes, se asegura que la transmisión de *"streams"* sea eficiente. Para lograr la confiabilidad, el que manda, transmite un paquete y luego espera su acuse de recibo antes de transmitir otro.

Los datos sólo fluyen entre las máquinas en una sola dirección a la vez, aún cuando la red sea capaz de realizar comunicaciones simultáneas en ambos sentidos. La red estará totalmente inactiva durante los momentos en que las máquinas retarden sus respuestas (ejemplo; mientras las máquinas calculan las sumas de control o las rutas). Si se imagina una red con largos retrasos en la transmisión, el problema es claro: Un protocolo con acuse de recibo positivo desperdicia una parte sustancial del ancho de banda porque debe retrasar el envío de un nuevo paquete hasta no recibir el acuse de recibo del paquete previo.

La técnica de la Ventana Deslizante es una forma más compleja que la del acuse de recibo y retransmisión que el sencillo método mostrado anteriormente. Los protocolos de la ventana deslizante usan mejor el ancho de banda de la red porque le permiten al que envía transmitir múltiples paquetes antes de esperar un acuse de recibo.

La manera más sencilla de conceptualizar la operación de las Ventanas Deslizantes es imaginándose la secuencia de paquetes a ser transmitidos como lo muestra la figura. El protocolo pone una pequeña ventana en la secuencia y transmite todos los paquetes que quepan dentro de ella.

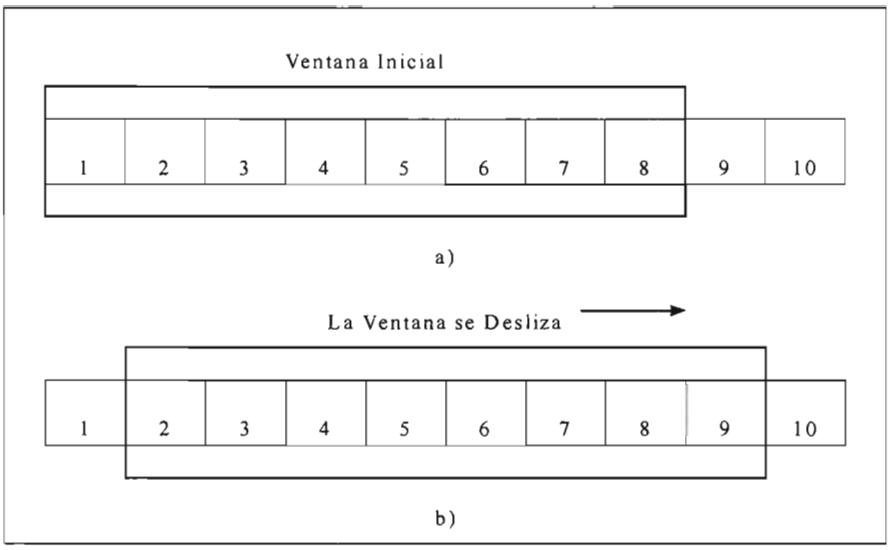


Figura III.21.- Ventajas Deslizantes.

Ventanas deslizantes: a) Un protocolo de ventana deslizante con 8 paquetes dentro de la ventana, y b) La ventana moviéndose de tal manera que se pueda enviar el paquete 9 una vez que se ha recibido el acuse de recibo para el paquete 1. Sólo los paquetes sin acuse de recibo son retransmitidos.

Técnicamente, el número de paquetes sin acuse de recibo que pueden existir en un momento dado está limitado por el tamaño de la ventana a un número pequeño y fijo. Por ejemplo, en un protocolo de ventana deslizante con tamaño de ventana de 8, el que envía tiene permitido transmitir 8 paquetes antes de recibir un acuse de recibo.

Como la muestra la Figura III.21, una vez que el que envía recibe un acuse de recibo del primer paquete dentro de la ventana, la "mueve" longitudinalmente y envía el siguiente paquete. La ventana continúa moviéndose mientras se estén recibiendo los acuses de recibo.

El desempeño de los protocolos de ventana deslizante depende del tamaño de la ventana y de la velocidad a la que la red acepte los paquetes. La Figura III.21 muestra un ejemplo de la operación del protocolo de ventana deslizante cuando envía tres paquetes. Nótese que el que envía manda los tres primeros paquetes antes de recibir acuse de recibo alguno.

Cuando el tamaño de la ventana es 1, el protocolo de la ventana deslizante es exactamente igual que el protocolo simple de acuse de recibo positivo. Al incrementar el tamaño de la ventana, es posible eliminar la inactividad de la red totalmente.

Esto es, en el caso continuo, el que envía podría transmitir paquetes tan rápido como la red pudiera transmitirlos. El punto principal es: debido a que un protocolo de ventana deslizante bien configurado mantiene a la red totalmente saturada de paquetes, obtiene un *"throughput"* sustancialmente mas alto que el del protocolo simple con acuse de recibo positivo.

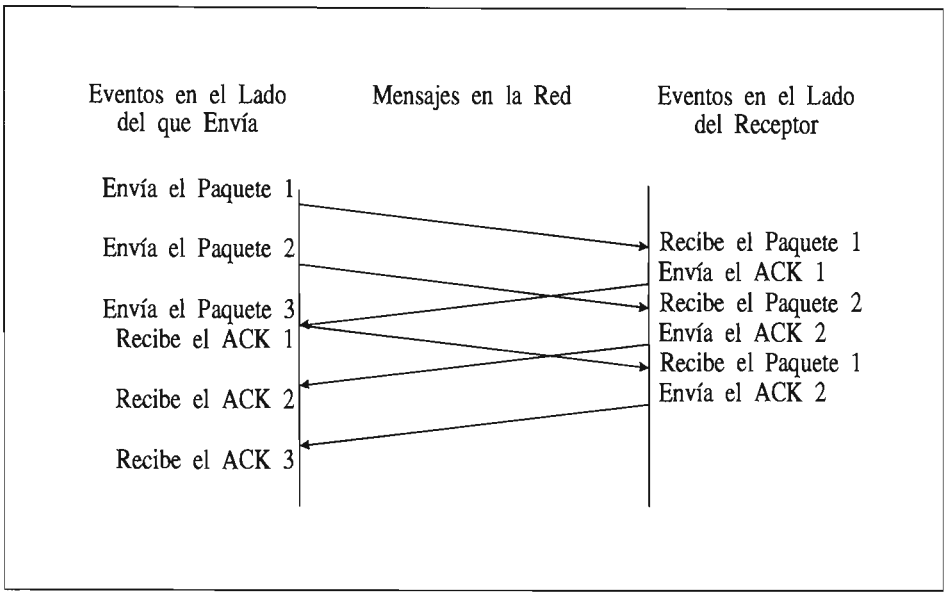


Figura III.22.- Un Ejemplo de tres Paquetes Transmitidos usando un Protocolo de Ventana Deslizante.

El concepto clave es que el que envía puede transmitir todos los paquetes de la ventana sin esperar ningún acuse de recibo.

Conceptualmente, un protocolo de ventana deslizante, siempre recuerda qué paquetes han sido notificados como recibidos y mantiene un *"timer"* separado para cada paquete sin acuse de recibo. Si un paquete se pierde, el *"timer"* expira y el que envía retransmite el paquete. Cuando el que envía mueve su ventana, deja atrás a todos los paquetes con acuse de recibo. En el lado del receptor, el software del protocolo mantiene una ventana similar, aceptando y acusando de recibido los paquetes como van llegando.

Así, la ventana separa la secuencia de paquetes en tres conjuntos: los que están a la izquierda de la ventana son los que han sido transmitidos, recibidos y notificados exitosamente; los que están a la derecha son los que todavía no son transmitidos y los que están dentro de la ventana son los que están siendo transmitidos. El paquete con el número mas bajo dentro de la ventana es el primer paquete de la secuencia que no ha sido notificado como recibido.

III.12.5.- El Protocolo de Control de la Transmisión (Transmission Control Protocol, **TCP**).

Ahora que se ha entendido el principio de la ventana deslizante, se examinará el servicio de *"stream"* confiable proporcionado por la familia de Protocolos TCP/IP. El servicio se define como *"Transmission Control Protocol"* o **TCP**. El servicio confiable de *"stream"* es tan importante que al protocolo a menudo se le llama TCP/IP. Es importante entender que: **TCP** es un protocolo de comunicación, no una pieza de software.

La diferencia entre un protocolo y el software que lo implanta es análoga a la diferencia entre la definición de un lenguaje de programación y un compilador, lo que ocurre es que frecuentemente se olvida la diferencia entre la definición y la implantación.

El **Protocolo TCP** especifica el formato de los datos y acuses de recibo que dos computadoras intercambian para lograr una transferencia confiable, al igual que los procedimientos

usados por las computadoras para asegurarse de que los datos lleguen correctamente. Especifica cómo el software de TCP distingue entre los múltiples destinos en una máquina dada y cómo las máquinas que se comunican se recuperan de errores tales como paquetes perdidos o duplicados. El Protocolo también especifica cómo dos computadoras inician una transferencia de flujos y cómo se ponen de acuerdo cuando está completa.

Es importante también entender lo que el Protocolo no incluye. Aunque la especificación TCP describe cómo las aplicaciones usan el TCP en términos generales, no dicta los detalles de la interfase entre una aplicación y TCP. Esto es, la documentación del Protocolo sólo discute las operaciones que TCP ofrece; no especifica los procedimientos exactos que los programas invocan para tener acceso a estas operaciones.

La razón para no especificar la interfase para la programación de aplicaciones es flexibilidad. En particular, porque los programadores usualmente lo implantan sobre el sistema operativo de las computadoras y deben utilizar la interfase que cada sistema operativo ofrezca. Ésta le da al programador la flexibilidad que hace posible tener una sola especificación para TCP que se puede usar para implantarlo en una gran variedad de máquinas.

Debido a que TCP asume muy poco acerca del sistema de comunicaciones subyacente, se puede usar con una gran variedad de sistemas de entrega de paquetes, incluyendo IP. Por ejemplo, TCP se puede implantar sobre líneas telefónicas, redes locales, redes de fibra óptica de alta velocidad o redes lentas. De hecho, la gran variedad de sistemas de entrega que TCP puede usar es una de sus fuerzas principales.

III.12.5.1.- Puertos, Conexiones y Puntos de Conexión.

TCP, al igual que el *"User Datagram Protocol"*, (UDP) (que se verá en la siguiente sección), reside arriba de IP en el esquema de protocolos por capas. TCP permite que las múltiples aplicaciones de una máquina dada se comuniquen de manera concurrente y demultiplexa[9] el tráfico TCP entrante entre las aplicaciones. TCP usa los números de puerto para identificar el destino final dentro de la máquina. Cada puerto tiene asignado un número entero pequeño que lo identifica.

Exactamente, ¿qué son los puntos de conexión? Una conexión consiste de un circuito virtual entre dos aplicaciones, así que es natural asumir que una aplicación sirve como el punto de conexión.

TCP define un punto de conexión como un par de enteros; (nodo, puerto), donde nodo es la dirección IP de un nodo y puerto es un puerto TCP en dicho *"host"*. Por ejemplo, el punto de conexión (128.10.2.3,25) especifica el puerto TCP 25 en la máquina con dirección IP 128.10.2.3.

Recuérdese que una conexión se define por sus dos puntos de conexión. Así, si hay una conexión de la máquina (18.26.0.36) a la máquina (128.10.2.3), podría definirse por los puntos de conexión:

(18.26.0.36,1069) y (128.10.2.3,25).

Mientras tanto, otra conexión podría estar en progreso desde la máquina (128.9.0.32) a la misma máquina de (128.10.2.3), identificada por sus puntos de conexión:

(128.9.0.32, 1184) y (128.10.2.3,53).

Hasta aquí el ejemplo ha sido muy sencillo porque los puertos usados en todos los puntos de conexión han sido únicos. Sin embargo, la abstracción de conexión permite múltiples conexiones

9 Del inglés "demultiplex" que es la operación de extraer las diferentes señales que viajan en un solo canal. Es la operación inversa al multiplexaje..

compartiendo un punto de conexión. Por ejemplo, se podría agregar otra conexión a las dos de arriba desde la máquina (192.100.202.5.139):

(192.100.202.5,1184) y (128.10.2.3,53).

Podría parecer extraño que dos conexiones puedan usar el puerto TCP 53 de la máquina 128.10.2.3 de forma simultánea, pero no existe ninguna ambigüedad porque TCP asocia los mensajes entrantes con una conexión en lugar de un puerto, usa ambos puntos de conexión para identificar la conexión apropiada. La idea importante a recordar es: Debido a que TCP identifica una conexión por un par de puntos de conexión, un puerto TCP dado puede compartirse por múltiples conexiones en la misma máquina.

III.12.5.2.- Aperturas Pasivas y Activas.

A diferencia de UDP, TCP es un protocolo orientado a la conexión que requiere que ambos puntos estén de acuerdo a participar. Esto es, antes de que el tráfico TCP pueda pasar por una Internet, las aplicaciones de ambos lados deben ponerse de acuerdo en que se desea la conexión. Para hacer esto, la aplicación de un lado realiza una función de apertura pasiva al contactar a su sistema operativo e indicarle que aceptará una conexión entrante.

En ese momento, el sistema operativo asigna un número de puerto TCP para su lado de la conexión. La aplicación en el otro lado entonces contacta a su sistema operativo usando la petición de apertura activa para establecer la conexión. Los dos módulos de software TCP se comunican para establecer y verificar una conexión. Una vez que se ha creado la conexión, las aplicaciones pueden empezar a transferir datos; los módulos de software de TCP en cada extremo intercambian mensajes que garantizan la entrega confiable. Posteriormente se explicarán los detalles de esta comunicación después de examinar el formato de un mensaje TCP.

III.12.5.3.- Segmentos, "Streams" y Números de Secuencia.

TCP ve el flujo de datos como una secuencia de octetos o bytes que divide en segmentos para su transmisión. Normalmente, cada segmento viaja a través de la red en un solo datagrama IP.

TCP usa un mecanismo especializado de ventana deslizante para resolver dos importantes problemas: transmisión eficiente y control de flujo. El mecanismo de la ventana deslizante hace posible enviar múltiples segmentos antes de que llegue un acuse de recibo.

Este mecanismo también resuelve el problema de control de flujo extremo a extremo al permitir que el receptor restrinja la transmisión hasta que tenga suficiente espacio en el buffer para meter más datos.

El mecanismo de la ventana deslizante de TCP opera a nivel de octetos, no a nivel de segmentos o paquetes. Los octetos en el flujo de datos se numeran secuencialmente y el que envía mantiene tres apuntadores asociados con cada conexión. Los apuntadores definen una ventana deslizante tal como la ilustra la siguiente figura. El primer apuntador marca la izquierda de la ventana deslizante, separando los octetos que han sido enviados y con acuse de recibo de los que todavía no se envían.

Un segundo apuntador marca la derecha de la ventana deslizante y defina el último octeto de la secuencia que se puede enviar antes de que se reciban mas acuses de recibo. El tercer apuntador marca la frontera dentro de la ventana que separa aquellos octetos que ya se enviaron de los que todavía no se envían.

El software del protocolo manda todos los octetos de la ventana sin retraso, por lo que la frontera dentro de la ventana generalmente se mueve muy rápido de izquierda a derecha.

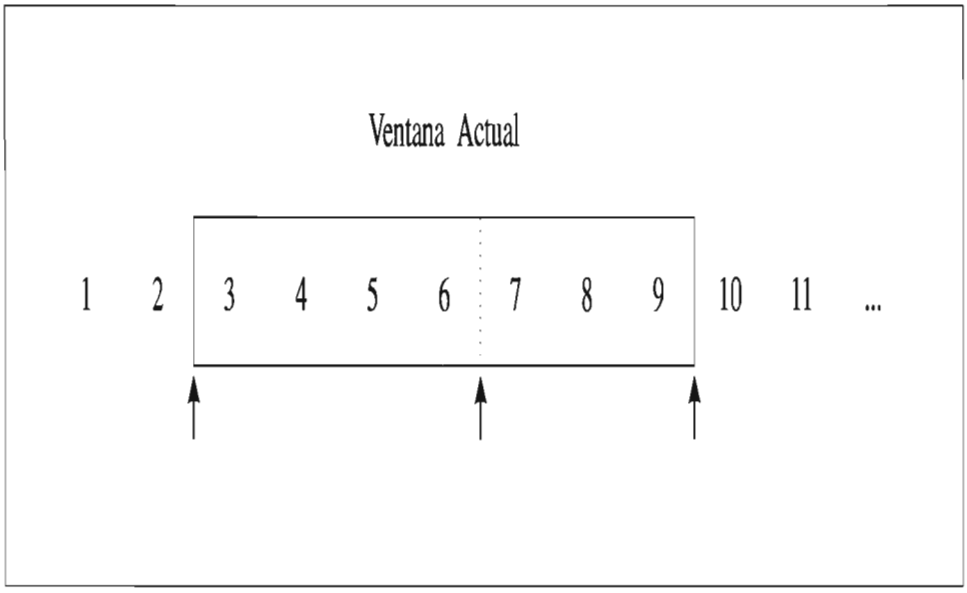


Figura III.23.- Ventana Actual.

III.12.5.4.- Un Ejemplo de una Ventana Deslizante de TCP.

Los octetos 1 y 2 ya fueron enviados y se recibió el acuse de recibo, los octetos 3 a 6 ya fueron enviados pero no ha llegado su acuse de recibo, los octetos 7 a 9 todavía no han sido mandados pero serían enviados sin demora alguna y los octetos 10 en adelante no se pueden enviar hasta que la ventana se mueva.

Se ha descrito cómo la ventana TCP del que envía se mueve y se ha mencionado que el receptor debe mantener una ventana similar para armar el *"stream"*. Es importante entender que debido a que las conexiones TCP son full dúplex, dos transferencias proceden inmediatamente sobre cada conexión, una en cada dirección.

Las transferencias son totalmente independientes porque en cualquier momento los datos pueden fluir a través de la conexión en una dirección o en ambas. Así, el software de TCP en cada extremo mantiene dos ventanas por conexión (para un total de cuatro), una se desplaza a lo largo de los datos del *"stream"* que se están enviando, mientras las otras se desplazan a lo largo de los datos recibidos.

III.12.5.5.- Tamaño de Ventana Variable y Control de Flujo.

Una diferencia entre el protocolo de la ventana deslizante de TCP y el protocolo simplificado de ventana deslizante presentado al principio, es que TCP permite que el tamaño de la ventana cambie con el tiempo. Cada acuse de recibo, el cual especifica cuántos octetos se han recibido, contiene un aviso de la ventana que especifica cuántos octetos adicionales de datos el receptor está preparador para aceptar.

Este anuncio de ventana se puede ver como el tamaño actual del buffer del receptor. En respuesta a un aviso de la ventana incrementado, el que envía incrementa el tamaño de su ventana deslizante y procede a enviar octetos sin acuse de recibo. En respuesta a un decremento en el aviso de la ventana el que envía decrementaría el tamaño de su ventana y dejaría de enviar los octetos a la

derecha de la frontera de la ventana. El software de TCP no debe contradecir los avisos previos al encoger la ventana después de que recibe la aceptación de los octetos del *"stream"*.

En vez de eso, si los avisos acompañan los acuses de recibo son cada vez más pequeños, el tamaño de la ventana cambiará en el momento en que se mueva. La ventaja de usar una ventana de tamaño variable es que ofrece tanto control de flujo así como también una transferencia confiable. Si los *"buffers"* del receptor se comienzan a llenar, ya no podrá tolerar más paquetes, así que enviará un aviso de la ventana. En un caso extremo el receptor manda un aviso de la ventana de cero para detener todas las transmisiones. Posteriormente, cuando haya espacio disponible en el buffer el receptor mandará un aviso de la ventana distinto a cero para activar nuevamente el flujo de datos[10].

El tener un mecanismo para el control del flujo es esencial en un ambiente de Internet, donde las máquinas de diferentes velocidades y tamaños se comunican a través de Redes y Puertas (*"gateways"*) de diferentes capacidades y velocidades.

En realidad, hay 2 problemas independientes de flujo. Primero, los protocolos de Internet necesitan un control de flujo de extremo a extremo, entre las máquinas fuente y destino. Por ejemplo, cuando una mini-computadora se comunica con un gran *"mainframe"*, la mini-computadora necesita regular la entrada de datos o el software del protocolo se saturará muy rápido.

Así, TCP debe implantar control de flujo de extremo a extremo para garantizar una entrega confiable. Segundo, los protocolos de Internet necesitan un mecanismo de control de flujo que les permita a los sistemas intermedios (como los *"gateways"*) controlar una fuente que mande mas tráfico del que la máquina pueda tolerar.

Cuando las máquinas intermedias se saturan, esta condición se llama congestión, todos los mecanismos que resuelven este problema se llaman mecanismos de control de congestión. TCP usa el esquema de la ventana deslizante para resolver el problema del control de flujo de extremo a extremo; no tiene un mecanismo explícito para el control de la congestión.

Posteriormente se verá que una implantación cuidadosamente programada puede detectar y recuperarse de la congestión mientras que una mala implantación la puede empeorar. En particular, un esquema de retransmisión cuidadosamente seleccionado puede ayudar a evitar la congestión mientras que un esquema pobre puede complicarlo.

III.12.5.6.- Formato del Segmento de TCP.

La unidad de transferencia entre el software TCP de dos máquinas se llama segmento. Los segmentos son intercambiados para establecer conexiones, transferir datos, mandar acuses de recibo, anunciar el tamaño de la ventana y cerrar las conexiones. Debido a que TCP usa *"piggybacking"*, un acuse de recibo que viaja de la máquina A hacia la B puede viajar en el mismo segmento en que viajan los datos de A hacia B aún cuando el acuse de recibo se refiere a los datos enviados de B hacia A[11]. La siguiente figura muestra el formato del segmento TCP.

---

10 Hay dos excepciones en la transmisión cuando el tamaño de la ventana es cero. Primero, el que envía está autorizado a transmitir un segmento con el bit de urgente encendido. Segundo, para evitar un *"deadlock"* potencial que pueda surgir si un anuncio distinto a cero se pierde después de que el tamaño de la ventana llega a cero, el que envía prueba una ventana distinta a cero periódicamente.

11 En la práctica, el *"piggybacking"* no ocurre usualmente a menos que el recipiente retarde los acuses de recibo.

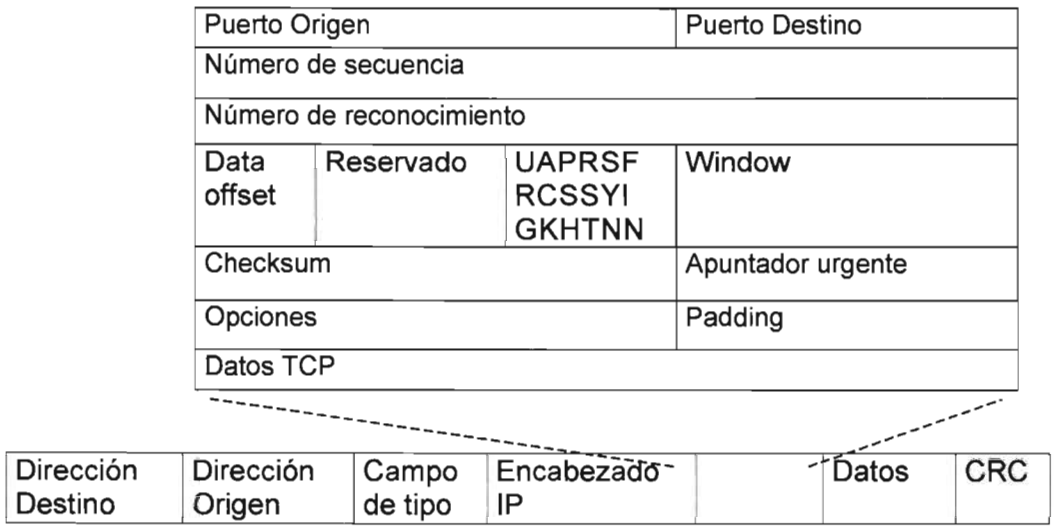


Figura III.24.- El Formato de un Segmento TCP con una Cabecera o Encabezado (*"Header"*) TCP, seguido por Datos.

Cada segmento se divide en dos partes; encabezado y datos. El encabezado, conocido como *encabezado TCP*, lleva la identificación esperada e información de control. Los campos "Puerto Fuente" y "Puerto Destino" contienen los números de puerto TCP que identifican las aplicaciones en los extremos de la conexión.

El campo "Número de Secuencia" identifica la posición de los datos del segmento en el flujo de que envía. El campo "Número de Acuse de Recibo" identifica el número de octeto del que la fuente espera recibir notificación. Debe notarse que el número de secuencia se refiere al flujo que viaja en la misma dirección del segmento, mientras que el "Número de Acuse de Recibo" se refiere al *"stream"* que viaja en la dirección opuesta al segmento.

El campo *"HLEN"* [12] contiene un entero que especifica la longitud del encabezado del segmento medido en múltiplos de 32 bits. Es necesario porque la longitud del campo "Opciones" varía dependiendo de las opciones que se hayan incluido. Así, el tamaño del encabezado TCP varía dependiendo de las opciones seleccionadas. El campo de 6 bits marcado como "Reservado" es necesario para usos futuros.

Algunos segmentos llevan solo un acuse de recibo mientras que otros llevan datos. Otros más, llevan peticiones para establecer o cerrar una conexión. El software de TCP usa el campo de 6 bits etiquetado como "Bits de Código" para determinar el propósito y contenido del segmento. Los seis bits dicen cómo interpretar los otros campos del encabezado (*"Header"*) de acuerdo a la tabla.

12 La especificación dice que el campo es el *desplazamiento* del área de datos dentro del segmento.

Bit (de izquierda a derecha)	*Significado si el bit está encendido*
URG	El campo del apuntador Urgente es válido
ACK	El campo del Acuse de Recibo es válido
PSH	Este segmento solicita un push
RST	Reinicializa la comunicación
SYN	Sincroniza los números de secuencia
FIN	El que envía ha llegado al fin de su flujo de bytes.

Tabla III.16.- Bits del Campo *"Código"* del Encabezado TCP.

El software de TCP avisa cuántos datos espera recibir cada vez que manda un segmento al especificar el tamaño del buffer en el campo "WINDOW". El campo contiene un entero sin signo de 32 bits en el orden de bytes estándar de la red. Los anuncios de la ventana ofrecen otro ejemplo de piggybacking porque acompañan a todos los segmentos, lo mismo los que llevan datos que los que sólo llevan un acuse de recibo.

III.12.5.7.- Datos Fuera de Banda.

Aunque TCP es un protocolo orientado a la conexión, algunas veces es importante para el programa al final de una conexión enviar datos *fuera de banda*, esto es, sin esperar a que el programa al otro lado de la conexión consuma los octetos del *"stream"*. Por ejemplo, cuando TCP se usa para dar *"login"* a una sesión remota, el usuario puede decidir enviar una secuencia de teclas que interrumpan o aborten el programa. Tales señales son más útiles cuando un programa de la máquina remota deja de funcionar correctamente. Estas señales se deben enviar sin esperar a que el programa lea los octetos del *"stream"* TCP (o un usuario no sería capaz de abortar los programas que dejan de leer la entrada).

Para utilizar el señalamiento fuera de banda, TCP permite que el que envía especifique los datos como *urgentes*, lo que significa que el programa receptor deberá ser notificado de su llegada tan pronto como sea posible sin importar su posición actual en el *"stream"*. El protocolo especifica que cuando se encuentren datos urgentes, el receptor deberá notificar a cualquier aplicación que esté asociada con la conexión que cambie a "Modo Urgente". Después de que todos los datos urgentes se han consumido, TCP le dice a la aplicación que regrese a la operación normal.

Los detalles exactos de cómo TCP le informa a la aplicación dependen del sistema operativo de la computadora en cuestión. El mecanismo usado para marcar los datos como urgentes cuando se transmiten en un segmento consiste en el bit URG del campo "Apuntador Urgente". Cuando el bit URG se enciende, el apuntador urgente especifica la posición en la ventana donde los datos urgentes terminan.

III.12.5.8.- Opción de Tamaño Máximo del Segmento.

No todos los segmentos enviados en una conexión son del mismo tamaño. Sin embargo, ambos extremos necesitan ponerse de acuerdo en el tamaño máximo de segmento que transferirán. El software de TCP usa el campo "Opciones" para negociar con el software de TCP al otro lado de la conexión; una de las opciones permite que el software TCP especifique el *tamaño máximo de segmento* (MSS) que está esperando recibir.

Por ejemplo, cuando una pequeña computadora personal que sólo tiene unos cuantos cientos de bytes de buffer se conecta a una supercomputadora, puede negociar un MSS que restrinja los

segmentos de tal manera que quepan en el buffer. Es especialmente importante para las computadoras conectadas a las redes locales de alta velocidad escoger un tamaño máximo de segmento que llene los paquetes o no harán un buen uso del ancho de banda.

III.12.5.9.- Cálculo de la Suma de Control ("Checksum").

El campo *"Checksum"* del Encabezado TCP contiene una suma de control de 16 bits usada para verificar la integridad de los datos así como también del Encabezado TCP. Para calcular la Suma de Control, el software de TCP en la máquina que envía realiza el siguiente procedimiento: antepone un *pseudo encabezado* al segmento, le pospone suficientes bytes con valor 0 para que su longitud sea un múltiplo de 16 bits y calcula la suma de control sobre todo el segmento resultante. TCP no cuenta los ceros agregados como *"Pad"* en la longitud del segmento ni los transmite. También, asume que el campo de suma de control en sí mismo tiene puros ceros para los propósitos de la suma de control.

Al igual que otros *"checksums"*, TCP usa aritmética de 16 bits y toma el complemento a uno de la suma con complemento a uno. En el *"site"* receptor, el software de TCP realiza los mismos cálculos para verificar que el segmento ha llegado intacto. El propósito de usar un pseudo encabezado al igual que en UDP, es permitir que el receptor verifique que el segmento ha llegado a su destino correcto. Este Encabezado incluye tanto la dirección IP del destino así como el número de puerto. Tanto la dirección IP destino como la fuente son importantes para TCP porque debe usarlas para identificar la conexión a la que pertenece un segmento dado. Por lo tanto, siempre que llega un datagrama con un segmento TCP, IP debe pasar a las direcciones IP fuente y destino al igual que el segmento en sí. La figura muestra el formato del pseudo encabezado usando en el cálculo de la suma de control.

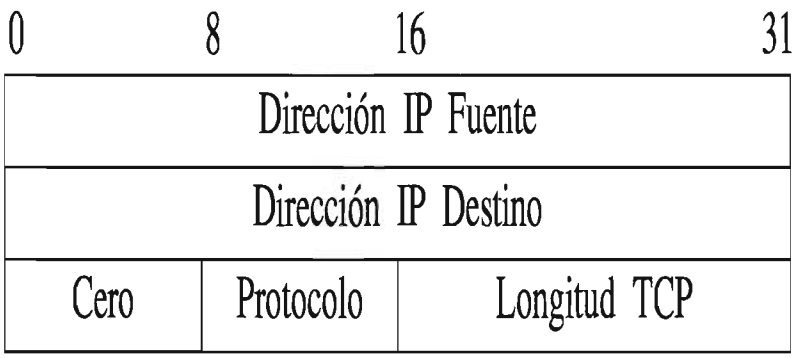


Figura III.25.- El Formato del Pseudo-Encabezado usado en el Cálculo de la Suma de Control, (*"Checksum"*).

En el lado del receptor, la información es extraída del datagrama IP que llevó el segmento. TCP le asigna al campo "Protocolo" el valor que el sistema de entrega subyacente usará en su campo "tipo de protocolo". Para los datagramas IP que llevan TCP, el valor es 6. El campo "Longitud TCP" especifica la longitud total del segmento TCP incluyendo el Encabezado TCP. En el lado del receptor, la información del pseudo encabezado es extraída e incluida en la suma de control para verificar que el segmento llegó al destino correcto intacto.

III.12.5.10.- Acuses de Recibo y Retransmisiones.

Debido a que TCP manda datos en segmentos de longitud variable, y porque los segmentos retransmitidos pueden incluir más datos que el original, los acuses de recibo no se pueden referir fácilmente a los datagramas o a los segmentos. En su lugar, se refieren a una posición en el *"stream"* usando los números de secuencia. El receptor colecta los datos de los segmentos que van llegando y reconstruye una copia exacta del *"stream"* que se está enviando.

Debido a que los segmentos viajan en datagramas IP, se pueden perder o entregarse en desorden; el receptor usa los números de secuencia para reordenar los segmentos. En cualquier momento, el receptor habrá reconstruido cero o mas octetos contiguamente desde el principio del *"stream"*, pero puede haber piezas adicionales de datagramas que llegaron en desorden.

El receptor siempre manda el aviso del *"stream"* que se ha recibido correctamente. Cada aviso especifica un valor de secuencia que es el número adicionando un uno en la última posición de octeto en el que ha recibido. Así, el que envía recibe constante retroalimentación del receptor a medida que va avanzando a lo largo del *"stream"*. Esta idea se puede resumir así: Los Acuses de Recibo siempre especifican el número de secuencia del siguiente octeto que el receptor espera recibir.

El esquema de acuse de recibo se llama *acumulativo* porque reporta qué cantidad se ha acumulado del *"stream"*. Los acuses de recibo acumulativos tienen ventajas y desventajas. Una ventaja es que los acuses de recibo son fáciles de generar y no ambiguos. Otra ventaja es que los acuses de recibo extraviados no necesariamente fuerzan la retransmisión. La principal desventaja es que el que envía no recibe información de todas las transmisiones exitosas, sólo de una posición en el *"stream"* que ha sido recibida.

Para entender porqué la carencia de información acerca de todas las transmisiones exitosas hace al protocolo menos eficiente, supóngase una ventana de 500 octetos que comienza en la posición 101 del *"stream"* y supóngase que el que envía ha transmitido todos los datos de la ventana mandando 5 segmentos. Supóngase que el primer segmento se perdió pero todos los demás llegaron intactos. El receptor continúa enviando acuses de recibo, pero todos ellos especifican el octeto 101, el siguiente octeto contiguo que espera recibir. No hay manera de que el receptor le diga al que envía que la mayor parte de los datos de la ventana actual ya llegaron.

Cuando ocurre un *"timeout"* en el lado del que envía, éste deberá escoger entre dos esquemas potencialmente ineficientes. Podría escoger retransmitir los 5 segmentos en lugar de mandar solo el que falta. Por supuesto, cuando el segmento retransmitido llegue, el receptor habrá recibido correctamente todos los datos de la ventana y habrá mandado un acuse de recibo indicando que espera el octeto 5101 a continuación.

Sin embargo, ése acuse de recibo podría no llegarle al que envía lo suficientemente rápido como para prevenir la retransmisión innecesaria de los otros de la ventana.

Si el que envía siguiera la política retransmitir sólo el primer segmento sin acuse de recibo, deberá espera el acuse de recibo antes de poder decidir qué y cuánto enviar. Así, se convertiría en un protocolo sencillo con acuse de recibo positivo y podría perder las ventajas de tener una ventana grande.

III.12.5.11.- Establecimiento de una Conexión Orientada.

Para establecer una conexión, TCP usa el mecanismo llamado *"Three Way Handshake" o* "Apretón de manos en tres sentidos". En el caso más simple, el *"handshake"* o apretón de manos procede como se muestra en la Figura III.26.

El *"three way handshake"* realiza dos importantes funciones: Garantiza que ambos lados están listos para transferir datos (y que ambos saben que el otro está listo), y permite que ambos estén de acuerdo en los números iniciales de secuencia. Los números de secuencia se envían y se notifican de recibido durante el *"handshake"*.

Cada máquina debe escoger un número de secuencia inicial aleatorio que usará para identificar los bytes del flujo que está enviando. Los números de secuencia no pueden comenzar siempre en el mismo valor. En particular, TCP no puede escoger meramente la secuencia 1 cada vez que abra una conexión. Por supuesto, es importante que ambos lados estén de acuerdo en un número inicial, para que números de los octetos usados en los acuses de recibo concuerden con los usados en los segmentos de datos.

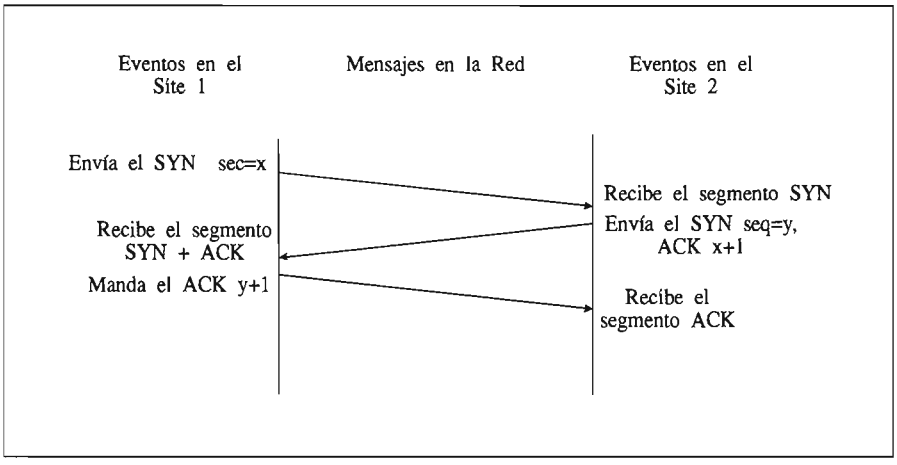


Figura III.26.- Conexión Orientada.

III.12.5.12.- Números Iniciales de Secuencia.

Para ver cómo las máquinas pueden estar de acuerdo en los números de secuencia para dos *"streams"* después de sólo tres mensajes, recuérdese que cada segmento contiene tanto un campo de número de secuencia como un campo de acuse de recibo. La máquina que inicia el *"handshake"*, llamada A, pasa su número de secuencia, x, en el campo de secuencia del primer segmento SYN del *"handshake"*.

La segunda máquina, llamada B, recibe el SYN, graba el número de secuencia y contesta enviando su número de secuencia inicial en el campo de secuencia al igual que un acuse de recibo que especifica que B está esperando el octeto *x+1*. En el mensaje final, A "notifica de recibido" de B todos los octetos hasta el *y*. En todos los casos, los acuses de recibo siguen la convención de usar el número del siguiente octeto esperado.

Se ha descrito cómo TCP usualmente realiza el *"three way handshake"* intercambiando segmentos que contienen una mínima cantidad de información. Debido al diseño del protocolo, es posible enviar datos junto con los números de secuencia iniciales en los segmentos del *"handshake"*. En tales casos, el software de TCP debe retener los datos hasta que el *"handshake"* termine. Una vez que se ha establecido una conexión, el software de TCP puede liberar los datos retenidos y entregárselos rápidamente a una aplicación.

III.12.5.13.- Cerrando una Conexión TCP.

Dos programas que usan TCP para comunicarse pueden terminar la conversación de una manera agradable usando la operación *"close"*. Internamente, TCP usa un *"handshake"* modificado para cerrar las conexiones. Debe recordarse que las conexiones TCP son full dúplex y que tienen dos *"streams"* independientes, uno en cada dirección. Cuando una aplicación le dice a TCP que no tiene mas datos para enviar, TCP cerrará la conexión *en una dirección.*

Para cerrar su mitad de la conexión, el TCP que envía termina de transmitir los datos restantes, espera a que el receptor mande el acuse de recibo y envía entonces un segmento con el bit FIN encendido. El TCP receptor manda su acuse de recibo del segmento FIN y le informa a la aplicación de su lado que no hay mas datos disponibles (ejemplo: usando el mecanismo *end of file* del sistema operativo).

Una vez que se ha cerrado la conexión en una dirección, TCP se rehusa a aceptar mas datos de esa dirección. Mientras tanto, los datos pueden continuar viajando en la dirección opuesta hasta que el que envía los rechaza. Por supuesto que, los acuses de recibo siguen llegando al que envía aún cuando la conexión se haya cerrado. Cuando ambas direcciones se han cerrado, el software de TCP de cada punto borra su registro de la conexión.

Los detalles del cierre de una conexión son un poco mas ingeniosos que lo que se acaba de explicar porque TCP usa un *"three way handshake"* modificado para cerrar una conexión. La siguiente figura ilustra el procedimiento.

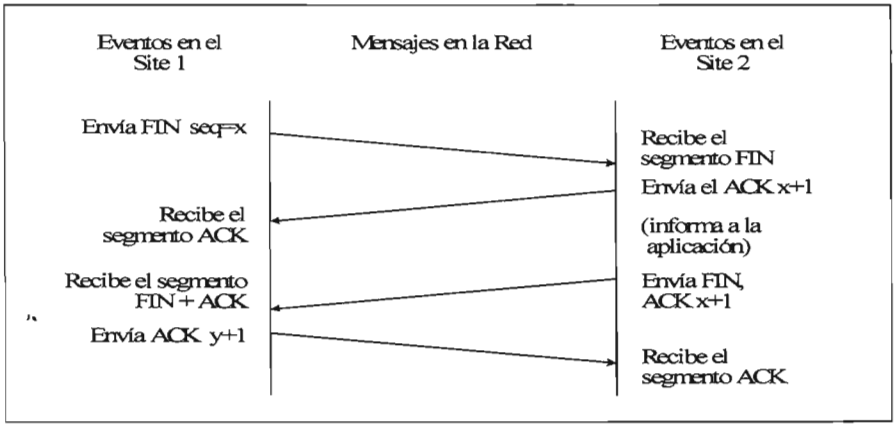


Figura III.27.- El "Three Way Handshake Modificado Usado para Cerrar las Conexiones. El Sitio que Recibe el Primero Segmento FIN Notifica su llegada Inmediatamente y Espera antes de Enviar el Segundo Segmento FIN.

La diferencia entre el *"handshake"* usado para establecer una conexión del usado para terminarla ocurre después de que una máquina recibe el segmento FIN inicial. En lugar de generar un segundo segmento FIN inmediatamente, TCP manda un acuse de recibo y entonces le informa a la aplicación acerca de la petición de terminar la conexión. Informarle a la aplicación acerca de esta petición y obtener una respuesta puede tomar una considerable cantidad de tiempo (ejemplo: puede involucrar interacción humana). El acuse de recibo evita la retransmisión del segmento FIN inicial durante la espera. Finalmente, cuando la aplicación le indica al TCP que cierre la conexión, TCP manda el segundo segmento FIN y el sitio original contesta con el tercer mensaje, un ACK.

III.12.5.14.- Reinicialización de una Conexión TCP.

Normalmente, una aplicación usará la operación *"close"* para terminar una conexión cuando termine de usarla, de esta manera el cierre de las conexiones se considera una parte normal del uso, análogo a cerrar un archivo. Algunas veces surgen condiciones anormales que obligan a una aplicación o al software de la red a romper una conexión. TCP ofrece un mecanismo de Reinicialización para tales desconexiones anormales.

Para reinicializar una conexión, un lado inicia la terminación enviando un segmento con el bit RST del campo de "Códigos" encendido. El otro lado responde a un segmento reset inmediatamente abortando la conexión. TCP también le informa a la aplicación que ha ocurrido una Reinicialización, lo que implica que las transferencias en ambas direcciones cesan inmediatamente y que los recursos tales como el buffer se liberan.

III.13.- Números de Puertos Reservados.

Al igual que UDP, TCP combina el enlace estático y dinámico de los puertos, usando un conjunto de *asignaciones de puertos bien conocidos* para los programas comúnmente invocados (ejemplo: el correo electrónico), pero dejando disponibles la mayor parte de los números de puertos para que el sistema operativo los asigne a los programas que los necesiten. La especificación establece que sólo los números de puerto menores a 1024 serán usados para los puertos bien conocidos; los restantes hasta el 65535 para las diferentes aplicaciones.

La Tabla III.17 muestra algunos de los puertos TCP actualmente asignados. Se debe resaltar que aunque los números de puerto de TCP y de UDP son independientes, los diseñadores han escogido usar los mismos números de puerto para cualquier servicio que se pueda acceder por TCP o por UDP. Por ejemplo, un servidor de nombre de dominios se puede acceder por ambos transportes. En cualquier protocolo, el número de puerto 53 está reservado para los servidores del sistema de nombre de dominios.

Decimal	*Nombre*	*Nombre en UNIX*	*Descripción*
0			Reservado
1	TCPMUX	-	Multiplexor TCP
5	RJE	echo	Echo
9	DISCARD	discard	Descartar
11	USERS	systat	usuarios Activos
13	DAYTIME	daytime	Hora del día
15	-	netstat	Programa para ver el estado de la red
17	QUOTE	qotd	Cita del día
19	CHARGEN	chargen	Generador de Caracteres
20	FTP-DATA	ftp-data	File Transfer Protocol (datos)
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Conexión de Terminal Virtual
25	SMTP	smtp	Simple Mail Transport Protocol
37	TIME	time	Hora
42	NAMESERVER	name	Nombre del host servidor
43	NICNAME	whois	Programa que Identifica a los usuarios
53	DOMAIN	nameserver	Servidor de Nombres de Dominios
77	-	rje	Cualquier servicio RJE privado
79	FINGER	finger	Programa que da información de usuarios en un sistema
93	DCP	-	Device Control Protocol
95	SUPDUP	supdup	Protocolo SUPDUP
101	HOSTNAME	hostnames	Nombre NIC del host name servidor
102	ISO-TSAP	iso-tsap	ISO-TSAP
103	X400	x400	Servicio de Mail X.400
104	X400-SND	x400-snd	Envío de mail X.400
111	SUNRPC	sunrpc	Llamadas a Procedimientos Remotos de SUN
113	AUTH	auth	Servicio de Autenticación
117	UUCP-PATH	uucp-path	Servicio de Rutas UUCP
119	NNTP	nntp	USENET News Transfer Protocol
129	PWDGEN	-	Protocolo Generador de Passwords
139	NETBIOS-SSN	-	Servicio de Sesiones NETBIOS
160-223	Reservados		

Tabla III.17.- Ejemplos de los Números de Puerto TCP Actualmente Asignados. En la Medida de lo Posible, UDP usa los mismos Números.

III.14.- Protocolo de Datagrama de usuario ("User Datagram Protocol", UDP).

Además de TCP, existe otro protocolo en la capa de transporte, el *"User Datagram Protocol"*, especificado en el RFC 768. [Postel, 1980].

El **UDP** ofrece un servicio de conexión para los procesos de la capa de aplicación. Le permite a un proceso enviar mensajes a otros procesos con un mínimo de mecanismos involucrados. Un ejemplo del uso de este protocolo es en la administración centralizada de redes con SNMP.

UDP trabaja sobre IP, al igual que TCP. Debido a que es un protocolo no confiable (al igual que el protocolo subyacente IP), y que no está orientado a la conexión, UDP tiene muy poco que hacer. Esencialmente sólo le agrega la capacidad de direccionamiento de puertos a IP y realiza la Suma de Control. Esto se entenderá mejor al examinar el formato de su encabezado, mostrado en la siguiente tabla.

Puerto Origen	Puerto Destino
Longitud del mensaje	Checksum
Datos	
Datos	
Datos	

Tabla III.18.- El Encabezado de UDP.

El encabezado incluye los puertos origen y destino. Como en el caso de TCP, se debe hacer uso de los puertos al realizar una transmisión. El campo "Longitud" contiene la longitud de todo el segmento UDP, incluyendo el encabezado. La suma de control al igual al que se usa en TCP e IP sirve para verificar la integridad de esta porción de información.

III.15.- Protocolos de Aplicación y Servicios.

No es posible apreciar los detalles técnicos de Internet sin conocer los servicios que proporciona. Mucha de la discusión acerca de los servicios se enfoca a los llamados protocolos, los cuales dan la fórmula para enviar mensajes, especificar los detalles de los formatos de dichos mensajes y describir cómo controlar las condiciones de error. Más importante aún, es que nos permiten definir los estándares de comunicación.

De alguna forma los protocolos son a la comunicación lo que los programas a la computación. Un lenguaje de programación nos permite especificar o comprender la computación sin necesidad de conocer los detalles de cualquier conjunto de instrucciones del CPU. Similarmente un protocolo permite entender la comunicación de datos sin la necesidad de conocer los detalles del *hardware* de algún fabricante en particular.

Al hacer referencia a que TCP/IP no era una pieza de *software* independiente y es en realidad un servicio de comunicación de las diferentes aplicaciones a las que otorga la capacidad de transportar la misma para simular que sé esta llevando información de un sitio a otro de manera transparente para el usuario.

De los servicios más relevantes y usados de manera conocida, está el correo electrónico, el navegador de Internet, (*"Netscape"* o *"Mosaic"*), el servicio de Información a distancia, el World Wide Web, el servicio de nombres de dominio (DNS), entre otros.

III.15.1.- Protocolo de Transferencia de Archivos ("File Transfer Protocol", **FTP**).

La transferencia de archivos, es una de las actividades de mayor frecuencia en una red, el Protocolo **FTP** provee de un mecanismo confiable y eficiente para llevar a cabo esta tarea.

Dado un protocolo de transporte confiable de extremo a extremo como el TCP, la transferencia de archivos podría parecer trivial. Sin embargo, los detalles de autorización, el nombre y la representación entre máquinas heterogéneas hace que el protocolo sea complejo. Además, el FTP ofrece muchas facilidades que van más allá de la función de transferencia misma.

Acceso interactivo

Proporciona una interfase interactiva que permite a las personas interactuar fácilmente con los servidores remotos. Por ejemplo, un usuario puede pedir una lista de todos los archivos de un directorio en una máquina remota. Incorpora ayuda en línea, mostrando información al usuario acerca de los comandos posibles que se puedan invocar.

Especificación de formato

El FTP permite al cliente especificar el tipo y formato de datos almacenados. Por ejemplo, el usuario puede especificar si un archivo contiene datos de texto o binarios, así como, si los archivos de texto utilizan los conjuntos de caracteres ASCII o EBCDIC.

Control de autenticación

El FTP requiere que los clientes se identifiquen, mediante el envío de un nombre de conexión y una clave de acceso al servidor antes de pedir la transferencia de archivos.

*III.15.1.1.- **FTP** y el Modelo Cliente-Servidor.*

Como en otros servidores, el protocolo FTP trabaja bajo el procesamiento cliente-servidor. Los clientes se valen del TCP para conectarse a un servidor. Un proceso servidor maestro espera las conexiones y crea un proceso esclavo para manejar cada conexión. Igual que otros servicios, el proceso servidor se denomina **"ftpd"**, mientras que el cliente se llama **"ftp"**.

Sin embargo, a diferencia de casi todos los servidores el proceso esclavo no ejecuta todos los cómputos necesarios. Por el contrario, el esclavo acepta y maneja la conexión de control de cliente, pero utiliza un tercer proceso para manejar una conexión de transferencia de datos separada. La conexión de control transporta comandos que indican al servidor qué archivo transferir. La conexión de transferencia de datos, que también usa el TCP como protocolo de transporte, transporta todas las transferencias de datos. Por lo general, el cliente y el servidor crean un proceso separado para manejar la transferencia de datos.

El proceso de control del cliente se conecta al proceso de control del servidor mediante una conexión TCP, mientras que los procesos de transferencia de datos asociados utilizan su propia conexión TCP. En general, los procesos de conexión y la conexión de control permanecen activos mientras el usuario continúa con la sesión de FTP.

Sin embargo, el FTP establece una nueva conexión de transferencia de datos para cada transferencia de archivos. De hecho, muchas de las implantaciones crean un nuevo par de procesos de transferencia de datos, así como también una nueva conexión TCP cada vez que el servidor necesite enviar información al cliente. La idea puede resumirse como sigue:

Las conexiones de transferencia de datos y los procesos de transferencia de datos que los emplean pueden crearse de manera dinámica cuando se necesitan, pero la conexión de control continúa a través de una sesión.

Una vez que la conexión de control desaparece, la sesión se termina y el software en ambos extremos termina todos los procesos de transferencia de datos.

Por supuesto, las implantaciones de cliente, que se ejecuten en una computadora sin el soporte de sistema operativo para diversos procesos, pueden tener una estructura menos compleja.

Tales implantaciones a menudo sacrifican la generalidad utilizando un solo programa de aplicación para ejecutar la transferencia de datos y las funciones de control. Sin embargo, el protocolo

requiere incluso que tales clientes utilicen diversas conexiones TCP, una para el control y otras para la transferencia de datos.

Cuando un cliente establece una conexión inicial con un servidor, el cliente utiliza un número de puerto de protocolo aleatorio asignado localmente, pero se pone en contacto con el servidor en un puerto bien conocido (21). A pesar de que un servidor utilice sólo un puerto de protocolo puede aceptar las conexiones de muchos clientes, puesto que el TCP se vale de ambos puntos extremos para identificar una conexión.

Cuando los procesos de transferencia crean una nueva conexión TCP para un enlace FTP, no pueden usar el mismo par de números de puerto utilizados en la conexión de control. Por el contrario, el cliente obtiene un puerto no utilizado en su máquina y se vale del puerto para ponerse en contacto con el proceso de transferencia de datos en la máquina del servidor. Este proceso de transferencia de datos puede usar el puerto bien conocido (20), reservado para la transferencia de datos FTP.

Sin embargo debido a que desde un mismo cliente se pueden manejar varias conexiones a un mismo servidor, para que el proceso de transferencia en el servidor, acepte solo conexiones del proceso de transferencia apropiado, y gracias a que el protocolo utiliza dos conexiones, el proceso de control de cliente se encarga de obtener un puerto local aleatorio para la conexión de transferencia y comunicar este número de puerto al servidor a través de la conexión de control.

Posteriormente, el servidor crea el proceso de transferencia, que espera a que el proceso de transferencia en el cliente solicite desde el número de puerto informado a través de la conexión de control, una conexión y así iniciar la transferencia de datos.

Además de enviar comandos del usuario al servidor, el FTP utiliza la conexión de control para permitir los procesos de control cliente y servidor, y así, coordinar el uso de puertos de protocolo TCP asignados dinámicamente y la creación de procesos de transferencia de datos que utilicen tales puertos.

Los diseñadores del FTP, lo crearon de tal forma que FTP utiliza el protocolo de terminal virtual de red TELNET. Aunque FTP no permite la negociación de opciones, emplea sólo la definición básica NVT. De este modo, la administración de una conexión de control FTP es mucho más sencilla que la administración de una conexión estándar de TELNET. Sin importar las limitaciones, usar la definición de TELNET, en lugar de intentar una, ayuda a simplificar considerablemente al FTP.

*III.15.1.2.- Operación de **FTP**.*

Para iniciar **FTP**, se debe proporcionar el nombre o dirección IP de la máquina a la cual desea conectarse. Solamente se puede utilizar el nombre, si el sistema tiene algún método para convertir el nombre a su dirección IP, como en el caso del Servicio de Nombre de Dominio. También se puede especificar un número de puerto si el servidor **"ftpd"** no escucha en el puerto estándar.

Cuando se establezca la conexión, se solicitará identificación de usuario y contraseña. Una vez que se establezca con éxito la conexión, se ingresará al modo de comandos de **"ftp"**. Bajo ambientes UNIX, si no se especifica nombre o dirección, se ingresa directamente al modo de comando de **"ftp"**.

Los usuarios ven al FTP como un sistema interactivo. Una vez que se invoca, el cliente ejecuta repetidamente las siguientes operaciones: leer una línea de entrada, analizar la línea para extraer un comando y sus argumentos, así como ejecutar el comando con los argumentos especificados. Por ejemplo, para iniciar la versión del FTP disponible UNIX, el usuario invoca el programa *ftp*: % **ftp**

El cliente FTP despliega un indicador para el usuario. Después del indicador, el usuario puede teclear cualquiera de los comandos de la siguiente tabla.

!	cr	macdef	proxy	send
$	delete	mdelete	sendport	status
debug	mdir	Put	struct	dir
mget	pwd	sunique	disconnect	mkdir
quit	tenex	form	mls	quote
trace	get	mode	recv	type
glob	mput	remotehelp	user	hash
nmap	rename	verbose	help	ntrans
reset	?	Cdup	lcd	Open
rmdir	runique	Close	ls	Prompt

Tabla III.19.- Tabla de Comandos.

Para obtener información acerca de un comando, el usuario teclea el comando de ayuda (*"Help Command"*) como en los siguientes ejemplos (la salida se muestra en el formato que produce).

ftp> ***help ls***
ls *lista el contenido del directorio remoto*
*ftp>****help cdup***
cdup *cambia el directorio de trabajo remoto por un directorio padre*
ftp> ***help glob***
glob *conmutación de metacaracteres de expansión de los nombres de archivo local*
ftp> ***help bell***
bell *hace un sonido cuando el comando se termina*

Para ejecutar un comando, el usuario teclea el nombre del comando:

ftp> **bell**
Bell mode on (modo de sonido activado).

III.15.1.3.- Ejemplo de una Sesión ***FTP****.*

```
# ftp 192.100.188.34
Connected to 192.100.188.34.
220 dicns FTP server (UNIX(r) System V Release 4.0) ready.
Name (192.100.188.34:root): root
331 Password required for root.
Password:
230 User root logged in.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.100.188.41,1221) (0 bytes).
total 2288
lrwxrwxrwx  1  root   root      9 Mar  5 16:49 bin -> ./usr/bin
drwxrwxr-x 16  root   sys      5120 Aug 27 14:26 dev
```

```
drwxrwxr-x  5  root   sys      512 Mar  5 17:43 devices
drwxrwxr-x 22  root   sys     3072 Aug 27 14:27 etc
drwxr-xr-x  9  root   sys      512 Oct 25  1994 kernel
226 ASCII Transfer complete.
ftp> ls a*
200 PORT command successful.
150 ASCII data connection for /bin/ls (192.100.188.41,1225) (0 bytes).
---r--          1       root    other  0 Aug 15 12:17 abc
lrwxrwxrwx      1       root    root   14 Mar  5 16:49 aliases -> ./mail/aliases
-rw-r--r--      1       root    bin    75 Mar  6 10:19 auto_home
-rw-r--r--      1       root    bin    83 Mar  5 16:49 auto_master
lrwxrwxrwx      1       root    root   16 Mar  5 16:49 autopush -> ../sbin/autopush
226 ASCII Transfer complete.
ftp> get abc
local: abc remote: abc  def
200 PORT command successful.
150 ASCII data connection for abc (192.100.188.41,1227) (0 bytes).
226 ASCII Transfer complete.
ftp> close
221 Goodbye.
ftp> quit
#
```

El usuario requiere la copia de un archivo y para ello utiliza el comando *"get"*. En el ejemplo, el comando *"get"* va seguido por dos argumentos que especifican el nombre del archivo remoto y el nombre de la copia local. El nombre del archivo remoto es **abc** y la copia local **def**. Una vez que se lleva a acabo la transferencia, el usuario teclea *"close"* para interrumpir a la conexión con el servidor y, luego, *"quit"* para dejar al cliente.

Los mensajes de información se encuentran entremezclados con los comandos que teclea el usuario. Los mensajes FTP siempre comienzan con un número de 3 dígitos seguido de texto. La mayor parte viene del servidor, otra salida viene del cliente local.

Por ejemplo, el mensaje que comienza con 220 viene del servidor y contiene el nombre de dominio de la máquina en la que se ejecuta el servidor.

Los mensajes de control y error entre el cliente y el servidor FTP comienzan con un número de tres dígitos seguido de texto. El software interpreta el número; el texto está dirigido a los usuarios.

La sesión de ejemplo también ilustra una característica del FTP descrita al principio: la creación de nuevas conexiones TCP para transferencia de datos. Observe que el comando PORT está en la salida. El comando de cliente PORT reporta que un nuevo número de puerto TCP ha sido obtenido para usarse como conexión de datos. El cliente envía la información de puerto al servidor a través de la conexión de control; los procesos de transferencia de datos en ambos extremos se valen del nuevo número de puerto cuando se forma una conexión. Luego de que se completa la transferencia los procesos de transferencia de datos cierran la conexión.

*III.15.1.4.- **FTP** Anónimo.*

Para proporcionar acceso a los archivos públicos, muchas de las localidades TCP/IP permiten el FTP anónimo. El acceso al FTP anónimo significa que el cliente no necesita una cuenta o clave de acceso, sino especificar un nombre de conexión anónimo y una clave de acceso de invitado. El servidor permite que el usuario anónimo se conecte pero restringe su acceso únicamente a los archivos públicos disponibles.

El usuario invoca al FTP anónimo especificando *"anonymous"* en el nombre del usuario y cualquier cosa (su *"e-mail"* completo en algunos sistemas) como contraseña (*"password"*).

III.15.1.5.- TELNET ("Telecommunications Network Protocol").

TELNET ofrece el servicio de *"login"* remoto. Permite a un usuario desde un sistema cliente, iniciar una sesión en un sistema remoto y por lo que respecta al usuario, aparecerá como si estuviera sentado frente al *"host"* remoto. Una vez que la conexión se ha establecido, el proceso cliente emula una terminal conectada al proceso servidor. Al igual que FTP; **TELNET** usa TCP como transporte. El estándar de **TELNET** se encuentra en el RFC 854.

Esto es un poco más complicado de lo que parece a primera vista, por la amplia variedad de terminales y computadoras existentes, cada una con sus propios códigos de control y características de terminal. Cuando se está conectado directamente a un servidor, la unidad central de procesamiento (CPU) de éste debe administrar la conversión de los códigos de terminal, lo que impone una severa carga en la CPU del servidor. Con varias conexiones remotas activas, la CPU del servidor puede gastar mucho tiempo administrando las conversiones.

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

El Protocolo TELNET utiliza el concepto de terminal virtual de red (NVT) para definir ambos extremos de una conexión TELNET. Cada extremo de la conexión tiene un teclado y una impresora lógicos. La impresora lógica puede desplegar caracteres, y el teclado lógico puede generar caracteres. La impresora de red es por lo general una pantalla de terminal, en tanto que el teclado lógico es por lo general el teclado del usuario, aunque puede ser algún archivo o cualquier otro flujo de entrada.

III.15.1.6.- Protocolos de Terminal Virtual.

El estándar TELNET se basa en la idea de una terminal de red virtual NVT (*"Network Virtual Terminal"*). El término "virtual" se usa por que NVT no existe físicamente, es un dispositivo imaginario que presenta las características de una terminal. La idea es liberar a los *"hosts"* de la carga de tener que mantener las características de todas las terminales con las que se tiene que comunicar.

Con TELNET, tanto el dispositivo del usuario como el del servidor tienen que mapear las características de sus terminales a la descripción de una NVT.

El Protocolo de Terminal Virtual ofrece un lenguaje común, mediante la definición de una terminal virtual y un protocolo para transferir información y controlarla a través de la red. La implantación del protocolo de terminal virtual traduce a lenguaje NVT para realizar la transmisión al otro lado de la conexión. La implantación receptora del protocolo NVT traduce entonces de lenguaje NVT a lenguaje nativo.

EL NVT define:

- La forma en la que la información será enviada, por ejemplo, en conjuntos de bytes o en mensajes con algún formato previo.
- Cómo serán enviadas las señales de control de terminal virtual y cómo distinguirlas de la información

- El modo de transferencia de la información que se usará: half dúplex o full dúplex, sincronía o asíncrona y cómo se controla dicha transferencia
- Cómo se transfieren las interrupciones especiales de prioridad y cómo deberán interpretarse.
- La manera en que se le entrega la información al usuario.

*III.15.1.7.- El Servicio **TELNET** y el Modelo Cliente-Servidor.*

La especificación de TELNET, define un protocolo entre un cliente y un Servidor TELNET, esta especificación dice muy poco acerca de cómo el proceso TELNET se relaciona con las capas inferiores, específicamente con la de transporte, o sea la interfase con TCP, varias implantaciones comerciales de TCP para computadoras personales incorporan TCP como parte del *"kernel"*, mientras que TELNET corre como una aplicación del sistema operativo.

TELNET es un protocolo de las capas de presentación y de aplicación que corre sobre TCP. TCP y los protocolos de las capas de abajo proporción la conexión confiable entre los procesos cliente y el servidor TELNET. Como todas las aplicaciones de las capas superiores, el servidor usa un puerto conocido de TCP, en este caso el número 23, es decir escucha por el puerto 23 para aceptar las solicitudes de clientes TELNET. Mientras que cuando un cliente establece una conexión inicial con un servidor, el cliente utiliza un número de puerto de aleatorio asignado localmente.

En sistemas UNIX, el proceso servidor se conoce como **"telnetd"**. El cliente (el extremo que está llamando) es un programa, llamado por lo general TELNET, que intenta la conexión con el servidor. Un pariente de TELNET es el programa **"rlogin"**, común en máquinas UNIX

Cuando se establece una conexión, **"telnetd"** inicia un proceso en el servidor que usualmente es un proceso de *"login"* y posteriormente un *"shell"*.

Si el anfitrión y la máquina remota utilizan una interfase gráfica como **X** o **"Motif"**, los sistemas se deberán instruir para permitir el paso de información en ventanas de un lado al otro, de lo contrario, la máquina remota intentará abrir las ventanas en el servidor. Cuando el usuario sale de una sesión de red, TELNET cierra la conexión TCP.

En la mayoría de las implantaciones, el servidor de TELNET es un servidor concurrente, es decir acepta múltiples conexiones a la vez. El hecho de que estas aplicaciones trabajen de manera cooperativa, permite que un cliente TELNET se pueda usar para otros propósitos, es decir conectarse con otros servidores que operan por supuesto en otros puertos bien conocidos, como SMTP, HTTP.

TELNET debe ser capaz de solicitar aquélla información que tenga que ser enviada como información urgente de TCP y recibir notificaciones TCP urgentes de TELNET.

Opcionalmente, TELNET puede usar las capacidades de PUSH de TCP para indicar cuándo una información debe enviarse a su destino. Esto es útil si TCP intenta enviar segmentos de tamaño fijo y retarda la transmisión hasta que recibe suficiente información para llenar un segmento. Debido a que las entradas de los usuarios son de diferente longitud y generalmente pequeñas, el PUSH de TCP se puede usar después de un <CR LF> para asegurarse de que la información del usuario se envíe inmediatamente.

III.15.1.8.- Negociación de Opciones de TELNET.

El Protocolo TELNET trata ambos extremos de la conexión como si fueran terminales virtuales de red. Los dos programas en cada extremo (**TELNET** y **Telnetd**) administran la conversión de la terminal virtual a los dispositivos físicos reales.

El concepto de terminales virtuales permite a TELNET interconectarse con cualquier tipo de dispositivo, siempre y cuando haya mapeo disponible de los códigos virtuales al dispositivo físico.

En TELNET las opciones son negociables, permitiéndosele al cliente y al servidor reconfigurar sus conexiones. Por ejemplo, en una conexión se mandan 7 bits de datos y utiliza bytes con el octavo bit activo para pasar la información de control, como el comando de interrupción de un proceso.

Sin embargo, TELNET tiene una opción que permite al cliente y al servidor pasar 8 bits de datos. El cliente y el servidor deben negociar y acordar el paso de datos de 8 bits antes de transferirlos.

Este proceso es sencillo: un extremo pregunta si se acepta una función y el otro extremo contesta positiva o negativamente. Si se acepta, se envían los códigos necesarios. De esta forma queda rápidamente cubierta la lista de funciones aceptadas por ambos extremos.

La cantidad de opciones de TELNET es grande: algunas son críticas mientras que otras negocian detalles pequeños. Por ejemplo, el protocolo original fue diseñado en un ambiente half-duplex en donde era necesario decirle al otro extremo *"go ahead"* antes de que enviara más datos. Una de las opciones controla la manera de operar de TELNET (Half dúplex o Full Dúplex). Otra opción le permite al servidor de la máquina remota determinar el tipo de terminal del usuario. Esto es importante para el software que genera las secuencias de control.

*III.15.1.9.- Operación de **TELNET**.*

El programa TELNET es útil cuando se está frente a una máquina de poca potencia o frente a una terminal y desea utilizar las capacidades de procesamiento de otra máquina, o si otra máquina tiene alguna herramienta en particular que no desea cargar en su máquina local.

Para iniciar TELNET, se debe proporcionar el nombre o dirección IP de la máquina a la cual desea conectarse. Solamente se puede utilizar el nombre, si el sistema tiene algún método para convertir el nombre a su dirección IP, como en el caso del Servicio de Nombre de Dominio, DNS. También se puede especificar un número de puerto si el servidor **"telnetd"** no escucha en el puerto estándar.

Cuando se establezca la conexión, se solicitará identificación de usuario y contraseña. Una vez que se establezca con éxito la conexión, su sesión se comportará como si usted estuviera en la máquina remota, con todos los comandos válidos de dicho sistema operativo. Todas las instrucciones serán relativas al servidor, por lo que un comando de directorio mostrará el directorio de trabajo del servidor, no el del cliente. Para ver el directorio del cliente, se tendrá que entrar en modo de comando.

A continuación aparece un ejemplo de una sesión de registro de entrada y salida de TELNET llamando desde una estación de trabajo UNIX (llamada tpci _ hpws2) a otra (llamada tpci_hpWS4).

tpci_hpws2% telnet tpci_hpws4
Trying...
Connected to tpci_hpws4.
Escape character is] .
HP-UX tpci_hpws4 A.09.01 A 9000/720 (ttys2)
login: tparker
password: xxxxxxxx
tpci_hpws4-1> pwd
/u1/tparker
tpci_hpws4-2> cd docs
tpci_hpws4-3> pwd
/u1/tparker/docs
tpci_hpws4-2> <Ctrl+d>
Connection closed by foreign host.
tpci hpws2>

Para terminar la sesión remota, simplemente emita el comando de salida (en el ejemplo anterior, la combinación de teclas Ctrl+D de UNIX), y regresará a su máquina local.

*III.15.1.10.- Comandos del Protocolo **TELNET**.*

Cuando se establece una sesión TELNET se dispone de varias opciones de servicio. Durante el curso de una sesión TELNET, los valores se pueden modificar, siempre que ambos extremos estén de acuerdo (un extremo puede estar impedido para habilitar o deshabilitar un servicio por decisión del administrador o de ajuste de recursos). El Protocolo TELNET utiliza cuatro verbos para ofrecer, rehusar, solicitar o evitar servicios: *will, won't, do, y don't*, respectivamente. Estos verbos se diseñaron para funcionar por pares. La siguiente sesión TELNET, tiene activo el despliegue de estos verbos mediante el uso del comando *"Toggle Options"* de TELNET:

tpci_server-1> telnet	*(Se entra a modo de comando)*
telnet toggle options	*(Se habilita el despliegue de opciones)*
Will show option processing.	
telnet> open tpci_hpws4	*(Se intenta una conexión)*
Trying...	
Connected to tpci_hpws4.	
Escape character is '^]'.	
SENT do SUPPRESS GO AHEAD	*(Se negocian condiciones de trabajo)*
SENT will TERMINAL TYPE (don't reply)	
SEND will NAWS (don't reply)	
RCVD do 36 (reply)	
sent wont 36 (don't reply)	
RECD do TERMINAL TYPE (don't reply)	
RCVD will SUPPRESS GO AHEAD (don't reply)	
RCVD do NAWS (don't reply)	
Sent suboption NAWS 0 80 (80) 0 37 (37)	
Received suboption Terminal type - request to send.	
RCVD will ECHO (reply)	
SEND do ECHO (reply)	
RCVD do ECHO (reply)	
SENT wont ECHO (don't reply)	
HP-UX tpci_hpws4 A.09.01 A 9000/720 (ttys2)	*(inicia sesión)*
login:	

La siguiente tabla muestra un conjunto parcial de códigos de comandos TELNET. Hay otros códigos adicionales para funciones de impresión, como tabuladores horizontales y verticales y alimentaciones de forma, pero por razones de brevedad éstos se omitieron de la tabla.

Parte del conjunto de comandos TELNET incluye seis funciones terminales (IP, AO, AYT, EC, EL y GA) que son comunes en la mayor parte de las definiciones de terminal, y por lo tanto están definidas formalmente en el estándar de TELNET.

Código	Valor	Descripción
Abortar salida (AO)	245	Ejecuta el proceso hasta su terminación pero no envía la salida.
Está usted ahí (AYT)	246	Consulta el otro extremo para asegurarse de que una aplicación esté funcionando.
Ruptura (BRK)	243	Envía una instrucción de ruptura
Marca de datos	242	Porción de datos de un Sync
Do	253	Solicita al otro extremo que ejecute o acuse recibo de lo que el otro extremo ejecute
Don't	254	Demanda al otro extremo que deje de ejecutar o que confirme que el otro extremo ya no está ejecutando
Borrar carácter (EC)	247	Borra un carácter del flujo de salida
Borra línea (EL)	248	Borra una línea del flujo de salida
Adelante (GA)	249	Indica permiso para seguir adelante al utilizar comunicaciones de medio dúplex (sin eco)
Interpretar como comando (IAC)	255	Interpretar lo que sigue como si fuera un comando
Interrumpir proceso (IP)	244	Interrumpe, suspende, aborta o da por terminado el proceso
NOP	241	No operación
SB	250	Subnegociación de una opción
SE	240	Fin de una subnegociación
Hill	251	Instruye al otro extremo para que empiece a ejecutar o confirme que este extremo está ejecutando ahora
Won't	252	Se rehusa a ejecutar o rechaza la ejecución del otro extremo

Tabla III.20.- Tabla de Comandos TELNET.

Los comandos TELNET se envían en un paquete conocido como comando. Típicamente el comando contendrá 2 ó 3 bytes: la instrucción interpretar como comando (IAC), el código de comando que se está enviando y cualquier parámetro opcional correspondiente al comando, también codificado.

III.15.1.11.- ***TN3270.***

Muchas macro-computadoras utilizan EBCDIC, en tanto que la mayor parte de máquinas más pequeñas se apoyan en ASCII. Esto puede causar un problema al tratar de usar TELNET desde máquinas basadas en EBCDIC hacia máquinas basadas en ASCII, porque los códigos que se estén transfiriendo no serán precisos. A fin de corregir lo anterior, se creó una aplicación TELNET conocida como **TN3270**, que proporciona la conversión entre ambos formatos.

Cuando se utiliza TN3270 para conectarse entre dos máquinas, TELNET mismo establece la conexión inicial, y a continuación uno de los extremos se ajusta para la conversión. Si una máquina ASCII está llamando a una máquina EBCDIC, la conversión entre ambos formatos se realiza en el extremo EBCDIC (servidor), a menos que entre ambos exista una compuerta, en cuyo caso dicha compuerta puede llevar a cabo la conversión. TELNET ofrece el servicio de *"login"* remoto. Permite que un usuario interactivo de un sistema cliente inicie una sesión en un sistema remoto. Una vez que la conexión se ha establecido, el proceso cliente pasa los golpes del teclado del usuario al proceso servidor. Al igual que FTP, TELNET usa TCP. El estándar de TELNET se encuentra en el RFC 854. [Postel y Reynolds, 1983].

*III.16.- Sistemas de Nombres de Dominios ("Domain Name System", **DNS**).*

Los primeros sistemas de computadoras forzaban a los usuarios a utilizar direcciones numéricas que identificaban cada *"host"* en una red. Actualmente el servicio de nombres de dominio permite que los usuarios manejen nombres simbólicos y significativos.

Este es solo un servicio para hacer la utilización de la red más amigable. Las computadoras funcionan perfectamente usando direcciones IP, sin embargo, la gente prefiere estos nombres simbólicos ya que son fáciles de recordar.

Inicialmente el conjunto de nombres simbólicos era plano, pero conforme las redes crecieron se tuvo la necesidad de implementar otro tipo de esquemas, como el servidor BIND (*"Berkeley Internet Name Domain"*) de Internet.

El servidor BIND, permite crear y mantener una base de datos distribuida de nombres de *"hosts"* y direcciones de computadoras en una red. Por *"default"* un sistema UNIX se configura para usar el archivo */etc/hosts*. Sin embargo, si se tiene una red muy grande, actualizar este archivo en cada computadora puede consumir mucho tiempo. Usando BIND, el administrador del sistema no tendrá que actualizar el archivo de *"host"* en cada máquina.

III.16.1.- El Servidor de Nombres.

La función básica del servidor de nombres es atender las consultas de clientes relativas a nombres y direcciones de *"host"*. Con el servidor de nombres, la red es dividida en jerarquías de dominios. El espacio de nombres es organizado como un árbol, de acuerdo con las características de las organizaciones o administrativas. Cada nodo, llamado un dominio, tiene una etiqueta. El nombre de un dominio esta dado por la concatenación de todas las etiquetas de los dominios desde la *raíz* hasta el dominio referido, listados de derecha a izquierda, separados por puntos. Cada etiqueta es única en el dominio. Todo el espacio es dividido en áreas llamadas zonas, cada zona generalmente se asocia con un área administrativa. Un ejemplo de nombre de un *"hosts"* en la empresa ACME, es:

servidor.acme.com

El dominio superior para organizaciones comerciales es COM; Acme es un subdominio de COM y servidor es el nombre del *"host"*. Los dominios superiores para otros tipos de organizaciones establecidos por el NIC de Internet son:

EDU organizaciones educacionales.
GOV organizaciones gubernamentales.
MIL departamentos militares.
ORG organizaciones misceláneas.

III.16.1.1.- Tipos de Servidores.

Existen varios tipos de servidores. Estos son:

- Servidores maestros.
- Servidores de almacenamiento temporal.
- Servidores remotos.
- Servidores esclavos.

III.16.1.1.1.- Servidores Maestros.

Un Servidor Maestro de un Dominio es la autoridad en ese dominio. Este servidor mantiene todos los datos correspondientes a este dominio. Cada dominio deberá tener por lo menos dos servidores maestros: un maestro primario, y uno o más secundarios para respaldar el servicio si el primero no esta disponible o esta sobrecargado. Un servidor puede ser un maestro para múltiples dominios, siendo primario para algunos y secundario para otros.

III.16.1.2.1.- Primario.

Un Servidor Maestro Primario es aquel que carga la base de datos desde un archivo en disco. Este servidor puede delegar autoridad a otros servidores de su dominio.

III.16.1.2.2.- Secundario.

Un Servidor Maestro Secundario es un servidor al que le es delegada autoridad y recibe datos para un dominio desde un servidor maestro primario. Durante el arranque, el servidor secundario solicita todos los datos de la zona al servidor maestro primario. Este servidor verifica periódicamente con el servidor primario para verificar si se requiere actualizar los datos.

III.16.1.3.- Servidores Remotos.

Todas las solicitudes son redirigidas en su totalidad hacia un servidor de nombres de otra maquina. Un servidor remoto es una opción para quienes les gustaría tener el servicio de nombres en su sistema pero no tienen los recursos para hacerlo, por lo que se apoyan en el servidor de nombres de otro equipo, por ejemplo una computadora personal corriendo MS-DOS o Windows 9x, este tipo de servicio también se conoce como ***Resolvedor***.

III.16.1.4.- Servidores Esclavos.

Un servidor esclavo es un servidor que siempre envía las consultas que no puede resolver localmente hacia una lista de servidores que si lo pueden hacer, denominados *"forwarders"*, en lugar de interactuar con los servidores de nombres maestros, para el dominio raíz y otros. Las consultas hacia los servidores *"forwarders"* son recursivas. Es decir se intentan en el orden especificado hasta que la lista es agotada.

Bajo este esquema varios *"hosts"* podrían correr un servidor esclavo de otro servidor de nombres en un *"host"* más poderoso con acceso total a Internet, ese *"host"* desarrollaría un *caché* mucho mas completo, agilizando las consultas mas frecuentes de toda el área.

III.16.1.5.- Resolución de Nombres.

Los servidores de nombres obtienen información acerca del espacio de nombres de un dominio. Debido a la limitada inteligencia de algunos resolvedores, los servidores de nombres no solo pueden brindar información acerca de la zona para la que son autoridad, sino también para otros dominios, este proceso se conoce como resolución.

Debido a que el espacio de nombres esta estructurado como un árbol invertido, un servidor de nombres necesita un solo dato para determinar el punto de entrada dentro de este árbol hacia su objetivo: los nombres y direcciones de los servidores de nombres del dominio raíz. Un servidor de nombres puede consultar a un servidor raíz acerca de cualquier dominio dentro del árbol y el servidor raíz lo conducirá en su búsqueda.

III.16.1.6.- Servidores del Dominio Raíz.

Los servidores del dominio raíz saben que servidores son la autoridad para todos los dominios del nivel más alto. (De hecho los servidores del dominio raíz son autoridades para el dominio de nivel más alto en los Estados Unidos).

Dada una consulta acerca de cualquier nombre de dominio, los servidores raíz pueden cuando menos proveer los nombres y direcciones de los servidores autoridades para el dominio de nivel más alto al que pertenece el dominio consultado. Y esos servidores de nombres de nivel más alto pueden proveer la lista de los servidores autoridades para el dominio del segundo nivel al que pertenece el dominio consultado. Cada servidor de nombre consultado proporciona al cliente que inicio la consulta información de como llegar cada vez mas cerca hacia el dominio que esta buscando o le provee esta respuesta en caso de conocerla.

Los servidores de nombres raíz son muy importantes para la resolución, por esto el DNS provee mecanismos como el *"caché"* para reducir la carga de estos servidores raíz. Pero en ausencia de otra información la resolución tiene que empezar con los servidores raíz esto hace que estos servidores sean cruciales para el DNS, ya que si todos ellos estuvieran ocupados por un periodo prolongado el proceso de resolución en toda la Internet fallaría.

Para proteger contra esto Internet tiene varios servidores raíz diseminados en distintas partes de la red. Algunos pertenecen a MILNET, uno en la NASA, uno en Europa y otros en el *"Backbone"* de NSFNET. Al ser el punto focal para muchas consultas estos servidores raíz se mantienen muy ocupados recibiendo 20 000 consultas por hora. Si embargo el proceso de resolución funciona muy bien en la Internet, en este proceso de resolución para la dirección de un *"host"* real en un dominio real se hace a través del árbol del espacio de dominio de nombres.

III.16.1.7.- Iteración y Recursión.

Existen dos tipos de consultas: recursivas e iterativas. En el proceso recursivo mucho del trabajo recae en un solo servidor, inicialmente el resolvedor envía una consulta recursiva a un servidor de nombres acerca de un dominio particular. El servidor de nombres consultado esta entonces obligado a responder esta consulta o a enviar un mensaje de error si el dominio no existe.

Este servidor de nombres no puede transferir al cliente hacia otro servidor ya que la consulta es recursiva. Si el servidor consultado no es la autoridad para los datos solicitados tendrá que consultar a otros servidores de nivel mas bajo, por lo tanto los obliga a encontrar la respuesta y regresársela (es decir les pasa "la bolita"). Este proceso se repite hasta encontrar la respuesta o hasta que sea imposible continuar la búsqueda recursiva.

En una consulta iterativa un cliente que consulta a un servidor de nombres, es transferido hacia otro servidor más cercano (dentro del árbol) al dominio buscado, si este no conoce la respuesta a la solicitud del cliente, el servidor dará su mejor respuesta, apoyado únicamente en la base de datos local (incluyendo su *"caché"*), ya que este no realizará ninguna consulta adicional.

Este proceso se repite como en el ejemplo anterior, ayudando al cliente al redirigirlo hacia otros servidores de nombres más cercanos hacia los datos buscados.

Usualmente en un sistema UNIX, el resolvedor consulta al servidor de nombres local mediante una consulta recursiva, este a su vez consulta a otros servidores de nombres en búsqueda de la respuesta para el resolvedor, mediante una consulta interactiva. Cada servidor de nombres que consulta lo redirige hacia otros de nivel inferior en el espacio de nombres y por lo tanto más cercanos hacia el objetivo.

Finalmente el servidor de nombres local consulta al servidor de nombres autoridad del dominio buscado, el cual regresa la respuesta. Este a su vez responde al resolvedor.

*III.16.1.8.- El Caché **DNS**.*

Un servidor de nombres que procesa una consulta recursiva puede requerir realizar otras consultas para encontrar la respuesta. Sin embargo este descubre que mucha de la información acerca del espacio de nombres de dominio se repite continuamente. Cada vez que es transferido hacia otros servidores, aprende que estos servidores de nombres son autoridades para una zona específica y también aprende su dirección.

Al final del proceso de resolución puede almacenar toda esta información para agilizar una futura referencia a esta los servidores de nombres guardan en un archivo de caché todos los datos para agilizar lás consultas sucesivas, la próxima vez que un resolvedor consulta al servidor de nombres acerca de algún dominio el proceso es agilizado al consultar primero el caché local, si esta información se encuentra ahí no se tiene que realizar ninguna consulta posterior y por lo tanto no se es tan dependiente de otros servidores como los del dominio raíz.

*III.17.- Protocolo de Transferencia de Correo Simple ("Simple Mail Transfer Protocol", **SMTP**).*

SMTP proporciona un protocolo para el intercambio de correo entre dos sistemas usando una conexión TCP. La definición de SMTP se encuentra en el RFC 821. [Postel, 1982]. El estándar para el formato de los mensajes de correo se encuentra en el RFC 822. [Crocker, 1982], el RFC 974. [Patridge, 1986] especifica la manera de enrutar el *e-mail*.

El correo electrónico, además se conoce como un sistema de mensajes basado en una computadora (*"Computer Based Message System"*, CBMS), es un mecanismo que les permite a los usuarios de las terminales crear e intercambiar mensajes. A menos que el usuario (receptor o transmisor) desee una copia impresa del mensaje, todo se realiza de manera electrónica. Algunos sistemas de correo electrónico sólo sirven para los usuarios de una sola computadora, la mayoría permiten el intercambio de mensajes en una red de computadoras.

III.17.1.- Funcionamiento.

Aunque los mensajes transferidos por SMTP usualmente siguen el formato definido en el RFC 822, a SMTP no le importa el formato o contenido del mensaje. Esta idea se expresa con frecuencia diciendo que SMTP usa la información escrita sobre el "sobre" del correo, no mira adentro. Solo hay dos excepciones: SMTP estandariza el conjunto de caracteres del mensaje como ASCII de 7 bits y le antepone a los mensajes entregados la información de registro que contiene la ruta que el mensaje siguió.

El correo es creado por el programa del usuario y se coloca en una cola de correo listo para salir junto con los otros mensajes de este usuario y del *"host"* local. La cola se atiende por un transmisor

SMTP, el cual es típicamente un proceso presente del servidor en el *"host"*. El transmisor SMTP toma los mensajes de la cola y les transmite al *"host"* destino apropiado, vía transacciones SMTP sobre una o varias conexiones de TCP en el puerto 25. Un *"host"* debe tener múltiples transmisores SMTP activos simultáneamente cuando tiene un volumen grande de correo listo para salir, además, debe tener la capacidad de crear receptores SMTP, dependiendo del tamaño de la demanda, con la finalidad de no retardar el correo de los demás usuarios.

La entrada que requiere un transmisor SMTP se encuentra en la cola del correo lista para salir. Aunque la estructura de esta cola varía dependiendo del sistema operativo del *"host"*, cada mensaje de la cola conceptualmente tiene dos partes:

- El texto del mensaje.
- Una lista de destinatarios.

El texto del mensaje incluye el encabezado especificado por la norma del RFC 822 y el cuerpo del mensaje creado por el usuario. El transmisor SMTP busca la información en la cola y abre una conexión TCP para entregar el correo. Siempre que el transmisor SMTP esté listo para completar la entrega de un mensaje en particular a uno o varios usuarios de un *"host"*, borra los destinatarios correspondientes de la lista de mensajes. Cuando todos los destinatarios de un mensaje son procesados, el texto del mensaje y la lista de destinatarios de ese mensaje se borra de la cola. El transmisor SMTP puede realizar diversas optimizaciones. Si un mensaje es enviado a usuarios múltiples de un *"host"*, el texto del mensaje se envía una sola vez. El transmisor SMTP puede además transferir múltiples mensajes sobre una sola conexión TCP.

El transmisor SMTP debe ser capaz de responder a varios errores. El *"host"* destino puede estar fuera de su alcance, apagado, o la conexión TCP puede fallar mientras que el correo se está transfiriendo. El transmisor debe volver a poner el mensaje en la cola para entregarlo mas tarde. Esta es una política a criterio del administrador del sistema, pero generalmente el transmisor seguirá intentando entregarlo por varios días.

Otra serie de errores ocurren con las direcciones destino son erróneas o cuando el destinatario se ha mudado a otro sistema. El transmisor SMTP debe enfrentarse a estos problemas y enviar el mensaje o regresar un mensaje de error al remitente del mensaje.

El protocolo SMTP ofrece una operación confiable, pero no garantiza la recuperación de los archivos que el *"host"* pierda. Cuando un mensaje se entrega exitosamente no se le entrega ningún acuse de recibo al destinatario y no se garantiza la entrega. Sin embargo, el sistema de correo es lo suficientemente confiable como para que esto no sea un motivo de alarma.

El receptor SMTP acepta los mensajes recién llegados y los coloca en los buzones apropiados de los usuarios o los copia a la cola local de correo. Para hacer este trabajo, el receptor SMTP verifica los destinos del correo local relacionados con los problemas de transmisión, la escasez de espacio en disco, etcétera. La estrategia general es que el transmisor indiqué cuándo ha finalizado la transferencia. Así, el transmisor es que mayor responsabilidad tiene sobre la recuperación de errores o los errores ocurridos durante la transmisión cuando éstos causan duplicación y no la pérdida de mensajes. Los mecanismos de recuperación de errores del receptor están sujetos a los de las conexiones TCP.

En la mayoría de los casos, los mensajes viajan directamente del remitente al destinatario. Ocasionalmente el correo pasa primero por sistemas intermedios. Una forma de que esto suceda, es cuando el transmisor especifica una ruta destino en la que existe una serie de servidores.

III.17.2.- Protocolo de Oficina Postal ("Postal Office Protocol", **POP3**).

En ciertos tipos de nodos pequeños en Internet es impráctico mantener un Sistema de Transporte de Mensajes (MTS). Por ejemplo, una *"Workstation"* puede no tener suficientes recursos para permitir un servidor SMTP y un sistema asociado de entrega de correo local, residente y que este corriendo en forma continua. Similarmente, puede ser caro (o incosteable) mantener una computadora personal interconectada a una red con arquitectura TCP/IP durante un periodo largo (esto es que el nodo carece de conectividad).

A pesar de estas restricciones, algunas estaciones si pueden recibir correo, ya que algunas de estas soportan un agente de usuario (UA) que puede interaccionar con un servidor de correo.

Bajo este esquema, un nodo que puede soportar un sistema MTS, ofrece el servicio de "oficina postal" a los otros nodos. El Protocolo **POP** (*"Postal Office Protocol"*) Versión 3, conocido como **POP3**, fue diseñado para permitir a una estación de trabajo acceder dinámicamente un buzón en un *"host"* servidor.

Usualmente, esto significa que el POP3 permite a una estación de trabajo leer correo desde un buzón que el servidor de correo administra. Este servidor recibe el correo dirigido a cierto usuario y lo deposita en su buzón, en espera de que este sea leído. Haciendo uso de la terminología de la arquitectura cliente-servidor, el término "cliente" se refiere a una estación que hace uso del servicio POP3, mientras que el término "servidor" se refiere a un *"host"* que ofrece el servicio de POP3 a esa estación.

En este trabajo no se especifica como un cliente deposita correo en el sistema MTS, sin embargo podemos resumir este procedimiento en el siguiente párrafo:

Cuando el agente usuario en un cliente desea introducir un mensaje en el sistema de transporte, establece una conexión SMTP con un *"host"* capaz de enviar correo. Este *"host"* podría ser, pero no necesariamente, el *"host"* que corre el servidor POP3.

III.17.2.1.- Operación Básica.

Inicialmente, el *"host"* servidor inicia el servicio POP3 que utiliza el puerto TCP 110 para esperar solicitudes de conexión. Cuando un cliente desea hacer uso del servicio, establece una conexión TCP con el *"host"* servidor. Una vez que la conexión se ha establecido, el servidor POP3 envía un saludo. A continuación, el cliente y el servidor POP3 intercambian comandos y respuestas respectivamente hasta que la conexión es cerrada o abortada.

Los comandos de POP3 consisten de una palabra clave, posiblemente seguida de uno o más argumentos. Todos los comandos son terminados por el par CRLF. Las palabras clave y los argumentos consisten de caracteres ASCII imprimibles y están separados por un solo carácter de espacio. Las palabras clave constan de tres o cuatro caracteres y cada argumento puede tener hasta 40 caracteres de longitud.

Las respuestas de POP3 consisten de un indicador de status y una palabra clave posiblemente seguida de información adicional. Todas las respuestas son terminadas por un par CRLF. Actualmente existen dos indicadores de estatus: positivo ("+OK") y negativo ("-ERR").

Las respuestas a ciertos comandos son multilínea. En estos casos, que son mencionados posteriormente, después de enviar la primera línea de la respuesta y un CRLF, se envía cualquier línea adicional, cada una terminada por un par CRLF.

Cuando todas las líneas de la respuesta han sido enviadas, se envía una línea final, que consiste de un byte de terminación (código decimal 046, ".") y un par CRLF. Por lo tanto una respuesta multilínea es terminada con 5 bytes ("CRLF.CRLF").

Cuando se examina una respuesta multilínea, el cliente checa cada línea para determinar si empieza con el byte de terminación. Si es así y si este es seguido por otros caracteres diferentes al par CRLF, entonces el primer byte de la línea (el punto) es ignorado. Si el par CRLF sigue inmediatamente al punto, entonces la respuesta del servidor POP3 ha terminado y la línea que contiene ". CRLF" no es considerada como parte de la respuesta multilínea.

Una sesión POP3 se lleva acabo a través de diferentes estados durante su tiempo de vida. Una vez que la conexión TCP ha sido abierta y el servidor POP3 ha enviado el saludo, la sesión entra al estado de AUTORIZACIÓN. En este estado, el cliente debe identificarse con el servidor POP3.

Una vez que el servidor ha validado su identificación, el servidor adquiere recursos asociados con el buzón del cliente y la sesión pasa al estado de TRANSACCIÓN. En este estado, el cliente solicita diversas acciones al servidor POP3.

Cuando el cliente emite el comando QUIT, la sesión entra al estado de ACTUALIZACIÓN (UPDATE). En este estado, el servidor POP3 libera cualquier recurso adquirido durante el estado de TRANSACCIÓN y envía un mensaje de despedida al cliente. Por último se cierra la conexión TCP.

Un servidor POP3 puede tener un *"timer"* para terminar automáticamente después de cierto tiempo de inactividad. Este *"timer"* debe ser de por lo menos de 10 minutos de duración. La recepción de cualquier comando del cliente durante este intervalo, es suficiente para reinicializar el *"timer"*. Cuando el *"timer"* expira, la sesión no entra en el estado de UPDATE, el servidor cerrará la conexión TCP sin borrar los mensajes o mandar respuestas al cliente.

III.17.2.2.- El Estado de Autorización.

Una vez que la conexión TCP ha sido abierta por un cliente POP3, el servidor POP3 manda una línea de saludo. Esta puede ser cualquier cadena terminada con un CRLF. Un ejemplo podría ser:

S: +OK POP3 server ready

Este saludo es una respuesta del POP3 que siempre ira precedido de un estatus positivo.

La sesión POP3 esta ahora en el estado de AUTORIZACIÓN. El cliente debe entonces identificarse con el servidor POP3, mediante la combinación de los comandos USER y PASS.

El cliente debe primero emitir el comando USER seguido de un *"login-id"* válido en el servidor. Si el servidor POP3 responde con un indicador de estatus positivo (*"+OK"*), entonces el cliente debe emitir el comando PASS seguido de la contraseña (*"Password"*) del usuario para completar la autenticación o el comando QUIT para terminar la sesión POP3.

Si el servidor POP3 responde con un indicador de estado negativo (*"-ERR"*) al comando USER, entonces el cliente debe emitir un nuevo comando de autenticación o puede emitir el comando QUIT. Cuando el cliente emite el comando PASS, el servidor POP3 usa el par de argumentos de los comandos USER y PASS para determinar si al cliente se le dará acceso al buzón apropiado.

Una vez que el servidor POP3 ha determinado que el cliente puede tener acceso al buzón apropiado, el servidor POP3 adquiere acceso exclusivo (*"lock"*) al buzón, esto es necesario para prevenir que los mensajes sean modificados o borrados (por otra sesión) antes de que la sesión entre en el estado UPDATE. Si el acceso exclusivo es adquirido con éxito, el servidor POP3 responde con un indicador de estado positivo.

La sesión POP3 entra ahora en el estado de TRANSACCIÓN, sin mensajes marcados como borrados. Si el buzón no puede ser abierto por alguna razón (por ejemplo, un acceso exclusivo no puede ser adquirido, se le niega el acceso al cliente al buzón apropiado, o el contenido del buzón no puede ser interpretado), el servidor POP3 responde con un indicador de estatus negativo.

Si el acceso exclusivo pudo ser adquirido pero el servidor POP3 responde con un indicador de estatus negativo, el servidor POP3 debe liberar el acceso exclusivo antes de rechazar el comando.

Después de regresar un indicador de estatus negativo, el servidor puede cerrar la conexión. Si el servidor no cierra la conexión, el cliente puede emitir un nuevo comando de autenticación y volver a empezar o el cliente puede emitir el comando QUIT.

Después que el servidor ha abierto el buzón, este asigna un número a cada mensaje, y anota el tamaño en bytes de cada mensaje. Al primer mensaje en el buzón se le asigna el número 1, al segundo se le asigna 2, así hasta el n-esimo mensaje. En los comandos y respuestas de POP3, todos los números de mensajes y tamaños de mensajes son expresados en base 10 (es decir en decimal).

III.17.2.3.- Es Estado de Transacción.

Una vez que el cliente se ha identificado con éxito con el servidor POP3 y el servido POP3 ha abierto el buzón apropiado mediante un acceso exclusivo, la sesión POP3 esta ahora en el estado de TRANSACCIÓN.

El cliente puede ahora usar cualquiera de los comandos POP3 repetidamente. Después de cada comando, el servidor POP3 emite una respuesta. Eventualmente, el cliente emite el comando QUIT y la sesión POP3 entra en el estado UPDATE.

III.17.2.4.- Formato de los Mensajes.

Se asume que todos los mensajes transmitidos durante una sesión POP3 se ajustan al estándar de mensajes de texto Internet (RFC822).

Es importante notar que el tamaño en bytes de un mensaje en el *"host"* servidor puede diferir del contador de bytes asignado al mensaje debido a convenciones locales en la designación del fin de línea. Usualmente, durante el estado de AUTORIZACIÓN de la sesión POP3, el servidor POP3 puede calcular el tamaño de cada mensaje en bytes cuando este abre el buzón. Por ejemplo, si el *"host"* representa internamente el fin de línea como un solo carácter, entonces el servidor POP3 simplemente cuenta cada ocurrencia de este carácter en un mensaje como dos bytes. Nótese que líneas en el mensaje que empiezan con el byte de terminación no son tomadas en cuenta, ya que el cliente POP3 eliminará todos los bytes de terminación cuando se reciba una respuesta multilínea.

III.17.2.5.- Consideraciones de Seguridad.

En algunos servidores POP3 el comando APOP sirve para autenticar la identificación y el origen del usuario en el cliente y da protección a una sesión POP3, mediante el mecanismo de cifrado de llave pública.

Esta característica es deseable ya que la contraseña de una sesión POP3 viaja como texto claro por la red, y puede ser interceptada mediante un *"sniffer"*. Un servidor POP3 que implementa tanto el comando APOP como el PASS, no debe permitir el uso de ambos métodos en el acceso de un usuario dado; esto es, para un nombre de usuario (USER Name) se puede permitir el PASS o el APOP pero no ambos.

III.18.- Administración de Redes TCP/IP.

Los protocolos de administración de redes fueron desarrollados para permitir a los administradores manejar los dispositivos, dar seguimiento a los eventos críticos de la red y colectar información relacionada con las tendencias de crecimiento de las rutas de comunicación así como del desarrollo de la red y todo desde una estación de administración centralizada.

El primer protocolo de administración de redes no propietario que ha sido ampliamente aceptado fue desarrollado por la comunidad Internet para el uso del conjunto de protocolos TCP/IP. Inicialmente, se crearon para satisfacer necesidades básicas. Por ejemplo, para realizar el manejo centralizado del crecimiento local de direcciones IP asociadas a ruteadores en una red global Internet.

El grupo de estudio conocido como IETF (Internet Engieneering Task Force) fue asignado al problema del manejo de ruteadores Internet. Este grupo diseñó una plataforma de trabajo que vino a constituir la fundación del conjunto de protocolos de manejo Protocolo de Administración de Red Simple (Simple Network Management Protocol, SNMP).

Dos de los criterios más importantes, que son utilizados en los protocolos de manejo de red, y que son parte del diseño de la plataforma de trabajo SNMP, son:

El protocolo no debe aumentar significativamente el tráfico en la red para satisfacer las necesidades de administración.

El agente de protocolo, en el dispositivo de manejo, no debe disminuir las capacidades de operación básicas o primarias que deba satisfacer el dispositivo en el trabajo que tenga asignado. Un mínimo de ciclos de CPU y de memoria deben ser utilizados para propósitos de manejo o administración.

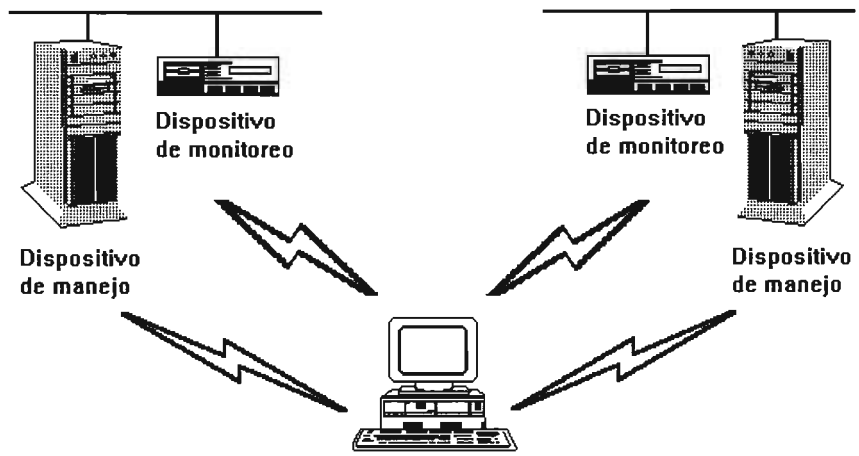


Figura III.28.- Organización y Administración.

III.18.1.- Agentes de Manejo.

Un agente de manejo es una base de datos de información relacionada con un dispositivo y su ambiente de trabajo; estando este dispositivo instalado en el dispositivo de manejo o en el de monitoreo. Los datos contenidos en la base de datos del agente dependerá de las funciones del dispositivo. Por ejemplo, un ruteador puede contener información relacionada con su propia tabla de ruteo, el total de paquetes transmitidos y recibidos por el protocolo de capa de red, el número de los paquetes no validados e información variada.

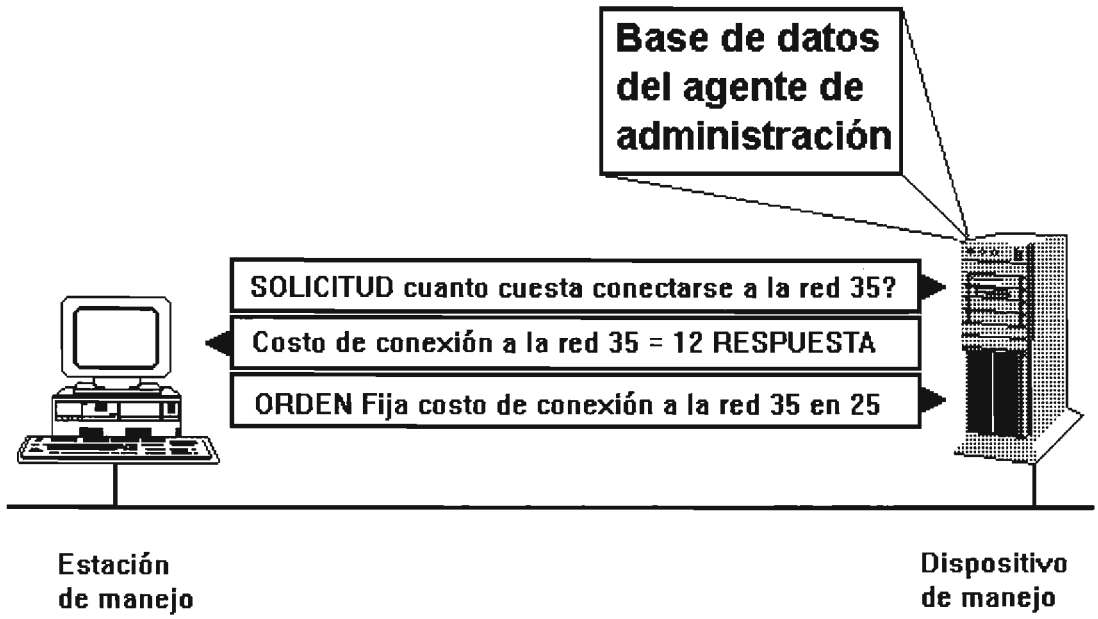


Figura III.29.- Agentes de Manejo.

La estación de manejo realiza las siguientes solicitudes al agente en el dispositivo de manejo:

- Recuperación de información relacionada con el dispositivo.
- Actualización o anexión de entradas en la base de datos.
- Fijar un valor máximo a una variable crítica.

El agente en el dispositivo de manejo no ofrece información, porque lo podría alejar de su tarea específica y primaria. La única excepción a esta regla es que el agente podrá enviar una señal de alarma a la estación de manejo en el caso de que se sobrepase un valor de condición crítica.

*III.19.- Protocolo de Administración de Red Simple ("Simple Network Management Protocol", **SNMP**).*

El Protocolo **SNMP** (*"Simple Network Management Protocol"*) es actualmente una familia de especificaciones que provee un significado a la colecta de información de la red para el caso de la administración desde los mismos dispositivos de la red. Este protocolo también provee un método, para los dispositivos, que les permite reportar problemas que se estén experimentando en el manejo de la estación.

Una estación de manejo SNMP realiza solicitudes (de poleo) al software para obtener datos de dispositivos en la red. La estación de manejo presenta los datos a la administración para que sean utilizados en el diagnóstico y el manejo del dispositivo.

Los protocolos de la familia de protocolos SNMP son:

- SMI (Structure and Identification of Management Information)
- MIB (Management Information Base)
- SNMP (Simple Network Management Protocol)

III.19.1.- Estructuración e Identificación (SMI).

La especificación SMI define la estructura de la base de datos del agente SNMP. Cuando se construye la base de datos, lo primero que debe hacerse es decidir la estructura que deberá tener.

La estructura define el número de campos de cada entrada así como su tamaño y el tipo de datos que podrá contener cada uno.

Por ejemplo, la estructura de la base de datos de unos libros de direcciones puede contener los campos:

- Nombre
- Dirección
- Estado
- Código Postal
- Teléfono.

Cada registro tendrá entonces cinco campos, que son Nombre, Dirección, Estado, Código Postal y Teléfono. El último campo contendrá sólo números. Estos campos podrán visualizarse con una ficha de registro o en formato de tabla. SMI define la estructura de la base de datos del agente SNMP exactamente de la misma manera.

III.20.- Información de Manejo (MIB).

El Protocolo **MIB** describe los objetos, o las entradas, que deben ser incluidas en la base de datos del agente SNMP. Por esta razón, los agentes SNMP son referidos algunas veces como MIBs. Los objetos en un MIB deben estar definidos de la manera en que los desarrolladores del software de la estación conocen a disposición (los nombres de los objetos y sus valores correspondientes). Esta información se incluye en la especificación MIB.

Existen tres categorías de la especificación MIB:

Estándar.

Esta especificación incluye un conjunto común de objetos aceptados y ratificados por el grupo de estándares Internet. El primer estándar MIB que se dio a conocer constaba de 114 objetos, este fue mejorado posteriormente y presentando como MIB II, conteniendo 172 objetos. La información que proveen estas especificaciones MIB está dirigida a ruteadores de manejo IP.

RMON (*"Remote Monitoring"*)

MIB es actualmente un proceso de ratificación por la comunidad Internet para que constituya un estándar MIB. RMON posee funciones diferentes a MIB II. Puede contener objetos para el monitoreo de los medios de transmisión de la red, como pueden ser los relacionados con la utilización de medio, el número total de paquetes transmitidos sin errores e información variada sobre este respecto.

RMON también puede utilizarse para realizar el monitoreo de dispositivos que no tienen un agente SNMP. Un dispositivo de monitoreo RMON es identificado como un casi agente del dispositivo sin agente.

Experimental.

Esta categoría incluye información específica relacionada con otros aspectos de la red y de los dispositivos de manejo considerada como de gran valía y que no existe en otros estándares MIB. Una vez que la especificación experimental de MIB sea refinada y llevada a niveles competitivos de eficiencia, será reclasificada como estándar.

Privado (o de Empresa).

Ésta se ha diseñado para uso individual de compañías que requieren colectar datos particulares de sus propios dispositivos de red. Permite que se definan objetos propios, que pueden ser específicos y no estar definidos en la categoría estándar.

*III.21.- Protocolo **SNMP**.*

El Protocolo **SNMP** (*"Simple Network Management Protocol"*) fue diseñado para permitir la administración y manejo de la red a través del uso de una aplicación consola para realizar las solicitudes MIB de SNMP. La estructura de manejo declara a un protocolo de manejo capaz (con un mínimo de sobrecarga en el nodo de manejo) de hacer la toma de datos de la estación y de la propia red.

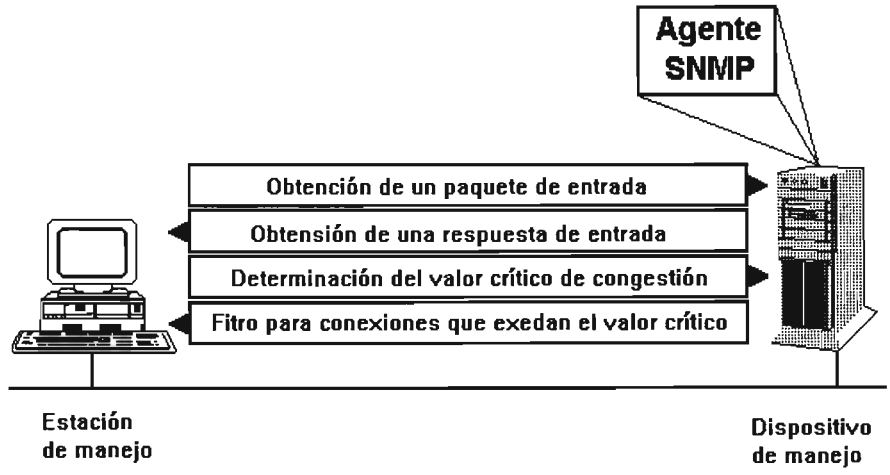


Figura III.31.- Protocolo SNMP.

Lo anterior es completado constituyendo a SNMP como un protocolo cliente-servidor con únicamente cuatro operaciones:

GET
Utilizado para recuperar un objeto simple en el MIB.

GET-NEXT
Usado en tablas de transferencia (tablas transversas).

SET

Se aplica para manipular información de administración.

TRAP
Sirven para realizar reportes — alarmas — de eventos críticos.

SNMP fue diseñado específicamente para ser un protocolo de transporte independiente. Lo que significa que las solicitudes de SNMP sobre los agentes pueden hacerse utilizando cualquier protocolo de transporte como TCP/IP, IPX/SPX, AppleTalk y cualquier otro.

III.22.- SNMP II.

El cuerpo de estándares de Internet ha ratificado a SNMP II. Este añade las siguientes características a la funcionalidad del protocolo SNMP:

Seguridad mejorada

Estación de comunicaciones con manejo interno (no sólo el manejo del agente).

Operación GET-BULK. Actualmente, una base de datos como una tabla de ruteo debe ser recuperada entrada por entrada (registro a registro) utilizando el operador GET-NEXT. El operador GET-BULK permite hacer la solicitud de la tabla completa en un sólo tiempo.

CAPÍTULO IV.

CONECTIVIDAD PARA REDES DE ÁREA LOCAL.

IV.1.- Introducción.

El dispositivo de comunicación más básico de conectividad entre redes es el módem. Los módems se han convertido en dispositivos habituales y constituyen el equipamiento estándar en la mayoría de los equipos que se venden hoy en día. En realidad, cualquiera que haya utilizado Internet o un PC-fax, ha utilizado un módem. Además de los módems, también se utilizan otros dispositivos para conectar pequeñas LAN en una gran red de área extensa (WAN). Cada uno de estos dispositivos tiene su propia funcionalidad junto con algunas limitaciones. Simplemente, se pueden utilizar para extender la longitud del medio de red o para proporcionar acceso a una red mundial en Internet. Los dispositivos utilizados para extender las LAN incluyen repetidores, *bridges* (puentes), *routers* (encaminadores), *brouters* (b-encaminadores) y *gateways* (pasarelas).

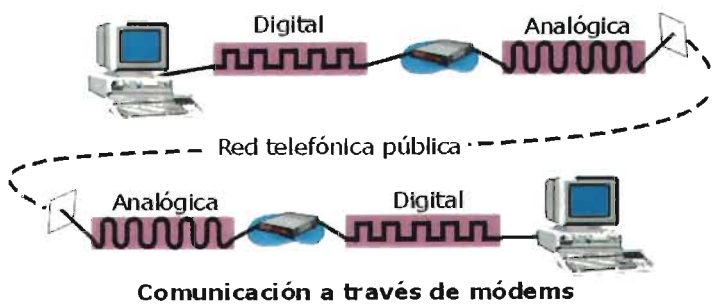
IV.2.- Tecnología de Módems.

Un módem es un dispositivo que permite a los equipos comunicarse a través de una línea telefónica.

Cuando los equipos están demasiado alejados como para conectarse a través de un cable estándar, se puede llevar a cabo la comunicación entre ellos mediante un *módem*. En un entorno de red, los módems actúan como un medio de comunicación entre redes y como una forma de conectar el mundo que existe más allá de la red local.

IV.2.1.- Funciones Básicas de un Módem.

Los equipos no se pueden conectar a través de una línea telefónica, puesto que éstos se comunican enviando pulsos electrónicos digitales (señales electrónicas) y una línea telefónica sólo puede enviar ondas (sonido) analógicas.
Una señal digital tiene un formato binario. La señal puede tener un valor de 0 ó 1. Una señal analógica se puede representar como una curva suavizada que puede representar un rango infinito de valores.
El módem que se encuentra en el PC emisor convierte las señales digitales en ondas analógicas y transmite estas ondas analógicas a través de la línea telefónica. El módem que recibe la señal, convierte las señales analógicas que le llegan en señales digitales para que las reciba el PC.



Comunicación a través de módems

En otras palabras, un módem emisor *MO*dula las señales digitales en señales analógicas y un módem receptor *DE*modula las señales que recibe en señales digitales.

IV.2.2.- Hardware del Módem.

Los módems se conocen como equipamiento de comunicaciones de datos (ECD) y comparten las siguientes características:

- Una interfase de comunicación serie (RS-232).
- Una interfase de línea telefónica RJ-11 (enchufe telefónico de cuatro hilos).

Están disponibles tanto módems externos como internos. Un módem interno se instala en una ranura de expansión del equipo al igual que otra tarjeta.

Un módem externo es una pequeña caja que se conecta al equipo a través un cable serie (RS-232) desde el puerto serie del equipo hasta la conexión del cable en el módem. El módem utiliza un cable con un conector RJ-11C para conectarse a la pared.

IV.2.3.- Estándares de Módems.

Los estándares son necesarios puesto que permiten a los módems de un fabricante poder conectarse con los módems de otro fabricante.

Hayes-compatible.

A principios de los años ochenta, una compañía denominada Hayes Microcomputer Products desarrolló un módem denominado Hayes Smartmodem. Este módem se convirtió en un estándar frente a otros tipos de módems y surgió la frase «Hayes-compatible», al igual que el PC personal de IBM generó el término «IBM-compatible». Como la mayoría de los vendedores se ajustaron a los estándares de Hayes, casi todos los módems de redes LAN podían comunicarse con el resto.

Los primeros módems Hayes-compatible enviaban y recibían datos a 300 bits por segundo (bps). Actualmente, los fabricantes de módems ofrecen módems con velocidades de 56,600 bps o más.

Estándares internacionales

Desde finales de los años ochenta, el International Telecommunications Union (ITU; Unión internacional de las telecomunicaciones) ha desarrollado estándares para los módems. Estas especificaciones, conocidas como las series V, incluyen un número que indica el estándar. Como punto de referencia, el módem V.22bis a 2,400 bps tardaría 18 segundos en enviar una carta de 1,000 palabras. El módem V.34 a 9,600 bps tardaría sólo cuatro segundos en enviar la misma carta y el estándar de compresión V.42bis en un módem de 14,400 bps puede enviar la misma carta en sólo tres segundos.

En la siguiente tabla se presentan los estándares de compresión y sus correspondientes parámetros. Los estándares de compresión y los bps tienen que estar necesariamente relacionados. El estándar se podría utilizar con cualquier velocidad de módem.

Estándar	bps	Fecha	Notas
V.17	14,400		Para transmisiones FAX a través de la línea telefónica
V.21	300		Transmisiones de datos por líneas telefónicas
V.22	1,200		Transmisiones de datos por líneas telefónicas y líneas dedicadas
V.22bis	2,400	1984	Transmisiones de datos por líneas telefónicas dedicadas
V.23	600/1,200		Transmisiones de datos por líneas telefónicas y dedicadas.
V.25			Estándares de llamada y contestación automática.
V.26	2,400		Transmisiones de datos por líneas dedicadas.
V.26bis	1,200/2,400		Transmisiones de datos por líneas telefónicas
V.26ter	2,400		Transmisiones de datos por líneas telefónicas y dedicadas
V.27	4,800		Transmisiones de datos por líneas dedicadas
V.27bis	2,400/4,800		Transmisiones de datos por líneas dedicadas.
V.27ter	2,400/4,800		Transmisiones de datos por líneas telefónicas
V.29	9,600		Transmisiones de datos por líneas dedicadas
V.32	9,600	1984	Transmisiones de datos por líneas telefónicas
V.32bis	14,400	1991	Transmisiones de datos por líneas telefónicas utilizando comunicaciones síncronas
V.32ter	19,200	1993	Se comunicará sólo con otro V.32ter.
V.33	14,400	1993	Transmisiones de datos por líneas dedicadas
V.34	28,800	1994	Transmisiones de datos por líneas telefónicas con la posibilidad de bajar la velocidad cuando haya problemas en la línea
V.35	48,000		Transmisiones de datos por líneas dedicadas
V.42	57,600	1995	Compatible con versiones de V.módems anteriores. Estándar de corrección de errores en líneas ruidosas
V.42bis	56,600		Comprensión de datos 4:1 para transferencias de alta velocidad
V.90	56,600	1998	Estándar de módem a 56K; resolvió la competencia para los estándares entre los estándares U.S. Robotic X2 y Rockwell K56 Flex.

IV.2.4.- Rendimiento del Módem.

Inicialmente, la velocidad del módem se medía en bps o en la tasa denominada «baudios», y se asumió erróneamente que ambas unidades eran idénticas.

«Baudios» se refiere a la velocidad de oscilación de la onda de sonido que transporta un bit de datos sobre la línea telefónica. El término se deriva del nombre del telégrafo e ingeniero francés Jean-Maurice-Emile Baudot. A principios de 1980, la tasa de baudios se equiparó con la velocidad de transmisión de los módems. Hoy en día, 300 baudios equivalen a 2.300 bits por segundo.

Con el tiempo, los ingenieros de comunicaciones aprendieron a comprimir y codificar los datos, de forma que cada modulación de la onda permitía transportar más de un bit de datos. Este desarrollo significa que la tasa de bps puede ser superior a la tasa de baudios. Por ejemplo, un módem que modula a 28.800 baudios puede enviar a 115.200 bps. Por tanto, el parámetro actual para controlar la velocidad de los módems es bps.

Algunos de los estándares de la industria relativa a los módems más recientes, V.42bis/compresión de datos MNP5, tienen velocidades de transmisión de 57.600 bps, llegando algunos hasta los 76.800 bps.

IV.2.5.- Tipos de Módems.

Existen tres tipos diferentes de módems, puesto que los distintos entornos de comunicación requieren diferentes métodos de envío de datos. Estos entornos se pueden dividir en dos áreas relacionadas con el ritmo de las comunicaciones:

- Asíncrona.
- Síncrona.

El tipo de módem que utiliza una red depende de si el entorno es asíncrono o síncrono.

Comunicación asíncrona (Async)

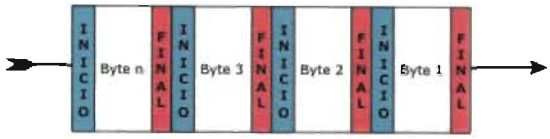
La *comunicación asíncrona,* conocida como «async», es probablemente la forma de conexión más extendida. Esto es debido a que *async* se desarrolló para utilizar las líneas telefónicas.

Cada carácter (letra, número o símbolo) se introduce en una cadena de bits. Cada una de estas cadenas se separa del resto mediante un bit de inicio de carácter y un bit de final de carácter. Los dispositivos emisor y receptor deben estar de acuerdo en la secuencia de bit inicial y final. El equipo destino utiliza los marcadores de bit inicial y final para planificar sus funciones relativas al ritmo de recepción, de forma que esté preparado para recibir el siguiente byte de datos.

La comunicación no está sincronizada. No existe un dispositivo reloj o método que permita coordinar la transmisión entre el emisor y el receptor. El equipo emisor sólo envía datos y el equipo receptor simplemente los recibe. A continuación, el equipo receptor los comprueba para asegurarse de que los datos recibidos coinciden con los enviados. Entre el 20 y el 27 por 100 del tráfico de datos en una comunicación asíncrona se debe al control y coordinación del tráfico de datos. La cantidad real depende del tipo de transmisión, por ejemplo, si se está utilizando la paridad (una forma de comprobación de errores).

Las transmisiones asíncronas en líneas telefónicas pueden alcanzar hasta 28.800 bps. No obstante, los métodos de compresión de datos más recientes permiten pasar de 28.800 bps a 115.200 bps en sistemas conectados directamente.

Control de errores. Debido al potencial de errores que puede presentar, *async* puede incluir un bit especial, denominado *bit de paridad,* que se utiliza en un esquema de corrección y comprobación de errores, denominado *comprobación de paridad.* En la comprobación de paridad, el número de bits enviados debe coincidir exactamente con el número de bits recibidos.



ASÍNCRONA

El estándar de módem original V.32 no proporcionaba control de errores. Para ayudar a evitar la generación de errores durante la transmisión de datos, Microcom desarrolló su propio estándar para el control de errores en los datos enviados de forma asíncrona, el *Microcom Networking Protocol* (MNP; Protocolo de conexión de Microcom). El método funcionó tan bien que el resto de compañías no sólo adoptaron la versión inicial del protocolo, sino también las versiones posteriores, denominadas clases. Actualmente, diferentes fabricantes de módems incorporan los estándares MNP Clases 2, 3 y 4.

En 1989, el *Comité Consultatif Internationale de Telégraphie et Teléponie* (CCITT; Comité internacional de consulta telegráfica y telefónica) publicó un esquema de control de errores asíncronos denominado V.42. Este estándar implementado en hardware caracterizó dos protocolos de control de errores. El primer esquema de control de errores es el procedimiento de acceso por enlace (LAPM), pero también utiliza MNP Clase 4. El protocolo LAPM se utilizó para las comunicaciones entre dos módems con estándar V.42. Si sólo uno de los módems sigue el estándar MNP 4, se tiene que el protocolo adecuado a utilizar sería MNP 4.

Mejora del rendimiento de la transmisión. El rendimiento de las comunicaciones depende de dos elementos:

- La velocidad de envío de señales o canales describe la rapidez de codificación de los bits en el canal de comunicación.
- Rendimiento total que mide la cantidad de información útil que se desplaza a través del canal.

La eliminación de elementos redundantes o secciones vacías permite en la compresión mejorar el tiempo requerido para el envío de los datos. El Protocolo de compresión de datos MNP Clase 5 de Microcom es un ejemplo de un estándar actual de compresión de datos. Utilizando la compresión de datos, puede mejorar el rendimiento, duplicando, a menudo, el rendimiento total. Se puede reducir la transmisión de los datos en la mitad cuando los dos extremos de un enlace de comunicaciones utilizan el protocolo MNP Clase 5.

El estándar V.42bis, dado que describe cómo implementar la compresión de datos en hardware, obtiene incluso el mayor rendimiento posible. Por ejemplo, un módem a 56,6 Kbps utilizando V.90 puede conseguir un rendimiento total de 100 Kbps.

Aunque la compresión de datos puede mejorar el rendimiento, no se trata de una ciencia exacta. Muchos factores afectan al porcentaje actual de compresión de un documento o archivo. Un archivo de texto, por ejemplo, se puede comprimir, de forma más efectiva, que un archivo gráfico complejo. Es posible, incluso, tener un archivo comprimido que sea más grande que el original. Recuerde que los porcentajes de compresión que mencionan los distribuidores se fundamentan normalmente en el mejor de los casos.

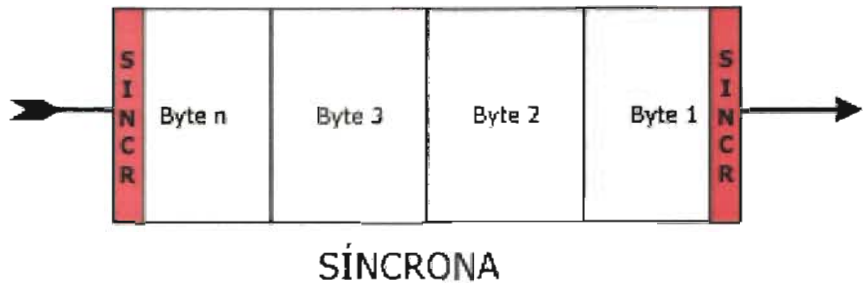
Coordinación de los estándares. Los módems asíncronos, o serie, son más baratos que los módems síncronos, puesto que los asíncronos no necesitan la circuitería y los componentes necesarios para controlar el ritmo que de las transmisiones síncronas requieren los módems síncronos.

Comunicación síncrona

La *comunicación síncrona* confía en un esquema temporal coordinado entre dos dispositivos para separar los grupos de bits y transmitirlos en bloques conocidos como «tramas». Se utilizan caracteres especiales para comenzar la sincronización y comprobar periódicamente su precisión.

Dado que los bits se envían y se reciben en un proceso controlado (sincronizado) y cronometrado, no se requieren los bits de inicio y final. Las transmisiones se detienen cuando se alcanza el final de una trama y comienzan, de nuevo, con una nueva. Este enfoque de inicio y final es mucho más eficiente que la transmisión asíncrona, especialmente cuando se están transfiriendo grandes paquetes de datos. Este incremento en eficiencia es menos destacable cuando se envían pequeños paquetes.

Si aparece un error, el esquema de corrección y detección de errores síncrono genera una retransmisión.



SÍNCRONA

Los protocolos síncronos realizan un número de tareas que no realizan los protocolos asíncronos.

Principalmente son:

- Formatear los datos en bloques.
- Agregar información de control.
- Comprobar la información para proporcionar el control de errores.

Los principales protocolos de comunicaciones síncronas son:

- Control síncrono de enlace de datos (SDLC, *Synchronous Data Link Control).*
- Control de enlace de datos de alto nivel (HDLC, *High-level Data Link Control).*
- Protocolo de comunicaciones síncronas binarias (bysnc).

La comunicación síncrona se utiliza en la mayoría de todas las comunicaciones de red y digitales. Por ejemplo, si está utilizando líneas digitales para conectar equipos remotos, debería utilizar módems síncronos, en lugar de asíncronos, para conectar el equipo a la línea digital. Normalmente, su alto precio y complejidad ha mantenido a los módems síncronos fuera del mercado de los equipos personales.

Línea digital abonada asimétrica (ADSL, *Asymetric Digital Subscriber Line)*

La última tecnología de módem disponible es una línea digital abonada asimétrica (ADSL). Esta tecnología convierte las líneas telefónicas actuales de par trenzado en vías de acceso para las comunicaciones de datos de alta velocidad y multimedia. Estas nuevas conexiones pueden transmitir por encima de los 8 Mbps para el abonado y de hasta 1Mbps desde el propio abonado.

No obstante, ADSL no está exenta de inconvenientes. La tecnología requiere un hardware especial, incluyendo un módem ADSL en cada extremo de la conexión. Además, necesita un cableado de banda amplia, que está disponible actualmente en muy pocas localizaciones y existe un límite en la longitud de conexión.

Expansión de una red usando componentes

A medida que crece una empresa, también lo hacen sus redes. Las LAN tienden a sobrepasar las posibilidades de sus diseños iniciales. Comprobará que una LAN es demasiado pequeña cuando:

- El cable comience a saturarse con el tráfico de la red.
- Los trabajos de impresión tardan mucho tiempo en imprimirse.
- Las aplicaciones que generan tráfico en la red, como pueden ser las bases de datos, experimentan tiempos de respuesta excesivos.

Normalmente, el momento llega cuando los administradores necesitan expandir el tamaño o mejorar el rendimiento de sus redes. Pero claro, las redes no son más grandes por el hecho de añadir más PC o más cableado. Cada topología o arquitectura tiene sus límites. No obstante, existen componentes que se pueden instalar para incrementar el tamaño de la red dentro del entorno actual.

Estos componentes son:

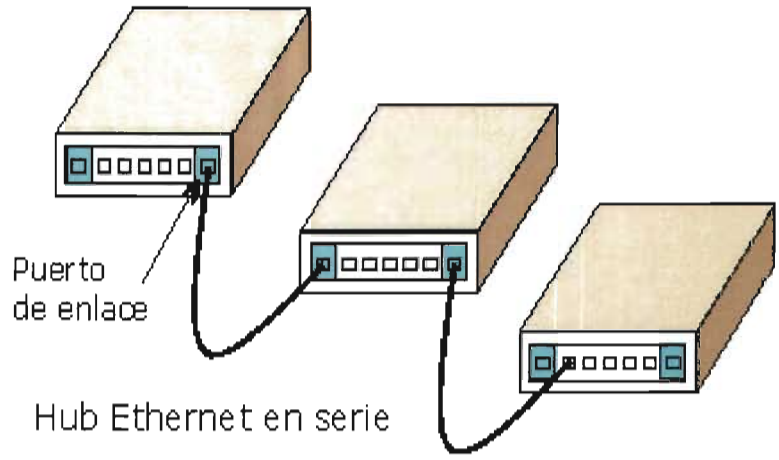
- Segmentos existentes de LAN, de forma que cada segmento se convierte en su propia LAN.
- Unir dos LAN separadas.
- Conectarse con otras LAN y entornos de computación para unirlos en una WAN considerablemente más grande.

Los componentes que permiten a los ingenieros conseguir estos objetivos son:

- Hubs (concentradores).
- Repetidores.
- Bridges (puentes).
- Routers (encaminadores).
- Brouters (b-encaminadores).
- Gateways (pasarelas).

IV.3.- Concentradores (Hubs).

Es el componente hardware central de una topología en estrella. Además, los hubs se pueden utilizar para extender el tamaño de una LAN. Aunque la utilización de un hub no implica convertir una LAN en una WAN, la conexión o incorporación de hubs a una LAN puede incrementar, de forma positiva, el número de estaciones. Este método de expansión de una LAN es bastante popular, pero supone muchas limitaciones de diseño.



Es importante tener cuidado cuando se conectan los hubs. Los cables de paso se conectan de forma diferente que los cables estándares de enlace. Compruebe con los fabricantes si se necesita un cable de enlace estándar o un cable de paso.

IV.4.- Repetidores.

Cuando las señales viajan a través de un cable, se degradan y se distorsionan en un proceso denominado «atenuación». Si un cable es bastante largo, la atenuación provocará finalmente que una señal sea prácticamente irreconocible. La instalación de un repetidor permite a las señales viajar sobre distancias más largas.

Un repetidor funciona en el nivel físico del modelo de referencia OSI para regenerar las señales de la red y reenviarla a otros segmentos.

El repetidor toma una señal débil de un segmento, la regenera y la pasa al siguiente segmento. Para pasar los datos de un segmento a otro a través del repetidor, deben ser idénticos en cada segmento los paquetes y los protocolos Control lógico de enlace (LLC; *Logical Link Control).* Un repetidor no activará la comunicación, por ejemplo, entre una LAN (Ethernet) 802.3 y una LAN (Token Ring) 802.5.

Los repetidores no traducen o filtran señales. Un repetidor funciona cuando los segmentos que unen el repetidor utilizan el mismo método de acceso. Un repetidor no puede conectar un segmento que utiliza CSMA/CD con un segmento que utiliza el método de acceso por paso de testigo. Es decir, un repetidor no puede traducir un paquete Ethernet en un paquete Token Ring.

Los repetidores pueden desplazar paquetes de un tipo de medio físico a otro. Pueden coger un paquete Ethernet que llega de un segmento con cable coaxial fino y pasarlo a un segmento de fibra óptica. Por tanto, el repetidor es capaz de aceptar las conexiones físicas.

Los repetidores constituyen la forma más barata de extender una red. Cuando se hace necesario extender la red más allá de su distancia o limitaciones relativas a los nodos, la posibilidad de utilizar un repetidor para enlazar segmentos es la mejor configuración, siempre y cuando los segmentos no generen mucho tráfico ni limiten los costos.

Ni aislamiento ni filtrado. Los repetidores envían cada bit de datos de un segmento de cable a otro, incluso cuando los datos forman paquetes mal configurados o paquetes no destinados a utilizarse en la red. Esto significa que la presencia de un problema en un segmento puede romper el resto de los segmentos. Los repetidores no actúan como filtros para restringir el flujo del tráfico problemático.

Además, los repetidores pasarán una «tormenta» de difusión de un segmento al siguiente, y así a través de toda la red. Una «tormenta» de difusión se produce cuando el número de mensajes de difusión que aparece en la red es superior al límite del ancho de banda de la red. El rendimiento de la red va a disminuir cuando un dispositivo está respondiendo a un paquete que está continuamente circulando por la red o a un paquete que está continuamente intentando contactar con un sistema que nunca responde.

Implementación de un repetidor. Los pasos a considerar cuando se decide implementar repetidores en la red son:

- Conectar dos segmentos de medio similar o no similar.
- Regenerar la señal para incrementar la distancia transmitida.
- Pasar todo el tráfico en ambas direcciones.
- Conectar dos segmentos de la forma más efectiva en cuanto al costo.

Los repetidores mejoran el rendimiento dividiendo la red en segmentos y, por tanto, reduciendo el número de equipos por segmento.

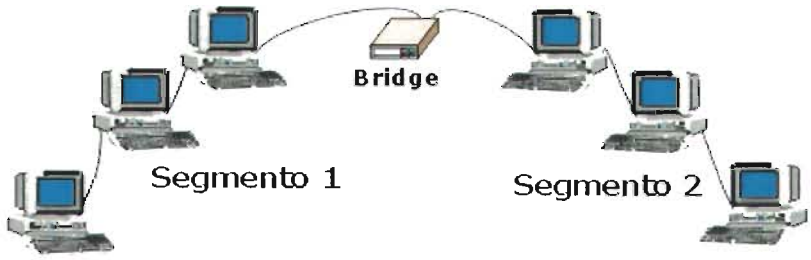
No utilice un repetidor cuando:

- Existe un tráfico de red altísimo.
- Los segmentos están utilizando diferentes métodos de acceso.
- Es necesario el filtrado de datos.

IV.5.- Bridges (Puentes).

Al igual que un repetidor, un bridge puede unir segmentos o grupos de trabajo LAN. Sin embargo, un bridge puede, además, dividir una red para aislar el tráfico o los problemas. Por ejemplo, si el volumen del tráfico de uno o dos equipos o de un departamento está sobrecargando la red con los datos y ralentizan todas las operaciones, el bridge podría aislar a estos equipos o al departamento.

Los Puentes ("Bridges") se pueden utilizar para:



- Extender la longitud de un segmento.
- Proporcionar un incremento en el número de equipos de la red.
- Reducir los cuellos de botella del tráfico resultante de un número excesivo de equipos conectados.
- Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo que la red sea más eficiente.
- Enlazar medios físicos diferentes como par trenzado y Ethernet coaxial.

Los bridges trabajan a nivel de enlace de datos del modelo de referencia OSI y, por tanto, toda la información de los niveles superiores no está disponible para ellos. Más que distinguir entre un protocolo y otro, los bridges pasan todos los protocolos que aparecen en la red. Todos los protocolos se pasan a través de los bridges, de forma que aparecen en los equipos personales para determinar los protocolos que pueden reconocer.

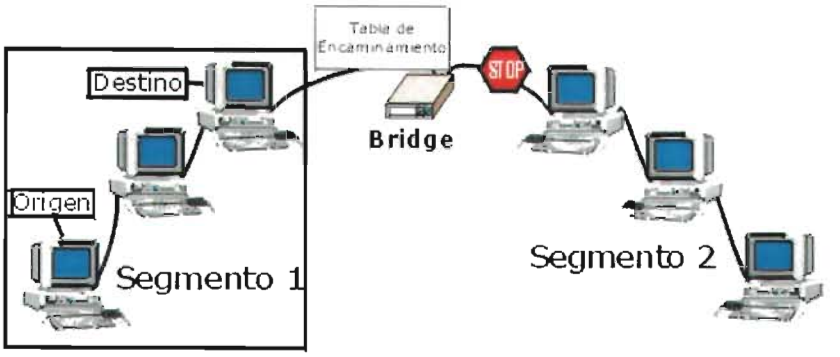
Los bridges trabajan en el nivel MAC y, por ello, algunas veces se conocen como bridges de nivel MAC.

Un bridge de nivel MAC:

- Escucha todo el tráfico.
- Comprueba las direcciones origen y destino de cada paquete.
- Construye una tabla de encaminamiento, donde la información está disponible.
- Reenvían paquetes de la siguiente forma:
    - Si el destino no aparece en la tabla de encaminamiento, el bridge reenvía el paquete a todos los segmentos.
    - Si el destino aparece en la tabla de encaminamiento, el bridge reenvía el paquete al segmento correspondiente (a menos que este segmento sea también el origen).

Un bridge funciona considerando que cada nodo de la red tiene su propia dirección. Un bridge reenvía paquetes en función de la dirección del nodo destino.

Realmente, los bridges tienen algún grado de inteligencia puesto que aprenden a dónde enviar los datos. Cuando el tráfico pasa a través del bridge, la información sobre las direcciones de los equipos se almacena en la RAM del bridge. El bridge utiliza esta RAM para generar una tabla de encaminamiento en función de las direcciones de origen.



Inicialmente, la tabla de encaminamiento del bridge está vacía. Cuando los nodos transmiten los paquetes, la dirección de origen se copia en la tabla de encaminamiento. Con esta información de la dirección, el bridge identifica qué equipos están en cada segmento de la red.

Creación de la tabla de encaminamiento. Los bridges generan sus tablas de encaminamiento en función de las direcciones de los equipos que han transmitido datos en la red. Los bridges utilizan, de forma específica, las direcciones de origen (dirección del dispositivo que inicia la transmisión) para crear una tabla de encaminamiento.

Cuando el bridge recibe un paquete, la dirección de origen se compara con la tabla de encaminamiento. Si no aparece la dirección de origen, se añade a la tabla. A continuación, el bridge compara la dirección de destino con la base de datos de la tabla de encaminamiento.

- Si la dirección de destino está en la tabla de encaminamiento y aparece en el mismo segmento de la dirección de origen, se descarta el paquete. Este filtrado ayuda a reducir el tráfico de la red y aislar segmentos de la red.

- Si la dirección de destino está en la tabla de encaminamiento y no aparece en el mismo segmento de la dirección de origen, el bridge envía el paquete al puerto apropiado que permite alcanzar la dirección de destino.

- Si la dirección de destino no está en la tabla de encaminamiento, el bridge envía el paquete a todos sus puertos, excepto al puerto desde donde se originó el envío.

Resumiendo, si un bridge conoce la localización del nodo de destino, envía el paquete a dicha localización. Si no conoce el destino, envía el paquete a todos los segmentos.

Segmentación del tráfico de red. Un bridge puede segmentar el tráfico mediante su tabla de encaminamiento. Un equipo en el segmento 1 (origen), envía datos a otro equipo (destino) también localizado en el segmento 1. Si la dirección de destino está en la tabla de encaminamiento, el bridge puede determinar que el equipo destino está también en el segmento 1. Dado que los equipos origen y destino están en el mismo segmento 1, se tiene que el paquete no se reenvía a través del bridge al segmento 2.

Por tanto, los bridges pueden utilizar las tablas de encaminamiento para reducir el tráfico de la red controlando los paquetes que se envían al resto de los segmentos. Este control (o restricción) del flujo del tráfico de red se conoce como «segmentación del tráfico de red».

Una red grande no está limitada a un solo bridge. Se pueden utilizar múltiples bridge para combinar diferentes redes pequeñas en una red más grande.

Los bridges tienen todas las características de los repetidores, pero también proporcionan más ventajas. Ofrecen mejor rendimiento de red que los repetidores. Las redes unidas por bridges se han dividido y, por tanto, un número menor de equipos compiten en cada segmento por los recursos disponibles.

Visto de otra forma, si una gran red Ethernet se dividió en dos segmentos conectados por un bridge, cada red nueva transportaría un número menor de paquetes, tendríamos menos colisiones y operaría de forma mucho más eficiente. Aunque cada red estaría separada, el bridge pasaría el tráfico apropiado entre ellas.

Un bridge puede constituir una pieza de equipamiento autónoma, independiente (un bridge externo) o se puede instalar en un servidor. Si el sistema operativo de red (NOS) lo admite, puede instalar una o más tarjetas de red (NIC) generando un bridge interno.

Su popularidad en grandes redes de debe a que:

- Son sencillos de instalar y transparentes a los usuarios.
- Son flexibles y adaptables.
- Son relativamente baratos.

IV.6.- Diferencias entre Bridge y Repetidor.

Los bridges trabajan a un nivel superior del Modelo OSI que los repetidores. Esto significa que los bridges tienen más inteligencia que los repetidores y pueden tener más características relativas a los datos en las cuentas.

Mientras que los bridges parecen repetidores en el sentido que pueden regenerar los datos, este proceso se lleva a cabo a nivel de paquete. Esto significa que los bridges pueden enviar paquetes sobre distancias más largas utilizando una variedad de medios de larga distancia.

IV.7.- Ruteadores, ("Routers").

En un entorno que está formado por diferentes segmentos de red con distintos protocolos y arquitecturas, el bridge podría resultar inadecuado para asegurar una comunicación rápida entre todos los segmentos. Una red de esta complejidad necesita un dispositivo que no sólo conozca las direcciones de cada segmento, sino también, que sea capaz de determinar el camino más rápido para el envío de datos y filtrado del tráfico de difusión en el segmento local. Este dispositivo se conoce como «router».

Los routers trabajan en el nivel de red del modelo de referencia OSI. Esto significa que pueden conmutar y encaminar paquetes a través de múltiples redes. Realizan esto intercambiando información específica de protocolos entre las diferentes redes. Los routers leen en el paquete la información de direccionamiento de las redes complejas teniendo acceso a información adicional, puesto que trabajan a un nivel superior del modelo OSI en comparación con los bridges.

Los routers pueden proporcionar las siguientes funciones de un bridge:

- Filtrado y aislamiento del tráfico.
- Conexión de segmentos de red.

Los routers tienen acceso a más información en los paquetes de la que tienen los bridges y utilizan esta información para mejorar la entrega de los paquetes. Los routers se utilizan en redes complejas puesto que proporcionan una mejor gestión del tráfico. Los routers pueden compartir con otro router el estado y la información de encaminamiento y utilizar esta información para evitar conexiones lentas o incorrectas.

IV.7.1.- ¿Cómo Funcionan los Ruteadores?

Los ruteadores mantienen sus propias tablas de encaminamiento, normalmente constituidas por direcciones de red; también se pueden incluir las direcciones de los hosts si la arquitectura de red lo requiere. Para determinar la dirección de destino de los datos de llegada, las tablas de encaminamiento incluyen:

- Todas las direcciones de red conocidas.
- Instrucciones para la conexión con otras redes.
- Los posibles caminos entre los routers.
- El costo de enviar los datos a través de estos caminos.

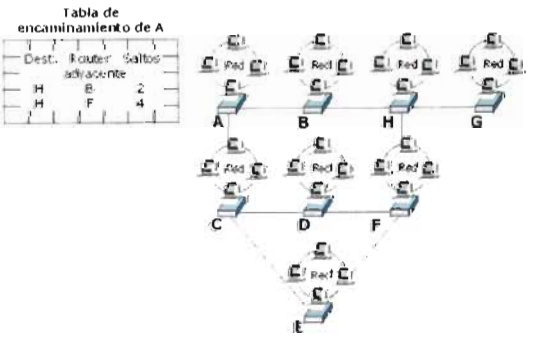
Un router utiliza sus tablas de encaminamiento de datos para seleccionar la mejor ruta en función de los caminos disponibles y del costo.

La tabla de encaminamiento que mantiene un bridge contiene las direcciones del subnivel MAC para cada nodo, mientras que la tabla de encaminamiento que mantiene un router contiene números de red. Aunque los fabricantes de ambos tipos de equipamiento han seleccionado utilizar el término «tabla de encaminamiento», tienen diferente significado para cada uno de los dispositivos.

Los routers requieren direcciones específicas. Entienden sólo los números de red que les permiten comunicarse con otros routers y direcciones NIC locales. Los routers no conversan con equipos remotos.

Cuando los routers reciben paquetes destinados a una red remota, los envían al router que gestiona la red de destino. En algunas ocasiones esto constituye una ventaja porque significa que los routers pueden:

- Segmentar grandes redes en otras más pequeñas.
- Actuar como barrera de seguridad entre los diferentes segmentos.
- Prohibir las «tormentas» de difusión, puestos que no se envían estos mensajes de difusión.



Los routers son más lentos que los bridges, puesto que deben realizar funciones complejas sobre cada paquete. Cuando se pasan los paquetes de router a router, se separan las direcciones de origen y de destino del nivel de enlace de datos y, a continuación, se vuelven a generar. Esto activa a un router para encaminar

desde una red Ethernet TCP/IP a un servidor en una red Token Ring TCP/IP.

Dado que los routers sólo leen paquetes direccionados de red, no permiten pasar datos corruptos a la red. Por tanto, al no permitir pasar datos corruptos ni tormentas de difusión de datos, los routers implican muy poca tensión en las redes.

Los routers no ven la dirección del nodo de destino, sólo tienen control de las direcciones de red. Los routers pasarán información sólo si conocen la dirección de la red.

Esta capacidad de controlar el paso de datos a través del router reduce la cantidad de tráfico entre las redes y permite a los routers utilizar estos enlaces de forma más eficiente que los bridges.

La utilización de un esquema de direccionamiento basado en router permite a los administradores poder dividir una gran red en muchas redes separadas, y dado que los routers no pasan e incluso controlan cada paquete, actúan como una barrera de seguridad entre los segmentos de la red. Esto permite reducir bastante la cantidad de tráfico en la red y el tiempo de espera por parte de los usuarios.

Protocolos que permiten encaminar. No todos los protocolos permiten encaminar.

Los protocolos que encaminan son:

- DECnet.
- Protocolo de Internet (IP).
- Intercambio de paquetes entre redes (IPX).
- OSI.
- Sistema de red de Xerox (XNS).
- DDP (Apple Talk).

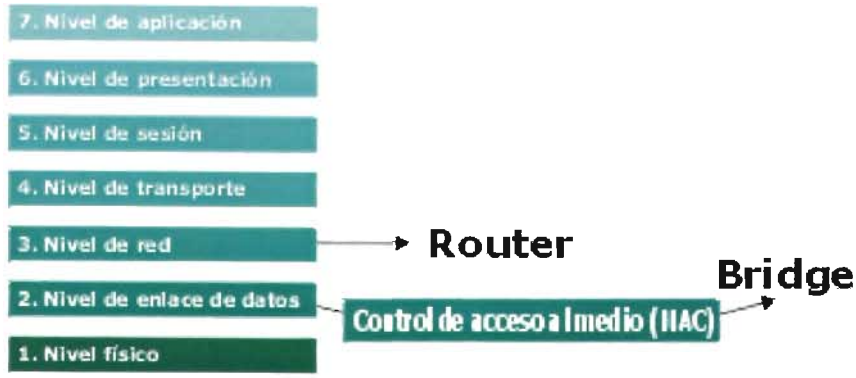
Los protocolos que no pueden encaminar son:

- Protocolo de transporte de área local (LAT), un protocolo de Digital Equipment Corporation.
- NetBEUI (Interfase de usuario extendida NetBIOS).

Los routers pueden utilizar en la misma red múltiples protocolos.

Selección de los caminos. A diferencia de los bridges, los routers pueden establecer múltiples caminos activos entre los segmentos LAN y seleccionar entre los caminos redundantes. Los routers pueden enlazar segmentos que utilizan paquetes de datos y acceso al medio completamente diferentes, permitiendo utilizar a los routers distintos caminos disponibles. Esto significa que si un router no funciona, los datos todavía se pueden pasar a través de routers alternativos.

Un router puede escuchar una red e identificar las partes que están ocupadas. Esta información la utiliza para determinar el camino sobre el que envía los datos. Si un camino está ocupado, el router identifica un camino alternativo para poder enviar los datos.



Un router decide el camino que seguirá el paquete de datos determinando el número de saltos que se generan entre los segmentos de red. Al igual que los bridges, los routers generan tablas de encaminamiento y las utilizan en los siguientes algoritmos de encaminamiento:

- **OSPF** («Primer camino abierto más corto») es un algoritmo de encaminamiento basado en el estado del enlace. Los algoritmos de estado de enlace controlan el proceso de encaminamiento y permiten a los routers responder rápidamente a modificaciones que se produzcan en la red.

- **RIP** (Protocolo de información de encaminamiento) utiliza algoritmos con vectores de distancia para determinar la ruta. El Protocolo de control de transmisión/Protocolo de Internet (TCP/IP) e IPX admite RIP.

- **NLSP** (Protocolo de servicios de enlace NetWare) es un algoritmo de estado de enlace a utilizar con IPX.

IV.7.2.-Tipos de Ruteadores.

Los tipos principales de routers son:

- **Estático**. Los ruteadores estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.

- **Dinámico**. Los ruteadores dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de instalación y configuración. Son más sofisticados que los ruteadores estáticos, examinan la información de otros ruteadores y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

Características de los dos tipos de ruteadores:

Ruteadores estáticos	Ruteadores dinámicos
Instalación y configuración manual de todos los routers	Configuración manual del primer ruteadores. Detectan automáticamente redes y routers adicionales.
Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento	Pueden seleccionar una ruta en función de factores tales como costo y cantidad del tráfico de enlace.

Ruteadores estáticos	Ruteadores dinámicos
Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.	Pueden decidir enviar paquetes sobre rutas alternativas.
Se consideran más seguros puesto que los administradores especifican cada ruta	Pueden mejorar la seguridad configurando manualmente el router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones.

IV.7.3.- Diferencias entre Puentes ("Bridges") y Ruteadores.

Los bridges y los routers se configuran para realizar las mismas cosas: enviar paquetes entre redes y enviar datos a través de los enlaces WAN, lo que plantea una cuestión importante: cuándo utilizar un bridge o cuando utilizar un router

El bridge, que trabaja en el subnivel MAC del nivel de enlace de datos del modelo OSI, utiliza sólo la dirección del nodo. Para ser más específicos, un bridge trata de localizar una dirección del subnivel MAC en cada paquete. Si el bridge reconoce la dirección, mantiene el paquete o lo reenvía al segmento apropiado. Si el bridge no reconoce la dirección, envía el paquete a todos los segmentos excepto al segmento del cual ha partido el paquete.

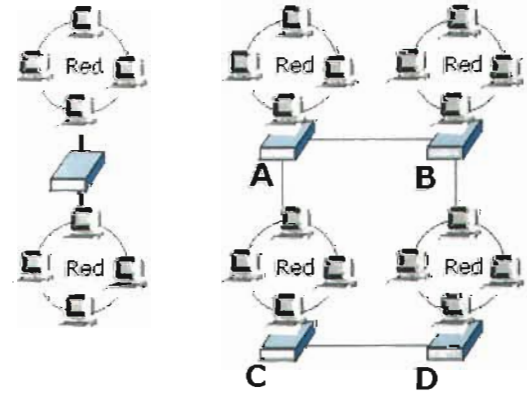
Primero, el bridge reconoce o no la dirección del subnivel MAC del paquete y, a continuación, envía el paquete.

Difusión. El envío de paquetes es la clave para entender las diferencias que plantean los bridges y los routers. Con los bridges, los datos de difusión enviados se dirigen a cada equipo desde todos los puertos del bridge, excepto desde el puerto a través del cual ha llegado el paquete. Es decir, cada equipo de todas las redes (excepto la red local a partir de la cual se ha generado la difusión) recibe un paquete de difusión. En las redes pequeñas esto puede que no tenga mucho impacto, pero en una red grande se puede generar el suficiente tráfico de difusión que provoque una bajada de rendimiento de la red, incluso filtrando las direcciones de la misma.

El router, que trabaja a nivel de red y tiene en cuenta más información que el bridge, determinando no sólo qué enviar, sino también dónde enviarlo. El router reconoce no sólo una dirección, al igual que el bridge, sino también un tipo de protocolo. De forma adicional, el router puede identificar las direcciones de otros routers y determinar los paquetes que se envían a otros routers.

Múltiples caminos. Un bridge sólo puede reconocer un único camino entre las redes. Un router puede buscar diferentes caminos activos y determinar en un momento determinado cuál resulta más adecuado.

Si un router A realiza una transmisión que necesita enviarse al router D, puede enviar el mensaje al router C o al B, y el mensaje será enviado al router D. Los routers tienen la posibilidad de evaluar ambos caminos y decidir la mejor ruta para esta transmisión.



Bridge Router

Conclusión. Cuatro son los aspectos que ayudan a distinguir las diferencias entre un bridge y un router, y determinar la opción más apropiada en una determinada situación:

- El bridge reconoce sólo las direcciones locales a subnivel MAC (las direcciones de las NIC en su propio segmento). Los routers reconocen direcciones de red.
- El bridge difunde (envía) todo lo que no reconoce y lo envía a todas las direcciones que controla, pero sólo desde el puerto apropiado.
- El router trabaja sólo con protocolos encaminables.
- El router filtra las direcciones. Envía protocolos particulares a direcciones determinadas (otros routers).

IV.7.4.- B-routers.

Un B-router combina las cualidades de un bridge y un router. Un B-router puede actuar como un router para un protocolo y como un bridge para el resto.

Los B-routers pueden:

- Encaminar protocolos encaminables seleccionados.
- Actuar de bridge entre protocolos no encaminables.
- Proporcionar un mejor costo y gestión de interconexión que el que proporcionan los bridges y routers por separado.

IV.8.- Gateways.

Los gateways activan la comunicación entre diferentes arquitecturas y entornos. Se encargan de empaquetar y convertir los datos de un entorno a otro, de forma que cada entorno pueda entender los datos del otro entorno. Un gateway empaqueta información para que coincida con los requerimientos del sistema destino. Los gateways pueden modificar el formato de un mensaje para que se ajuste al programa de aplicación en el destino de la transferencia. Por ejemplo, los gateways de correo electrónico, como el X.400, reciben mensajes en un formato, los formatean y envían en formato X.400 utilizado por el receptor, y viceversa.

Un gateway enlaza dos sistemas que no utilizan los mismos:

- Protocolos de comunicaciones.
- Estructuras de formateo de datos.
- Lenguajes.
- Arquitectura.

Los gateways interconectan redes heterogéneas; por ejemplo, pueden conectar un servidor Windows NT de Microsoft a una Arquitectura de red de los sistemas IBM (SNA). Los gateways

modifican el formato de los datos y los adaptan al programa de aplicación del destino que recibe estos datos.

Los gateways son de tarea específica. Esto significa que están dedicados a un tipo de transferencia. A menudo, se referencian por su nombre de tarea (gateway Windows NT Server a SNA).

Un gateway utiliza los datos de un entorno, desmantela su pila de protocolo anterior y empaqueta los datos en la pila del protocolo de la red destino.

Para procesar los datos, el gateway:

- Desactiva los datos de llegada a través de la pila del protocolo de la red.
- Encapsula los datos de salida en la pila del protocolo de otra red para permitir su transmisión.

Algunos gateways utilizan los siete niveles del Modelo OSI, pero, normalmente, realizan la conversión de protocolo en el nivel de aplicación. No obstante, el nivel de funcionalidad varía ampliamente entre los distintos tipos de gateways.

Una utilización habitual de los gateways es actuar como traductores entre equipos personales y miniequipos o entornos de grandes sistemas. Un gateway en un host que conecta los equipos de una LAN con los sistemas de miniequipo o grandes entornos (mainframe) que no reconocen los equipos conectados a la LAN.

En un entorno LAN normalmente se diseña un equipo para realizar el papel de gateway. Los programas de aplicaciones especiales en los equipos personales acceden a los grandes sistemas comunicando con el entorno de dicho sistema a través del equipo gateway. Los usuarios pueden acceder a los recursos de los grandes sistemas sólo cuando estos recursos están en sus propios equipos personales.

Normalmente, los gateways se dedican en la red a servidores. Pueden utilizar un porcentaje significativo del ancho de banda disponible para un servidor, puesto que realizan tareas que implican una utilización importante de recursos, tales como las conversiones de protocolos. Si un servidor gateway se utiliza para múltiples tareas, será necesario adecuar las necesidades de ancho de banda y de RAM o se producirá una caída del rendimiento de las funciones del servidor.

Los gateways se consideran como opciones para la implementación, puesto que no implican una carga importante en los circuitos de comunicación de la red y realizan, de forma eficiente, tareas muy específicas.

IV.9.- Servicios de Conexión.

Proveedores de servicios *(carriers).*

Un módem no sirve para nada a menos que pueda comunicarse con otro equipo. Toda la comunicación vía módem tiene lugar sobre algunos tipos de líneas o cableado de comunicaciones. Decidir el tipo de cable así como los proveedores y sus servicios relacionados, marca la diferencia en cuanto costo y rendimiento en una red.

Es difícil y costoso desplazar datos rápidamente sobre grandes distancias. Los tres factores que debe tener en cuenta un administrador cuando considera la implementación de las comunicaciones vía módem son:

- Rendimiento total.
- Distancia.
- Costo.

Necesita aplicar estos factores cuando decida qué tipo de líneas telefónicas se instalan en la red.

Líneas telefónicas

Están disponibles dos tipos de líneas telefónicas para las comunicaciones vía módem:

- **Líneas de llamada:** Las líneas de llamada son las líneas telefónicas habituales. Son lentas, requieren que los usuarios realicen, de forma manual, una conexión para cada comunicación y pueden no resultar fiables para la transmisión de datos. No obstante, para algunas empresas resulta práctico para la transferencia de archivos y actualización de las bases de datos utilizar, de forma temporal, un enlace de comunicación de llamada entre los sitios durante un determinado período de tiempo al día. Los proveedores de servicios están continuamente mejorando el servicio de las líneas de llamada. Algunas líneas digitales admiten velocidades de transmisión de datos de hasta 56 Kbps utilizando corrección de errores, compresión de datos y módems síncronos.

- **Líneas alquiladas (dedicadas):** Las líneas alquiladas o dedicadas proporcionan conexiones dedicadas a tiempo completo y no utilizan una serie de conmutadores para completar la conexión. La calidad de esta línea es, a menudo, superior a la calidad de la línea telefónica diseñada para la transmisión de voz únicamente. El rango de velocidad de estas líneas va desde los 56 Kbps hasta por encima de los 45 Mbps. La mayoría de los proveedores de servicios de larga distancia utilizan circuitos conmutados para proporcionar un servicio similar a una línea dedicada. Tenemos, por tanto, las «redes privadas virtuales» (VPN; *Virtual Private Network)*

Servicio de acceso remoto (RAS).

Frecuentemente, las empresas necesitan poder comunicarse más allá de los límites que establece una única red. La mayoría de los sistemas operativos de red proporcionan, para lograr este objetivo, un servicio denominado Servicio de acceso remoto (RAS). Para establecer una conexión remota, se requieren dos servicios: RAS y un servicio de cliente conocido como conexión de llamada (DUN; *Dial-Up Networkin).* El servidor o la estación de trabajo utiliza RAS para conectar los equipos remotos a la red por medio de una conexión de llamada a través de un módem. Los equipos remotos utilizan DUN, la otra parte del servicio, para conectarse al servidor RAS. Estos dos servicios juntos proporcionan la capacidad de extender una red y pueden realmente convertir una LAN en una WAN. Un servidor RAS, a menudo, actúa para su red como una interfaz de Internet, puesto que muchos proveedores de servicios de Internet utilizan acceso por líneas telefónicas.

Los equipos separados y las LAN se pueden conectar entre ellos a través de la red telefónica pública conmutada, de redes de conmutación de paquetes o, a través de la red digital de servicios integrados.

Una vez que el usuario ha realizado una conexión, la línea telefónica se hace transparente (invisible al usuario), y los usuarios en los clientes remotos pueden acceder a todos los recursos de la red de la misma forma que accederían si estuvieran sentados delante de sus equipos en la red.

IV.10.- Conexiones RAS

La conexión física a un servidor RAS se puede realizar utilizando diferentes medios:

- **Red telefónica pública conmutada (PSTN)**. Este servicio es conocido como el sistema telefónico público.
- **X.25**. Este servicio de red de conmutación de paquetes se puede utilizar para realizar conexiones de llamada o directas.
- **Red digital de servicios integrados (RDSI)**. Este servicio proporciona acceso remoto de alta velocidad, pero a un costo superior que una conexión de llamada. Una conexión RDSI requiere una tarjeta RDSI en lugar de un módem.

IV.10.1.- Protocolos RAS.

RAS admite tres protocolos de conexión.

- **SLIP *(Serial Line Interfaz Protocol).*** Es el primero y data de 1984. Tiene un número de limitaciones. SLIP no admite direccionamiento IP dinámico o los protocolos NetBEUI o IPX, no puede cifrar la información de la entrada en el sistema y sólo lo admiten los clientes RAS.
- **PPP *(Point to Point Protocol).*** superan muchas de las limitaciones de SLIP. Además de TCP/IP, admiten los protocolos IPX, NetBEUI, Apple Talk y DECnet. Por otro lado, también admiten contraseñas cifradas.
- **PPTP *(Point to Point Tuneling Protocol)***. El Protocolo de encapsulación punto a punto (PPTP) constituye una parte esencial de la tecnología VPN. Al igual que PPP, no establece diferencias entre los protocolos. PPTP proporciona transmisiones seguras a través de redes TCP/IP puesto que las conexiones son cifradas. Esto permite activar enlaces seguros en Internet.

IV.10.2.- RAS y Seguridad.

Los métodos actuales que permiten garantizar la seguridad en el acceso remoto pueden variar con el sistema operativo. Las funciones de seguridad RAS incluyen:

- **Auditoria**. Se puede mantener un seguimiento de auditoria que identifique los usuarios y los momentos de conexión al sistema.
- **Retrollamada**. RAS se puede configurar para generar una llamada al host que está solicitando una conexión y se puede restringir la lista de estos números de teléfonos de los host para evitar el uso no autorizado del sistema.
- **Host de seguridad**. Un host de seguridad puede requerir pasos de autenticación adicionales, además de los que existen en la red donde se encuentra el host.

- **Filtrado PPTP**. Este proceso de filtrado puede evitar el procesamiento de todos los paquetes, excepto PPTP. Proporciona una transferencia segura de datos sobre VPN, evitando que los intrusos puedan acceder al servidor.

IV.10.3.- Instalación de RAS.

Para planificar una instalación RAS, comenzamos por obtener la documentación apropiada sobre la red y sus usuarios. La información que necesitará incluye:

- Especificaciones, controladores y configuraciones del módem (necesitará un módem que admita RAS).
- Tipo de puerto de comunicaciones a configurar.
- Si la conexión será de llamada de entrada, llamada de salida o ambas.
- Protocolos de los clientes.
- Requerimientos de seguridad.

IV.10.4.- Configuración del RAS.

El RAS se tiene que configurar una vez instalado. Prepárese para configurar los puertos de comunicaciones, protocolos de red y cifrado RAS.

Configuración de redes de llamada. Se deben configurar estas conexiones cuando el servidor se va a utilizar para llamar a otras redes, a Internet o a otros equipos. El método de configuración depende de los sistemas operativos de red y del equipo en uso.

IV.10.5.- Limitaciones del RAS.

La utilización de una conexión RAS no constituye siempre la mejor opción para conseguir la expansión de una red. No obstante, proporciona muchas posibilidades y oportunidades no disponibles en otros casos. Es importante tener claro cuándo seleccionar RAS o cuándo elegir una opción diferente.

Utilice RAS si los requerimientos de ancho de banda no son superiores a 128 Kbps, si no requiere una conexión a tiempo completo o si debe mantener costos de sistemas bajos. No utilice RAS si necesita un ancho de banda superior al proporcionado por un módem asíncrono o si necesita una conexión a tiempo completo dedicada.

Protocolo de encapsulación punto a punto (PPTP).

Este protocolo admite múltiples protocolos VPN. Este soporte permite a los clientes remotos conectar y acceder a redes de organizaciones seguras vía Internet. Utilizando PPTP, el cliente remoto establece una conexión al servidor RAS sobre Internet utilizando PPTP.

PPTP proporciona la forma de encaminar paquetes de los protocolos IP, IPX o del protocolo punto a punto NetBEUI sobre una red TCP/IP. La encapsulación de estos paquetes de protocolos distintos, permite enviar cualquiera de estos paquetes a través de una red TCP/IP. Esta WAN virtual se genera a partir de redes públicas tales como Internet.

Introducción a las WAN

A pesar de que las LAN funcionan bien, tienen limitaciones físicas y de distancia. Dado que las redes LAN no resultan adecuadas para todas las comunicaciones previstas en la empresa, éstas deben ser capaces de conectar las LAN con otros tipos de entornos para asegurar el acceso a los servicios de comunicaciones completos.

La utilización de componentes tales como bridges o routers, junto con los proveedores de servicios de comunicaciones, permite que una LAN se pueda expandir a partir de un proceso de expansión que permite a un área local poder cubrir una red de área extensa admitiendo comunicaciones a nivel de estado, de país, o incluso, a nivel mundial. Para el usuario, la WAN es transparente y parece similar a una red de área local. Una WAN no se puede distinguir de una LAN cuando se ha implementado de forma apropiada.

La mayoría de las WAN son combinaciones de LAN y otros tipos de componentes conectados por enlaces de comunicaciones denominados «enlaces WAN». Los enlaces WAN pueden incluir:

- Redes de conmutación de paquetes.
- Cables de fibra óptica.
- Transmisores de microondas.
- Enlaces de satélite.
- Sistemas coaxiales de televisión por cable.

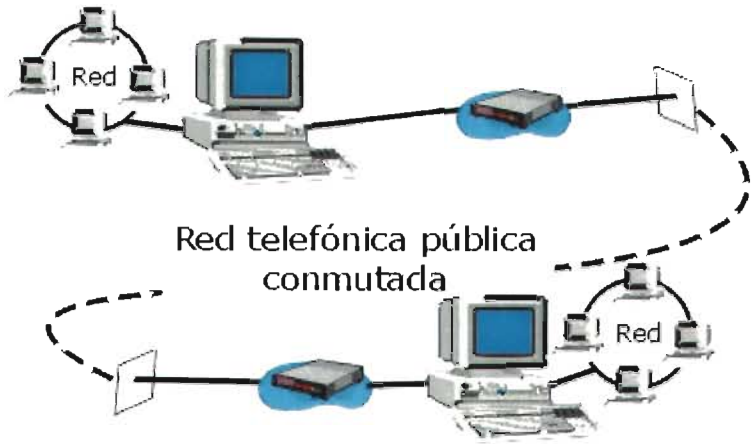
Los enlaces WAN, tales como las conexiones telefónicas de área extensa, son demasiado caros y complejos de comprar, implementar y mantener para la mayoría de las empresas y, normalmente, se opta por alquilar a los proveedores de servicios.

Las comunicaciones entre las LAN supondrán algunas de las siguientes tecnologías de transmisión:

- Analógica.
- Digital.
- Conmutación de paquetes.

Conectividad analógica

La misma red que utiliza nuestro teléfono está disponible para los equipos. El nombre de esta red mundial es la Red telefónica pública conmutada (PSTN). En el marco de la informática, podemos pensar en PSTN como un gran enlace WAN que ofrece líneas telefónicas de llamada de grado de voz.



Conexiones de redes a través de módems

Líneas de llamada.

El hecho de que PSTN fuese diseñada principalmente para la comunicación de voz hace que sea lenta. Las líneas analógicas de llamada requieren módems que pueden incluso hacerlas más lentas todavía. Por otro lado, la calidad de la conexión es inconsistente debido a que PSTN es una red de circuitos conmutados. Cualquier sesión de comunicación única será tan buena como los circuitos enlazados para esta sesión determinada. Sobre largas distancias, por ejemplo, país a país, pueden resultar considerablemente inconsistentes en los circuitos de una sesión a la siguiente.

Líneas analógicas dedicadas

A diferencia de las líneas de llamada que deben volver a abrir la sesión cada vez que se utilizan, las líneas analógicas dedicadas (o alquiladas) se mantienen abiertas en todo momento. Una línea analógica alquilada es más rápida y fiable que una conexión de llamada. Sin embargo, es relativamente cara puesto que el proveedor de servicio está dedicando recursos a la conexión alquilada, independientemente de si se está utilizando la línea o no.

¿De llamada o dedicada?

Ningún tipo de servicio es el mejor para todos los usuarios. La mejor opción dependerá de un número de factores destacando:

- La cantidad de tiempo de conexión que se utilizará.
- El costo del servicio.
- La importancia de tener tasas de transferencia de datos superiores y más fiable que una línea condicionada.
- La necesidad de tener una conexión 24 horas al día.

Si no es frecuente la necesidad de establecer la conectividad, pueden resultar más adecuadas las líneas de llamada. Si es necesario una conexión de alto nivel de fiabilidad y de utilización continua, entonces no resulta adecuada la calidad del servicio que proporciona una línea de llamada.

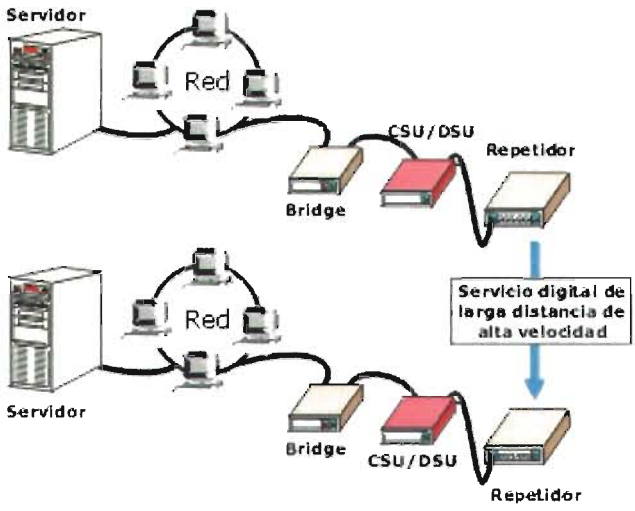
Conectividad digital.

En algunos casos, las líneas analógicas proporcionan conectividad suficiente. No obstante, cuando una organización genera demasiado tráfico WAN, se tiene que el tiempo de transmisión hace que la conexión analógica sea ineficiente y costosa.

Las organizaciones que requieren un entorno más rápido y seguro que el proporcionado por las líneas analógicas, pueden cambiar a las líneas de servicios de datos digitales (DDS). DDS proporciona comunicación síncrona punto a punto a 2.4, 4.8, 9.6 o 56 Kbps. Los circuitos digitales punto a punto son dedicados y suministrados por diferentes proveedores de servicio de telecomunicaciones. El proveedor de servicio garantiza ancho de banda completo en ambas direcciones configurando un enlace permanente desde cada punto final a la LAN.

La principal ventaja de las líneas digitales es que proporcionan una transmisión cerca del 99 por 100 libre de errores. Las líneas digitales están disponibles de diversas formas, incluyendo DDS, T1, T3, T4 y Switched-56.

No se requiere módem puesto que DDS utiliza comunicación digital. En su lugar, DDS envía datos desde un bridge o router a través de un dispositivo denominado Unidad de servicio de canales/Unidad de servicio de datos (CSU/DSU; *Channel Service Unit/Data Service Unit)*. Este dispositivo convierte las señales digitales estándar que genera el ordenador en el tipo de señales digitales (bipolar) que forman parte del entorno de comunicación síncrona. Además, contiene la electrónica suficiente para proteger la red del proveedor de los servicios DDS.



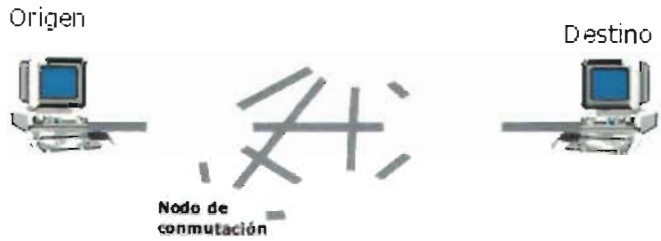
Servicio T1

Para velocidades de datos muy altas, el servicio T1 es el tipo de línea digital más utilizado. Se trata de una tecnología de transmisión punto a punto que utiliza dos pares de hilos (un par para enviar y otro para recibir) para transmitir una señal en ambos sentidos (full-duplex) a una velocidad de 1,544 Mbps. T1 se utiliza para transmitir señales digitales de voz, datos y vídeo.

Las líneas T1 están entre las más caras de todos los enlaces WAN. Los abonados que ni necesitan ni pueden generar el ancho de banda de una línea T1 pueden abonarse a uno a más canales T1 con incrementos de 64 Kbps, conocido como Fractional T-1 (FT-1).

Multiplexación. Desarrollado por los Laboratorios Bell, T1 utiliza la tecnología denominada *multiplexación.* Diferentes señales de distintas fuentes se reúnen en un componente denominado multiplexor y se envían por un cable para la transmisión. En el punto destino de recepción, los datos se convierten en su formato original. Esta perspectiva surgió cuando se saturaban los cables telefónicos que transportaban sólo una conversión por cable. La solución al problema, denominada red T-Portadora, permitió a los Laboratorios Bell transportar muchas llamadas sobre un cable.

División del canal. Un canal T1 puede transportar 1,544 megabits de datos por segundo, la unidad básica de un servicio T-Portadora. T1 la divide en 24 canales y muestrea cada canal 8.000 veces por segundo. Con este método, T1 permite 24 transmisiones simultáneas de datos sobre cada par de dos hilos.



Cada muestra del canal incorpora ocho bits. Cada uno de los 24 canales puede transmitir a 64 Kbps puesto que cada canal se muestrea 8.000 veces por segundo. Este estándar de velocidad de datos se conoce como DS-0. La velocidad de 1,544 Mbps se conoce como DS-1.

Las velocidades de DS-1 se pueden multiplexar para proporcionar incluso velocidades de transmisión superiores, conocidas como DS-1C, DS-2, DS-3 y DS-4. La siguiente tabla muestra las correspondientes velocidades de transmisión:

Nivel de señal	Sistema de portadora	Canales T-1	Canales de voz	Velocidad de datos (Mbps)
DS-0	N/A	N/A	1	0,064
DS-1	T1	1	24	1,544
DS-1C	T-1C	2	48	3,152
DS-2	T2	4	96	6,312
DS-3	T3	28	672	44,736
DS-4	T4	168	4.032	274,760

Servicio T3.

Los servicios de líneas alquiladas T3 y Fractional T3 proporcionan servicios de datos y voz desde 6 Mbps hasta 45 Mbps. Ofrecen los servicios de líneas alquiladas de más altas posibilidades disponibles hoy en día. T3 y FT-3 se diseñan para el transporte de grandes volúmenes de datos a alta velocidad entre dos puntos fijos. Una línea T3 se puede utilizar para reemplazar diferentes líneas T1.

Servicio Switched-56.

Las compañías telefónicas de larga y pequeña distancia ofrecen el servicio Switched-56, un servicio de llamada digital LAN a LAN que transmite los datos a 56 Kbps. Realmente, Switched-56 es una versión de circuito conmutado de una línea DDS a 56 Kbps. La ventaja de Switched-56 es que se utiliza por demanda, eliminando, por tanto, el costo de una línea dedicada. Cada equipo que utiliza este servicio debe estar equipado con una CSU/DSU que pueda llamar a otro sitio Switched-56.

Redes de conmutación de paquetes

La tecnología de paquetes se utiliza para transmitir datos sobre grandes áreas como ciudades, estados o países. Se trata de una tecnología rápida, conveniente y fiable. Las redes que envían paquetes procedentes de diferentes usuarios con muchos posibles caminos distintos, se denominan «redes de conmutación de paquetes» debido a la forma en la que empaquetan y encaminan los datos.

El paquete de datos original se divide en paquetes y cada paquete se etiqueta con una dirección de destino además de otra información. Esto permite enviar cada paquete de forma separada a través de la red.

En la conmutación de paquetes, éstos se transmiten por medio de las estaciones de una red de equipos a través de la mejor ruta existente entre el origen y destino.

Cada paquete se conmuta de forma separada. Dos paquetes de los mismos datos originales pueden seguir caminos completamente diferentes para alcanzar el mismo destino. Los caminos de datos seleccionados por los paquetes individuales se basan en la mejor ruta abierta en cualquier instante determinado.

El ordenador receptor es capaz de volver a generar el mensaje original, incluso cuando cada paquete viaja a lo largo de un camino diferente y los paquetes que componen el mensaje llegan en diferentes intervalos de tiempo o fuera de secuencia.

Los conmutadores dirigen los paquetes a través de los posibles caminos o conexiones. Estas redes, a menudo, se denominan conexiones muchos a muchos. Los intercambios en la red leen cada paquete y los envían utilizando la mejor ruta disponible en ese momento.

El tamaño del paquete debe ser pequeño. Si aparece un error en la transmisión, la retransmisión de un paquete pequeño es más fácil que la retransmisión de un paquete grande. Además, los paquetes pequeños ligan conmutadores sólo para cortos períodos de tiempo.

La utilización de las redes de conmutación de paquetes para enviar datos es similar a enviar inmensas cantidades de mercancías mediante camiones en lugar de cargar todas las mercancías en un tren. Si se produce un problema con la mercancía de un camión, es más fácil arreglar o recargar esta mercancía que el problema que se puede originar si el tren descarrila. Además, los caminos no conectan cruces o intersecciones (conmutadores) como lo hacen los trenes.

Las redes de conmutación de paquetes son rápidas y eficientes. Para gestionar las tareas de encaminamiento del tráfico y ensamblaje y desensamblaje de los paquetes, estas redes requieren algún componente inteligente por parte de los equipos y el software que controle la entrega. Las redes de conmutación de paquetes resultan económicas, puesto que ofrecen líneas de alta velocidad sobre la base de pago por transacción en lugar de hacerlo con una tarifa plana.

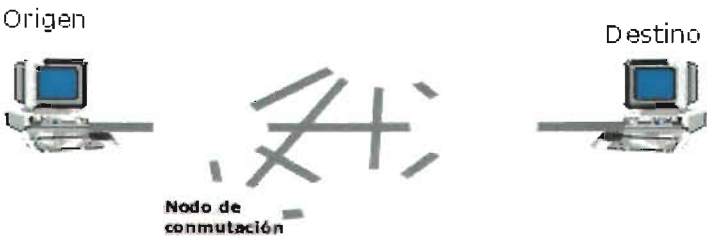
Circuitos virtuales.

Muchas de las redes de conmutación de paquetes utilizan *circuitos virtuales*. Se tratan de circuitos compuestos por una serie de conexiones lógicas entre el equipo emisor y el equipo receptor. El circuito cuyo ancho de banda se asigna por demanda no es un cable actual o permanente entre dos estaciones. La conexión se realiza después de que ambos equipos intercambien información y estén de acuerdo en los parámetros de la comunicación que establecen y mantienen la conexión. Estos parámetros incluyen el tamaño máximo de mensaje y el camino que tomarán los datos.

Los circuitos virtuales incorporan los siguientes parámetros de comunicaciones para asegurar la fiabilidad:

- Reconocimientos.
- Control de flujo.
- Control de errores.

Los circuitos virtuales pueden durar tanto como dura la conversación (temporal) o como la comunicación entre los equipos (permanente).



Circuitos virtuales conmutados (SVC). En los circuitos virtuales conmutados (SVC), la conexión entre los equipos de destino utiliza una ruta específica a través de la red. Los recursos de la red se dedican al circuito y se mantiene la ruta hasta que se termine la conexión. Se conocen como conexiones punto a muchos puntos.

Circuitos virtuales permanentes (PVC). Los circuitos virtuales permanentes (PVC) son similares a las líneas alquiladas. Son, por tanto, permanentes y virtuales, excepto que el cliente paga sólo por el tiempo que utiliza la línea.

Envío de datos a través de una WAN

Existen otros tipos de tecnología más avanzado con mayor ancho de banda, como:

- X.25.
- Frame Relay.
- Modo de transferencia asíncrono (ATM).
- Red digital de servicios integrados (RDSI).
- Interfase de datos de fibra distribuida (FDDI).
- Red óptica síncrona (SONET).
- Servicio de datos multimegabit conmutado (SMDS).

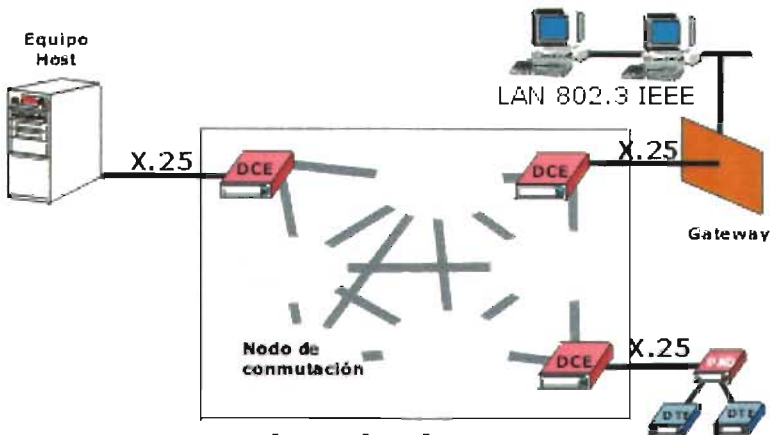
IV.11.- X.25.

X.25 es un conjunto de protocolos incorporados en una red de conmutación de paquetes. La red de conmutación de paquetes se originó a partir de los servicios de conmutación inicialmente utilizados para conectar terminales remotos a sistemas host basados en grandes entornos.

Una red de conmutación de paquetes X.25 utiliza conmutadores, circuitos y routers para proporcionar la mejor ruta en cualquier momento. A menudo, estos componentes (conmutadores, circuitos y routers) se describen como nubes, puesto que cambian rápidamente dependiendo de las

necesidades y disponibilidad. Estas nubes se utilizan para especificar la idea de situación cambiante o no existencia de un conjunto estándar de circuitos.

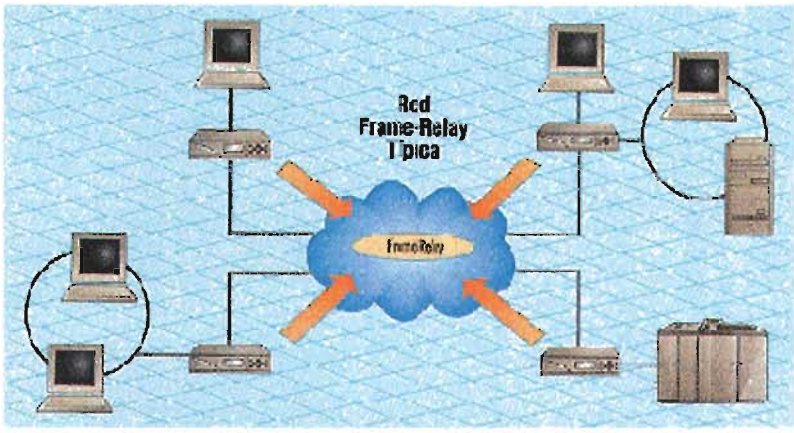
Las primeras redes X.25 utilizaban las líneas telefónicas para transmitir los datos. Se trataba de un medio no fiable que generaba bastantes errores, provocando que X.25 incorporase una amplia comprobación de errores. X.25 puede parecer demasiado lenta, debido precisamente a toda la comprobación de errores y la retransmisión.



Ejemplo de DTE

Hoy en día, el protocolo X.25 define la interfase entre un host u otro dispositivo en modo conmutación de paquetes y la red pública de datos (PDN) sobre un circuito de línea alquilada o dedicada. Se trata de una interfaz de equipamiento de terminal de datos/equipamiento de comunicaciones de datos (DTE/DCE).

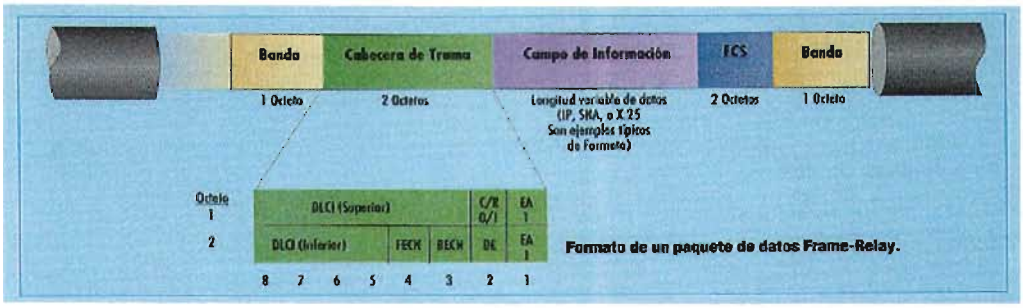
Ejemplos de DTE incluyen:



- Un equipo host con una interfaz X.25.
- Un ensamblador/desensamblador de paquetes (PAD) que recibe caracteres asíncronos introducidos desde un terminal a baja velocidad y los ensambla en paquetes para ser transmitidos a través de la red. Además, el PAD desempaqueta los paquetes recibidos de la red, de forma que los datos se pueden entregar como caracteres a los terminales.
- Un gateway entre la PDN y una LAN o WAN.

IV.12.- Frame Relay.

Frame Relay se trata de una tecnología avanzada de conmutación de paquetes, digital y de longitud variable en los paquetes. Con esta tecnología, los diseñadores han eliminado muchas de las funciones de registro y comprobación que no son necesarias en un entorno de fibra óptica más seguro y fiable.



Frame Relay es un sistema punto a punto que utiliza PVC para transmitir tramas de longitud variable en el nivel de enlace de datos. Los datos viajan desde una red sobre una línea digital alquilada hasta un conmutador de datos en una red Frame Relay. Pasan a través de la red Frame Relay y llegan a la red de destino.

Las redes Frame Relay se utilizan bastante, puesto que realizan de forma más rápida las operaciones básicas de conmutación de paquetes con respecto a otros sistemas de conmutación. Esto es debido a que Frame Relay utiliza PVC, lo que permite conocer el camino completo desde el origen hasta el final. Los dispositivos de Frame Relay no tienen la necesidad de realizar el ensamblaje y desensamblaje de los paquetes o proporcionar la mejor ruta.

Además, las redes Frame Relay proporcionan a los abonados el ancho de banda a medida que lo necesitan, permitiendo al cliente cualquier tipo de transmisión.

La tecnología Frame Relay requiere un router o bridge que admita Frame Relay para transmitir los datos con éxito a través de la red. Un router Frame-Relay necesita, al menos, un puerto WAN para una conexión a una red Frame Relay y otro puerto para la LAN.

IV.13.- Modo de Transferencia Asíncrono (ATM).

El Modo de Transferencia Asíncrono es una implementación avanzada de conmutación de paquetes que proporciona tasas de transmisión de datos de alta velocidad para enviar paquetes de tamaño fijo a través de LAN o WAN de banda amplia o banda base. ATM permite:

- Voz.
- Datos.
- Fax.
- Vídeo en tiempo real.
- Audio en calidad CD.
- Imágenes.
- Transmisión de datos multimegabit.

La CCITT definió ATM en 1988 como parte de la Red digital de servicios integrados de banda amplia (BISDN). Debido a la potencia y versatilidad de ATM, tiene una gran influencia en el desarrollo de las comunicaciones en red. Se adapta igualmente a entornos WAN que LAN y puede transmitir datos a muy altas velocidades (desde 155 Mbps hasta 622 Mbps o más).

IV.14.- Tecnología ATM.

ATM es un método de transmisión de celdas de banda amplia que transmite datos en celdas de 53 bytes en lugar de utilizar tramas de longitud variable. Estas celdas están constituidas por 48 bytes de información de aplicaciones y cinco bytes adicionales que incorporan información de la cabecera ATM. Por ejemplo, ATM dividirá un paquete de 1,000 bytes en 21 tramas de datos y colocará cada trama de datos en una celda. El resultado es una tecnología que transmite un paquete uniforme y consistente.

El equipamiento de la red puede conmutar, encaminar y desplazar tramas de tamaño uniforme más rápidamente que cuando se utilizan tramas de tamaño variable. La celda consistente y de tamaño estándar utiliza, de forma eficiente, búferes y reduce el trabajo necesario relativo al procesamiento de los datos de llegada. El tamaño uniforme de la celda también ayuda en la planificación del ancho de banda para las aplicaciones.

Teóricamente, ATM puede ofrecer tasas de rendimiento total de hasta 1.2 gigabits por segundo. Actualmente, no obstante, ATM mide su velocidad frente a las velocidades de la fibra óptica que pueden alcanzar hasta los 622 Mbps.

ATM se puede utilizar con la misma velocidad aproximadamente en las WAN y en las LAN. ATM para la implementación de una gran área, transmite sobre proveedores de servicio como AT&T y Sprint. Esto permite crear un entorno consistente que acaba con el concepto de WAN lenta y con las diferentes tecnologías utilizadas en los entornos LAN y WAN.

IV.14.1.- Componentes ATM.

Los componentes ATM están disponibles actualmente sólo para un número limitado de fabricantes. Todo el hardware en una red ATM debe ser compatible con ATM. La implementación de ATM en un entorno existente requerirá un amplio reemplazamiento del equipamiento. Ésta es una razón de por qué no se ha adoptado más rápidamente ATM.

Sin embargo, conforme madure el mercado de ATM, diferentes fabricantes serán capaces de proporcionar:

- Routers y conmutadores para conectar servicios de portadora sobre un esquema global.
- Dispositivos de enlace central para conectar todas las LAN dentro de una gran organización.
- Conmutadores y adaptadores que enlazan equipos personales a conexiones ATM de alta velocidad para la ejecución de aplicaciones multimedia.

El medio ATM no se restringe, se puede utilizar cualquier tipo, incluso el medio existente diseñado para otros sistemas de comunicaciones incluyendo:

- Cable coaxial.
- Cable de par trenzado.
- Cable de fibra óptica.

No obstante, estos medios de red tradicionales en sus formatos actuales no admiten las posibilidades de ATM. La organización denominada ATM Forum recomienda las siguientes interfaces físicas para ATM:

- FDDI (100 Mbps).
- Fiber Channel (155 Mbps).
- OC3 SONET (155 Mbps).
- T3 (45 Mbps).

Conmutadores ATM. Los conmutadores ATM son dispositivos multipuerto que pueden actuar de la siguiente forma:

- Como hubs para enviar datos desde un ordenador a otro dentro de una red.
- Como dispositivos similares a los routers para enviar datos a alta velocidad a redes remotas.

En algunas arquitecturas de red, tales como Ethernet o Token Ring, sólo puede transmitir un equipo en cada momento.

IV.14.2.- Consideraciones Relativas a ATM.

La tecnología ATM requiere un hardware especial y un ancho de banda excepcional para alcanzar su potencial. Las aplicaciones que admiten vídeo y voz van a saturar la mayoría de los entornos de red anteriores y frustrarán a los usuarios que intentan utilizar la red para realizar las tareas diarias. Además, la implementación y soporte de ATM requiere un experto que no siempre está disponible.

IV.15.- Red Digital de Servicios Integrados (RDSI).

La Red Digital de Servicios Integrados (RDSI) es una especificación de conectividad digital entre LAN que permite voz, datos e imágenes. Uno de los objetivos más originales de los desarrolladores de RDSI fue enlazar los hogares y las empresas a través de los hilos telefónicos de cobre. El plan de implementación de RDSI inicial planificó convertir de analógicos a digitales los circuitos telefónicos existentes.

Basic Rate RDSI divide su ancho de banda disponible en tres canales de datos. Dos de ellos desplazan los datos a 64 Kbps, mientras que el tercero lo hace a 16 Kbps.

Los canales de 64 Kbps se conocen como canales B. Éstos pueden transportar voz, datos o imágenes. El canal más lento de 16 Kbps se denomina el canal D. El canal D transporta el muestreo de señales y los datos de gestión del enlace. El servicio personal de Basic Rate RDSI se denomina 2B+D.

Un equipo conectado a un servicio RDSI puede utilizar los canales B juntos para un flujo de datos de 128 Kbps combinado. Se puede conseguir un rendimiento superior, si ambas estaciones de destino admiten la compresión.

Primary Rate RDSI utiliza el ancho de banda completo de un enlace T1 proporcionando 23 canales B a 64 Kbps y un canal D a 64 Kbps. El canal D se utiliza sólo para el muestreo de señales y gestión del enlace.

Las redes que quieren utilizar los servicios RDSI deben considerar si utilizar *Basic Rate* o *Primary Rate* en función de sus necesidades del rendimiento de los datos. RDSI es el reemplazamiento digital de PSTN y, como tal, se trata de un servicio de llamada. No está diseñado para ser un servicio disponible las 24 horas del día (como T1) o para constituir un servicio de ancho de banda por demanda (como puede ser Frame Relay).

IV.16.- Interfase de Datos Distribuidos en Fibra (FDDI).

La Interfase de Datos Distribuidos en Fibra (FDDI), es una especificación que describe una red de pase de testigo de alta velocidad (100 Mbps) que utiliza como medio la fibra óptica. Fue diseñada por el comité X3T9.5 del Instituto Nacional Americano de Estándares (ANSI) y distribuida en 1986. FDDI se diseñó para su utilización con grandes equipos de destino que requerían anchos de banda superiores a los 10 Mbps de Ethernet o 4 Mbps de las arquitecturas Token Ring existentes.

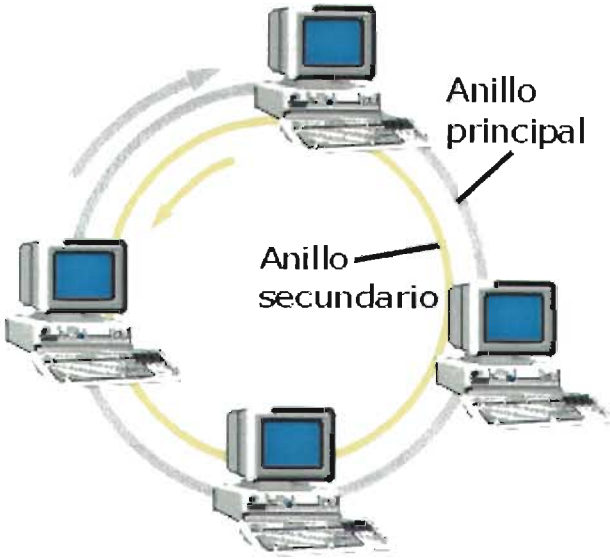
FDDI se utiliza para proporcionar conexiones de alta velocidad a varios tipos de red. FDDI se puede utilizar para redes de área metropolitana (MAN) que permiten conectar redes en la misma ciudad con una conexión de fibra óptica de alta velocidad. Está limitada a una longitud máxima de anillo de 100 kilómetros (62 millas) y, por tanto, FDDI no está diseñada realmente para utilizarse como tecnología WAN.

Las redes en entornos de altos destinos utilizan FDDI para conectar componentes, como pueden ser miniequipos grandes o pequeños, en una tradicional habitación de equipos. A veces se denominan «redes de destino de vuelta». Normalmente, estas redes manejan la transferencia de archivos más allá de la comunicación interactiva. Cuando se establece la comunicación con un gran sistema o mainframe, los miniequipos u equipos personales, a menudo, requieren uso constante en tiempo real del medio. Incluso podrían necesitar, de forma exclusiva, utilizar el medio durante amplios períodos de tiempo.

FDDI funciona con redes de enlace central (backbone) a las que se pueden conectar LAN de baja capacidad. No resulta prudente conectar todo el equipamiento de procesamiento de datos de una empresa a una única LAN, puesto que el tráfico puede sobrecargar la red y un fallo podría provocar que se detengan todas las operaciones de procesamiento de datos en la empresa.

Las LAN que requieren altas velocidades de datos y amplios anchos de banda pueden utilizar conexiones FDDI. Son redes formadas por equipos que desempeñan trabajos relativos a ingeniería u otros equipos que deben admitir aplicaciones de ancho de banda amplio como vídeo, diseño asistido por PC (CAD) y fabricación asistida por PC (CAM).

Cualquier oficina que requiera operaciones de red de alta velocidad podría considerar la utilización de FDDI. Incluso en las oficinas de las empresas, el hecho de necesitar generar gráficos para presentaciones y otra documentación puede saturar y ralentizar una red.



IV.16.1.- Pase de Testigo.

Mientras FDDI utiliza un sistema estándar de pase de testigo, existen diferencias entre FDDI y el estándar 802.5. Un equipo en una red FDDI puede transmitir tantas tramas como produce dentro de un tiempo determinado antes de abandonar el testigo. Tan pronto como finaliza la transmisión, el equipo libera el testigo.

Dado que un equipo libera el testigo cuando finaliza la transmisión, pueden aparecer, al mismo tiempo, tramas circulando por el anillo. Esto explica por qué FDDI ofrece un rendimiento superior que el proporcionado por las redes Token Ring, que sólo permiten una trama en un instante de tiempo.

IV.16.2.- Topología.

FDDI opera a 100 Mbps sobre una topología de doble anillo que admite 500 equipos en una distancia de hasta 100 kilómetros (62 millas).

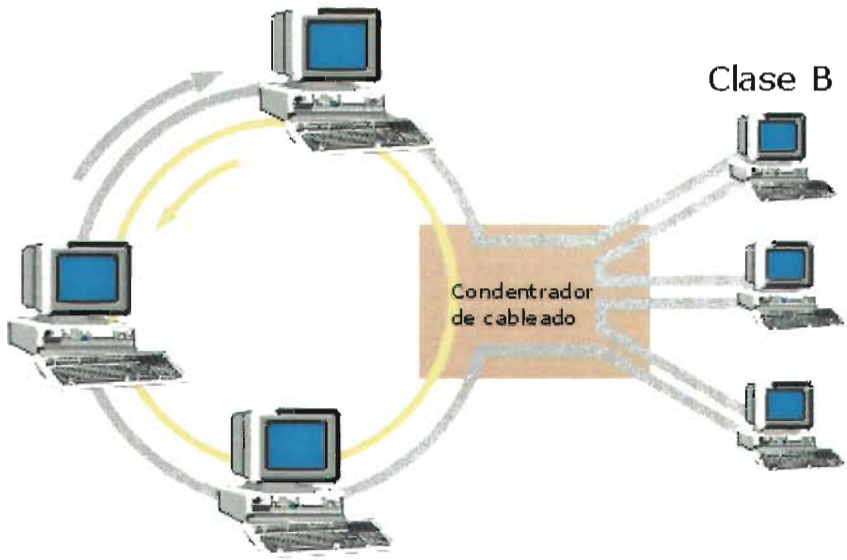
FDDI utiliza una tecnología de red compartida. Esto significa que puede transmitir más de un equipo al mismo tiempo. Aunque FDDI puede proporcionar servicio de 100 Mbps, el enfoque compartido puede saturarse. Por ejemplo, si 10 equipos transmiten a 10 Mbps, la transmisión total será igual a 100 Mbps. En la transmisión de vídeo o multimedia, incluso la tasa de transmisión de 100 Mbps puede generar un cuello de botella.

FDDI utiliza el sistema de pase de testigo en una configuración de doble anillo. El tráfico en una red FDDI está formado por dos flujos similares que circulan en direcciones opuestas alrededor de dos anillos que giran en sentido contrario. Un anillo se denomina «anillo principal» y el otro «anillo secundario».

Normalmente, el tráfico sólo circula por el anillo principal. Si el anillo principal falla, automáticamente FDDI reconfigura la red, de forma que los datos circulen por el anillo secundario en la dirección opuesta.

Una de las ventajas de la topología de anillo doble es la redundancia. Uno de los anillos se utiliza para la transmisión y el otro actúa como anillo de seguridad o reserva. Si aparece un problema, como un fallo en el anillo o una ruptura del cable, se reconfigura el anillo y continúa la transmisión.

La longitud total del cable de ambos anillos no debe exceder los 200 kilómetros (124 millas) y no puede admitir más de 100 equipos. No obstante, por el segundo anillo, que protege frente a fallos, se debe dividir por la mitad la capacidad total. Por tanto, cada red FDDI estará limitada a 500 equipos y 100 kilómetros (62 millas) de cable. Además, debe aparecer un repetidor cada dos kilómetros (1.24 millas) o menos.



Los equipos pueden conectarse a uno o a ambos cables FDDI en un anillo. Aquellos que se conectan a ambos anillos se denominan estaciones Clase A y aquellos que se conectan sólo a un anillo se denominan estaciones Clase B.

Si se produce un fallo en la red, las estaciones de Clase A pueden ayudar a reconfigurar la red mientras que las estaciones de Clase B no pueden.

FDDI en estrella.

Los equipos FDDI pueden admitir enlaces punto a punto a un hub. Esto implica que se puede implementar FDDI con una topología de anillo en estrella. Esto constituye una ventaja puesto que:

- Ayuda en la detección de problemas.
- Obtiene ventajas de las posibilidades de administración y detección de problemas de los hubs avanzados.

IV.16.3.- Envío de Señales (Baliza).

Todos los equipos en una red FDDI son responsables de la monitorización del proceso de pase de testigo. Para aislar fallos serios en el anillo, FDDI utiliza un sistema denominado *envío de señales o balizas (beaconing)*. Con el envío de balizas, el ordenador que detecta un fallo envía a la red una señal denominada «baliza». El equipo continúa con el envío hasta que recibe una baliza procedente de su vecino inmediatamente superior deteniendo, a continuación, el envío. Este proceso continúa hasta que el único equipo que envía una baliza es el equipo que está inmediatamente por debajo del fallo.

Si el equipo 1 falla, el equipo 3 detecta el fallo, inicia la baliza y continúa con ella hasta que recibe una baliza por parte del equipo 2. El equipo 2 continúa con el proceso hasta que recibe la baliza por parte del equipo 1. Dado que el equipo 1 es el que tiene el fallo, el equipo 2 continuará con la baliza e identificará la localización del fallo en el equipo 1.

Cuando el equipo que genera la baliza recibe finalmente su propia baliza, asume que se ha resuelto el problema y se regenera un testigo. A continuación, la red vuelve a su operativa normal.

IV.16.4.- Medio.

El medio principal de FDDI es el cable de fibra óptica. Esto significa que FDDI es:

- Inmune a interferencias o ruido electromagnético.

- Seguro, puesto que el cable de fibra óptica no emite una señal que puede ser monitorizada ni intervenida.

- Capaz de transmitir sobre distancias largas antes de necesitar un repetidor.

Además, FDDI se puede utilizar sobre cable de cobre, conocido como interfaz de datos distribuidos en cobre (CDDI), pero limitará seriamente sus posibilidades en cuanto a distancia.

IV.17.- Red óptica síncrona (SONET).

La Red Óptica Síncrona (SONET), es uno de los sistemas nuevos que aprovecha las ventajas de utilizar la tecnología de la fibra óptica. Puede transmitir datos por encima de un gigabit por segundo (Gbps). Las redes que se basan en esta tecnología son capaces de distribuir comunicación de voz, datos y vídeo.

SONET es un estándar para transporte óptico que fue formulado por la Asociación de estándares de proveedores de servicio de intercambio (ECSA; *Exchange Carriers Standars Association)* para ANSI. Además, SONET se ha incorporado en las recomendaciones de la Jerarquía digital síncrona de la CCITT, también conocida como la Unión Internacional de Telecomunicaciones (ITU), que establece los estándares para las telecomunicaciones internacionales.

SONET define los niveles de portadora-óptica (OC) y las señales de transporte síncronas equivalentes desde un punto de vista eléctrico (STS) para la jerarquía de transmisiones basada en fibra óptica.

SONET utiliza una tasa de transmisión básica STS-1 equivalente a 51.84 Mbps. No obstante, se pueden lograr señales de más alto nivel siendo estas señales múltiplos enteros de la tasa básica.

Por ejemplo, STS-3 es tres veces la tasa de STS-1 (3 X 51.84 = 155.52 Mbps). Una STS-12 sería una tasa de 12 x 51.84 = 622.08 Mbps.

SONET proporciona suficiente flexibilidad de carga útil que se puede utilizar como nivel de transporte fundamental para las celdas ATM de BISDN. BISDN es una red RDSI estándar que puede controlar servicios de voz, datos y vídeo. ATM es el estándar de CCITT que admite celdas para la comunicación de voz, datos, vídeo y multimedia en una red pública bajo BISDN. El Forum de ATM se está convirtiendo, junto con SONET, en el nivel de transporte para el tráfico basado en celdas.

IV.18.- Servicio de Datos Multimegabit Conmutado (SMDS).

El servicio de datos multimegabit conmutado (SMDS) es un servicio de conmutación proporcionado por algunos servicios de intercambio de portadoras locales. El rango de las velocidades de transmisión va desde 1 Mbps hasta los 34 Mbps con una conectividad muchos a muchos. A diferencia de una red de malla dedicada (una red con múltiples caminos activos), este servicio sin conexión ofrece un gran ancho de banda con costos de red reducidos.

SMDS utiliza la misma tecnología de transmisión de celdas de longitud fija que ATM. Una línea SMDS con el ancho de banda apropiado se conecta al proveedor de servicio local y puede proporcionar conexiones entre todos los sitios sin necesidad de realizar una llamada o un

procedimiento de arrebato. SMDS no realiza la comprobación de errores o control del flujo, es decir, lo deja para las estaciones que están conectadas.

SMDS es compatible con el estándar MAN 802.6 de IEEE así como con BISDN, pero SMDS proporciona servicios de administración y facturación no indicados en la especificación 802.6 de IEEE.

SMDS utiliza como interfase y método de acceso a la red un bus doble de cola distribuida (DQDB). SMDS constituye una topología de bus doble que forma un anillo no cerrado.

CAPÍTULO V

APLICACIÓN DE LA INTRANET COMO HERRAMIENTA PARA LA TOMA DE DECISIONES DE LA DIRECCIÓN GENERAL DE CONSERVACIÓN DE CARRETERAS DE LA SECRETARÍA DE COMUNICACIONES Y TRANSPORTES.

V.1.- Introducción.

Las Intranets en una organización realmente deben construirse con un objetivo central: ser un sistema que apoye el desempeño de los trabajadores, de manera que les ayude a crear y entregar valor en sus procesos y a sus clientes, socios, aliados, pares, relacionados, promotores y accionistas. Para cumplir con este objetivo, es necesario tener en cuenta los requerimientos de información y conocimiento del tipo institucional, del trabajador, de los productos y servicios, de los documentos, del contenido; pero sobretodo de los procesos medulares del negocio. Esto último se refiere a aquella información que está vinculada con las actividades y tareas que son propias de naturaleza central o del *core business* de la organización.

También se menciona los componentes de software más importantes de la plataforma de computación para soportar los requerimientos funcionales de una Intranet corporativa.

1. Los sistemas de soporte al desempeño.- Para apoyar el desempeño de la gente, se requieren varias cosas: datos, información, conocimiento sobre los insumos, procesos y productos que se manejan en una organización. Integrar todo esto en un sistema es lo que se denomina sistema de soporte al desempeño SSD o PSS (por sus siglas en el idioma inglés, performance support system).

El reto además es, integrarlo en un ambiente electrónicamente compartido por los trabajadores: una Intranet corporativa. Esto significa tener en la red de la organización las aplicaciones, sistemas, archivos, glosarios, fórmulas, normas, procedimientos, etc.; es decir todo aquello que requiera el trabajador para agregar valor en sus proceso. El objetivo único es constituir un medio que de manera permanente y sistemática contribuya al desempeño en términos de excelencia y competitividad de los trabajadores. De otra manera, estaríamos perdiendo el tiempo y los otros recursos de los accionistas de la organización.

Es irrelevante el tipo de organización (corporación, empresa, institución), en la nueva economía el trabajador debe estar considerado como socio estratégico del negocio; por tanto a él debiéramos entregarle la mejor herramienta para la consecución de sus objetivos.

2. Criterios para construir una Intranet corporativa.- En una organización, el equipo de desarrollo de Web sites bien pudiera construir una Intranet a partir de varios criterios y formas, cada uno de ellos con suficientes argumentos que justifiquen su elección. En efecto, cualquiera de los siguientes criterios pudiera ser factible para el desarrollo desde el punto de vista de la plataforma tecnológica:

- institucional,
- trabajador,
- productos y servicios,
- documentos,

- contenido,
- procesos medulares.

Criterios para organizar una Intranet Corporativa:

En términos de un sistema de soporte al desempeño organizacional, existe sólo un criterio que prima sobre los demás: el de los procesos medulares del negocio. Cualquier otro pasa a ser secundario frente a este último.

Para que una Intranet sea un sistema de soporte al desempeño para los trabajadores, es imprescindible que esté centrada en los procesos medulares del negocio. Cómo hemos mencionado antes, sólo así contribuirá con valor para la organización. Los demás criterios, deberán estar alrededor o en una condición periférica y no por eso decimos que dejan de ser importantes.

De esta manera, una Intranet en términos de criterios deberá estar conformada por:

- Criterio central: procesos medulares del negocio,

- Criterios periféricos: institucional, servicios al personal, productos y servicios, documentos y contenido.

Criterios para organizar una Intranet Corporativa.
Visión funcional: periferia del soporte al desempeño

3. El criterio central: los procesos medulares del negocio.- Se debe disponer de información sobre los procesos de la cadena de valor, sus dueños, insumos, productos, indicadores, requerimientos de competencias, etc. Lo qué es, y el cómo hacerlo. Cada proceso debiera tener una constitución de componentes de información, algunos estructurados como provenientes de bases de datos, glosarios, normas y procedimientos; etc. y otros no estructurados como foros, opiniones, preguntas y respuestas; etcétera.

El objetivo principal de un proceso es hacer algo pero en términos de productividad y competitividad. Lo productivo nos indicará la forma eficaz y eficiente de cómo estamos haciendo las cosas (valor interno), y lo competitivo nos dirá su relación en el mercado (valor externo).

Los procesos, son las cosas que hacemos ya sea de naturaleza cotidiana o sistemática, o de naturaleza emergente o no sistemática. Para ser productivos y competitivos en los procesos, necesitamos además de hacer; medir, comparar, aprender y cambiar. Para cumplir esto, requerimos que alrededor de cada proceso se constituya una comunidad de usuarios, que incluya a los proveedores y clientes de cada proceso y que puedan interactuar entre ellos, intercambiar sus experiencias, apoyarse unos a otros, conocer las mejores prácticas, sacar lecciones de su trabajo; es decir: aprender. Para ilustrar este objetivo, a continuación mostraremos un ejemplo de una arquitectura de componentes para una Intranet basada en ciertos procesos medulares. Algo importante: una Intranet es como una casa, cada quién tiene un diseño de ella, lo que veremos es una arquitectura que corresponde a una organización en particular con requerimientos específicos de información.

4. Los criterios secundarios.- Al mismo tiempo, una Intranet debiera satisfacer otros requerimientos que son complementarios y necesarios en el marco de un sistema de soporte al desempeño. Así tenemos que, además una Intranet en una organización debiera verse también como un:

- **folleto o *brochure***, desde el punto de vista institucional,
- **sistema de servicios al personal**, desde el punto de vista del trabajador,

- **catálogo**, desde el punto de vista de mercadeo y venta de los productos y servicios,
- **sistema de flujo de trabajo o *workflow***, desde el punto de vista de los documentos,
- **base de conocimientos**, desde el punto de vista del contenido.

5. Portales Horizontales y Verticales en una Intranet corporativa.- Una práctica que se recomienda a los diseñadores de páginas Web, es integrar los criterios central y secundarios en una misma y robusta Intranet. Esto se pueden lograr si se aplican la técnica de desarrollo acelerado de portales, es decir se construye una plataforma conformada por programas esqueletos y plantillas basadas en estándares de contenido, medios y técnicos para la generación rápida de los portales de la Intranet.

El portal horizontal, lo debiera constituir la parte correspondiente a los procesos medulares del negocio, y dejar que cada uno de los criterios secundarios de la Intranet (institucional, servicios al personal, productos y servicios, flujo de documentos y contenido o de bases de conocimiento) constituya un portal vertical en particular. De manera que, aplicando un enfoque sistémico, cada portal horizontal o vertical pueda verse como una Intranet en particular, el conjunto también se verá como una Intranet pero corporativa.

6. Contenido estructurado y no estructurado para una Intranet corporativa.- Las organizaciones están en la búsqueda que su gente sea la ventaja competitiva, el factor diferenciador e inigualable en su mercado y entorno. Uno de los medios para lograr esto, es la capacidad de respuesta y de actuación a través de la información que dispongan. La información de los libros, revistas, manuales, cursos; generalmente está organizada, y preparada para una fácil e inmediata comprensión y por lo general proviene de experiencias pasadas y/o de vivencias de otros. Esta información en la mayoría de las veces, ya es conocida por los trabajadores y sus competidores; por tanto no será necesariamente una fuente para tener una ventaja competitiva en el mercado.

De otro lado, la información proveniente de la experiencia y del trabajo cotidiano, y que tal vez todavía no sido totalmente registrada y puesta de manera organizada; puede decirse que está más cerca de marcar una ventaja competitiva en la decisión y acción organizacional. Este tipo de conocimiento generalmente se maneja en los foros, casos de estudio, comentarios, opiniones; etc.

En el desarrollo de las Intranets, tanto al tratar la parte de los procesos medulares del negocio como de los criterios secundarios, deberíamos tener presente estos dos tipos de información y sus principales formas de expresión.

A continuación, se muestran algunas de las formas más frecuentes de información estructurada y no estructurada formuladas como secciones de contenido específicamente para la parte correspondiente a los procesos medulares del negocio en una Intranet. Estas secciones tal vez sean las más conocidas, pero también estamos seguros que existen otras que no se reseñan aquí.

Tomado esta parte como modelo, los lectores podrían construir las secciones de contenido para los criterios secundarios de la Intranet (institucional, servicios al personal, productos y servicios, flujo de documentos, contenido o de bases de conocimiento); en términos de secciones estructuradas y no estructuradas e información.

Secciones de contenido e información en una Intranet corporativa para los Procesos Medulares del Negocio	
Estructurado	**No estructurado**
Consulta, 1. Glosario 2. Directorios 3. Biblioteca 4. Archivo 5. Buscador	**Consulta,** • Buscador inteligente
Diálogo, 1. Encuestas cerradas	**Diálogo,** Preguntas y respuestas • Comentarios / opiniones • Ideas / sugerencias • Contribuciones / colaboraciones • Testimonio de terceros
Colaboración, Convenios	**Colaboración,** Foros • Grupos de discusión • Mesas virtuales de trabajo • Chats • Clubes de usuario
Aprendizaje, • Cursos en línea • Políticas / Normas / Reglas de negocio • Procesos / Procedimientos técnicos • Propiedad intelectual • Aseguramiento de la calidad	**Aprendizaje,** Proyectos • Simulaciones / Juegos de negocio • Casos de estudio • Consultoría / Asesoría • Mejores prácticas, lecciones aprendidas • Eventos tecnológicos y de procesos
Noticias, • Noticias de prensa	**Noticias,** 1. Novedades 2. Alertas tecnológicas 3. Anuncios en la materia
Información del negocio 1. Planes y resultados del negocio 2. Sistema balanceado de indicadores 3. Portafolio del negocio	**Información del negocio** • Innovaciones • Nuevos desarrollos y Prototipos

7. Plataforma de software para una Intranet corporativa.- A efecto de responder a las exigencias del nivel de contenido y de información expresado en la tabla anterior, se requiere dotar de una batería robusta de software que responda a las exigencias de los trabajadores navegantes de la organización. En la medida que se vaya desarrollando la Intranet corporativa y empiecen a "salir al aire" las diferentes secciones, la dotación de software deberá ir creciendo.

Alguno de este software como los *browser*, diccionarios, enciclopedias; serán de propósito general, otros como los LMS (sistema administrador del aprendizaje) serán de propósito específico, y otros como los simuladores, CRM serán de uso directo en las operaciones del negocio.

Los paquetes y programas recomendados son, entre otros:

Software de propósito general:

- Browser o Visualizador
- Buscador inteligente
- Traductor inteligente
- Diccionarios
- Enciclopedias
- DBMS – Bases de datos
- Administrador de mensajería
- Administrador de colaboración
- Workflow
- Aplicaciones de escritorio
- Sistemas y Aplicaciones administrativas

Software de propósito específico:

- Software de autor
- Software de medios
- LMS - Sistema administrador del aprendizaje

Software de negocio:

- Agentes
- Simuladores
- Sistemas y Aplicaciones de Negocio
- ERP
- CRM

8. Conclusiones.- Diseñar, desarrollar e implantar una Intranet Corporativa, requiere un trabajo previo de estrategia en términos de planificación y conceptualización del servicio que se ofrece atender en la organización. En la nueva economía hay sólo una razón: que la Intranet sea un sistema que apoye el desempeño de la gente.

Uno de los factores de éxito en la Intranet, es orientarla primero a los procesos medulares del negocio. La arquitectura de contenido requerida para este fin deberá permitir manejar tanto el contenido de naturaleza estructurada como el no estructurado.

Lo relativo a los procesos medulares del negocio, su cadena, insumos, sub-procesos, productos y resultados, requerimientos de información y de conocimiento; etc. son imprescindibles para el levantamiento de la arquitectura de la Intranet.

La participación de los usuarios en una Intranet puede ser de varias maneras no excluyentes: de manera individual, agrupados en comunidades de conocimiento o comunidades prácticas, y como expertos de contenido en las secciones de información de su competencia.

Para la construcción de una robusta Intranet, se recomienda armar al menos dos equipos de desarrollo, uno que se encargue del portal horizontal basado en los procesos medulares del negocio y el segundo de los portales verticales basados en los criterios institucional, servicios al personal, productos y servicios, flujo de documentos y contenido o de bases de conocimiento. Ambos equipos deberán trabajar de manera coordinada, integrada y alineada. Importante: el portal vertical de contenido deberá convertirse en una base de conocimientos para la organización, base fundamental para la implantación de la gerencia del conocimiento.

Dependiendo de la naturaleza y carga del contenido, la dotación de software deberá ir de acuerdo a la implantación de la Intranet corporativa.

V.2.- Misión.

La Secretaría de Comunicaciones y Transportes, que tiene como misión el de "Dotar al país con comunicaciones y transportes que hagan posible la integración de todos los mexicanos entre sí y con el resto del mundo, aprovechando los avances tecnológicos y generando valor agregado para las diversas actividades económicas y sociales del país, de manera equilibrada, sostenida y en armonía con las particularidades culturales y del medio ambiente".

V.3.- Visión.

Su visión es de "Ser un agente de cambio en el país mediante la promoción y la generación de mas y mejores servicios e infraestructura de comunicaciones y transportes, que sean accesibles a todos los mexicanos y coadyuven al mejoramiento de la calidad de vida y a la construcción de una sociedad más igualitaria y más justa, siempre trabajando con las más elevadas normas de calidad y ética profesional, estableciendo sinergias entre los distintos órdenes de gobierno y con la sociedad en general".

V.4.- Objetivos de Calidad.

- Disminuir el número de trámites en los servicios ofrecidos por la Secretaría de Comunicaciones y Transportes.
- Disminuir el tiempo de respuesta en los servicios ofrecidos por la Secretaría de Comunicaciones y Transportes.
- Incrementar el nivel de satisfacción de los usuarios con relación a los servicios que ofrece la Secretaría de Comunicaciones y Transportes.

Con todo esto la Secretaría de Comunicaciones y Transportes, la cual pretende lograr con este proceso de calidad el de desarrollar una nueva cultura y filosofía de trabajo, promover una actitud de servicio enfocada al cliente o usuario, transformar las áreas de la Secretaría y sus órganos desconcentrados en instituciones de calidad que garanticen a la sociedad una respuesta ágil, eficiente y oportuna a sus demandas y espectativas, ampliar su horizonte mediante capacitación y adopción de nuevas técnicas de trabajo, y fomentar la integración de los servidores públicos a través del trabajo en equipo y la creación de círculos de calidad.

V.5.- Organigrama de la Secretaría de Comunicaciones y Transportes (S.C.T.).

La Secretaria de Comunicaciones y Transportes cuenta con una estructura organizacional representada como se muestra en la Figura V.1. Por lo que representa el objetivo del secretario de la dependencia, así como sus funciones son los siguientes:

Objetivo.

Atender en nombre del Ejecutivo Federal en la esfera administrativa, el despacho de los asuntos que integran por disposición de la Ley su competencia y, en el orden político, asumir la responsabilidad que en su carácter de Secretario tiene de asociarse al ejercicio de las facultades del Presidente de la República, en el marco de los objetivos de la planeación nacional.

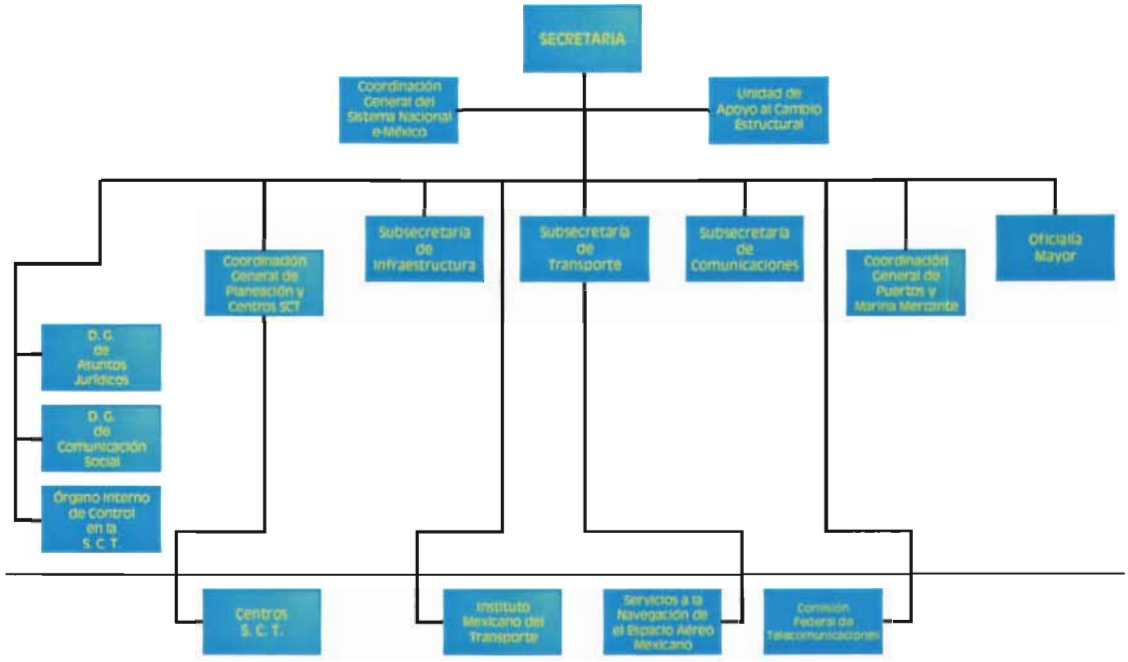


Figura V.1.

Funciones.

- Coordinar, dirigir y supervisar el despacho de los asuntos de la competencia de la Secretaría.
- Fijar, dirigir y controlar la política de la Secretaría y de las entidades del Sector.
- Coordinar y evaluar los programas y operación de las entidades del Sector a su cargo en los términos de la legislación aplicable.
- Someter al acuerdo del Presidente de la República los asuntos encomendados a la Secretaría y al Sector, que así lo ameriten y desempeñar las comisiones y funciones específicas que le confiera, informándole sobre su desarrollo.
- Proponer al Ejecutivo Federal los proyectos de iniciativa de leyes, reglamentos, decretos, acuerdos y órdenes sobre los asuntos de la competencia de la Secretaría y del Sector.
- Aprobar el anteproyecto de programa y de presupuesto de egresos de la Secretaría, así como coordinar y evaluar los correspondientes a las entidades del Sector Comunicaciones y Transportes.

- Dar cuenta al Congreso de la Unión del estado que guarda su ramo y el Sector correspondiente e informar siempre que sea requerido por cualquiera de las Cámaras que lo integran, cuando se discuta un proyecto de ley o se estudie un asunto concerniente a la Secretaría.

- Representar al Presidente de la República en los juicios constitucionales de amparo, en los términos de los artículos 14 de la Ley Orgánica de la Administración Pública Federal y 19 de la Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, así como en las controversias constitucionales y acciones de inconstitucionalidad a que se refiere el artículo 105 de la propia Constitución y su Ley reglamentaria, en los casos en que lo determine el Titular del Ejecutivo Federal.
- Autorizar y expedir los manuales de organización, de procedimientos y de servicios al público, necesarios para el funcionamiento de la Secretaría y disponer la publicación en el **Diario Oficial de la Federación** del Manual de Organización General de la Secretaría.

- Otorgar las concesiones para la explotación y operación de los servicios públicos que por ley le corresponda a la Secretaría y resolver, en su caso, sobre su prórroga y caducidad, nulidad, rescisión o revocación.

- Aprobar la organización y el funcionamiento de la Secretaría y adscribir orgánicamente a las unidades administrativas a que se refiere el Reglamento Interior.

- Acordar las bases sobre los nombramientos del personal de la Secretaría y resolver sobre las proposiciones que los servidores públicos hagan para la designación de su personal de confianza, de su remoción y creación de plazas.

- Designar a los servidores públicos que deban ejercer las facultades que impliquen la titularidad de las acciones o partes sociales que integran el capital social de empresas de participación estatal mayoritaria del Sector.

- Proponer al Presidente de la República la requisa de las vías generales de comunicación, de los modos de transporte que en ellas operan y de los servicios auxiliares y conexos; así como el rescate de las concesiones.

- Crear comités de coordinación entre la Secretaría y las entidades del Sector, a fin de coadyuvar en el mejoramiento de sus funciones.

- Resolver los recursos administrativos que le competan; así como las dudas que se susciten con motivo de la interpretación y aplicación del Reglamento Interior.

V.6.- Subsecretaría de Infraestructura.

Objetivo.

Impulsar el desarrollo y modernización de la infraestructura carretera tanto federal como concesionada, mediante la coordinación de los programas de construcción, ampliación, reconstrucción y conservación, que permitan la movilización de personas y bienes en menores tiempos de recorrido y en mejores condiciones de operación y seguridad.

Funciones.

- Establecer y vigilar la aplicación de las políticas, normas, sistemas y procedimientos para la ejecución de las acciones en materia de infraestructura carretera, a cargo de las áreas de su responsabilidad.

- Someter a la consideración del Secretario del Ramo los acuerdos de su competencia, así como las propuestas de organización de las unidades administrativas adscritas.

- Programar, controlar y evaluar el funcionamiento de las unidades administrativas de su adscripción; definir medidas de mejoramiento administrativo, de desconcentración y delegación de facultades en sus subalternos.

- Definir, integrar y expedir normas oficiales mexicanas, así como expedir y certificar copias de documentos o constancias que existan en sus archivos en los casos que procedan.

- Dirigir, controlar y evaluar la realización de los programas de construcción, ampliación, reconstrucción y conservación de la red carretera y puentes federales, así como dirigir la política para desarrollar el sistema de carreteras de cuota.

- Dirigir y coordinar la formulación de los proyectos de programas y presupuestos de las unidades administrativas que tenga adscritas y participar en los correspondientes a las entidades del Sector.

- Otorgar los permisos y autorizaciones dentro del ámbito de su competencia, así como declarar administrativamente su nulidad o revocación, sin perjuicio de que tales facultades puedan ser delegadas; suscribir los contratos, convenios, acuerdos y documentos relativos al ejercicio de sus atribuciones, así como resolver sobre las licitaciones públicas en el ámbito de su competencia y opinar sobre convenios, contratos, concesiones, permisos y autorizaciones que celebre u otorgue la Secretaría en asuntos de su competencia

V.7.- Semblanza de la Dirección General de Conservación de Carreteras (D.G.C.C.)

A partir de 1574 los cambios que se abrieron en el territorio nacional fueron auspiciados por el sistema de "Consulados", por lo que al finalizar la época colonial el país contaba ya con una pequeña red carretera y caminos de herradura.

Ya en la época independiente, entre 1821 y 1861 las funciones correspondientes a la obra pública se encontraban diseminadas en diversas instancias, hasta que el Presidente Juárez las integró en la Secretaría de Fomento, Comunicaciones y Obras.

En 1891 cuando se crea la Secretaría de Comunicaciones y Obras Públicas (SCOP), la cual tenía a su cargo la planeación, construcción y conservación de los caminos del país. Posteriormente, en 1917 y dentro de la Secretaría, fue constituida la Dirección de Caminos y Puentes a cargo de las funciones de su especialidad.

En el año de 1925, se integra como organismo público descentralizado la Comisión Nacional de Caminos, constituida por los Departamentos de Proyectos, Construcción, Cooperación, Puentes, Conservación y Contabilidad. En 1958, el Congreso de la Unión aprobó las modificaciones a la Ley de las Secretarías y Departamentos de Estado presentadas por el ejecutivo, y que establecían la separación funcional de la Obra Pública de la entonces Secretaría de Comunicaciones y Transportes.

Posteriormente en 1960, dependiendo de la Secretaría de Obras Públicas, se crean las Direcciones Generales de Construcción de Carreteras Federales, Carreteras en Cooperación y de Conservación de Carreteras Federales, esta última integrada por los Departamentos de Obra, Técnico y Administrativo, dedicándose a la construcción y conservación de red estatal y federal de carreteras, en coordinación con las autoridades locales responsables.

Para 1970, la Dirección General de Conservación de Carreteras Federales cambió su denominación a la Dirección General de Conservación de Obras Públicas, teniendo a su cargo el mantenimiento de la red nacional de caminos tanto federales como estatales y vecinales. Esta Dirección General estaba integrada por los Departamentos de Obras, Técnico, de Proyectos, de Programación y Presupuesto y de una Oficina Administrativa.

Conforme a las modificaciones aprobadas a la Ley Orgánica de la Administración Pública Federal en 1982, desaparece la Secretaría de Asentamientos Humanos y Obras Públicas y se transfieren a la Secretaría de Comunicaciones y Transportes las funciones de infraestructura y con ellas las de construcción y mantenimiento de la red nacional de caminos, a cargo de la Dirección General de Conservación de Obras Públicas.

En 1987, de acuerdo al Programa de Modernización Administrativa, la Estructura Orgánica de la Dirección General de Conservación de Obras Públicas se fortalece al elevar el nivel jerárquico de los Departamentos de Obras, Precios Unitarios, Normas Técnicas y Concursos de Proyectos al de Subdirección, a fin de dar cumplimiento a los programas encomendados. Esta estructura quedó registrada ante la Secretaría de Programación y Presupuesto el 16 de junio del mismo año con un total de 21 órganos.

El 17 de Noviembre de 1989, como resultado de los ajustes efectuados en el Sector Público, esta Unidad Administrativa cambió su denominación a la de Dirección General de Construcción y Conservación de Obra Pública.

Según el Diario Oficial de fecha 19 de marzo de 1994, se publicó el Reglamento Interior de la Secretaría, en el que se modificó el nombre de esta Unidad Administrativa al de Dirección General de Conservación de Carreteras con iguales funciones.

En Noviembre de 1995, la Coordinación Sectorial de Energía e Industria de la Secretaría de Hacienda y Crédito Público (S.H.C.P.), autorizó la estructura orgánica y ocupacional no básica con vigencia a partir de agosto del mismo año.

En 2002, se autorizó la hoy vigente estructura orgánica que puede verse en el apartado "Directorio" de la página de esta Dirección General de Conservación de Carreteras.

La Dirección General de Conservación de Carreteras tiene como misión, el proporcionar información sobre la conservación de carreteras, con calidad y oportunidad, así como facilitar su flujo para eficientar la comunicación entre la Dirección General y las Residencias Generales de Conservación de Carreteras.

Visión.

"Ofrecer a través de medios informáticos de vanguardia, información oportuna y de calidad, relativa a la conservación de la red carretera federal libre de peaje, para todos los usuarios internos y externos del sector".

Objetivos de Calidad.

- Difundir a través de Internet el estado de la adjudicación de contratos.
- Difundir a través de la página Web los avances del Programa Nacional de Conservación de Carreteras.
- Mantener informado al usuario de Internet sobre las emergencias en las carreteras federales libres de peaje provocadas por fenómenos naturales.
- Establecer una red interna en la D.G.C.C., capaz de proporcionar información a los Mandos Medios, sobre los aspectos que se consideren necesarios.

Organigrama de la DGCC.

La Dirección General de Conservación de Carreteras cuenta con una estructura organizacional cuya estructura orgánica es: (Figura V.2).

Objetivo.

Conservar en condiciones óptimas de funcionamiento la red carretera y puentes federales libres de peaje, mediante el desarrollo de programas de reconstrucción y conservación, con la finalidad de proporcionar al usuario seguridad y abatir los costos del transporte, así como establecer las normas y criterios en materia de conservación de la infraestructura carretera federal de libre peaje.

Funciones.

- Participar en la definición de la política y los programas de transporte carretero en el ámbito de su competencia e intervenir en la integración de programas para la modernización de la red carretera federal libre de peaje y puentes.

- Emitir los lineamientos en materia de conservación de la infraestructura carretera; determinar las normas y criterios para la realización de los programas y obras, así como llevar a cabo el seguimiento de los mismos.

- Tramitar la contratación de los estudios y proyectos de conformidad con la normatividad aplicable en la materia.

- Normar y supervisar los estudios y proyectos que realicen los centros SCT y otras unidades administrativas para la reconstrucción y conservación, de la red carretera federal libre de peaje, y demás obras bajo su responsabilidad; establecer las políticas con relación a las obras por administración directa y por contrato que realizarán los centros SCT, así como supervisar que se ejecuten conforme a las normas, especificaciones, proyectos, precios unitarios y programas aprobados y, en su caso, conforme a lo estipulado en los contratos.

- Participar mediante opinión técnica en el otorgamiento de permisos para la ejecución de obras dentro del derecho de vía o fuera de él, en carreteras federales libres de peaje cuando afecte obras viales o su funcionamiento; normar y supervisar el proyecto, instalación y operación de señalamiento y dispositivos de seguridad que instale la propia Secretaría u otras dependencias, entidades o particulares en la red a su cargo, así como intervenir en el estudio y autorización de los vehículos de carga que deben transitar por las carreteras y puentes federales libres de peaje.

- Promover la utilización intensiva de la mano de obra local y la organización de comunidades para que participen y aporten esfuerzos en la reconstrucción y conservación de carreteras federales libres de peaje.

- Emitir las normas y lineamientos relacionados con la administración, operación y mantenimiento de la maquinaria y equipo de construcción propiedad de la Secretaría, para la conservación de carreteras y puentes federales libres de peaje.

- Supervisar los trabajos de conservación de carreteras y puentes federales libres de peaje que realicen las unidades administrativas de la Secretaría, así como integrar y mantener actualizado el inventario de los mismos y llevar el registro cartográfico correspondiente por entidad federativa.

- Analizar y opinar sobre las solicitudes para modificar y conservar las carreteras y puentes federales libres de peaje, fijando las normas de conservación que corresponda, así como aprobar el proyecto y el programa de dichas obras.

- Intervenir en el estudio de las normas de construcción de la Secretaría y de los precios unitarios, así como normar la administración, operación y mantenimiento de la maquinaria y el equipo de construcción destinado a los programas de conservación de las carreteras y puentes federales libres de peaje.

- Desarrollar sistemas que permitan conformar bases de datos de información general relativa a la conservación de las carreteras y puentes federales libres de peaje.

Problemática.

Los constantes cambios meteorológicos en el mundo, nos acarrea a nosotros una serie de emergencias a las cuales se les tiene que hacer frente de la manera más rápida posible y la más efectiva, a todos los desastres naturales, como son los sismos, huracanes, erupción volcánica, etcétera.

Otro importante motivo es la mala información producida por retrasos en trámites y documentación manejada en toda la Republica Mexicana, incluso en la propia Dirección General, con las diferentes áreas que la conforman, se presenta este mismo problema de retrasos de información necesaria y oportuna, para la atención de estas emergencias, así como el mismo proyecto, plasmado en un programa de obra anual, donde se reflejan las necesidades más importantes de cada estado de la republica, con su presupuesto asignado, para atender también, el mantenimiento normal requerido por una carretera.

Todo esto es realmente muy importante, por los altos costos que conlleva el mantenimiento de una carretera, debido a que el simple hecho de la construcción de un kilómetro cuadrado por carril es de 2.5 millones de pesos, a esto si le sumamos el segundo carril de un cuerpo carretero, serian 5 millones de pesos en un solo kilómetro cuadrado, y el costo de mantenimiento de ese mismo tramo equivale a dos veces lo mismo.

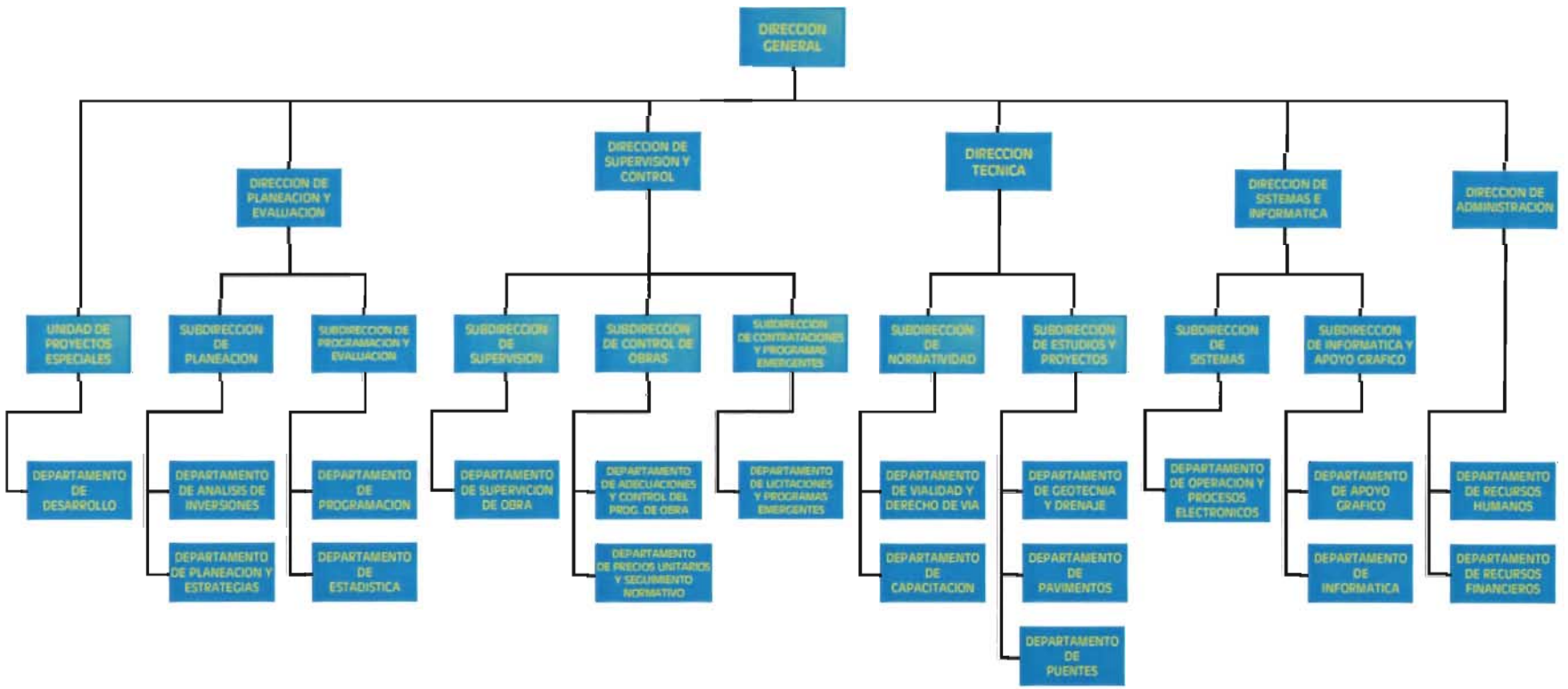

DIRECCION GENERAL
UNIDAD DE PROYECTOS ESPECIALES
DEPARTAMENTO DE DESARROLLO
DIRECCION DE PLANEACION Y EVALUACION
SUBDIRECCION DE PLANEACION
DEPARTAMENTO DE ANALISIS DE INVERSIONES
DEPARTAMENTO DE PLANEACION Y ESTRATEGIAS
SUBDIRECCION DE PROGRAMACION Y EVALUACION
DEPARTAMENTO DE PROGRAMACION
DEPARTAMENTO DE ESTADISTICA
DIRECCION DE SUPERVISION Y CONTROL
SUBDIRECCION DE SUPERVISION
DEPARTAMENTO DE SUPERVICION DE OBRA
SUBDIRECCION DE CONTROL DE OBRAS
DEPARTAMENTO DE ADECUACIONES Y CONTROL DEL PROG. DE OBRA
DEPARTAMENTO DE PRECIOS UNITARIOS Y SEGUIMIENTO NORMATIVO
SUBDIRECCION DE CONTRATACIONES Y PROGRAMAS EMERGENTES
DEPARTAMENTO DE LICITACIONES Y PROGRAMAS EMERGENTES
DIRECCION TECNICA
SUBDIRECCION DE NORMATIVIDAD
DEPARTAMENTO DE VIALIDAD Y DERECHO DE VIA
DEPARTAMENTO DE CAPACITACION
SUBDIRECCION DE ESTUDIOS Y PROYECTOS
DEPARTAMENTO DE GEOTECNIA Y DRENAJE
DEPARTAMENTO DE PAVIMENTOS
DEPARTAMENTO DE PUENTES
DIRECCION DE SISTEMAS E INFORMATICA
SUBDIRECCION DE SISTEMAS
DEPARTAMENTO DE OPERACION Y PROCESOS ELECTRONICOS
SUBDIRECCION DE INFORMATICA Y APOYO GRAFICO
DEPARTAMENTO DE APOYO GRAFICO
DEPARTAMENTO DE INFORMATICA
DIRECCION DE ADMINISTRACION
DEPARTAMENTO DE RECURSOS HUMANOS
DEPARTAMENTO DE RECURSOS FINANCIEROS

Figura V.2.

Solución.

La información es el eslabón indispensable que une a todos los componentes de la organización, para su supervivencia en un ambiente competitivo y poco amigable. A decir verdad las compañías actuales funcionan por la información.

Aunque la teoría y la práctica en las áreas funcionales de la administración de la información han ido madurando, la tecnología de la información ha aumentado la complejidad y la velocidad de la respuesta ante el cambio ambiental.

El análisis y diseño de sistemas computarizados aplicados a las organizaciones es un campo estimulante y de gran dinamismo. Conforme se difunde con gran rapidez, el uso de computadoras dentro de las organizaciones, surgen muchas inquietudes acerca de la forma de usarlas para mejorar a la productividad de la organización.

Es por ello que los analistas de sistemas con frecuencia se enfrentan a estas cuestiones y por lo tanto están obligados a entender al usuario potencial y a las computadoras, para integrar un mejor diseño de los sistemas de información. Más aun, el analista debe aprender a desarrollar y a mantener las relaciones de trabajo con las personas del equipo responsable del análisis de sistemas.

El campo del analista de sistemas se ha desplazado de una activada fundamentalmente técnica hacia el apoyo del usuario final. Por esta razón el analista esta obligado a tratar a personas, y a lograr que la información sea útil en la toma de decisiones.

Para ello se utilizan sistemas de gestión, como en este caso la Intranet, la cual contiene información acerca de cada estado de la republica determinada, que proporciona un entorno que sea a la vez conveniente y eficiente para ser utilizado al extraer y almacenar información en las páginas de la misma.

Es por eso que el uso de la planeación estratégica y un control equilibrado, son cada vez más importantes para hacer que la dirección de las áreas involucradas sean funcionales y concuerden con los objetivos de la DGCC para responder a las exigencias de los estados.

La importancia de la información en la mayoría de las organizaciones, y por lo tanto el valor de la Intranet, ha llevado al desarrollo de una gran cantidad de conceptos, estrategias y técnicas para la gestión eficiente de los datos.

Debido a la importancia de la conservación de los caminos, por muchas de las emergencias ocasionadas por los fenómenos meteorológicos, así como la propia vida útil del tramo carretero, constituyendo nuestros caminos, como las arterias y venas del territorio mexicano, estas formadas por corredores carreteros, tramos, subtramos, ramales, entronques, puentes y caminos rurales, todo esto vinculado a una toma de decisiones rápida y acertada, por los directivos de esta Dirección General, se diseño una Intranet para la administración y concentración con todo lo referente para la ayuda, y pronta respuesta a lo mismo.

De esta manera los Directivos, podrán tomar las decisiones pertinentes, rápidas y más confiables, también para la asignación de recursos, tanto financieros, humanos, maquinaria y equipo, al estado correspondiente.

V.8.- INTRANET.

La Dirección General de Conservación de Carreteras cuenta con el equipo de transmisión como Ruteadores de estas características

El producto del Cisco MC3810 utiliza el encaminamiento del IOS del Cisco para proporcionar funcionamiento superior y la dirección incomparable de la interfase. Las tecnologías probadas de la conmutación y del encaminamiento del Cisco permiten que usted diseñe las redes que integran datos de la herencia, Ethernet, voz análoga o digital, fax y vídeo en una red de comunicaciones común que reduzca perceptiblemente costos de la red.

Interfases de Red	Ethernet 1 x 10Base-T, Serial sincrono, Canalizado de T1/E1 con construcción en CSU/DSU y un respaldo opcional de nX64
Voz	Puertos análogos 1-6 RJ45 –FXS, FXO, E&M, tipos de comienzo de parpadeo I, II, III, IV, V, comienzo inmediato, de retardo, de tierra, laso, señalización de batería. Canales digitales de 1-24 con conexión cruzada, T1/E1, señales CAS, Q.SIG, Transparentes a CCS. Canales digitales de interfase S/T 1-8.
Tarifas de compresión de voz	64, 32, 8 Kbps.
Compresión de voz algorítmica	G.711, G.729, G.729a, G.726.
Soporte de Fax	T.30, grupo de 3 fax, 2.4-14.4 Kbps.
Soporte de video	Interfase de Rs-366. Emulación de circuito ATM y CBR. Base de IP LAN vía HDLC, PPP o Frame Relay
Soporte Cisco IOS	Cisco IOS Release 12.0 IP, IP Plus, Enterprise Plus, ATM, Multimedia Conference Manager.
Memoria DRAW	32 MB DRAW
Memoria Flash	8 MB expandible a 16 MB
Tipo de Procesador	40 MHz MP860 Motorola PowerPC QUICC
Componentes estándar	Alta velocidad de consola y puertos auxiliares 19 pulgadas.

Los Switch son de estas características:

El Switch Vertical de marca Enterasys Netwoks, modelo Horizon VH-2400S2, provisto de 24 puertos de RJ45 10/100 Mbps y dos ranuras opcionales para expansión, así como una ranura dedicada a la administración del equipo.

El funcionamiento de Alambre-velocidad y las características industria que conducen permiten que la Vertical integre en pequeño a las redes de tamaño mediano, haciéndole una solución ideal de la conmutación del borde de la empresa.

Los concentradores cuentan con estas características:

UTP	24 puertos, 10BASE-T
Largo de los cables	10BASE-T a 100 metros
Perdida de Inserción	El máximo de perdida de inserción de 10BASE-T es a 11.5 dB a una frecuencia entre 5.0 y 10 MHz
Impedancia	10BASE-T de 75 a 165 ohms

Servidor marca DELL, modelo PowerEdge 2600.

Procesadores	2 procesadores Intel Xeon de 3.06 GHz, con la tecnología micro arquitectura NetBurst y tecnología Hyper-Threading
Bus frontal	Bus frontal de 533 MHz que permite un mejor rendimiento en comparación con las velocidades de los buses frontales de sistemas anteriores.
Caché	Caché L2 de 1MB para los procesadores de 3.06 GHz
Conjunto de chips	Conjunto de Chips Intel E7500
Memoria	6 sockets DDR DIMM que soportan hasta un máximo de 6 GB de memoria principal. 256 MB / 512 MB / 1 GB PC2100DDR en pares para intervalos.
Ranuras de Entradas y Salidas I/O	2 PCI-X de 64 bits y 133 MHz (Soportan tarjetas 3.3v) 4 PCI-X de 6 bits y 100 MHz (Soporta tarjetas 3.3v) 1 PCI de 32 bits y 33 MHz (Soporta tarjetas anteriores 5v o tarjetas universales)
Controladores de Unidad de Disco	Controlador dual integrado PCI Ultra320 LVD SCSI LSI Logic 53C1030
Controlador RAID	PERC4/Di (Controlador RAID U320 de doble canal con caché de 128 MB respaldado por batería) PERC3/DC (Controlador RAID PCI de doble canal) PERC3/QC (Controlador RAID PCI de cuatro canales)
Discos Duros	(Funcionalidad hot-plug que requiere la incorporación de un controlador RAID) Hasta 8 unidades de disco SCSI con capacidad hot-plug de 1" Unidades de disco SCSI Ultra 160 y Ultra 320 de 10,000 y 15,000 RPM disponibles
Máximo Almacenamiento interno	Hasta 1.168 TB
Puertos	Puertos duales para Bus Serial Universal (USB)
Gráficos	Controlador integrado ATI-Rage XL con 8 MB en memoria SDRAM (no tiene capacidad de crecimiento)

Vista del equipo completo de frente:

Vista de la segunda parte del equipo:

Con los cuales se realiza la conexión de la red y el enlace con la Intranet.

La Intranet se ha diseñado con el software de Macromedia Dremweaber UltraDev ver 4.0, en la que la pagina principal, contiene dos barras de menús, una en posición vertical y la otra en horizontal, donde la horizontal contiene todos los datos sobre la propia Dirección General, y en la segunda, contiene información sobre la toma de decisiones de los directivos, la cual es considerada como el objetivo principal de esta Intranet, y la digitalización de un mapa sensitivo de la republica.

En la primer opción del menú Horizontal, denominada "Directorios", contiene un submenú el cual contendrá el directorio de la Dirección General, con Nombre, Cargo, Correo Electrónico y Teléfonos, la segunda opción, presentara el directorio de los Centros SCT, conteniendo también el Nombre del Estado, Cargo, Nombre del Responsable, Correo Electrónico y Teléfonos, y la ultima opción del menú "Directorios", dispondrá de un directorio telefónico de instancias externas a la D.G.C.C.

La segunda opción del menú Horizontal, denominada "Correo Electrónico", presenta una conexión directa con el servidor de correos de la Secretaría, con la que es posible la consulta de correos por usuario, enviada a cada mando medio.

La pagina al servidor de correo electrónico, le solicita al usuario su clave de usuario y una contraseña, con las cuales podrá revisar su correo electrónico. Esta conexión es muy importante debido a la rapidez y gran manejo de información a nivel nacional, de asuntos importantes para ayuda a la toma de decisiones.

La tercera opción del menú Horizontal, denominada "Página principal SCT", contiene la liga a la pagina de la Secretaría de Internet, disponible a cualquier persona interesada a conocer algo de la misma dependencia, así como lo que se esta realizando a nivel global dentro de la misma en le área de noticias. Figura V.3.

La cuarta opción del menú Horizontal, denominada "Política de Calidad", contendrá un vínculo a una pagina, sobre el sistema de gestión de calidad de la D.G.C.C.

En el menú principal (Vertical), contendrá las diferentes ligas como: "Inicio", "PNCC 2003", "Resumen del PNCC", "Resumen Subsecretaria", "Licitaciones", "Maquinaria", "Obs. Form. por Org. de Cont.", "Sistema Gest. de la Cal.", "Carreteras Limpias", "Descentralización", "Corredores Carreteros", "Publicaciones".

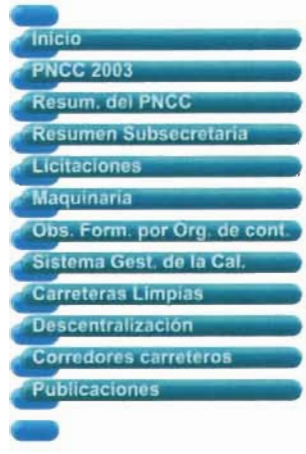


Figura V.3.

En la primer opción del menú principal (vertical), denominada como "PNCC 2003", contiene la liga a la página del Programa Nacional de Conservación de Carreteras

La página principal del programa contiene todos los vínculos con los estados (Figura V.4) y estos a su vez con su programa. (Figura V.5).

La segunda opción del menú, denominado como "Resumen del PNCC", presenta un resumen de los programas del 2002 y 2003.

Figura V.4.

Programa Nacional de Conservación de Carreteras Federales 2003

30 de Noviembr

NUM.	NOMBRE DE LA OBRA	UBICACION	META	RECURSOS FISCALES	CREDITO EXTERNO	TOTAL ASIGNACION	AV. FIS. UNIDAD	%
	AGUASCALIENTES			56,570,330.94	0.00	56,570,330.94		99.8
	RECONSTRUCCIÓN			1,700,000.00	0.00	1,700,000.00	3.00	100.0
	Reconstrucción de Puentes		3.00	1,700,000.00	0.00	1,700,000.00	3.00	100.0
1	Canal La Misión (Aguascalientes - Lím. Edos. Ags./Zac)	41+120	1.00	674,000.00		674,000.00	1.00	100.0
2	El Saucillo (Aguascalientes - Lím. Edos. Ags./Zac)	42+930	1.00	640,000.00		640,000.00	1.00	100.0
3	PIV Entr. Rincón de Romos (Aguascalientes - Lím. Edos. Ags./Zac)	44+680	1.00	386,000.00		386,000.00	1.00	100.0
	CONSERVACIÓN			54,330,330.94	0.00	54,330,330.94		99.8
	Conservación Periódica		174.01	37,952,589.00	0.00	37,952,589.00		100.0
	Recuperación de Pavimento y Carpeta		4.00	4,000,000.00	0.00	4,000,000.00	4.00	100.0
4	Aguascalientes - Zacatecas (2 Cpos.)	16.0-18.0	4.00	4,000,000.00		4,000,000.00	4.00	100.0
	Carpeta		16.00	7,663,000.00	0.00	7,663,000.00	16.00	100.0
5	Aguascalientes - Zacatecas (2 Cpos.)	18.0-26.0	16.00	7,663,000.00		7,663,000.00	16.00	100.0
	Renivelación y Riego de Sello		79.81	20,032,418.00	0.00	20,032,418.00	79.81	100.0
6	Aguascalientes - Zacatecas (2 Cpos.)	10.3-16.0	11.40	3,000,000.00		3,000,000.00	11.40	100.0
7	Aguascalientes - Jalpa (2 Cpos.)	2.5-8.2	11.40	2,430,418.00		2,430,418.00	11.40	100.0
8	Rincón de Romos - Cienega Grande *	0.0 - 3.0	4.00	1,000,000.00		1,000,000.00	4.00	100.0
9	León - Aguascalientes (2 Cpos.)	110.9-127.6	33.40	9,192,000.00		9,192,000.00	33.40	100.0
10	Aguascalientes - Zacatecas	58.0 - 62.7	4.70	1,460,000.00		1,460,000.00	4.70	100.0
11	Quelos - Aguascalientes (2 Cpos.)	78.0-81.5	7.00	1,550,000.00		1,550,000.00	7.00	100.0
12	Acceso a Pabellón de Arteaga **	0.0 - 4.7	7.91	1,400,000.00		1,400,000.00	7.91	100.0

Figura V.5.

Dentro del año 2002, se despliega un submenú, el cual contiene el resumen "por Programa" (Figura V.6), "por Entidad Federativa" (Figura V.7), las gráficas de los estados donde hubo mayor inversión en el año (Figura V.8), en la cual también se presenta una tabla indicando los estados graficados, así como una comparativa de lo asignado en dinero y su porcentaje contra lo erogado, al igual que el avance físico y financiero en porcentajes, con un cuadro de observaciones referente a la inversión, "Graficas Avance físico" (Figura V.9).

RESUMEN NACIONAL AVANCE FISICO - FINANCIERO

CIERRE DEL EJERCICIO 2002

PROGRAMA	META	ASIGNACION RECURSOS FISCALES ($)	ASIGNACION CREDITO EXTERNO ($)	TOTAL ASIGNACION ($)	AVANCE FISICO	
					AVANCE	o/o
		3,434,481,613.08	1,341,217,000.00	4,775,698,613.08		99.8
TOTAL FORANEO		3,377,575,972.96	1,340,202,000.00	4,717,777,972.96		99.8
RECONSTRUCCION		419,393,180.31	552,509,467.00	971,902,647.31		98.8
Reconstrucción de Tramos de la Red Federal (km)	379.3	149,257,783.00	476,405,051.00	625,662,834.00	373.6	98.2
Reconstrucción de Puentes	116.0	270,135,397.31	76,104,416.00	346,239,813.31	116.0	100.0
CONSERVACION		2,911,731,908.47	784,022,533.00	3,695,754,441.47		98.0
a) Conservación Periódica	6,139.4	1,430,584,600.00	784,022,533.00	2,214,607,133.00		99.8
CAR Carpeta (km)	490.8	157,342,314.99	58,276,043.31	215,618,358.30	490.8	100.0
CS Carpeta y Riego de Sello (km)	36.7	9,789,099.00	6,345,000.00	16,134,099.00	36.7	100.0
RPC Recuperación de Pavimento y Carpeta (km)	705.9	251,051,036.79	317,002,287.00	568,053,323.79	705.9	100.0
RPM Recuperación de Pavimento y Microcarpeta (km)	32.1	19,357,189.17	0.00	19,357,189.17	32.1	100.0
RPS Recuperación de Pavimento y Riego de Sello (km)	94.0	21,790,317.00	20,433,000.00	42,223,317.00	94.0	100.0
REC Renivelaciones y Carpeta (km)	857.8	224,767,567.29	266,998,589.38	491,766,156.67	851.6	99.4
REM Renivelación y Microcarpeta (km)	44.2	8,314,129.79	20,266,846.94	28,580,976.73	44.2	100.0
ROG Renivelación y Open Graded (km)	65.0	18,059,894.62	9,221,000.00	27,280,894.62	65.0	100.0
RES Renivelaciones y Riego de Sello (km)	1,723.6	390,560,143.71	63,121,216.37	453,681,360.08	1,715.7	99.4
MIC Carpeta Delgada (km)	142.2	51,696,751.83	0.00	51,696,751.83	142.2	100.0
RSE Riego de Sello (km)	1,843.9	167,055,702.98	3,664,550.00	170,720,252.98	1,843.9	100.0
FRC Fresado y Carpeta (km)	25.0	0.00	18,694,000.00	18,694,000.00	25.0	100.0

Figura V.6.

Dentro del año 2003, se despliega un submenú, el cual contiene el resumen "por Programa" (figura V.10), "por Entidad Federativa" (Figura V.11), las gráficas de los estados donde hubo mayor inversión en el año (Figura V.12), en la cual también se presenta una tabla indicando los estados graficados, así como una comparativa de lo asignado en dinero y su porcentaje contra lo erogado, al igual que el avance físico y financiero en porcentajes, con un cuadro de observaciones referente a la inversión, "Gráficas Avance Físico" (Figura V.13), "Gráficas Recursos Asignados contra Recursos Erogados" (Figura V.14).

RESUMEN NACIONAL AVANCE FISICO - FINANCIERO

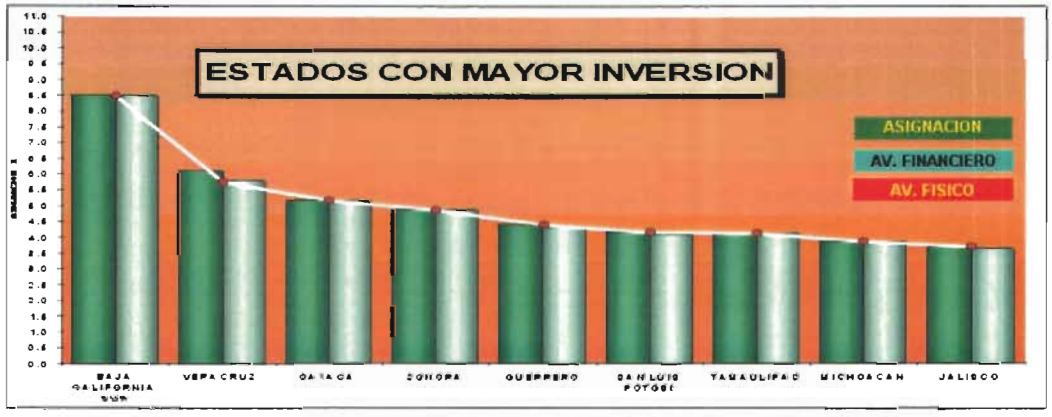
CIERRE DEL EJERCICIO 2002

ENTIDAD	RECURSOS FISCALES	CREDITO EXTERNO	ASIGNACION 2002	AV. FISICO %
AGUASCALIENTES	41,017,570.00	12,413,000.00	53,430,570.00	100.0
BAJA CALIFORNIA	129,200,162.00	40,043,770.00	169,243,932.00	100.0
BAJA CALIFORNIA SUR	380,753,838.00	24,640,000.00	405,393,838.00	100.0
CAMPECHE	75,563,371.69	27,906,000.00	103,469,371.69	100.0
COAHUILA	88,346,025.00	27,848,000.00	116,194,025.00	100.0
COLIMA	45,452,288.33	11,605,500.00	57,057,788.33	100.0
CHIAPAS	154,118,641.67	16,560,000.00	170,678,641.67	100.0
CHIHUAHUA	103,103,040.15	58,106,249.00	161,209,289.15	100.0
DURANGO	89,988,582.80	81,710,000.00	171,698,582.80	100.0
GUANAJUATO	126,194,915.00	41,115,000.00	161,309,915.00	100.0
GUERRERO	174,641,689.00	35,198,000.00	209,839,689.00	100.0
HIDALGO	104,841,485.00	31,045,007.00	135,886,492.00	100.0
JALISCO	141,620,696.00	34,344,607.00	175,965,303.00	100.0
MEXICO	70,864,000.00	33,860,000.00	104,724,000.00	100.0
MICHOACAN	122,336,244.00	63,066,011.00	185,402,255.00	100.0
MORELOS	35,113,456.00	61,105,000.00	96,218,456.00	100.0
NAYARIT	60,991,185.00	33,060,100.00	94,051,285.00	100.0
NUEVO LEON	102,899,283.00	69,440,000.00	172,339,283.00	100.0
OAXACA	174,916,740.00	72,024,000.00	246,940,740.00	100.0
PUEBLA	78,996,978.00	44,150,000.00	123,146,978.00	100.0
QUERETARO	51,459,722.00	16,440,303.00	67,900,025.00	100.0
QUINTANA ROO	46,923,128.00	10,538,332.00	57,461,460.00	100.0
SAN LUIS POTOSI	121,620,577.00	77,064,000.00	198,684,577.00	100.0
SINALOA	68,620,836.00	70,672,000.00	139,292,836.00	100.0
SONORA	173,006,339.00	58,909,309.00	231,915,648.00	100.0
TABASCO	[illegible]	[illegible]	[illegible]	[illegible]

Figura V.7.

PROGRAMA NACIONAL DE CONSERVACION DE CARRETERAS FEDERALES 2002

CIERRE DEL EJERCICIO 2002



	BAJA CALIFORNIA SUR	VERACRUZ	OAXACA	SONORA	GUERRERO	SAN LUIS POTOSI	TAMAULIPAS	MICHOACAN	JALISCO
ASIGNACION $	405,393,838.0	292,067,293.0	246,940,740.0	231,915,648.00	209,839,689.0	198,684,577.0	197,138,749.0	185,402,255.0	175,965,303
ASIGNACION %	8.5	6.1	5.2	4.9	4.4	4.2	4.1	3.9	3.7

Figura V.8.

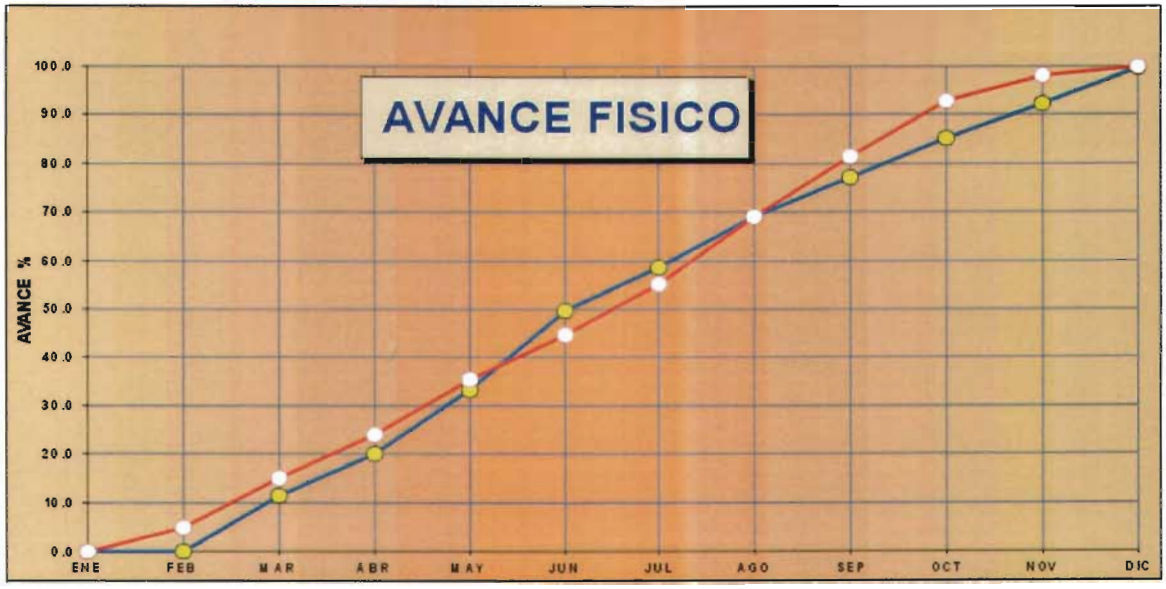


Figura V.9.

RESUMEN NACIONAL AVANCE FISICO

30 DE NOVIEMBRE 2003

PROGRAMA	META	ASIGNACION RECURSOS FISCALES $	ASIGNACION CREDITO EXTERNO $	TOTAL ASIGNACION $	AVANCE FIS	
					AVANCE	
		3,613,744,825.00	935,544,800.00	4,549,288,825.00		
TOTAL FORANEO		3,588,458,525.00	932,832,564.00	4,521,291,089.00		
RECONSTRUCCION		276,348,331.00	334,767,372.00	610,107,703.00		
Reconstrucción de Tramos de la Red Federal (km)	207.2	131,461,864.00	252,650,198.00	384,112,162.00	162.9	
Reconstrucción de Puentes	91.0	143,878,367.00	82,117,174.00	225,995,541.00	82.1	
CONSERVACION		3,264,718,951.00	596,331,592.00	3,861,042,543.00		
a) Conservación Periódica	7,570.9	1,622,823,638.00	598,331,592.00	2,219,155,230.00		
RPC Recuperación de Pavimento y Carpeta (km)	685.1	369,757,765.76	182,415,883.00	552,173,648.76	589.9	
REC Renivelaciones y Carpeta (km)	490.9	247,431,428.05	111,009,933.00	358,441,361.05	446.7	
CAR Carpeta (km)	335.9	136,241,253.99	13,879,008.00	150,120,261.99	303.3	
RES Renivelaciones y Riego de Sello (km)	2,087.5	376,987,239.53	109,212,888.00	486,200,127.53	1,967.9	
ROG Renivelación y Open Graded (km)	28.6	8,931,376.00	641,824.00	9,573,200.00	28.6	
RSE Riego de Sello (km)	3,511.3	341,618,398.23	31,982,907.18	373,601,305.41	3,384.4	
MIC Carpeta Delgada (km)	128.5	33,918,120.00	4,342,596.00	38,260,716.00	128.5	
RCS Renivelación Carpeta y Riego de Sello (km)	60.6	17,938,812.00	0.00	17,938,812.00	60.6	
RPS Recuperación de Pavimento y Riego de Sello (km)	89.9	48,283,142.89	336,000.00	48,619,142.89	78.4	
REM Renivelación y Carpeta Delgada (km)	18.4	8,991,205.00	24,552.82	9,015,757.82	18.2	
FRC Fresado y Carpeta (km)	35.0	19,345,000.00	16,044,000.00	35,389,000.00	35.0	

Figura V.10.

RESUMEN NACIONAL AVANCE FISICO

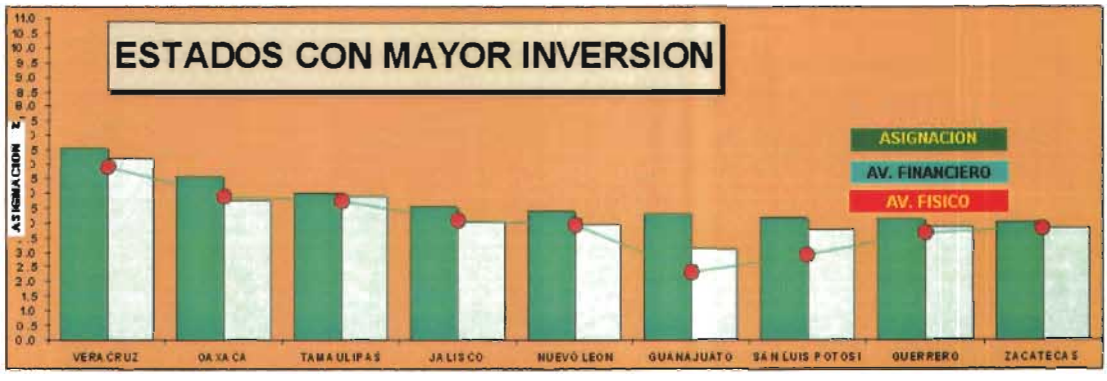
30 DE NOVIEMBRE DE 2003

E N T I D A D	RECURSOS FISCALES	CREDITO EXTERNO	ASIGNACION	AV. FISICO %
AGUASCALIENTES	56,570,330.94	0.00	56,570,330.94	99.8
BAJA CALIFORNIA	139,942,775.70	0.00	139,942,775.70	97.3
BAJA CALIFORNIA SUR	118,278,747.19	24,950,000.00	143,228,747.19	96.9
CAMPECHE	58,783,949.10	40,793,000.00	99,576,949.10	96.6
COAHUILA	131,031,583.69	27,019,480.00	158,051,063.69	91.6
COLIMA	42,860,361.74	6,800,000.00	49,660,361.74	98.5
CHIAPAS	141,750,812.13	23,610,000.00	165,360,812.13	96.0
CHIHUAHUA	161,401,997.24	16,232,882.00	177,634,879.24	90.9
DURANGO	164,545,211.93	15,015,659.00	179,561,870.93	88.2
GUANAJUATO	98,192,365.51	97,300,162.00	195,492,527.51	53.7
GUERRERO	159,626,013.03	28,381,576.00	188,007,589.03	88.5
HIDALGO	87,419,307.74	9,938,600.00	97,357,907.74	91.5
JALISCO	138,180,829.06	67,549,284.00	205,730,113.06	90.2
MEXICO	95,561,413.39	22,762,569.00	118,323,982.39	99.0
MICHOACAN	129,200,346.46	52,298,000.00	181,498,346.46	94.6
MORELOS	31,288,644.25	38,650,000.00	69,938,644.25	94.9
NAYARIT	75,485,510.74	16,189,241.00	91,674,751.74	87.4
NUEVO LEON	157,328,920.55	41,613,550.00	198,942,470.55	89.9
OAXACA	200,794,414.64	51,860,000.00	252,654,414.64	88.2
PUEBLA	144,391,461.83	1,200,000.00	145,591,461.83	97.3
QUERETARO	60,966,600.74	46,108,000.00	107,074,600.74	79.7
QUINTANA ROO	51,471,236.71	9,034,483.00	60,505,719.71	97.1
SAN LUIS POTOSI	106,104,597.44	83,852,000.00	189,956,597.44	70.2

Figura V.11.

PROGRAMA NACIONAL DE CONSERVACION DE CARRETERAS FEDERALES 2003

30 DE NOVIEMBRE DE 2003

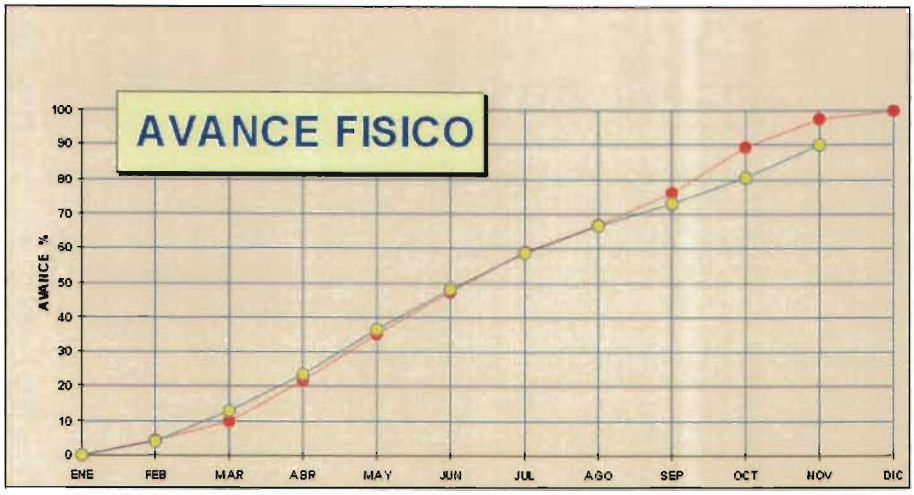


	VERACRUZ	OAXACA	TAMAULIPAS	JALISCO	NUEVO LEON	GUANAJUATO	SAN LU IS POTOSI	GUERRERO	ZACATECAS
ASIGNACION $	299,160,520.6	252,654,414.6	227,428,142.7	205,730,113.1	198,942,470.6	195,492,527.5	189,956,597.4	188,007,589.0	182,921,421.0
ASIGNACION %	6.6	5.6	5.0	4.5	4.4	4.3	4.2	4.1	4.0
EROGADO $	283,393,303.1	216,216,734.0	223,723,594.9	182,648,757.2	179,069,405.4	143,257,191.0	171,017,357.3	176,832,563.4	175,453,542.5

Figura V.12.

PROGRAMA NACIONAL DE CONSERVACION DE CARRETERAS FEDERALES 2003

30 DE NOVIEMBRE DE 2003



OBSERVACIONES

AVANCE FISICO PROGRAMADO AL 30 DE NOVIEMBRE (97.6%)
AVANCE FISICO REAL AL 30 DE NOVIEMBRE (90.1%)

Figura V.13.

PROGRAMA NACIONAL DE CONSERVACION DE CARRETERAS FEDERALES 2003

30 DE NOVIEMBRE DE 2003

OBSERVACIONES

AVANCE FINANCIERO PROGRAMADO AL 30 DE NOVIEMBRE (96.0%)

Figura V.14.

La tercer opción del menú, denominado como "Resumen Subsecretaría", presenta los tres cuadros resumen de los principales programas de conservación que maneja la Dirección General.

Dentro de la misma opción se encuentra un submenú en el cual se muestra el cuadro resumen del programa de inversiones en el año 2003 (Figura V.15), también el cuadro resumen del programa de licitaciones de las obras y supervisiones (Figura V.16), y la última opción de este submenú, presenta el vínculo con el cuadro resumen sobre las licitaciones de los diferentes estudios y proyectos realizados en el 2003 (Figura V.17).

Seguimiento del Programa de Inversión en Infraestructura Carretera 2003 PEF

Programa	Presupuesto anual autorizado	Presupuesto programado en el período	Monto adjudicado (mdp) (1)	Avance al 31 de julio de 2003			
				Ejercido (mdp) (3)	En trámite de pago (4)	Total (5)	Avance programad
CONSTRUCCIÓN Y MODERNIZACIÓN							
Obra							
Estudios y Proyectos							
Derecho de vía							
Supervisión							
Otros							
CONSERVACION	**4,526.5**	**2,476.3**	**4,446.1**	**2,013.6**	**447.8**	**2,461.4**	**9**
Obra	4,448.1	2,436.0	4,406.0	2,008.5	441.0	2,449.5	1
Estudios y Proyectos	50.0	27.4	14.0	0.1	1.6	1.7	
Supervisión	26.1	12.9	26.1	5.0	5.3	10.3	7
Otros*	2.3	0.0	0.0	0.0	0.0	0.0	
CAMINOS RURALES							
Obra							
Estudios y Proyectos							
Supervisión							
Otros							
EMPLEO TEMPORAL							
PET normal Obra							
PET Emergencias							

Figura V.15.

La cuarta opción de este menú principal, se refiere al rubro de "Licitaciones", en la cual si realizo otros cuadros resumen, sobre las licitaciones realizadas en los años 2002 y 2003.

Dentro del submenú, del año 2002 y del 2003, los cuadros resumen se les dio diferentes ordenamientos a las bases de datos para la fácil ubicación de alguna licitación en especial de los directivos. Los diferentes ordenamientos de la base de datos, fueron los siguientes:

1. "Ord. Entidad Fed.", Ordenada por cada Estado de la República Mexicana y en orden alfabético. (Figura V.18) y del año 2003 (Figura V.21).
2. "Ord. Prov. o contrat.", Ordenada por el nombre del Proveedor o de la empresa contratista a la cual se le asignó la obra. (Figura V.19) y del año 2003 (Figura V.22).
3. "Ord. Importe del contrat.", Ordenada por uno de los datos más importantes de cada obra es la columna del importe del contrato. (Figura V.20) y del año 2003 (Figura V.23).

Seguimiento del Programa de Licitaciones 2003 para Infraestructura Carretera (PEF)

Programa	Total de obras	Total de tramos	Licitadas	Revalidadas	Monto adjudicado (mdp) (1)	Avance físico (%)	Pendiente Por licitar	Pendiente Por revalidar
CONSTRUCCIÓN Y MODERNIZACIÓN								
Obra								
Derecho de vía								
Supervisión								
Otros								
CONSERVACION	**1,481**	**1,481**	**1,451**	**27**	**4,432.1**	**58.6%**	**3**	
Obra	1,448	1,448	1,419	26	4,406.0	58.6%	3	
Supervisión	33	33	32	1	26.1		0	
otros*					0.0			
CAMINOS RURALES								
Obra								
Supervisión								
Otros								
EMPLEO TEMPORAL								
PET normal Obra								
PET Emergencias								
TOTAL	**1,481**	**1,481**	**1,451**	**27**	**4,432.1**		**3**	**0**

(1) El monto adjudicado se refiere al total de los recursos comprometidos por fallos o contratos

***Nota: el concepto "otros" se refiere a las adquisiciones (23.684 mdp se cancelan por instrucciones de Oficialía Mayor)**

Figura V.16.

Seguimiento del Programa de Licitaciones 2003 para Estudios y Proyectos

Programa		Total de tramos	Total de proyectos	Licitados o en proceso de licitación	Por administración en proceso	Monto adjudicado (mdp) (1)	Avance físico (%)	Por licitar	De adm
CONSTRUCCIÓN Y MODERNIZACIÓN									
Total		**982**	**991**	**605**	**324**	**4,596.5**		**68**	
CONSERVACION		**299**	**299**	**150**	**0**	**14.0**	**5.8%**	**149**	
CAMINOS RURALES									
AUTOPISTAS DE CUOTA									
SERVICIOS TECNICOS									
TOTAL		**299**	**299**	**150**	**0**	**14.0**			

Figura V.17.

Resultados de las Licitaciones del
Programa Nacional de Conservación de Carreteras 2002

Información de acuerdo a COMPRANET
Febrero de 2003

Entidades	No. de licitación	No. de contrato	Proveedor o contratista	Fec susc del c
AGUASCALIENTES	00009002-034-02	2-A-CB-A-037-Y-0-2	CR Y CIA S.A. DE C.V.	11/0
AGUASCALIENTES	00009014-086-01	2-A-CB-A-501-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	18/0
AGUASCALIENTES	00009014-087-01	2-A-CB-A-502-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	18/0
AGUASCALIENTES	00009014-088-01	2-A-CB-A-503-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	18/0
AGUASCALIENTES	00009014-089-01	2-A-CB-A-504-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	18/0
AGUASCALIENTES	00009014-090-01	2-A-CB-A-505-W-0-2	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A. DE C.V.	19/0
AGUASCALIENTES	00009014-091-01	2-A-CB-A-506-W-0-2	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A. DE C.V.	19/0
AGUASCALIENTES	00009014-092-01	2-A-CB-A-507-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	19/0
AGUASCALIENTES	00009014-093-01	2-A-CB-A-508-W-0-2	GRUPO INGENIEROS CIVILES Y ARRENDADORES DE MAQUINARIA, S.A.	14/0
AGUASCALIENTES	00009014-094-01	2-A-CB-A-509-W-0-2	L.A.E. SERGIO LUEVANO REYES	20/0
AGUASCALIENTES	00009014-095-01	2-A-CB-A-510-W-0-2	ARRENDADORA Y CONSTRUCTORA MAYA, S.A. DE C.V.	20/0
AGUASCALIENTES	00009014-096-01	2-A-CB-A-511-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	20/0
AGUASCALIENTES	00009014-097-01	2-A-CB-A-512-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	20/0
AGUASCALIENTES	00009014-100-01	2-A-CB-D-515-W-0-2	PAVIMENTOS Y MAQUINARIA, S.A. DE C.V.	12/0
BAJA CALIFORNIA	00009055-044-01	1-B-CB-A-502-W-0-2	ARRENDADORA DEL COLORADO DEL NORTE, S.A. DE C.V.	30/0
BAJA CALIFORNIA	00009002-017-02	2-B-CB-A-020-Y-0-2	UNIVERSO INGENIERIA Y PROYECTO, S.A. DE C.V.	12/0
BAJA CALIFORNIA	00009055-045-01	2-B-CB-A-503-W-0-2	ALTA INGENIERIA 2000 S.A. DE C.V.	30/0
BAJA CALIFORNIA	00009055-046-01	2-B-CB-A-504-W-0-2	ARRENDADORA LASSELLE, S.A. DE C.V.	30/0
BAJA CALIFORNIA	00009055-047-01	2-B-CB-A-505-W-0-2	JAUREGUI FELIX FERNANDO	30/0
BAJA CALIFORNIA	00009055-048-01	2-B-CB-A-506-W-0-2	JAUREGUI FELIX FERNANDO	30/0
BAJA CALIFORNIA	00009055-049-01	2-B-CB-A-507-W-0-2	JAUREGUI FELIX FERNANDO	30/0
BAJA CALIFORNIA	00009055-050-01	2-B-CB-A-508-W-0-2	ARRENDADORA DEL COLORADO DEL NORTE, S.A. DE C.V.	30/0
BAJA CALIFORNIA	00009055-003-02	2-B-CB-A-517-W-0-2	ARRENDADORA LASSELLE, S.A. DE C.V.	12/0
BAJA CALIFORNIA	00009055-004-02	2-B-CB-A-518-W-0-2	CONSTRUCTORA EPYCSA S.A. DE C.V.	12/0

Figura V.18.

Resultados de las Licitaciones del
Programa Nacional de Conservación de Carreteras 2002

Información de acuerdo a COMPRANET
Febrero de 2003

Entidades	No. de licitación	No. de contrato	Proveedor o contratista	Fecha de suscripción del contrato
CHIAPAS	00009019-057-02	2-G-CB-A-615-W-0-2	ABASTECEDORA DE MATERIALES MAREAS S.A DE C.V	19/12/2002
QUINTANA ROO	00009059-009-02	2-W-AA-A-517-W-0-2	ABASTECEDORA DE MATERIALES MAREAS S.A DE C.V	11/09/2002
QUINTANA ROO	00009059-013-02	2-W-AA-A-522-W-0-2	ABASTECEDORA DE MATERIALES MAREAS S.A DE C.V	19/09/2002
QUINTANA ROO	00009059-025-02	3-W-CB-A-506-W-0-3	ABASTECEDORA DE MATERIALES MAREAS S.A DE C.V	16/12/2002
QUERETARO	00009034-027-01	2-V-CB-A-509-W-0-2	ABRAHAM GONZÁLEZ MARTELL	28/01/2002
QUERETARO	00009034-005-02	2-V-CB-D-515-W-0-2	ABRAHAM GONZÁLEZ MARTELL	10/04/2002
QUINTANA ROO	00009059-029-01	2-W-CB-A-503-W-0-2	ABRAHAM RODRÍGUEZ HERRERA	29/01/2002
QUINTANA ROO	00009059-031-01	2-W-CB-A-505-W-0-2	ABRAHAM RODRÍGUEZ HERRERA	30/01/2002
QUINTANA ROO	00009059-022-02	3-W-CB-A-503-W-0-3	ABRAHAM RODRÍGUEZ HERRERA	16/12/2002
GUANAJUATO	00009054-015-02	3-K-CB-A-506-W-0-3	ACARREOS, TERRACERIAS Y EDIFICACION S.A. DE C.V.	11/12/2002
GUANAJUATO	00009054-017-02	3-K-CB-A-508-W-0-3	ACARREOS, TERRACERIAS Y EDIFICACION S.A. DE C.V.	13/12/2002
GUANAJUATO	00009054-020-02	3-K-CB-A-514-W-0-3	ACARREOS, TERRACERIAS Y EDIFICACION S.A. DE C.V.	13/12/2002
CHIAPAS	00009019-008-02	2-G-CF-A-531-W-0-2	ADMINISTRACION Y SERV. TEC. A LA CONSTR. S.A. DE C.V.	09/07/2002
QUERETARO	00009034-025-01	2-V-CB-A-507-W-0-2	AGACEL,AGREGADOS Y ASFALTOS S.A. DE C.V.	28/01/2002
QUERETARO	00009034-026-01	2-V-CB-A-508-W-0-2	AGACEL,AGREGADOS Y ASFALTOS S.A. DE C.V.	28/01/2002
PUEBLA	00009050-041-01	2-U-CB-D-502-W-0-2	AGREGADOS LAS DERRUMBADAS S.A. DE C. V.	08/02/2002
PUEBLA	00009050-042-01	2-U-CB-D-503-W-0-2	AGREGADOS LAS DERRUMBADAS S.A. DE C. V.	25/02/2002
PUEBLA	00009050-043-01	2-U-CB-D-504-W-0-2	AGREGADOS LAS DERRUMBADAS S.A. DE C. V.	25/02/2002
QUERETARO	00009034-022-01	2-V-CB-A-504-W-0-2	AGREGADOS Y DERIVADOS DEL CENTRO S.A. DE C.V.	28/01/2002
OAXACA	00009047-069-01	2-T-CB-A-507-W-0-2	ALARCON ALCANTARA FILEMON JUAN DE DIOS	22/01/2002
CHIHUAHUA	00009021-105-01	2-H-CB-A-519-W-0-2	ALBATROS DISEÑO Y CONSTRUCCION S.A. DE C.V.	04/02/2002
SAN LUIS POTOSI	00009036-091-01	2-X-CB-A-605-W-0-2	ALCH CONSTRUCCION S.A. DE C.V.	13/02/2002
SAN LUIS POTOSI	00009036-022-02	2-X-CB-A-613-W-0-2	ALCH CONSTRUCCION S.A. DE C.V.	17/04/2002
SAN LUIS POTOSI	00009036-031-02	2-X-CB-A-616-W-0-2	ALCH CONSTRUCCION S.A. DE C.V.	14/05/2002

Figura V.19.

Resultados de las Licitaciones del Programa Nacional de Conservación de Carreteras 2002

Información de acuerdo a COMPRANET
Febrero de 2003

ación	No. de contrato	Proveedor o contratista	Fecha de suscripción del contrato	Importe total
3-02	2-C-CE-A-527-W-0-2	FABRICACION Y COLOCACION DE PAVIMENTO, S.A. DE C.V.	12/04/2002	$68,425,399.03
3-02	2-C-CE-A-526-W-0-2	CANALES Y TERRACERIAS DEL PACIFICO, S.A. DE C.V.	17/04/2002	$49,975,579.46
7-02	2-C-CE-A-525-W-0-2	FABRICACION Y COLOCACION DE PAVIMENTO, S.A. DE C.V.	12/04/2002	$41,585,524.01
9-02	2-K-CE-A-502-W-0-2	CONSTRUCTORA AZACAN SA DE CV	26/09/2002	$37,815,902.46
1-02	2-C-CB-A-516-W-0-2	FABRICACION Y COLOCACION DE PAVIMENTO, S.A. DE C.V.	22/03/2002	$36,218,956.62
3-02	2-J-CB-A-518-W-0-2	ROSTEC DE MEXICO S.A. DE C.V.	16/05/2002	$35,152,244.44
3-02	2-C-CB-A-521-W-0-2	CONSTRUCTORA GUSA S.A. DE C.V.	26/03/2002	$29,160,519.04
3-02	2-X-CB-D-611-W-0-2	TRANSPORTACIONES Y CONSTRUCCIONES TAMAULIPECOS S.A. DE C.V.	14/05/2002	$28,361,367.20
3-02	2-G-CB-A-520-W-0-2	FREYSSINET DE MEXICO, S.A. DE C.V.	14/05/2002	$27,363,836.80
5-02	2-L-CB-A-507-W-0-2	PAVIMENTOS Y CONSTRUCCIONES DE GUERRERO S.A. DE C.V.	06/02/2002	$25,397,533.47
2-02	2-4-CB-D-545-W-0-2	PROYECTO Y CONSTRUCCIONES DEL USUMACINTA S.A. DE C.V.	17/06/2002	$24,077,237.28
7-01	2-2-CB-D-501-W-0-2	GIFER, S.A. DE C.V.	18/02/2002	$23,625,009.34
5-02	2-C-CE-A-524-W-0-2	TERRACERIAS, PAVIMENTOS Y CAMINOS S.A. DE C.V.	09/04/2002	$21,811,492.70
5-02	2-C-CB-A-518-W-0-2	GRUPO ASFALTOS PROCESADOS, SA DE CV	22/03/2002	$21,379,631.38
9-01	2-S-CB-A-017-W-0-2	TRANSPORTACIONES Y CONSTRUCCIONES TAMAULIPECOS S.A. DE C.V.	31/01/2002	$20,388,181.80
9-02	2-X-CB-D-607-W-0-2	VIASLIDADES Y CONSTRUCCIONES TORRES, S.A. DE C.V.	17/04/2002	$20,282,220.85
1-02	2-4-CB-D-544-W-0-2	PROYECTO Y CONSTRUCCIONES DEL USUMACINTA S.A. DE C.V.	17/06/2002	$20,257,481.58
5-02	2-Y-CB-D-517-W-0-2	INGENIEROS Y EQUIPOS MECANICOS S.A. DE C.V.	20/05/2002	$19,138,000.11
2-02	2-2-CB-A-516-W-0-2	MATERIALES Y CONSTRUCCIONES VILLA DE AGUAYO, S.A. DE C.V.	05/04/2002	$18,996,563.46
1-02	2-P-CB-D-515-W-0-2	CONSTRUCCIONES Y CARRETERAS, S.A. DE C.V.	25/04/2002	$18,894,121.19
1-02	2-Q-CB-D-505-W-0-2	CAMINOS Y PAVIMENTOS DEL SUR, S.A. DE C.V.	17/04/2002	$18,244,515.86
1-02	2-X-CB-A-612-W-0-2	GENERAL DE CONSTRUCCIONES Y MAQUINARIA, S.A. DE C.V.	17/04/2002	$18,161,411.43
3-02	2-L-CB-A-546-W-0-2	INGENIERIA SUPERVISION Y CONSTRUCCION S.A. DE C.V.	13/12/2002	$17,387,969.72
1-02	2-Z-CB-A-D-550-W-0-2	COMPAÑIA CONSTRUCTORA MAS, S.A. DE C.V.	23/12/2002	$17,176,402.85

Figura V.20.

Resultado de las licitaciones del

Programa Nacional de Conservación de Carreteras

Octubre 2003

Entidad	No. de Licitación	No. de Contrato	Proveedor o Contratista
Aguascalientes	00009014-047-02	3-A-CB-A-W-521-0-3	DESARROLLO Y LOTIFICACIONES DE TERRENOS DE AGUASCALIENTES, S.A DE C.V
Aguascalientes	00009014-047-02	3-A-CB-A-W-521-0-3	DESARROLLO Y LOTIFICACIONES DE TERRENOS DE AGUASCALIENTES, S.A DE C.V
Aguascalientes	00009014-047-02	3-A-CB-A-W-521-0-3	DESARROLLO Y LOTIFICACIONES DE TERRENOS DE AGUASCALIENTES, S.A DE C.V
Aguascalientes	00009014-035-02	3-A-CB-A-W-509-0-3	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A DE C.V
Aguascalientes	00009014-033-02	3-A-CB-A-W-507-0-3	PAVIMENTOS Y MAQUINARIA, S.A DE C.V.
Aguascalientes	00009014-034-02	3-A-CB-A-W-508-0-3	PAVIMENTOS Y MAQUINARIA, S.A DE C.V.
Aguascalientes	00009014-038-02	3-A-CB-A-W-512-0-3	ARRENDADORA Y CONSTRUCTORA MAYA, S.A DE C.V
Aguascalientes	00009014-041-02	3-A-CB-A-W-515-0-3	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A DE C.V
Aguascalientes	00009014-036-02	3-A-CB-A-W-510-0-3	ARRENDADORA Y CONSTRUCTORA MAYA, S.A DE C.V
Aguascalientes	00009014-037-02	3-A-CB-A-W-511-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-040-02	3-A-CB-A-W-514-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-041-02	3-A-CB-A-W-515-0-3	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A DE C.V
Aguascalientes	00009014-046-02	3-A-CB-A-W-520-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-043-02	3-A-CB-A-W-517-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-043-02	3-A-CB-A-W-517-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-042-02	3-A-CB-A-W-516-0-3	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A DE C.V
Aguascalientes	00009014-042-02	3-A-CB-A-W-516-0-3	MAQUINARIA Y CONSTRUCCIONES CAFA, S.A DE C.V
Aguascalientes	00009014-039-02	3-A-CB-A-W-513-0-3	PAVIMENTOS Y MAQUINARIA, S.A DE C.V.
Aguascalientes	00009014-045-02	3-A-CB-A-W-519-0-3	GRUPO DE INGENIEROS CIVILES Y ARRENDADORES DE MAQUINARIA, S.A DE C.V.
Aguascalientes	00009014-044-02	3-A-CB-A-W-518-0-3	CONSTRUCTORA Y URBANIZADORA BONATERRA, S.A DE C.V.
Aguascalientes	SCT.621.P208.01	3-A-CB-A-523-W-0-3	PAVIMENTOS Y MAQUINARIA, S.A DE C.V.
Aguascalientes	SCT.621.P208.02	3-A-CB-A-524-W-0-3	ING. JUAN JACOBO MUÑOZ MAYA
Aguascalientes	00009014-027-02	3-A-CB-A-W-501-0-3	ARRENDADORA Y CONSTRUCTORA MAYA, S.A DE C.V
Aguascalientes	00009014-028-02	3-A-CB-A-W-502-0-3	ARRENDADORA Y CONSTRUCTORA MAYA, S.A DE C.V
Aguascalientes	00009014-029-02	3-A-CB-A-W-503-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-030-02	3-A-CB-A-W-504-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.
Aguascalientes	00009014-031-02	3-A-CB-A-W-505-0-3	GRUPO CONSTRUCTOR BRM, S.A DE C.V.

Figura V.21.

Resultado de las licitaciones del
Programa Nacional de Conservación de Carreteras
Octubre2003

Entidad	No. de Licitación	No. de Contrato	Proveedor o Contratista
Campeche	CSCT-04-CB-03-P208-09	3-D-CB-A-532-W-0-3	ABASTECEDORA DE MATERIALES MAREAS, S.A. DE C.V.
Campeche	00009017-056-02	3-D-CB-A-513-W-0-3	ABASTECEDORA DE MATERIALES MAREAS, S.A. DE C.V.
Campeche	00009017-058-02	3-D-CB-A-515-W-0-3	ABASTECEDORA DE MATERIALES MAREAS, S.A. DE C.V.
Chiapas	00009019-057-02	2-Q-CB-A-815-W-0-2	ABASTECEDORA DE MATERIALES MAREAS, S.A. DE C.V.
Quintana Roo	00009059-025-02	3-W-CB-A-506-W-0-3	ABASTECEDORA DE MATERIALES MAREAS, S.A. DE C.V.
Queretaro	00009034-026-02	3-Y-CB-A-508-W-0-3	ABRAHAM GONZALEZ MARTELL
Quintana Roo	00009059-005-03	3-W-CB-A-520-W-0-3	ABRAHAM RODRIGUEZ HERRERA
Quintana Roo	00009059-022-02	3-W-CB-A-503-W-0-3	ABRAHAM RODRIGUEZ HERRERA
Coahuila	00009020-079-02	3-E-CB-A-533-W-0-3	ABSER, S.A. DE C.V.
Coahuila	0000-9020-059-02	3-E-CB-A-519-W-0-3	ABSER, S.A. DE C.V.
Coahuila	0000-9020-061-02	3-E-CB-A-521-W-0-3	ABSER, S.A. DE C.V.
Durango	0009022-053-02	3-J-CB-A-515-W-0-3	ABSER, S.A. DE C.V.
Durango	00009022-055-02	3-J-CB-A-521-W-0-3	ABSER, S.A. DE C.V.
Guanajuato	00009054-015-02	3-K-CB-A-506-W-0-3	ACARREOS, TERRACERIAS Y EDIFICACION, S.A. DE C.V.
Guanajuato	00009054-017-02	3-K-CB-A-508-W-0-3	ACARREOS, TERRACERIAS Y EDIFICACION, S.A. DE C.V.
Guanajuato	00009054-020-02	3-K-CB-A-511-W-0-3	ACARREOS, TERRACERIAS Y EDIFICACION, S.A. DE C.V.
Sonora	00009052-020-02	3-Z-CB-A-506-W-0-3	ACSA CONSTRUCTORES, S.A. DE C.V.
Sonora	00009052-026-02	3-Z-CB-A-512-W-0-3	ACSA CONSTRUCTORES, S.A. DE C.V.
Queretaro	00009034-027-02	3-Y-CB-A-509-W-0-3	AGACEL AGREGADOS Y ASFALTOS, S.A. DE C.V.
Queretaro	00009034-033-02	3-Y-CB-A-515-W-0-3	AGO CONSTRUCCIONES S.A. DE C.V.
Puebla	00009050-036-02	3-U-CB-A-508-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Puebla	00009050-040-02	3-U-CB-A-512-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Puebla	00009050-041-02	3-U-CB-A-513-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Puebla	00009050-039-02	3-U-CB-A-511-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Puebla	00009050-044-02	3-U-CB-A-516-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Tlaxcala	00009041-026-02	3-3-CB-A-511-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Tlaxcala	00009041-023-02	2-3-CB-A-524-W-0-2	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Tlaxcala	00009041-003-03	3-3-CB-A-520-W-0-3	AGREGADOS LAS DERRUMBADAS, S.A. DE C.V
Jalisco	00009026-040-02	3-N-CB-A-517-W-0-3	AGREGADOS Y CONSTRUCCIONES SAN PATRICIO

Figura V.22.

Resultado de las licitaciones del
Programa Nacional de Conservación de Carreteras
Octubre 2003

	No. de Contrato	Proveedor o Contratista	Fecha de suscripción del Contrato	Importe
	3-R-CB-A-543-Y-0-3	PROYECTOS Y SUPERVISION DE OCCIDENTE S.A DE C.V.	14-Oct-03	36,698.21
	2-4-CB-A-W-502-0-2	CONSORCIO CONSTRUCTOR MENDOZA E HIJOS, S.A. DE C.V.		38,840.00
	3-3-CB-A-521-Y-0-3	ANGEL GARCIA GARCIA Y ASOCIADOS, S.C.	15-Jul-03	58,674.06
	3-3-CB-A-523-Y-0-3	ANGEL GARCIA GARCIA Y ASOCIADOS, S.C.	15-Jul-03	67,119.29
	3-3-CB-D-522-Y-0-3	ANGEL GARCIA GARCIA Y ASOCIADOS, S.C.	15-Jul-03	81,133.63
	3-P-CB-A-568-Y-0-3	COLMICH CONSTRUCCIONES, S. A. DE C.V.		83,720.00
	3-P-CB-A-569-Y-0-3	SERVICIOS PROFESIONALES EN INFRAESTRUCTURA Y URBANIZACIÓN, S.A. DE C.V	27-Jun-03	84,582.50
	3-A-CB-A-525-Y-0-3	CONSTRUCCIONES Y SERVICIOS DE OBRA CIVIL, S.A. DE C.V.	22-May-03	86,570.59
8	3-X-CB-A-529-Y-0-3	LATINOAMERICANA DE INGENIERIA CIVIL, S.A. DE C.V.	19-May-03	89,906.95
	3-U-CB-A-546-Y-0-3	ROHCA INGENIERIA, S.A. DE C.V.	09-May-03	95,489.66
	3-H-CB-A-555-Y-0-3	TECOPSA, TERRACERIAS CONSTRUCCIONES Y PAVIMENTOS, S.A. DE C.V.	09-Jun-03	98,145.01
	3-B-CB-A-545-Y-0-3	ARMAV, Ingeniería y Construcción, S.A. de C.V.	7-Ago-03	98,899.71
	3-M-CB-A-201-Y-0-3	CONSTRUCTORA RAYSA, S.A. DE C.V.	16-Jun-03	98,948.74
	2-4-CB-A-W-503-0-2	CONSORCIO CONSTRUCTOR MENDOZA E HIJOS, S.A. DE C.V.		99,800.00
	3-B-CB-A-548-Y-0-3	Ing. Alejandro Rivera Valenzuela	7-Ago-03	99,926.75
	3-M-CB-A-202-Y-0-3	PROYECTO Y CONSTRUCCIÓN URBANA, SANITARIA Y AMBIENTAL, S.A. DE C.V.	16-Jun-03	101,051.26
	3-P-CB-A-564-W-0-3	ASESORIA Y CONSTRUCCIONES BRAVO, S.A. DE C.V.	27-Jun-03	106,543.66
	3-K-CB-A-535-Y-0-3	CONSTRUCTORA BONE, S.A. DE C.V.		122,450.00
	3-P-CB-A-571-Y-0-3	SERVICIOS PROFESIONALES EN INFRAESTRUCTURA Y URBANIZACIÓN, S.A. DE C.V	27-Jun-03	124,602.50
	3-4-CB-A-587-Y-0-3	COMERCIALIZADORA Y CONSTRUCTORA ZEUS, S.A. DE C.V.	10-Jul-03	125,001.34
	3-J-CB-A-558-Y-0-3	PROYECTOS CARRETEROS, S. A. DE C.V.	25-Jun-03	125,574.30
	3-P-CB-A-573-Y-0-3	SERVER INGENIERIA, S.A. DE C.V.	1-Jul-03	127,618.60
	3-O-CB-A-529-Y-0-3	FOVIG, GRUPO DE INGENIARIA INTEGRAL, S.A DE C.V.	31-Jul-03	129,863.78
	3-Y-CB-A-525-W-0-3	CONSTRUCTORA Y ARRENDADORA SOFIA, S.A. DE C.V.	25-Jul-03	132,639.51
	3-4-CB-A-585-Y-0-3	INMOBILIARIA Y COMERCIALIZADORA N4, S.A DE C.V	12-Jul-03	134,995.94
	3-H-CB-A-544-W-0-3	CONSTRUCTORA ARALTE, S.A. DE C.V.	29-Ene-03	136,967.01
	3-4-CB-A-586-Y-0-3	COMERCIALIZADORA Y CONSTRUCTORA ZEUS, S.A. DE C.V.	10-Jul-03	140,013.24
	3-P-CB-A-572-Y-0-3	ILCON S.A. DE C.V.	27-Jun-03	143,612.38
	3-O-CB-A-533-Y-0-3	OSO INGENIERÍA, S.A. DE C.V.	1-Ago-03	149,874.82

Figura V.23.

La quinta opción de este menú principal, se refiere al rubro de "Maquinaria", en la cual contiene el vínculo a una página donde se encuentran todos los Estados con una liga (Figura V.24) a un cuadro indicando la maquinaria que se tiene comprometida para obra por parte de cada Estado.

Relación de maquinaria comprometida

Aguascalientes	Durango	Nayarit	Sonora
Baja California	Guerrero	Nuevo León	Tabasco
Baja California Sur	Guanajuato	Oaxaca	Tamaulipas
Campeche	Hidalgo	Puebla	Tlaxcala
Coahuila	Jalisco	Querétaro	Veracruz
Colima	México	Quintana Roo	Yucatán
Chihuahua	Michoacán	San Luis Potosí	Zacatecas
Chiapas	Morelos	Sinaloa	Maq. Duplicada

Figura V.24.

En la tabla de Maquinaria contiene los datos de las empresas ejecutoras ganadoras, el número de licitación, el número de contrato, subprograma, nombre de la obra (Tramo), la ubicación de la obra o subtramo, fecha de inicio, fecha de término, duración en días, descripción de la maquinaria, marca, modelo, número de serie, si la maquinaria es propia o rentada o está por adquisición, su ubicación física y las condiciones en las que se encuentra, como puede ser en buenas, regulares o malas condiciones, con todos estos se puede hacer el análisis para el movimiento de maquinaria entre los Estados (Figura V.25).

La sexta opción de este menú principal, denominada "Obs. Form. Por Org. de cont." se refiere a las observaciones formuladas por los Órganos de control, en la cual contiene el vínculo a una página donde se encuentran todos los Estados con su liga (Figura V.26) respectiva a cada tabla con todas las observaciones formuladas por la Contraloría Interna de la Secretaria de Comunicaciones y Transportes, cuyas siglas son C.I.S.C.T., o por el Órgano Interno de Control de la Secretaría de Comunicaciones y Transportes, cuyas siglas son O.I.C.S.C.T., estos dos organismos son dependientes de la Secretaría de Contraloría de Desarrollo Administrativo, SECODAM, la cual se a convertido en la Secretaría de la Función Publica, así como la Auditoria Superior de la Federación, cuyas siglas son A.S.F. dependiente de la Cámara de Diputados y por la Contaduría Mayor de Hacienda y cuyas siglas son C.M.H., en las obras realizadas por Estado, de parte de las empresas ganadoras de las licitaciones, en dicha tabla se indica el Órgano de control que realiza la auditoria marcando con un número de control a cada obra auditada, también se indica la fecha en que se realizó la auditoria y su concepto de la obra, el seguimiento y la situación de la misma. (Figura V.27).

RELACION DE MAQUINARIA Y EQUIPO DE LAS EMPRESAS EJECUTORAS DE LAS OBRAS DE CONSERVACION DE CARRETERAS

PUEBLA

EMPRESA EJECUTORA GANADORA	No. DE LICITACION	No. DE CONTRATO	SUBPROGRAMA	NOMBRE DE LA OBRA (TRAMO)	UBICACIÓN (SUBTRAMO)	FECHA DE INICIO	FECHA DE TERMINACION	DURACION (DIAS)	MAQUINARIA Y EQUIPO								CONDICION FISICA		
									DESCRIPCION	MARCA	MODELO	No. DE SERIE	PROPIA	RENTADA	POR ASIGNAR	UBICACION FISICA	B	R	M
GRUPO CONSTRUCTOR GOLFO PACIFICO, S.A. DE C.V.	00009650-012-02			TRABAJOS DE CONSERVAC RUTINARIA BIANUAL, PUE-LIM PUE/OAX, ACCESO A PETLA, GPO	KM 131+750 AL 230+480, 0+000 AL 1+300	02-01-09			PICK-UP	DODGE	1999	215841	X			PUEBLA	X		
									CAMION 1.5 TONS	NISSAN	1999	214893	X			PUEBLA			
									PICK-UP	FORD	1988	000000	X			PUEBLA		X	
									CAMION PIPA	FORD		SS1413002	X			TIJUANA, BAJA CAL.			
									COMPACTAD. MANUAL	DYNAPAC		DSCA110026	X			TIJUANA, BAJA CAL.			
									CARGADOR	BOBCAT		B9GS200140	X			TIJUANA, BAJA CAL.			
									CAMION VOLTEO	FAMSA	1994	7945125	X			TIJUANA, BAJA CAL.			
									CAMION VOLTEO	INTERNATIONAL		C2121B-0099	X			TIJUANA, BAJA CAL.			
									PETROLIZADORA	SEAMAN GUNNISON		CYT41023	X			TIJUANA, BAJA CAL.			
									CAMION PLATAFORMA	DODGE		DFSD001453	X			PUEBLA			
									CAMION PLATAFORMA	FORD		0015-BJK	X			PUEBLA			
									CAMION PLATAFORMA	FORD		0012SHG	X			PUEBLA			
									CAMION VOLTEO	INTERNATIONAL		FB0000212	X			PUEBLA		X	
									CAMION VOLTEO	DODGE		KA451223	X			PUEBLA		X	
									COMPACTAD. MANUAL	DYNAPAC		CFS21555	X			PUEBLA			
									DEYERBADORA	BOBCAT		B9SC040123	X			PUEBLA			
									MINICARGADOR	BOBCAT		B9C0014522	X			TIJUANA, BAJA CAL.			
									MOTOCONFORMADORA	CATERPILLAR		CA00145	X			TIJUANA, BAJA CAL.			
									RETROEXCAVADORA	JHON DEERE		1486J9379	X			TIJUANA, BAJA CAL.			
									REVOLVEDORA	MPSA		SP0146	X			PUEBLA			
GRUPO CONSTRUCTOR JOCC, S.A. DE C.V.	00009650-014-02			TRABAJOS DE CONSERVACION RUTINARIA BIANUAL, PUEBLA-LIM. PUE/OAX, LIM. MORELOS-"T" CUATRO CAMINOS, PASO DE CUOTA-CUACNOPALAN, ACATEPEC, ECATEPEC (OAXSA) PASO POR CHIPILO, CHIPILO (OAXSA)	KM 76+000 AL 80+940, 103+200 AL 154+530, 0+000 AL 1+200, 0+000 AL 0+200, 0+000 AL 2+700, 0+000 AL 0+300	2 Ene 09			RETROEXCAVADORA	CASE	580SM	JAJ0137821	X			PUEBLA, PUE			
									CAMION PIPA	DODGE	1990	L19K111295U09	X			PUEBLA, PUE		X	
									REVOLVEDORA	MPSA	R10SHP		X			PUEBLA, PUE			
									PICK-UP	FORD			X			PUEBLA, PUE		X	
									PICK-UP	FORD			X			PUEBLA, PUE	X		
									CAMION VOLTEO	MERCEDES BENZ	1993	S9001416478	X			PUEBLA, PUE			
									PETROLIZADORA	SEAMAN GUNNISON	1580CRC			X		PUEBLA, PUE			
									MOTONIVELADORA	CATERPILLAR	120BH	87V09082	X			PUEBLA, PUE			
									COMPACTADOR NEUM.	DOC FACTOR		82065	X			PUEBLA, PUE		X	
									BALANINA		M10-09-151		X			PUEBLA, PUE		XH	
									CARGADOR FRONTAL	CATERPILLAR	936		X			PUEBLA, PUE			
									EXCAVADORA	CATERPILLAR	225		X			PUEBLA, PUE			
				TRABAJOS DE CONSERVACION RUTINARIA BIANUAL, PUEBLA-LIM PUE/OAX, PUEBLA-	4+300 AL 30+000, 2+500 AL				BARREDORA	BRGE		710 77VT1300JP	X			TEOPATLAN, PUE	X		
									CAMION PIPA	INTERNATIONAL	1986	FP66875	X			TEOPATLAN, PUE			
									CAMION VOLTEO	KENWORTH	1994	190555	X			TEOPATLAN, PUE			
									CAMION VOLTEO	MERCEDES BENZ	1993	3AM9001380017394	X			TEOPATLAN, PUE			
									COMPACTADOR	BOSCH		6464TR8	X			ACATZINGO, PUE			

Figura V.25.

Figura V.26.

OBSERVACIONES FORMULADAS POR LOS ORGANOS DE CONTROL

INFORMACIÓN AL 30 DE JUNIO DE 2003

TAMAULIPAS

ORGANO DE CONTROL	NUMERO	FECHA	CONCEPTO	SEGUIMIENTO	SITUACION
C.I.S.C.T.	10	20/03/97	BASES MAL ELABORADAS. DE LA REVISIÓN A CINCO CONCURSOS DE OBRA DE LA RESIDENCIA GENERAL DE CONSERVACIÓN DE CARRETERAS, NO SE ENCONTRÓ CONSTANCIA DE QUE SE HAYAN CELEBRADO LAS JUNTAS DE ACLARACIONES A LAS BASES DE LOS CONCURSOS.	MEDIANTE OFICIO CSCT.10.727.303.084 DE FECHA 7 DE MAYO DE 1997, EL SUBDIRECTOR DE OBRAS INSTRUYE AL RESIDENTE GENERAL PARA QUE EN LOS CONCURSOS SUBSECUENTES SE DEJE CONSTANCIA DE LA JUNTA DE ACLARACIONES A LAS BASES DE LICITACIÓN. ASIMISMO, EL RESIDENTE GENERAL HACE LO PROPIO CON LOS RESIDENTES DE OBRA. MEDIANTE OFICIO NÚMERO CSCT.727.411.213/97 DE FECHA 8 DE MAYO DE 1997. EN OFICIO Nº 09/002/146/98 DEL 8/07/98 LA DELEGACIÓN REGIONAL DA POR SOLVENTADA LA OBSERVACIÓN.	SOLVENTADA
C.I.S.C.T.	09	20/03/97	RETRASO EN EL REINTEGRO DEL SALDO DEL ANTICIPO. CON FECHA 20 DE JUNIO DE 1996, SE CELEBRÓ CONVENIO DE REDUCCIÓN DEL CONTRATO 5-2-CB-A-507-W-0-5, ESTABLECIÉNDOSE EL REINTEGRO DEL SALDO POR AMORTIZAR POR $223,878.03, CANTIDAD QUE SE CUBRIÓ UNA PARTE EN SEPTIEMBRE DE 1996, OTRA EN DICIEMBRE DE 1996 Y OTRA EN EL PAGO DE UNA ESCALATORIA DEL MES DE NOVIEMBRE.	MEDIANTE OFICIO CSCT.727.411.225/97 DEL 20/05/97, EL RESIDENTE GENERAL REQUIRIÓ A LA EMPRESA EL REINTEGRO DE $19,838.19 POR CONCEPTO DE INTERESES DE LOS IMPORTES DEL ANTICIPO ENTREGADO EN PARCIALIDADES. LA EMPRESA REINTEGRÓ DICHA CANTIDAD MEDIANTE CHEQUE DE CAJA NÚMERO 073001 DE CONFIA S.A. DE FECHA 9 DE OCTUBRE DE 1997. EN OFICIO Nº 09/002/146/98 DEL 8/07/98 LA DELEGACIÓN REGIONAL DA POR SOLVENTADA LA OBSERVACIÓN.	SOLVENTADA
C.M.H.	1	14/01/98	APERTURA DE PROPUESTAS EXTEMPORÁNEAS. CONTRATO 4-2-CB-A-522-W-0-4. C.P. 1996. SE LLEVO LA PRESENTACIÓN Y APERTURA EL 06 DE MAYO DE 1994, 10 DÍAS POSTERIORES A LA PUBLICACIÓN DE LA CONVOCATORIA SE INFRINGIÓ EL ARTICULO 34 DE LA LEY DE ADQUISICIONES Y OBRAS	EL RESIDENTE GENERAL COMENTÓ EN ACTA DEL 14 DE ENERO DE 1998, QUE EN RAZÓN QUE SON OBRAS QUE REQUIEREN DE ATENCIÓN URGENTE A FIN DE PREVER MAYORES COSTOS ECONÓMICOS O SOCIALES, LOS PLAZOS SE HAN FIJADO CON FUNDAMENTO A LO PRECEPTUADO EN EL SEGUNDO PÁRRAFO DEL ARTICULO 34 DE LA LEY DE ADQUISICIONES Y OBRAS PUBLICAS. MEDIANTE OFICIO OCMH-F-1460/98 DE FECHA 23/11/98 EL CONTADOR MAYOR DE HACIENDA CONSIDERA DESAHOGADAS LAS IRREGULARIDADES	SOLVENTADA

Figura V.27.

La séptima opción de este menú principal, denominado "Sistema Gestión de la Calidad" se refiere al Sistema de Gestión de la Calidad en la Dirección General de Conservación de Carreteras.

En este vínculo se accede a toda la información sobre los diferentes procedimientos a realizar por parte de la Dirección General con miras a la certificación en ISO 9000. En esta página se dividió toda la información en cinco grandes rubros, como son el Manual de Calidad, Procedimientos Generales, Procedimientos Específicos, Situación de las Acciones Preventivas y Correctivas y por último las Listas Maestras, cabe aclarar que a esta información solo tienen acceso todos los mandos medios y personal operativo relacionado con los procesos de la Calidad. (Figura V.28).

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES | SCT

SISTEMA DE GESTION DE CALIDAD EN LA DIRECCION GENERAL DE CONSERVACION DE CARRETERAS

MANUAL DE CALIDAD

Manual de Calidad de la Secretaria de Comunicaciones y Transportes.

Organigrama

Matriz de Responsabilidades

Calendario

Interacción de Procesos del SGC de la SCT

Interacción de Procesos en la DGCC

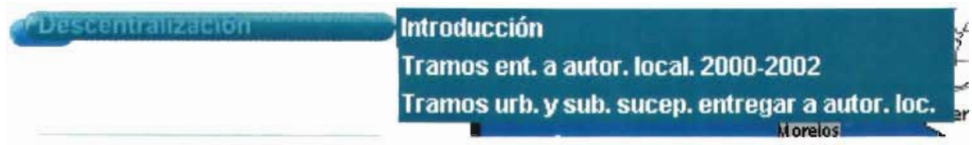
PROCEDIMIENTOS GENERALES

Procedimiento para Elaborar la Documentación del Sistema de Gestión de Calidad.	
Procedimiento de Control de Documentos.	**Anexo**
Procedimiento de Control de Registros.	
Procedimiento de Comunicación Interna.	
Procedimiento de Revisión del SGC por la Dirección.	
Procedimiento de Capacitación.	**Anexo**

Figura V.28.

La octava opción de este menú principal, denominada "Carreteras Limpias" se refiere al programa de concientización que está haciendo la Dirección General, para conservar las carreteras en estado limpio, por medio de presentaciones y anuncios espectaculares en las carreteras federales .

La novena opción de este menú principal, denominada "Descentralización", la Descentralización significa que el gobierno central transfiere el control y la autoridad a los gobiernos estatales, para que éstos, de acuerdo con sus necesidades locales específicas, planteen sus propios proyectos de desarrollo, los lleven a cabo y los evalúen.



La red federal se divide en red básica y red secundaria con una longitud cada una de:

1.- Red Básica: 23,658 kilómetros y 4,006 puentes, se les denomina a los tramos carreteros básicos, por pertenecer a tramos carreteros con alto volumen de tránsito, dentro de la cual existen dos divisiones, la primera son los Ejes Troncales, son 14 ejes que conectan las cinco mesorregiones y comunican capitales de estado, principales ciudades, fronteras y puertos marítimos, con un total de 10,076 km. y 1,520 puentes y la segunda son fuera de ejes, que comunican al resto de las principales ciudades, fronteras y puertos marítimos no considerados dentro de los ejes, con un total de 13,582 km. y 2,486 puentes.

2.- Red Secundaria: 17,675 kilómetros con 2,848 puentes, se consideran todos los demás tramos carreteros de importancia regional.

Dentro de esta opción, se activa un submenú y como primer vínculo, activa una página introductoria sobre las descentralizaciones, donde se hace mención sobre los Principales problemas que han impedido la descentralización, los compromisos de la Secretaria de Comunicaciones y Transportes, los compromisos de los gobiernos estatales, el compromiso de la Secretaría de Hacienda y Crédito Público y los beneficios para el gobierno estatal. (Figura V.29).

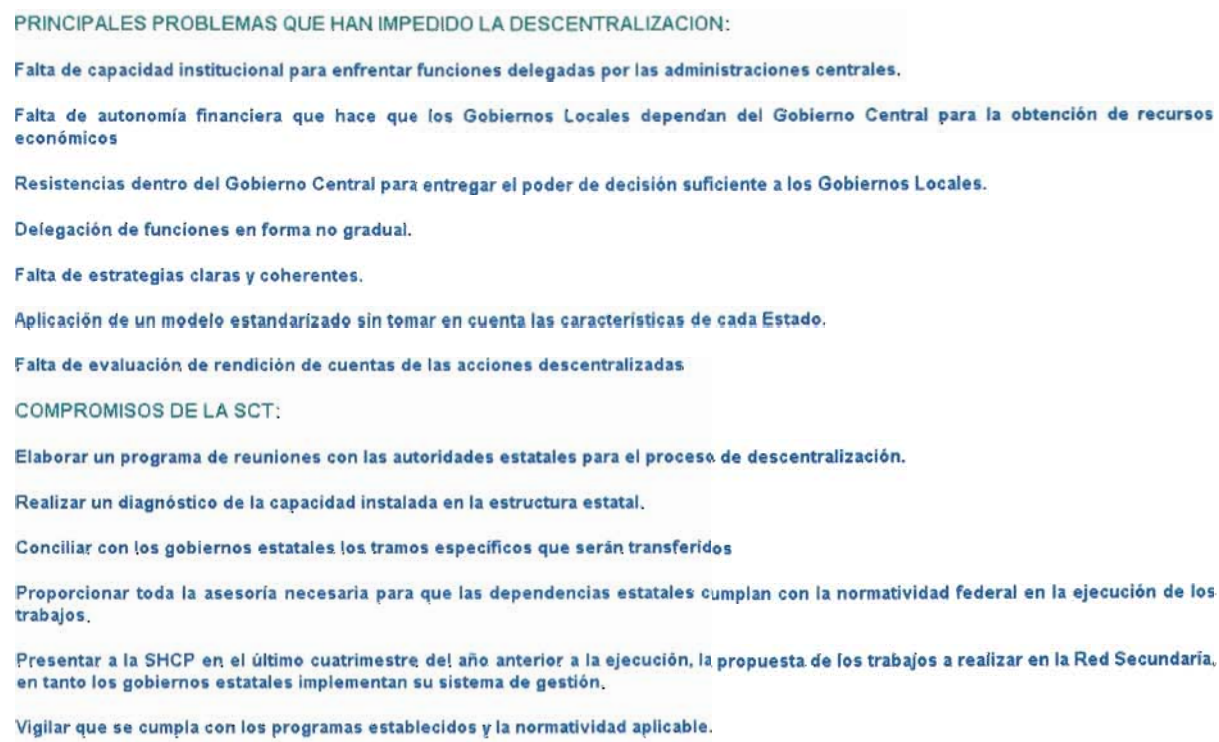


Figura V.29.

Dentro de esta opción, se activa un submenú y como segundo vínculo, denominada como "Tramos ent. a autor. local. 2000-2002" y se refiere a los tramos entregados a las autoridades locales en el periodo indicado, la cual activa una página con una tabla donde indica los Estados y el número de tramos entregados con un total de kilómetros. (Figura V.30).

TRAMOS ENTREGADOS A LAS AUTORIDADES LOCALES EN EL PERIODO 2000 - 2002

ESTADO	NUMERO	LONGITUD
BAJA CALIFORNIA	2	23.04
CAMPECHE	3	15.69
COAHUILA	16	62.68
COLIMA	2	9.80
CHIHUAHUA	5	28.10
GUANAJUATO	5	12.90
GUERRERO	3	12.11
HIDALGO	38	174.57
JALISCO	2	3.86
MORELOS	2	27.00
NUEVO LEON	8	46.83
OAXACA	4	16.60
QUERETARO	1	2.70
QUINTANA ROO	2	8.40
SAN LUIS POTOSI	9	30.98
TABASCO	2	9.70
VERACRUZ	21	77.17
TOTAL	125	562.14

Figura V.30.

Y como tercer vínculo, denominado como "Tramos urb. y sub. sucep. entregar a autor. loc." el cual se refiere a los tramos urbanos y suburbanos susceptibles de entregar a las autoridades locales, la cual activa una página con una tabla donde indica los Estados y el número de tramos susceptibles a su entrega con un total de kilómetros. (Figura V.31).

TRAMOS URBANOS Y SUBURBANOS SUSCEPTIBLES DE ENTREGAR A LAS AUTORIDADES LOCALES

ESTADO	NUMERO DE TRAMOS	LONGITUD TOTAL (KM)
AGUASCALIENTES	9	49.92
BAJA CALIFORNIA	4	51.40
BAJA CALIFORNIA SUR	21	227.62
CAMPECHE	10	23.23
COAHUILA	15	110.53
COLIMA	5	13.33
CHIAPAS	23	74.21
CHIHUAHUA	7	26.50
DURANGO	14	42.20
GUANAJUATO	21	58.25
GUERRERO	16	71.10
HIDALGO	17	77.26
JALISCO	30	118.42
MEXICO	27	74.25
MICHOACAN	52	185.20
MORELOS	36	210.49
NAYARIT	28	103.39
NUEVO LEON	4	15.49
OAXACA	51	161.20
PUEBLA	5	20.13
QUERETARO	19	43.55
QUINTANA ROO	14	49.00
SAN LUIS POTOSI	22	100.94
SINALOA	12	43.49
SONORA	22	88.90
TABASCO	11	51.33
TAMAULIPAS	25	116.54

Figura V.31.

La décima opción de este menú principal, denominada "Corredores carreteros", se define como Corredores carreteros a la Red carretera que conecta las cinco mesorregiones con que cuenta el país y que proporcionan acceso y comunicación permanente a las principales ciudades, fronteras y puertos marítimos.

Dentro de esta opción, se activa un submenú y como primer vínculo, activa una página en la cual se indican los 14 Corredores carreteros con los que cuenta el país. (Figura V.32).

Y como último vinculado a este submenú, activa una página en la Intranet, que presenta un cuadro resumen de los Corredores carreteros por Estado a cargo de la Dirección General de Conservación de Carreteras, en la cual se indican el número de ejes y un total de la longitud en kilómetros (Figura V.33) y representado en otra tabla, se especifica el nombre del tramo por Estado, con su ubicación, número de carriles, con su longitud lineal y el equivalente en kilómetros. (Figura V.34).

La onceava opción y última de este menú principal, denominada "Publicaciones", contiene el vínculo a una página donde se muestran los diferentes títulos de publicaciones realizadas en la Dirección General de Conservación de Carreteras y a la vez, estos títulos contienen una liga para poder descargar la publicación seleccionada. (Figura V.35).

Tramos a cargo de la Dirección General de Conservación de Carreteras*

NUMERO	NOMBRE DEL CORREDOR	LONGITUD (km)	
		D.G.C.C.	TOTAL
1	México-Nogales	617.213	2,379.00
	Ramal a Mexicali y Tijuana (R-1)	508.400	695.00
2	México-Nuevo Laredo	684.639	1,270.00
	Ramal a Piedras Negras (R-2)	328.640	465.00
3	Querétaro-Ciudad Juárez	747.815	1,755.00
4	Acapulco-Tuxpan	198.780	830.00
5	Mazatlán-Matamoros	533.700	1,245.00
6	Manzanillo-Tampico	603.222	1,132.00
	Ramal Zapotlanejo-Lázaro Cárdenas (R-6 Z)	153.190	662.00
	Ramal Uruapan-Ecuandureo (R-6 U)	141.050	62.00
7	Acapulco-Veracruz	98.120	851.00
8	Veracruz-Monterrey	846.940	977.00
	Ramal a Matamoros (R-8)	302.000	320.00
9	Transpeninsular de Baja California	1,539.810	1,776.00
10	Del Altiplano	304.900	581.00
11	Puebla-Progreso	592.490	1,320.00
12	Puebla-Oaxaca-Cd. Hidalgo	387.800	1,007.00
13	Transistmico	429.626	702.00
14	Circuito Peninsular de Yucatán	959.477	1,219.00
	TOTAL	9,977.812	19,248.000

Figura V.32.

Corredores Carreteros por Estado

Tramos a Cargo de la D.G.C.C. *

Estado	Ejes	Longitud (km)	
		Lineal	Equivalente
Aguascalientes	3	87.070	163.710
Baja California	9 y R-1	643.460	705.400
Baja California Sur	9	947.350	991.050
Campeche	11 y 14	616.987	633.487
Coahuila	2, 5 y R-2	485.690	801.580
Colima	6	49.240	96.980
Chiapas	12 y 13	293.086	349.786
Chihuahua	3	304.000	608.000
Durango	3 y 5	283.300	312.000
Guanajuato	2, 3 y R6-Z	208.209	357.228
Guerrero			
Hidalgo	4	33.080	63.880
Jalisco	1, 3 y 6	145.890	224.530
México	1 y 4	50.250	118.150
Michoacán	R-6 Z y R-6 U	235.050	320.350
Morelos	7	33.000	33.000
Nayarit	1	111.463	111.463
Nuevo León	2, 5 y 8	382.220	736.770
Oaxaca	12 y 13	511.390	521.290
Puebla	4, 10 y 7	207.120	235.420
Querétaro	2	8.800	17.600
Quintana Roo	14	431.500	495.800
San Luis Potosí	2 y 6	668.360	965.000
Sinaloa	1 y 5	347.580	510.180
Sonora	1 y R-1	676.120	884.240
Tabasco	11 y 14	244.790	324.280
Tamaulipas	2, 5, 8 y R-8	771.790	983.640
Tlaxcala	10	135.400	154.800
Veracruz	4, 6, 8, 10, 11 y 13	718.002	750.602
Yucatán	11 y 14	150.370	186.270
Zacatecas	3	197.245	297.930
Longitud Total (km)		9.077.942	12.061.446

Figura V.33.

Estado	Eje	Ramal	Tramo	Ubicación	No. de carriles	Long. Lineal (km)	Long. Equivalente (km)
AGUASCALIENTES							Arriba
AGS.	3		Lim. de Edos. Jal./Ags.-Aguascalientes	103+300 - 129+180	4	25.880	51.760
AGS.	3		Aguascalientes - Cosío	1+000 - 10+500	4	9.500	19.000
				10+500 - 13+300	6	2.800	8.400
				13+300 - 13+960	4	0.660	1.320
				13+960 - 15+120	6	1.160	3.480
				15+120 - 30+700	4	15.580	31.160
				30+700 - 31+100	6	0.400	1.200
				31+100 - 35+000	4	3.900	7.800
				35+000 - 45+000	2	10.000	10.000
				45+000 - 57+400	4	12.400	24.800
AGS.	3		Cosío II - Lím. Edos. Ags./Zac.	0+000 - 4+790	2	4.790	4.790
				TOTAL AGS.:		87.070	163.710
BAJA CALIFORNIA							Arriba
B.C.		R-1	Lim. de Edos. Son./B.C.-Mexicali	0+000 - 51+000	4	51.000	102.000
B.C.	9		Ensenada-Lázaro Cárdenas	11+800 - 22+000	4	10.200	20.400
				22+000 - 145+000	2	123.000	123.000
				145+000 - 193.660	2	48.660	48.660
				193+660 - 194+400	4	0.740	1.480
				194+400 - 196+000	2	1.600	1.600
B.C.	9		Lázaro Cárdenas-Punta Prieta	0+000 - 280+660	2	280.660	280.660
B.C.	9		Punta Prieta-Lim. Edos. B.C./B.C.S.	0+000 - 127+600	2	127.600	127.600
				TOTAL B.C.:		643.460	705.400
BAJA CALIFORNIA SUR							Arriba
B.C.S.	9		Lim. Edos. B.C./B.C.S.-Sta. Rosalía	220+000 - 7+000	2	213.000	213.000
B.C.S.	9		Sta. Rosalía-Loreto	0+000 - 0+400	4	0.400	0.800
				0+400 - 130+000	2	129.600	129.600
				136+800 - 193+000	2	56.200	56.200
B.C.S.	9		Loreto-Cd. Insurgentes	120+000 - 119+000	4	1.000	2.000
				119+000 - 0+000	2	119.000	119.000
B.C.S.	9		Cd. Insurgentes-La Paz	236+700 - 6+800	2	229.900	229.900
B.C.S.	9		La Paz-Sta. Anita (T. Aeropuerto)	44+050 - 200+000	2	155.950	155.950
B.C.S.	9		Sta. Anita - Cabo San Lucas	1+750 - 44+050	4	42.300	84.600

Figura V.34.

Publicaciones de la Dirección General de Conservación de Carreteras

Coloque el indicador del mouse sobre la publicación que desee descargar y de click con el boton izquierdo del mouse para iniciar la descarga del archivo correspondiente.

Guía de Emergencias 2003 (actualizado a Junio de 2003)

Portada Guía de Emergencias 2003 (actualizado a Junio 2003)

Guía de Emergencias 2003 Anexos (actualizado a Junio de 2003)

Manual de Bandereros (formato .zip)

"TOPES" Un problema estatal con costos muy altos para Guerrero (formato .zip)

Limpieza de Carreteras Guerrero (Basura en los Caminos) (formato .zip)

Descarga del paquete Acrobat Reader para archivos con extensión PDF (Software Gratuito)

Figura V.35.

CONCLUSIONES.

Una Intranet es una red privada que la tecnología Internet usó como arquitectura elemental. Una red interna se construye usando los protocolos TCP/IP para comunicación de Internet, que pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable. El hardware fundamental no es lo que construye una Intranet, lo que importa son los protocolos del software. Las Intranets pueden coexistir con otra tecnología de red de área local. En muchas compañías, los "sistemas patrimoniales" existentes que incluyen sistemas centrales, redes Novell, mini - computadoras y varias bases de datos, se están integrando en un Intranet. Una amplia variedad de herramientas permite que esto ocurra. El guión de la Interfaz Común de Pasarela (CGI) se usa a menudo para acceder a bases de datos patrimoniales desde una Intranet. El lenguaje de programación Java también puede usarse para acceder a bases de datos patrimoniales.

Con el enorme crecimiento de Internet, un gran número de personas en las empresas usan Internet para comunicarse con el mundo exterior, para reunir información, y para hacer negocios. A la gente no le lleva mucho tiempo reconocer que los componentes que funcionan tan bien en Internet serían del mismo modo valioso en el interior de sus empresas y esa es la razón por la que las Intranets se están haciendo tan populares. Algunas corporaciones no tienen redes TCP/IP: el protocolo requerido para acceder a los recursos de Internet. Crear una Intranet en la que todas las informaciones y recursos se puedan usar sin interrupciones tiene muchos beneficios. Las redes basadas en TCP/IP facilitan a las personas el acceso a la red remotamente, desde casa o mientras viajan. Contactar con una Intranet de este modo es muy parecido a conectar con Internet, La operabilidad interna entre redes es otro suplemento sustancial. Los sistemas de seguridad separan una Intranet de Internet. La red interna de una compañía está protegida por firewall: combinaciones de hardware y software que sólo permiten a ciertas personas acceder a ella para propósitos específicos. Se puede utilizar para cualquier cosa para la que se empleaban las redes existentes. La facilidad que tiene para publicar información en la WWW las ha convertido en lugares utilizados para enviar información de empresa como las noticias y procedimientos de la compañía. Las bases de datos empresariales con procesadores sencillos usan la Web y lenguajes de programación como Java.

Las Intranets permiten a los usuarios trabajar juntos de un modo más sencillo y efectivo. EL programa conocido como trabajo en grupo es otra parte importante de las redes internas. Nos permite colaborar en proyectos, compartir información, llevar a cabo conferencias visuales, y establecer procedimientos seguros para el trabajo de producción. EL software del servidor y del cliente gratuito y la multitud de servicios como los grupos de noticias, estimulan la expansión de Internet. La consecuencia de ese crecimiento avivó y provocó el desarrollo de las Intranets.

Una Intranet es una red privada empresarial o educativa que utiliza los protocolos TCP/IP de Internet para su transporte básico. Los protocolos pueden ejecutar una variedad de Hardware de red, y también, pueden coexistir con otros protocolos de red, como IPX. Aquellos empleados que están dentro de una Intranet pueden acceder a los amplios recursos de Internet, pero aquellos en Internet no pueden entrar en la Intranet, que tiene acceso restringido.

Una Intranet se compone frecuentemente de un número de redes diferentes dentro de una empresa que se comunica con otra mediante TCP/IP. Estas redes separadas se conocen a menudo como sub - redes. El software que permite a la gente comunicarse entre ella vía correo electrónico y tablones de mensaje públicos, y colaborar en la producción usando software de grupos de trabajo, está entre los programas de Intranets más poderoso. Las aplicaciones que permiten a los distintos departamentos empresariales enviar información, y a los empleados rellenar formularios de la empresa (como las hojas de asistencia) y utilizar la información corporativa financiera, son muy populares. La mayoría del software que se utiliza en las Intranets es estándar: software de Internet como el Netscape, Navigator y los navegadores Explorer para Web de Microsoft. Y los programas

personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el de guión de CGI.

Las Intranets también se pueden utilizar para permitir a las empresas llevar a cabo transacciones de negocio a negocio como: hacer pedidos, enviar facturas, y efectuar pagos. Para mayor seguridad, estas transacciones de Intranet a Intranet no necesitan nunca salir a Internet, pero pueden viajar por líneas alquiladas privadas. Son un sistema poderoso para permitir a una compañía hacer negocios en línea, por ejemplo, permitir que alguien en Internet pida productos. Cuando alguien solicita un producto en Internet, la información se envía de una manera segura desde Internet a la red interna de la compañía, donde se procesa y se completa el encargo. La información enviada a través de una Intranet alcanza su lugar exacto mediante los enrutadores, que examinan la dirección IP en cada paquete TCP/IP y determinan su destino. Después envía el paquete al siguiente direccionador.

Si este tiene que entregarse en una dirección en la misma subred de la Intranet desde la que fue enviado, llega directamente sin tener que atravesar otro enrutador. Si tiene que mandarse a otra subred de trabajo en la Intranet, se enviará a otra ruta. Si el paquete tiene que alcanzar un destino externo a la Intranet en otras palabras, Internet se envía a un enrutador que conecte con Internet.

Para proteger la información corporativa delicada, y para asegurar que los piratas no perjudican a los sistemas informáticos y a los datos, las barreras de seguridad llamadas firewalls protegen a una Intranet de Internet. La tecnología firewall usa una combinación de enrutadores, servidores y otro hardware y software para permitir a los usuarios de una Intranet utilizar los recursos de Internet, pero evitar que los intrusos se introduzcan en ella. Mucha Intranets tienen que conectarse a "sistemas patrimoniales": el hardware y las bases de datos que fueron creadas antes de construir la Intranet. A menudo los sistemas patrimoniales usan tecnologías más antigua no basada en los protocolos TCP/IP de las Intranets. Hay varios modos mediante los que las Intranets se pueden unir a sistemas patrimoniales. Un método común es usar los guiones CGI para acceder a la información de las bases de datos y poner esos datos en texto HTML inicializado. Haciéndolos asequibles a un navegador para Web.

Lo que distingue una Intranet de cualquier otro tipo de red privada es que se basa en TCP/IP: los mismos protocolos que se aplican a Internet. TCP/IP se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

En algunas empresas, puede haber una mezcla de Intranets basadas en TCP/IP y redes basadas en otra tecnología, como NetWare. En este caso, la tecnología TCP/IP de una Intranet se puede utilizar para enviar datos entre NetWare y otras redes, usando una técnica llamada IP canalizado. Las redes NetWare usan el protocolo IPX (Intercambio de Paquetes en Internet) como medio de entregar datos y las redes TCP/IP no pueden reconocer este protocolo. Cuando un paquete IP mediante un servidor NetWare específico y que se dedica a ofrecer el mecanismo de transporte del IP para los paquetes IPX.

Los datos enviados dentro de una Intranet deben separase en paquetes menores de 1,500 caracteres. TCP divide los datos en paquetes. A medida que crea cada paquete, calcula y añade un número de control a éstos. El número de control se basa en los valores de los bytes, es decir, la cantidad exacta de datos en el paquete.

Cada paquete, junto al número de control, se coloca en envases IP o "sobre" separados. Estos envases contienen información que detalla exactamente donde se van a enviar los datos dentro de la Intranet o de Internet. Todos los envases de una clase de datos determinada tienen la misma información de direccionamiento así que se pueden enviar a la misma localización para reagruparse.

Los paquetes viajan entre redes Intranets gracias a enrutadores de Intranets. Los enrutadores examinan todos los envases IP y estudian sus direcciones. Estos direccionadores determinan la ruta más eficiente para enviar cada paquete a su destino final. Debido a que él trafico en una Intranet cambia frecuentemente, los paquetes se pueden enviar por caminos diferentes y puedan llegar desordenados. Si el enrutador observa que la dirección está localizada dentro de la Intranet, el paquete se puede enviar directamente a su destino, o puede enviarse a otro enrutador. Si la dirección se localiza fuera de Internet, se enviará a otro enrutador para que se pueda enviar a través de ésta.

A medida que los paquetes llegan a su destino, TCP calcula un número de control para cada uno. Después compara este número de control con el número que se ha enviado en el paquete. Si no coinciden, TCP sabe que los datos en el paquete se han degradado durante él envió. Después descarta el paquete y solicita la retransmisión del paquete original.

TCP incluye la habilidad de comprobar paquetes y determinar que se han recibido todos. Cuando se reciben los paquetes no degradados, TCP los agrupa en su forma original, unificada. La información de cabecera de los paquetes comunica el orden de su colocación.

Una Intranet trata el paquete IP como si fuera cualquier otro, y envía el paquete a la red NetWare receptora, un servidor TCP/IP NetWare abre el paquete IP descarta el paquete IP, y lee el paquete IPX original. Ahora puede usar el protocolo IPX para entregar los datos en el destino exacto.

La organización Internacional para la Normalización (ISO) ha creado el modelo de referencia "Interconexión de Sistemas Abiertos" (OSI), que describe siete pilas de protocolos para comunicaciones informáticas. Estas pilas no conocen o no se preocupan de lo que hay en pilas adyacentes. Cada pila, esencialmente, sólo ve la pila recíproca en el otro lado. La pila destinada a enviar la aplicación observa y se comunica con la pila de aplicación en el destino. Esa conversación tiene lugar sin considerar, por ejemplo, qué estructura existe en la pila física, como Ethernet o Token Ring. TCP combina las pilas de aplicación, presentación y sesión del Modelo OSI en una que también se llama pila de aplicación.

Los protocolos como TCP/IP determinan cómo se comunican las computadoras entre ellas por redes como Internet. Estos protocolos funcionan conjuntamente, y se sitúan uno encima de otro en lo que se conoce comúnmente como pila de protocolo. Cada pila del protocolo se diseña para llevar a cabo un propósito especial en la computadora emisora y en la receptora. La pila TCP combina las pilas de aplicación, presentación y sesión en una también denominada pila de aplicación.

En este proceso se dan las características del envasado que tiene lugar para transmitir datos:

- La pila de aplicación TCP formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir. La pila de aplicación TCP realiza las operaciones equivalentes que llevan a cabo las tres pilas de OSI superiores: aplicaciones, presentación y sesión.

- La siguiente pila es la de transporte, que es responsable de la transferencia de datos, y asegura que los datos enviados y recibidos son de hecho los mismos, en otras palabras, que no han surgido errores durante él envió de los datos. TCP divide los datos que obtiene de pila de aplicación en segmento. Agrega una cabecera contiene información que se usará cuando se reciban los datos para asegurar que no han sido alterados en ruta, y que los segmentos se pueden volver a combinar correctamente en su forma original.

- La tercera pila prepara los datos para la entrega introduciéndolos en datagramas IP, y determinando la dirección Internet exacta para estos. El protocolo IP trabaja en la pila de Internet, también llamada pila de red. Coloca un envase IP con una cabecera en cada

segmento. La cabecera IP incluye información como la dirección IP de las computadoras emisoras y receptoras, la longitud del datagrama y el orden de su secuencia.

El orden secuencial se añade porque el datagrama podría sobrepasar posiblemente el tamaño permitido a los paquetes de red, y de este modo necesitaría dividirse en paquetes más pequeños. Incluir el orden secuencial les permitiría volverse a combinar apropiadamente.

Los puentes son combinaciones de hardware y software que conectan distintas partes de una red, como las diferentes secciones de una Intranet. Conectan redes de área local (LAN) entre ellas. Sin embargo, no se usan generalmente para conectar redes enteras entre ellas, por ejemplo: para conectar una Intranet con Internet; o una Intranet con otra, o para conectar una subred completa con otra. Para hacer eso, se usan piezas de tecnología más sofisticada llamadas enrutadores.

Cuando hay gran cantidad de tráfico en una red de área local Ethernet, los paquetes pueden chocar entre ellos, reduciendo la eficacia de la red, y atrasando el tráfico de la red. Los paquetes pueden colisionar porque se encamina mucho tráfico entre todas las estaciones de trabajo en la red.

Para reducir la proporción de colisiones, una LAN se puede subdividir en dos o más redes. Por ejemplo, una LAN se puede subdividir en varias redes departamentales. La mayoría del tráfico en cada red departamental se queda dentro de la LAN del departamento, y así no necesita viajar a través de todas las estaciones de trabajo en todas las LAN de la red. De este modo, se reducen las colisiones. Los puentes se usan para enlazar las LAN. El único tráfico que necesita cruzar puentes es el que navega con rumbo a otra LAN. Cualquier trafico con la LAN no necesita cruzar un puente.

Cada paquete de datos en una Intranet posee más información que la del IP. También incluye información de direccionamiento requerida para otra arquitectura de red básica, como Ethernet. Los puentes comprueban esta información de la red externa y entregan el paquete en la dirección exacta en una LAN.

Los puentes consultan una tabla de aprendizaje que contiene las direcciones de todos los nodos de la red. Si un puente descubre que un paquete pertenece a su LAN, mantiene el paquete en la LAN. Si descubre que la estación de trabajo está en otra LAN, envía el paquete. El puente actualiza constantemente la tabla de aprendizaje a medida que controla y encamina el tráfico.

Los puentes pueden conectar redes de área local de varias formas diferentes. Pueden conectar LAN usando conexiones en serie por líneas telefónicas tradicionales y módems, por líneas ISDN, y por conexiones directas por cable. Las unidades CSU / DSU se usan para conectar puentes con líneas telefónicas mediante conductividad remota.

Los puentes y enrutadores se combinan algunas veces en un solo producto llamado brouter. Un brouter ejecuta las tareas de ambos. Si los datos necesitan sólo enviarse a otra LAN en la red o sub – red, solamente actuará como un puente, entregando los datos basados en la dirección Ethernet. Si el destino es otra red, actuará como un enrutador, examinando los paquetes IP y encaminando los datos basados en la dirección IP.

Los enrutadores son los guardias de tráfico de las Intranets. Se aseguran que todos los datos se envían donde se supone que tienen que ir y de que lo hacen por la ruta más eficaz. Los enrutadores también son herramientas útiles para sacar el mejor rendimiento de la Intranet. Se emplean para desviar el tráfico y ofrecer rutas. Los enrutadores utilizan la encapsulación para permitir el envío de los distintos protocolos a través de redes incompatibles.

Los enrutadores abren el paquete IP para leer la dirección de destino, calcular la mejor ruta, y después enviar el paquete hacia el destino final. Si el destino está en la misma parte de una Intranet, el enrutador enviará el paquete directamente a la computadora receptora. Si el paquete se destina a otra Intranet o subred (o si el destino está en Internet), el enrutador considera factores como la

congestión de tráfico y él numero de saltos – términos que se refiere al número de enrutadores o pasarelas en una ruta dada. El paquete IP lleva consigo un segmento que cuenta los saltos y un enrutador no usará una red que exceda de un número de saltos predeterminado.

Las rutas múltiples dentro de un número aceptable de saltos, son convenientes para ofrecer variedad y para asegurar que los datos se pueden transmitir. Por ejemplo, si una ruta directa entre la Ciudad de México y Guadalajara no estuviera disponible, los enrutadores complejos enviarán los datos a Guadalajara por otro enrutador probablemente en otra ciudad en la Intranet, y esto sería transparente para los usuarios.

Los enrutadores tienen dos o más puertos físicos: los de recepción (de entrada) y los de envío (de salida). En realidad, cada puerto es bidireccional y puede recibir o enviar datos. Cuando se recibe un paquete en un puerto de entrada, se ejecuta una rutina de software denominada proceso de encaminamiento. Este proceso investiga la información de cabecera en el paquete IP y encuentra la dirección a la que se están enviando los datos. Luego compara esta dirección con una base de datos llamada tabla de encaminamiento que posee información detallando a que puertos deberían enviarse los paquetes con varias direcciones IP. Basándose en lo que encuentra en la tabla de encaminamiento, envía el paquete en un puerto de salida específico. Este puerto de salida envía después los datos al siguiente enrutador o al destino.

A veces. Los paquetes se mandan a un puerto de entrada de un enrutador antes de que pueda procesarlos. Cuando esto ocurre, los paquetes se envían a un área de contención especial llamada cola de entrada, un área de RAM en el enrutador. Esa cola de entrada específica está asociada con un puerto de entrada concreto. Un enrutador puede tener más de una cola de entrada, si varios puertos de entrada están enviando paquetes más aprisa que el enrutador puede procesarlos. Cada puerto de entrada procesará los paquetes de la cola en el orden en que se recibieron.

Si el tráfico a través del enrutador es muy denso, el número de paquetes en la cola puede ser mayor que su capacidad. (La capacidad de la cola se denomina longitud). Cuando esto ocurre, es posible que los paquetes se abandonen y de este modo no serán procesados por el enrutador, y no se enviarán a su destino. Aunque esto no significa que se tenga que perder la información. El protocolo TCP se diseño para tener en cuenta que los paquetes pueden perderse de camino a su destino final. Si nos envían todos los paquetes al receptor, TCP en la computadora receptora identifica y pide que se vuelvan a enviar los paquetes perdidos. Seguirá solicitando él reenvió de los paquetes hasta que reciban todos. Los enrutadores sofisticados pueden manejarse y los problemas diagnosticarse y resolverse usando software especial, como SNMP (Protocolo Simple de Administración de Red). TCP puede decidir que decisiones tiene que tomar porque hay varias banderas en el paquete, como el número de saltos en IP, que comunica a TCP lo que necesita para saber cómo actuar. Por ejemplo, la bandera ack, indica que esta respondiendo (reconociendo) a una comunicación previa.

Se utilizan varios tipos de tablas en ruta. En el tipo de Intranet más simple denominada tabla de encaminamiento mínimo. Cuando una Intranet se compone de una sola red TCP/IP o a Internet, se puede usar encaminamiento mínimo. En encaminamiento mínimo, un programa llamado ifconfig crea automáticamente la tabla, que contiene únicamente unas pocas entradas básicas. Puesto que hay muy pocos lugares a los que se pueden enviar los datos, sólo se necesita configurar un número mínimo de enrutadores.

Si una Intranet tiene solamente un número limitado de redes TCP/IP, se puede utilizar una tabla de encaminamiento estático. En este caso, los paquetes con direcciones específicas se envían a enrutadores específicos. Los enrutadores no desvían paquetes para modificar el tráfico variable de la red. El encaminamiento estático debería utilizarse cuando sólo hay una ruta para cada destino. Una tabla de encaminamiento estático permite a un administrador de Intranets añadir o eliminar entradas en ésta.

Las tablas de encaminamiento dinámico son las más sofisticadas. Deberían usarse cuando hay más de una manera para enviar datos desde un enrutador al destino final, y en Intranets más complejas. Estas tablas cambian constantemente a medida que varía el trafico de la red y las condiciones, así que siempre encaminan datos del modo más eficiente posible, teniendo en cuanta el estado actual del tráfico de la Intranet.

Las tablas de encaminamiento dinámico se construyen utilizando protocolos de encaminamiento. Estos protocolos son medios por los que se comunican los enrutadores, ofreciendo información sobre la manera más eficaz de encaminar datos dado el estado actual de la Intranet. Un enrutador con una tabla de encaminamiento dinámico puede desviar datos a una ruta de apoyo si la ruta primaria es reducida. También puede determinar siempre el método más eficiente de encaminar datos hacia su destino final. Los enrutadores exponen sus direcciones IP y conocen las direcciones IP de sus vecinos. Los enrutadores pueden usar esta información en un algoritmo para calcular la mejor ruta para enviar paquetes.

El protocolo de encaminamiento más común que realiza estos cálculos se conocen como RIP (Protocolo de Información de Encaminamiento). Cuando RIP determina la ruta más eficaz para enviar datos el camino con el menor número de saltos. Asume que cuantos menos saltos haya, más eficaz sera, un número de saltos mayor que 16, descartará la ruta.

El Protocolo de Pasarela Exterior (EGP) se usa en Internet donde se puede tener que atravesar muchos más enrutadores antes de que un paquete alcance su destino final.

El factor a tener en cuenta sobre Intranets y Tecnología de encaminamiento es que no es una situación "o se da una u otra", sino que pueden utilizar muchos tipos de tecnologías de encaminamiento, dependiendo de las necesidades de esa parte particular de la red. Algunas partes pueden ser capaces de emplear enrutadores con tablas de encaminamiento estático, mientras que otras partes pueden necesitar tablas de encaminamiento dinámico.

Probablemente la parte más usada de una Intranet que no tiene nada que ver con bases de datos de la empresa, páginas Web ostentosas. O contenido multimedia es el uso del correo electrónico. Las Intranets empresariales pueden emplear diferentes programas de correo electrónico, como cc: Mail Microsoft Mail o Lotus Notes, entre otros. Pero la Arquitectura más común que sirve de base al uso del e-mail de las redes internas es el protocolo llamado Protocolo simple de Transferencia de Correo, o SMTP.

Como se utiliza SMTP para repartir correo dentro de una Intranet:

- Como sucede con muchas aplicaciones de Intranets y de Internet, SMTP usa una arquitectura cliente / servidor. Cuando alguien quiere crear un mensaje, usa un agente usuario de correo o agente usuario (MUA o UA), software cliente que se ejecuta en un computador, para crear un fragmento de correo electrónico. Este MUA puede ser cualquiera de los programas e-mail, y puede ejecutarse en varias computadoras diferentes, incluyendo PC, Macintosh,, y estaciones de trabajo UNIX; Pegasus, Eudora. cc: Mail y Microsoft Mail para PC; y Eudora para Macintosh.

- Después de finalizar el mensaje, el MUA lo manda a un programa que se esta ejecutando en un servidor llamado agente de transferencia de correo (MTA) examina la dirección del receptor de mensaje. Si el receptor del mensaje está en la Intranet, el MTA envía el mensaje a otro programa servidor en la red interna denominado agente de entrega de correo (MDA). Si el receptor está ubicado en Internet o en otra red interna, el archivo llegará al receptor a través de Internet. El MDA examina la dirección del receptor, y envía el correo a la bandeja de entrada de la persona adecuada.

- Algunos sistemas de correo emplean otro protocolo e-mail llamado el Protocolo de Oficina de Correos (POP) conjuntamente con SMTP. Con POP, el e-mail no se entrega directamente en tu computadora. En lugar de eso, el correo se coloca a un buzón en el servidor. Para conseguir el coreo, alguien accede al servidor usando una contraseña y un nombre de usuario, y recupera el mensaje con un agente de correo.

- El receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo.

- SMTP sólo puede manejar la transferencia de correo electrónico de archivos de textos ASCII sencillos. Para enviar archivos binarios como hojas de cálculos, dibujos y documentos de procesador de texto, primero deben convertirlos en un formato ASCII codificándolos. Los archivos se pueden codificar usando varios métodos que incluyen codificación y Base64. Algunos programas de correo electrónico codificarán automáticamente archivos binarios. Cuando alguien recibe un archivo codificado, lo descodifica y después puede usar o examinar el archivo binario. Además muchos paquetes de correo electrónico descodifican automáticamente archivos codificados.

A menudo el correo electrónico creado en una Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, en otra Intranet, o un servidor en línea como América Online, Microsoft Network, o CompuServe. Aquí están los pasos que un mensaje típico tiene que seguir cuando se envía de una Intranet a otra red o Intranet.

- Un mensaje de correo electrónico se crea usando SMTP. Como ocurre con toda la información enviada a través de Internet, el mensaje es dividido por el Protocolo TCP de Internet en paquetes IP. La dirección la examina el agente de transferencia de correo de la Intranet. Si la dirección se encuentra en otra red, el agente de transferencia de correo enviará el correo a través de la Intranet mediante enrutadores al agente de transferencia de correo en la red receptora.

- Antes de que se pueda enviar el correo a través de Internet, puede que primero tenga que atravesar un *firewall*, una computadora que protege a la Intranet para que los intrusos no puedan acceder a ella. El firewall sigue la pista de los mensajes y los datos que entran y salen de la Intranet.

- El mensaje deja la Intranet y se envía a un enrutador Internet. El enrutador examina la dirección, determina dónde debería mandarse el mensaje, y después lo pone en camino.

- La red receptora obtiene el mensaje de correo electrónico. Aquí utiliza una pasarela para convertir los paquetes IP en un mensaje completo. Después la pasarela traduce el mensaje al protocolo particular que emplea la red (como el formato de correo de CompuServe), y lo pone en camino. Puede que el mensaje también tenga que atravesar un firewall en la red receptora.

- La red receptora examina la dirección de correo electrónico y envía el mensaje al buzón específico donde el mensaje está destinado a ir, o emplea el Protocolo de Oficina de Correo (POP) para entregarlo a un servidor de correo.

- Las pasarelas realmente pueden modificar los datos (si se necesita) para la conectividad. Para el correo electrónico, puede convertir el protocolo CompuServe en SMTP. Las pasarelas también se utilizan para conectar PC con sistemas centrales IBM, por ejemplo, ASCII con EBCDIC.

El centro de una Intranet es la World Wide Web. En muchos casos gran parte de la razón por la que se creó una Intranet en primer lugar es que la Web facilita la publicación de la información y formularios por toda la compañía usando el Lenguaje de Marcado de Hipertexto (HTML). La Web

permite la creación de páginas iniciales multimedia, que está compuesta de texto, gráficos, y contenidos multimedia como sonido y vídeo. Los enlaces de hipertexto te permiten saltar desde un lugar en la Web a otro, lo que significa que puedes saltar a lugares dentro de una Intranet o fuera en Internet desde una pagina inicial.

- Las Intranets están basadas en la arquitectura cliente / servidor. EL software navegador para Web, se ejecuta en una computadora local, y el software servidor en una Intranet anfitriona. El software cliente esta disponible para PC, Macintosh y estaciones de trabajo UNÍS. El software servidor se ejecuta en UNIX, Windows NT y otros sistemas operativos. El software cliente y el software servidor no necesitan ejecutarse en el mismo sistema operativo. Para una Intranet, primero pone en marcha tu navegador para Web. Si estás conectado directamente con tu Intranet, el programa TCP/IP que necesitas para ejecutar el navegador ya estará instalado en tu computadora.

- Cuando se ponen en marcha los navegadores, visitarán una cierta localización predeterminada. En una Intranet, esa localización puede ser una página Web departamental o una página Web por toda la compañía. Para visitar un sitio diferente, escribe la localización de la Intranet que quieres visitar, o pulsa en un enlace para dirigirte allí. El nombre para cualquier localización Web es el URL (localizador uniforme de recursos). Tu navegador para Web envía la petición URL usando http (Protocolo de Transferencia de Hipertexto) que define el modo en el que se comunican el navegador para Web y el servidor Web.

- Si la petición es de una página localizada en la Intranet, los navegadores envían la petición a esa página Web de la Intranet. Puede estar disponible una conexión de alta velocidad, puesto que las Intranet pueden construirse usando cables de alta velocidad, y todo el tráfico dentro de la Intranet se puede conducir por esos cables. La conexión Internet puede ser mucho más lenta debido a la cantidad de tráfico de Internet, y porque puede haber varias conexiones de baja velocidad que la petición desde la Intranet tendrá que atravesar. Los paquetes que componen la petición se encaminan hacia un enrutador de la Intranet, que envía en turnos la petición al servidor Web.

- El servidor Web recibe la petición usando http, la petición es para un documento específico. Devuelve la página inicial, documento u objetivo al navegador para Web cliente. La información se muestra ahora en la pantalla de la computadora en el navegador Web. Después de enviar el objeto al navegador para Web, la conexión http se cierra para hacer un uso más eficaz de los recursos de la red.

- Los URL constan de varias partes. La primera parte, el http://, detalla qué protocolo Internet hay que usar. El segmento www.zdnet.com" varía en longitud e identifica el servidor Web con el que hay que contactar. La parte final identifica un directorio específico en el servidor, y una página inicial, documento, u otro objeto de Internet o de la Intranet.

    - Cuando hay que conectar con un URL particular, la dirección con el URL debe ser igual que la dirección IP verdadera. El navegador para Web irá primero a un servidor DNS local en la Intranet de la empresa para obtener esta información si la dirección IP es local, el servidor DNS podrá resolver el URL con la dirección IP. Este enviará la dirección IP auténtica a la computadora.

    - El navegador para Web tiene ahora la dirección IP verdadera del lugar que estás intentando localizar. Utiliza esa dirección IP y contacta con el sitio. El sitio envía la información que se ha solicitado.

    - Si la información que se ha solicitado no está en Intranet, y si el servidor DBS local no tiene la dirección IP, el servidor DNS de Intranets debe obtener la información desde un servidor DNS en Internet. EL servidor DNS de Intranets contacta con lo que se

denomina servidor de dominio raíz, que se mantiene por un grupo llamado InterNIC. El servidor raíz de dominio le dice al servidor de Intranets qué servidor primario de nombres y qué servidor secundario de nombres tiene la información sobre el URL solicitado.

- El servidor de Intranets contacta ahora con el servidor primario de nombres. Si la información no se puede encontrar en el servidor primario de nombres, el servidor DNS de Intranets contacta con el servidor secundario. Uno de esos servidores de nombres tendrá la información exacta. Después devolverá la información al servidor DNS de Intranets.

- El servidor DNS de Intranets devuelve la información, el navegador para Web usa ahora la dirección IP para contactar con el sitio exacto.

Cuando alguien en una Intranet quiere contactar con una localización, por ejemplo, visitar un sitio Web, escribirá una dirección, como www.metahouse.com. Aunque de hecho, Internet no utiliza realmente estas direcciones alfanuméricas. En lugar de eso, emplea direcciones IP, que son direcciones numéricas, en cuatro números de 8 bits separados por puntos, como 123.5.56.255. Un servidor DNS, llamado también un servidor de nombres, empareja, direcciones alfanuméricas con sus direcciones IP, y te permite contactar con la localización exacta.

Al usar Java, los programadores pueden vincular datos corporativos desde una Intranets, permitiendo el uso de sistemas patrimoniales como bases de datos. Los programadores, editores y artistas pueden también utilizar Java para crear programación multimedia. Además Java será capaz de crear programas personalizados de Intranets de todo tipo desde informática para grupos de trabajo a comercio electrónico.

Java es similar al lenguaje informático C++, y está orientado a objetos, lo que significa que se pueden crear programas usando muchos componentes preexistentes, en lugar de tener que escribir todo el programa desde el principio. Esto será una gran ayuda para las Intranets, puesto que permitirá a los programadores de la empresa compartir componentes y de ese modo construir aplicaciones personalizadas mucho más aprisa.

Java es un lenguaje compilado, lo que significa que después de que el programa Java se escriba, debe ejecutarse a través de un compilador para transformar el programa en un lenguaje que pueda entender la computadora. Sin embargo Java se diferencia de otros lenguajes compilados. En otros lenguajes compilados, los compiladores específicos de la computadora crean un código ejecutable distinto para todos los computadores diferentes en los que se puede ejecutar el programa. Por el contrario, en Java se crea una sola versión compilada del programa llamada: código de bytes Java. Los intérpretes en los distintos computadores entienden el código de bytes Java y ejecutan el programa. De este modo, un programa Java se puede crear una vez, y usarse después en muchos tipos diferentes de computadora. Los programas Java diseñados para ejecutarse dentro de un navegador para Web se denominan apliques. Los apliques son un subconjunto de Java y por razones de seguridad no pueden leer o escribir archivos locales, mientras que Java lo puede hacer. Los navegadores que admiten Java posen intérpretes del código de bytes Java.

Después de que un aplique Java está compilado en códigos de bytes, se copia en un servidor Web de Intranets y el enlace necesario se introduce en HTML.

Cuando alguien en una Intranets visita una pagina inicial con un aplique Java en ella, el aplique se recibe automáticamente en su computadora. El aplique no espera la invitación. Por eso hay tanta preocupación por los virus que se están incrustando en los apliques. Para ejecutar el aplique Java, necesitaras un navegador para Web que tenga un intérprete de código de bytes que pueda ejecutar apliques Java.

Puesto que los apliques Java son programas que se pueden ejecutar en tu computadora, teóricamente podrían ser portadores de un virus como cualquier otro programa informático. Para asegurar que ningún virus puede infectar tu computadora cuando recibe un aplique Java, el aplique pasa primero a través de la verificación. Sin embargo, los apliques no se pueden leer o escribir en archivos locales que están normalmente involucrados en ataques víricos, así que esto debería reducir substanciales el riesgo de infección.

Después de que los códigos de bytes se hayan verificado, él interprete Java en el navegador los introduce en una área restringida en la memoria de tu computadora y los ejecuta. Se toman medidas adicionales para que ningún virus pueda perjudicarle.

El aplique Java está ejecutado. Los apliques pueden interrogar a las bases a datos presentando una lista de preguntas o cuestionarios al usuario. Pueden favorecer la búsqueda de sitios en la Intranet creando mecanismos de búsqueda lo más sofisticados posible con HTML. Más importante, puesto que los ciclos CPU del cliente se usan más que los del servidor, todo tipo de multimedia, incluyendo animación e interactividad, son posibles con los apliques Java.

Java tendrá Interfaces para Programas de Aplicación (API) y otro tipo de software "enganchado" para permitir a los programadores de Intranets integrar más fácilmente programas de Intranets como los navegadores para Web en bases de datos y redes corporativas existentes.

Cuando las Intranets sobrepasan un cierto tamaño, o se extienden por varias localizaciones geográficas, empiezan a ser difícil manejarlas como una sola red. Para resolver el problema, la Intranet se puede subdividir en varias sub – redes, subsecciones de una Intranet que las hacen más fáciles de administrar. Para el mundo exterior, la Intranet aparece todavía como si fuera una sola red.

- Si se está construyendo una Intranet y se quiere que esté conectada con Internet, se necesitaría una dirección IP única para la red, que será manejada por los Servicios Internic de Registro. Se puede disponer de tres clases de redes: Clase A, Clase B o Clase C. Generalmente, la clasificación de Clase A es mejor para las redes más grandes, mientras que la Clase C es mejor para las más pequeñas. Una red de Clase A puede estar compuesta de 127 redes y un total de 16,777.214 nodos en la red. Una red de Clase B puede estar compuesta de 16,383 redes y un total de 65,383 nodos. Una red de Clase C puede estar compuesta de 2,097.151 redes y 254 nodos.

- Cuando se le asigna una dirección a una Intranet, se asigna los dos primeros números IP de la dirección Internet numérica (llamados el campo de la netid) y los dos números restantes (llamados el campo de la host id) se dejan en blanco, para que la propia Intranet los pueda asignar, como 147.106.0.0. El campo de la host id consiste en un número para una subred y un número de anfitrión.

- Cuando una Intranet se conecta con Internet, un enrutador realiza el trabajo de enviar los paquetes desde Internet a la Intranet.

- Cuando las Intranets crecen, por ejemplo, si hay un departamento ubicado en otro edificio, ciudad o país, se necesita algún método para manejar el tráfico de red. Puede ser poco práctico y físicamente imposible encaminar todos los datos necesarios entre muchas computadoras diferentes extendidos por un edificio o por el mundo. Se necesita crear una segunda red denominada subred de trabajo o subred.

- Para tener un enrutador que dirija todo él trafico de entrada para un Intranet subdividida, se utiliza el primer byte del campo de la host id. Los bits que se usan para distinguir subredes se llaman números de subred.

- Cada computadora en cada subred recibe su propia dirección IP, como en una Intranet normal. La combinación del campo de la netid el número de subred, y finalmente un número de anfitrión, forman la dirección IP.

- El enrutador debe ir informado de que el campo de la hostid en las subredes tiene que tratarse de modo diferente que los campos del ahostid no subdivididos, si no en así, no podrá encaminar adecuadamente los datos. Para hacer esto, se emplea una mascara de subred. Una máscara de Subred es un número de 32 bits como 255.255.0.0, que se utiliza conjuntamente con los números en el campo del host id. Cuando se efectúa un cálculo usando la mascara de subred y la dirección IP, el enrutador sabe donde encamina el correo. La máscara de subred está incluida en los archivos de configuración de la red de los usuarios.

La mayoría de las Intranets no están construidas desde cero. Muchas son redes existentes, como Novell NetWare, que tienen que convertirse en una Intranet. A menudo, el primer paso en el movimiento hacia una Intranet puede introducirse en la propia red existente. Depues, la tecnología de Intranets puede introducirse en la propia red y convertirse en una Intranet.

Cuando una computadora en la red quiere conectar con Internet y solicitar información de ella, se envía una petición a un navegador en la Intranet. Este navegador enviará la petición al destino exacto en Internet. En la red NetWare, el sistema operativo NetWare se utiliza para manejar él tráfico de la red y la administración. Como método para encaminar paquetes a través de la red, NetWare emplea al protocolo IPX (Intercambio de Paquetes Internet). Aunque IPX se denomina intercambio de paquetes Internet, no ofrece realmente acceso a Internet o transporta la información de Internet. Las estaciones de trabajo pertenecientes a la red NetWare, y los servidores en la red, necesitan tener cargado IPX en la memoria para usar la red.

Para que las estaciones de trabajo en la red Novell consiga acceder a Internet o a la Intranet, necesitan ejecutar los protocolos TCP/IP que forman la base de Internet. Para hacer eso, debe instalarse una pila TCP/IP en cada computadora que permitirá la entrada a la Intranet. Esto significa que cada computadora tendrá instalado IPX y una pila TCP/IP, para permitir el acceso a Internet y a la red Ethernet. Básicamente, esto da como resultado "RAM de bote en bote" y es uno de los dolores de cabeza más fuertes para cualquiera que intente ejecutar ambas pilas de protocolos. Una unidad de servicio de canal/Unidad de Servicio de Datos (CSU/DSU) realiza la conexión física entre el enrutador de la Intranet y el Proveedor de Servicio Internet (IPS). EL ISP ofrece la autentica conexión Internet y servicios. Várias líneas digitales pueden conectar la CSU/DSU con el ISP, incluyendo una línea alquilada de 56 Kbps, una línea T1 de alta velocidad, o incluso una línea de mayor velocidad. La información solicitada se devuelve a través del CSU/DSU y del enrutador, y después se encamina a la computadora que pidió la información. Si la información está ubicada en una Intranet dentro de la compañía, el enrutador enviará la petición al anfitrión exacto, que después devolverá la información al solicitante. Algunos productos como NetWare/IP permitirán a las computadoras acceder a servicios de NetWare y a Internet. Esto significa que no tienen que ejecutar los protocolos IPX y TCP/IP, eliminando los problemas de memoria producidos por las múltiples pilas.

Cualquier Intranet es vulnerable a los ataques de personas que tengan el propósito de destruir o robar datos empresariales. La naturaleza sin límites de Internet y los protocolos TCP/IP exponen a una empresa a este tipo de ataques. Las Intranets requieren varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionan el control del tráfico; la encripción y las contraseñas para convalidar usuarios; y las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico.

El término genérico usado para denominar a una línea de defensa contra intrusos es firewall. Un *firewall* es una combinación de hardware/software que controla el tipo de servicios permitidos hacia o desde la Intranet.

Los servidores sustitutos son otra herramienta común utilizada para construir un *firewall*. Un servidor sustituto permite a los administradores de sistemas seguir la pista de todo el tráfico que entra y sale de una Intranet.

Un *firewall* de un servidor se configura para oponerse y evitar el acceso a los servicios no autorizados. Normalmente está aislado del resto de la Intranet en su propia subred de perímetro. De este modo si el servidor es "allanado", el resto de la Intranet no estará en peligro. Los sistemas de autenticación son una parte importante en el diseño de la seguridad de cualquier Intranet.

Los sistemas de autenticación se emplean para asegurar que cualquiera de sus recursos, es la persona que dice ser. Los sistemas de autenticación normalmente utilizan nombres de usuario, contraseñas y sistemas de encriptación.

El software para el bloqueo de sitios basado en el servidor de sitios puede prohibir a los usuarios de una Intranet la obtención de material indeseable. El software de control rastrea dónde ha ido la gente y qué servicios han usado, como HTTP para el acceso a la Web. El software para detectar virus basado en el servidor puede comprobar cualquier archivo que entra en la Intranet para asegurarse que está libre de virus.

Una manera de asegurarse de que las personas impropias o los datos erróneos no pueden acceder a la Intranet es usar un enrutador para filtrar. Este es un tipo especial de enrutador que examina la dirección IP y la información de cabecera de cada paquete que entra en la Intranet, y sólo permite el acceso a aquellos paquetes que tengan direcciones u otros datos, como correo electrónico, que el administrador del sistema ha decidido previamente que pueden acceder a la Intranet.

Los enrutadores para filtrar, algunas veces denominados enrutadores de selección, son la primera línea de defensa contra ataques a la Intranet. Los enrutadores para filtrar examinan cada paquete que se mueve entre redes en una Intranet. Un administrador de Intranets establece las reglas que utilizan los enrutadores para tomar decisiones sobre qué paquetes deberían admitir o denegar.

Las distintas reglas se pueden establecer para paquetes que entran y que salen de modo que los usuarios de Intranets puedan acceder a los servicios de Internet, mientras que cualquiera en Internet tendría prohibido el acceso a ciertos servicios y datos de la Intranet. Los enrutadores para filtrar pueden llevar el registro sobre la actividad de filtración. Comúnmente, siguen la pista a los paquetes sin permiso para pasar entre Internet y la Intranet, que indicarían que una Intranet ha estado expuesta al ataque.

Las direcciones de origen se leen desde la cabecera IP y se comparan con la lista de direcciones de origen en las tablas de filtros. Ciertas direcciones pueden ser conocidas por ser peligrosas y al incluir en la tabla permiten el enrutador denegar ese tráfico. El enrutador examina los datos en la cabecera IP que envuelve los datos y la información de cabecera de la pila de transporte. Eso significa que cualquier paquete contendrá datos, y dos conjuntos de cabeceras: una para la pila de transporte y otra para la pila de Internet. Los enrutadores para filtrar examinan todos estos datos y cabecera para decidir si permiten pasar a los paquetes. Los enrutadores pueden tener reglas diferentes para las subredes ya que pueden necesitar distintos niveles de seguridad. Una subred que contenga información privada financiera o competitiva puede tener muchas restricciones. Una subred de ingeniería puede tener menos restricciones en actividad que entran o salen.

Un enrutador para filtrar puede permitir a los usuarios tener acceso a servicios como Telnet y FTP, mientras que restringe el uso de Internet de estos servicios para acceder a la Intranet. Esta misma técnica se puede emplear para evitar que los usuarios internos accedan a datos restringidos de una Intranet. Por ejemplo, puede permitir a los miembros financieros el uso abierto de FTP mientras que deniega las peticiones FTP del departamento de ingeniería en el departamento de finanzas. Cierto tipo de servicios son más peligrosos que otros. Por ejemplo, FTP se utiliza para recibir archivos pero puede traer archivos que contengan un virus. Telnet y el comando roglin (que es como Telnet

pero con mayor riesgo de burlar la seguridad) están prohibidos por las reglas en la tabla de filtros que evalúan este tipo de servicio por él numero del puerto de origen o destino. Truncar direcciones es un método de ataque común. Para truncar direcciones, alguien externo a la Intranet falsifica una dirección de origen de modo que el enrutador le parezca que la dirección de origen es realmente de alguien de dentro de la Intranet. El bromista espera engañar al enrutador para filtrar para que le permita un mayor acceso a la Intranet que el que le permite una dirección externa original. Una vez que el enrutador se convenció de que el bromista estaba ya dentro de la Intranet, los archivos privados podrían enviarse potencialmente fuera de la Intranet. Los enrutadores pueden manejar direcciones truncadas.

Se puede establecer una regla que comunique al enrutador examinar la dirección de origen en cada cabecera IP que entre, pero que no salga. Si la dirección de origen es interna, pero el paquete proviene del exterior, el enrutador no admitirá el paquete.

Los *firewalls* protegen a las Intranets de los ataques iniciados contra ellas desde Internet. Están diseñados para proteger a una Intranet del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP.

Las computadoras de las Intranets sólo tienen permiso para acceder a Internet después de atravesar un *firewall*. Las peticiones tienen que atravesar un enrutador interno de selección, llamado también enrutador interno para filtrar o enrutador de obstrucción. Este enrutador evita que el trafico de paquetes sea "husmeado" remotamente. Un enrutador de obstrucción examina la información de todos los paquetes como cuál es su origen y cuál su destino. El enrutador compara la información que encuentra con las reglas en una tabla de filtros, y admite, o no, los paquetes basándose en esas reglas. Por ejemplo, algunos servicios, como roglin, no pueden tener permiso para ejecutarse. El enrutador no permite tampoco que cualquier paquete se envíe a localizaciones específicas del Internet sospechosas. Un enrutador también puede bloquear cada paquete que viaje entre Internet y la Intranet, excepto el correo electrónico. Los administradores de sistemas definen qué paquetes admitir y cuáles denegar. Cuando una Intranet está protegida por un *firewall*, están disponibles los servicios internos usuales de la red, como el correo electrónico, el acceso a las bases de datos corporativas y a los servicios de la Web, y el uso de programas para el trabajo en grupo.

Los *firewall* seleccionados de la subred tiene una manera más para proteger la Intranet: un enrutador exterior de selección, también denominado enrutador de acceso. Este enrutador selecciona paquetes entre Internet y la red de perímetro utilizando el mismo tipo de tecnología que el enrutador interior de selección. Puede seleccionar paquetes basándose en las mismas reglas que plica el enrutador interior de selección y puede proteger a la red incluso si el enrutador interno falla. Sin embargo, también puede tener reglas adicionales para la selección de paquetes diseñadas eficazmente para proteger al anfitrión bastón. Como un modo adicional para proteger a una Intranet del ataque, el anfitrión bastón se coloca en una red de perímetro, una subred, dentro del *firewall*. Si el anfitrión bastón estuviera en la Intranet en vez de en una red de perímetro y fuera, el intruso podría obtener acceso a la Intranet. Un anfitrión bastión es el punto de contacto principal para las conexiones provenientes de Internet para todos los servicios como el e-mail, el acceso FTP, y cualesquiera otros datos y peticiones. El anfitrión bastión atiende todas esas peticiones, las personas en la Intranet sólo se ponen en contacto con este servidor, y no contactan directamente con otros servidores de Intranets. De este modo, los servidores de Intranets están protegidos del ataque. Los anfitriones bastión también pueden configurarse como servidores sustitutos.

Una parte integral de muchos de los sistemas de seguridad es el servidor sustituto. Un servidor sustituto software y un servidor que se coloca en un *firewall* y actúa como intermediario entre computadoras en una Intranet e Internet. Los servidores sustitutos a menudo se ejecutan en anfitriones bastón. Solo el servidor sustituto en vez de las muchas computadoras individuales en la Intranet, interactúan con Internet, de este modo la seguridad se puede mantener porque el servidor puede estar más seguro que los cientos de computadoras individuales en la Intranet. Los

administradores de Intranets pueden configurar servidores sustitutos que puedan utilizarse para muchos servicios, como FTP, la Web y Telnet. Los administradores de Intranets deciden que servicios de Internet deben atravesar un servidor sustituto, y cuales no. Se necesita software especifico del servidor sustituto para cada tipo diferente de servicio Internet.

Cuando una computadora en la Intranet realiza una petición a Internet, como recuperar una página Web desde un servidor Web, la computadora interna se pone en contacto con el servidor Internet, El servidor Internet envía la página Web al servidor sustituto, que después la mandará a la computadora de la Intranet.

Los servidores sustitutos registran todo en tráfico entre Internet y la Intranet, por ejemplo, un servidor sustituto de Telnet podría seguir la pista de cada pulsación de una tecla en cada sección Telnet en la Intranet, y también podría seguir la pista de cómo reacciona al servidor externo en Internet con esas pulsaciones. Los servidores sustitutos pueden anotar cada dirección IP, fecha y hora de acceso, URL, número de bytes recibidos, etcétera. Esta información se puede utilizar para analizar cualquier ataque iniciado contra la red. También puede ayudar a los administradores de Intranets a construir mejor acceso y servicios para los empleados. Algunos servidores sustitutos tienen que trabajar con clientes sustitutos especiales. Una tendencia más popular es usar clientes con servidores sustitutos ya configurados como Netscape. Cuando se emplea este paquete ya hecho, debe configurarse especialmente para trabajar con servidores sustitutos desde el menú de configuración. Después el empleado de la Intranet usa el software cliente como de costumbre. El software cliente sabe salir hacia un servidor sustituto para obtener datos, en vez de hacia Internet.

Los servidores sustitutos pueden hacer algo más que hacer llegar las peticiones entre una Intranet e Internet. También pueden hacer efectivos los diseños de seguridad. Por ejemplo podría configurarse para permitir un envío de archivos desde Internet a una computadora de la Intranet, pero impedir que se manden archivos desde la red empresarial a Internet, o viceversa. De este modo, los administradores de Intranets pueden impedir que cualquier persona externa a la corporación reciba datos corporativos vitales. O pueden evitar que los usuarios de la Intranet reciban archivos que puedan contener virus. Los servidores sustitutos también se pueden utilizar para acelerar la actuación de algunos servicios de Internet almacenando datos. Por ejemplo, un servidor Web sustituto podría almacenar muchas paginas Web, a fin de que cuando alguien desde la Intranet quisiera obtener alguna de esas páginas Web, accediera ella directamente desde el servidor sustituto a través de líneas de la Intranet de alta velocidad, en lugar de tener que salir a través de Internet y obtener la página a menor velocidad desde las líneas de Internet.

Un *anfitrión bastión* (llamado también servidor bastón) es una de las defensas principales en el firewall de una Intranet. Es un servidor fuertemente fortificado que se coloca dentro del *firewall*, y es el punto de contacto principal de la Intranet e Internet. Al tener como punto de contacto principal un servidor aislado, duramente defendido, el resto de los recursos de la Intranet pueden protegerse de los ataques que se inician en Internet.

Los anfitriones bastión se construyen para que cada servicio posible de la red quede inutilizado una vez dentro de ellos, lo único que hace el servidor es permitir el acceso especifico de Internet. Así que, por ejemplo, no debería haber ninguna cuenta de usuarios en un servidor bastón, para que nadie pudiera entrar, tomar el control y después obtener acceso a la Internet. Incluso el Sistema de Archivos de Red (NFS), que permite a un sistema el acceso a archivos a través de una red en un sistema remoto, debería inhabilitarse para que los intrusos no pudieran acceder al servidor bastión es instalarlo en su propia subred como parte del *firewall* de una Intranet. Al colocarlos en su propia red, si son atacados, ningún recurso de la Intranet se pone en peligro.

Los servidores bastión registran todas las actividades para que los administradores de Intranets puedan decir la red ha sido atacada. A menudo guardan dos copias de los registros del sistema por razones de seguridad: en caso de que se destruya o falsifique un registro, el otro siempre estará disponible como reserva. Un modo de guardar una copia segura del registro es conectar el

servidor bastión mediante un puerto de serie con una computadora especializada, cuyo único propósito es seguir la pista del registro de reserva.

Los monitores automatizados son programas incluso más sofisticados que el software de auditoria. Comprueban con regularidad los registros del sistema del servidor bastión, y envían una alarma si encuentra un patrón sospechoso. Por ejemplo, se puede enviar una alarma si alguien intenta más de tres conexiones no exitosas. Algunos servidores bastión incluyen programas de auditoria, que examinan activamente si se ha iniciado un ataque en su contra. Hay varias maneras de hacer una auditoria: una manera de revisar esto es utilizar un programa de control que compruebe si algún software en el servidor bastión se ha modificado por una persona no autorizada. El programa de control calcula un número basándose en el tamaño de un programa ejecutable que hay en el servidor.

Después calcula con regularidad el número de control para ver si ha cambiado desde la última vez que lo hizo. Si ha cambiado, significa que alguien ha alterado el software, lo que podría indicar un ataque externo.

Cuando un servidor bastión recibe una petición de un servidor como puede ser enviar una pagina Web o repartir correo electrónico, el servidor no administra la petición él mismo; en su lugar, envía la petición al servidor de Intranets apropiado. EL servidor de Intranets maneja la petición, y después devuelve la información al servidor bastión; y será ahora cuando envíe la información requerida al solicitarme en Internet.

Puede haber más de un anfitrión bastión en un *firewall*; y cada uno puede administrar varios servicios de Internet para la Intranet. Algunas veces, un anfitrión bastión se puede utilizar como máquina víctima: un servidor despojado de casi todos los servicios excepto de uno específico de Internet. Las máquinas víctimas pueden emplearse para ofrecer servicios de Internet que son difíciles de manejar o cuyas limitaciones sobre la seguridad no se conocen aún, utilizando un enrutador sustituto o uno para filtrar. Los servidores se colocan en la máquina víctima en vez de en un anfitrión bastión con otros servicios. De ese modo, si se irrumpe en el servidor, los otros anfitriones bastión no estarán afectados.

Un medio de asegurar una Intranet es usar la encriptación: alterar datos para que sólo alguien con acceso a códigos específicos para descifrar pueda comprender la información. La encriptación se utiliza para almacenar y enviar contraseña para asegurarse de que ningún fisgón pueda entenderla. La encriptación se emplea también cuando se envían datos entre Intranets en Redes Privadas Muy Seguras (VSPN). Además la encriptación se usa para dirigir el comercio en Internet y proteger la información de la tarjeta de crédito durante la transmisión.

Las claves son el centro de la encriptación. Las claves son formulas matemáticas complejas (algoritmos), que se utilizan para cifrar y descifrar mensajes. Si alguien cifra un mensaje sólo otra persona con la clave exacta será capaz de descifrarlo. Hay dos sistemas de claves básicos: criptografía de claves secretas y de claves públicas. Se emplea un algoritmo para realizar una función de rehecho. Este proceso produce un resumen del mensaje único al mensaje. El resumen del mensaje se cifra con la clave privada del emisor que da lugar a una "huella digital".

El estándar de Encriptación de Datos (DES) es un sistema de claves secretas (simétrico); no hay componente de clave privada. El emisor y el receptor conocen la palabra secreta del código. Este método no es factible para dirigir negocios por Internet. RSA es un sistema de claves públicas (asimétrico), que utiliza pares de claves para cifrar y descifrar mensajes. Cada persona tiene una clave pública, disponible para cualquiera en un anillo de claves públicas, y una clave privada, guardada sólo en la computadora. Los datos cifrados con la clave privada de alguien sólo pueden descifrarse con su clave pública, y los datos cifrados con su clave pública sólo pueden descifrarse con su clave privada. Por tanto, RSA necesita un intercambio de claves públicas, esto se puede realizar sin necesidad de secretos ya que la clave pública es inútil sin la clave privada.

PGP, Privacidad de las buenas, un programa inventado por Philip Zimmermann, es un método popular empleado para cifrar datos. Utiliza MD5 (resumen del mensaje 5) y los sistemas cifrados de RSA para generar los pares de claves. Es un programa muy extendido que se puede ejecutar en plataformas UNIX, DOS y Macintosh. Ofrece algunas variaciones de funcionalidad, como la comprensión, que otros sistemas cifrados no brindan. Los pares de claves múltiples se pueden generar y ubicar en anillos de claves públicas y privadas.

Una de las primeras líneas de defensa de una Intranet es usar la protección de las contraseñas. Varias técnicas de seguridad, incluyendo la encriptación, ayudan a asegurarse de que las contraseñas se mantienen a salvo. También es necesario exigir que las contraseñas se cambien frecuentemente, que no sean adivinadas fácilmente o palabras comunes del diccionario, y que no se revelen simplemente. La autenticación es el paso adicional para verificar que la persona que ofrece la contraseña es la persona autorizada para hacerlo.

El servidor cifra la contraseña que recibe del usuario, utilizando la misma técnica de encriptación empleada para cifrar la tabla de contraseñas del servidor. Compara la contraseña cifrada del usuario con la contraseña cifrada en la tabla. Si los resultados encajan, el usuario tiene permiso para entrar en el sistema. Si los resultados no encajan, el usuario no tiene permiso.

Las contraseñas de la gente y los nombres de usuario en una Intranet se almacenan dentro de un formulario de tablas de un archivo que se encuentra en un servidor que verifica las contraseñas. A menudo, el nombre del archivo es password y el directorio en el que se encuentra dependiendo de la técnica de autenticación de contraseñas que se use, el archivo puede estar cifrado o no.

Un método para reconocer a un usuario es a través del Protocolo de Autenticación de Contraseñas (PAP). PAP no asigna la encriptación, pero la tabla de contraseñas en el servidor está normalmente cifrada. Cuando alguien quiere entrar a la red o a un recurso de la red protegido con una contraseña, se le pide el nombre de usuario y la contraseña. El nombre de usuario y la contraseña se envía después al servidor.

El sistema del Protocolo de Autenticación para Cuestionar el Handshake (CHAP) es un sistema de respuesta. El CHAP requiere una tabla de contraseñas no cifrada. Cuando alguien entra en un sistema con CHAP, el servidor genera una clave al azar que se envía al usuario para que cifre su contraseña.

La computadora del usuario emplea esta clave para cifrar su contraseña. Después la contraseña cifrada se devuelve al servidor. El servidor se remite a la tabla de contraseñas para la clave al azar, y cifra la contraseña con la misma clave que se envió al usuario. El servidor compara después la contraseña cifrada con la del usuario con la contraseña cifrada que creó. Si encajan, el usuario tiene permiso de entrada.

La clave de diferencia de CHAP en que el servidor continúa preguntando a la computadora del usuario a lo largo de la sesión. Además, se envía distintas preguntas que deben ser cifradas y devueltas por la computadora, sin intervención humana. De este modo CHAP limita tu ventana de vulnerabilidad. Una sesión no puede piratearse, puesto que el pirata no sería admitido una vez que la computadora no respondiera correctamente a los desafíos que se suceden periódicamente.

Sin importar qué tipo de sistemas de contraseñas se utilice, ni la tabla de contraseñas está cifrada o no, lo importante es proteger la tabla de contraseñas. El archivo debe protegerse contra el acceso FTP y debería haber acceso restringido al archivo para que sólo el administrador o alguien bajo el control del administrador pueda acceder a él.

Los virus son el mayor riesgo en la seguridad de las Intranets. Pueden dañar datos, ocupar y consumir recursos, e interrumpir operaciones. Los archivos de programas eran la principal fuente de problemas en el pasado, pero los nuevos virus de "macro" se pueden esconder en archivos de datos e

iniciarse, por ejemplo, cuando se ejecutan una macro en un programa de procesamiento de texto. El software para examinar virus basado en el servidor y el basado en el cliente poseen dispositivos que ayudan a proteger a la Intranet.

Un virus se esconde dentro de un programa. Hasta que ejecutes el programa infectado, el virus permanece inactivo, entonces el virus entra en acción. Algunas veces, lo primero que hará es infectar otros programas del disco duro copiándose de ellos.

Algunos virus colocan mensajes denominados V-marcadores o marcadores de virus dentro de programas que están infectados y ayudan a manejar las actividades víricas. Cada virus tiene un marcador de virus específico asociado con él. Si un virus se encuentra con uno de estos marcadores en otro programa, sabe que el programa ya está infectado y de ese modo no se reproduce allí.

Cuando un virus no encuentra ningún archivo sin marcar en una computadora, eso puede indicar al virus que no hay que infectar más archivos. En este momento, el virus empieza a estropear la computadora y sus datos. Los virus no pueden corromper los archivos de programas o de datos ya que cuando se ejecutan funcionan extrañamente, no funcionan o causan daños. Pueden destruir todos los archivos de tu computadora cuando se conecta y provocar otro tipo de averías.

El software para examinar virus se ejecuta en un servidor dentro del *firewall* de una Intranet. El software no comprueba la posible existencia de virus en cada paquete que entra en la Intranet, ya que eso sería imposible. En su lugar, sólo comprueba aquellos paquetes enviados con los tipos de servicios y protocolos Internet que indican que un archivo puede encontrarse en el proceso de transferencia desde Internet, comúnmente, e-mail que se envía mediante SMTP, (Protocolo Simple de Transferencia de Correo), el Protocolo de Transferencia de Archivos (FTP) y la World Wide Web (http; Protocolo Transferencia de Hipertexto). EL software emplea la tecnología de filtrado de paquetes para determinar qué paquetes se están enviando con estos protocolos.

Cuando el software encuentra paquetes que se envían con SMTP, FTP o HTTP, sabe que debe examinarlos más a fondo, para ver si tienen virus. El software para examinar virus funciona de varias maneras. Un método de detección es comprobar archivos para revelar marcadores de virus que indican la presencia de un virus. Los paquetes que no están utilizando SMTP, FTP o HTTP (como TNP) se admiten y el software no realiza ninguna acción en ellos.

Si se encuentra que el archivo está libre de virus, se le permite pasar. Si se encuentra que tiene virus, no se le permitirá entrar en la Intranet.

El software antivirus también debería ejecutarse en computadoras individuales dentro de la Intranet porque es posible que se pueda introducir un virus en la Intranet por disquetes, por ejemplo. Además de la protección contra virus, puede detectar virus y extirpar cualquier virus que encuentre.

El software para el bloqueo de sitios examina el URL de cada petición que sale de la Intranet. Los URL más propensos a no ser aceptados accederán a la Web (HTTP); grupos de noticias (NTP), ftp (FTP); gopher (gopher) y las conversaciones de Internet (irc). EL software toma cada uno de estos cinco tipos de URL y los pone en sus propias "cajas" separadas. El resto de la información de la Intranet que sale tiene permiso para pasar.

Cada URL en cada caja se comprueba en una base de datos de los URL de los sitios censurables. Si el software de bloqueo encuentra que algunos de los URL provienen de sitios desagradables, no permitirá que la información pase a la Intranet. Los productos como SurfWatch como prueban miles de sitios y enumeran varios miles en sus bases de datos que se han encontrado molestos.

El software para bloquear sitios comprueba después el URL con una base de datos de palabras (como "sexo") que puede indicar que el material que se solicita puede ser censurable. Si el

software de bloqueo encuentra un patrón que encaje, no permitirá que la información pase a la Intranet.

El software para bloquear sitios puede entonces emplear un tercer método para comprobar los sitios desagradables; un sistema de clasificación llamado PICS (Plataforma para la Selección de Contenido en Internet). Si el software para el bloqueo de sitios encuentra, basándose en el sistema de clasificación, que el URL es para un sitio que puede contener material censurable, no permitirá el acceso a ese sitio.

Debido a que Internet está creciendo tan deprisa, las bases de datos de sitios censurables podrían llegar a ser anticuados. Para resolver el problema, la base de datos se actualiza cada mes. El software para el bloqueo de sitios conectará automáticamente con un sitio en Internet, y recibirá la base de datos de sitios desagradables más nueva a través de FTP.

Los administradores de Intranets pueden encontrar sitios no enumerados en la base de datos y no filtrados por el software para bloquear sitios que ellos quieren bloquear. Para bloquear manualmente el acceso a esos sitios, pueden añadirlos simplemente a la base de datos.

El software utiliza filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar. Ambos observan los datos en la cabecera de cada paquete IP que entra y sale de la Intranet. Sin embargo, se diferencian en que los enrutadores para filtrar deciden si admiten o no a los paquetes. El software de supervisión simplemente deja pasar a los paquetes y sigue la pista a la información de los paquetes además delos datos como la dirección del emisor y destino, el tamaño del paquete, el tipo de servicio de Internet implicado (como la WEB o FTP) y la hora del día en la que se recogen en una base de datos.

Mientras que todos los paquetes deben pasar a través del servidor, el software no introduce necesariamente la información de cada paquete en la base de datos. Por ejemplo, la información acerca de los paquetes http (World Wide Web), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes del protocolo de transferencia de archivos (FTP), los paquetes e-mail (SMTP), los paquetes delos grupos de noticias (TNP) y los paquetes Telnet pueden seguirse, mientras que los paquetes de sonido fluido pueden ignorarse.

El software incluido con el programa del servidor permite a los administradores de redes examinar y analizar el tráfico de la Intranet y de Internet en un grado extraordinario. Puede mostrar la cantidad total del tráfico de la red por día y por horas, por ejemplo, y mostrar a cualquier hora a qué sitios de Internet se estaban transfiriendo. Puede incluso mostrar qué sitios estaban visitando los usuarios individuales en la Intranet, y los sitios más populares visitados en forma gráfica.

Algún software va más allá del análisis y permite a los administradores de Intranets cambiar el tipo de acceso a Internet de los usuarios de la Intranet, basándose en el tráfico, uso y otros factores. El software permitirá también a los administradores de Intranets prohibir que se visiten ciertos sitios de la Intranet.

Una Red Privada Virtual Segura (VSPN) o Red Privada Virtual (VPN) permite a los empresarios, siempre y cuando cada uno posea una Intranet, enviarse comunicaciones seguras por Internet y saber que nadie más será capaz de leer los datos. Esencialmente, crea un canal privado y seguro entre sus respectivas Intranets, incluso aunque los datos enviados entre ellas viajen por la Internet pública. Esto significa que las compañías no tienen que alquilar líneas caras entre ellas para mandar datos a través de un enlace seguro. Esta tecnología también se puede emplear para permitir a una compañía enlazar sucursales sin tener que alquilar líneas caras y saber que los datos se pueden leer por la gente de la VSPN.

Una de las razones más importantes por las que las empresas instalan una Intranet es para permitir a sus empleados trabajar mejor juntos. EL tipo de software más potente que deja a la gente

trabajar juntas está incluido en el extenso apartado de programas para trabajo en grupo y admite que los usuarios empleen la conferencia visual, comparta documentos, participen en discusiones y trabajen juntos de otro modo.

Las herramientas de búsqueda y de catalogación, como agentes, arañas, tractores y autómatas, algunas veces denominadas motores de búsqueda, se pueden utilizar para ayudar a la gente a encontrar información y se emplean para reunir información acerca de documentos disponibles en una Intranet. Estas herramientas de búsqueda son programas que buscan páginas Web, obtienen los enlaces de hipertexto en esas páginas y clasifican la información que encuentran para construir una base de datos. Cada motor de búsqueda tiene su propio conjunto de reglas. Algunos siguen cada enlace en todas las paginas que encuentran, y después en turno examinan cada enlace en cada una de esas paginas iniciales nuevas, etc. Algunos ignoran enlaces que dirigen a archivos gráficos, archivos de sonido y archivos de animación; algunos enlaces a ciertos recursos como las bases de datos WAIS; y a algunos se les dan instrucciones para buscar las páginas iniciales más visitadas.

Las Intranets se utilizan no sólo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlos - recibir y rellenar pedidos de bienes y servicios. Aunque para que esto ocurra, se debe diseñar una manera segura para enviar la información de la tarjeta de crédito por la notoriamente insegura Internet. Hay muchos métodos para hacer esto pero probablemente el que más se utilizará será un estándar llamado: el protocolo para la Transacción Electrónica Segura (SET), que ha sido aprobado por VISA, MasterCard, American Express, Microsoft y Nestcape, entre otras compañías. Es un sistema que permitirá a la gente con tarjetas bancarias hacer negocios seguros por las Intranets.

Con la evolución que cada día sufren los sistemas de computación, su fácil manejo e innumerables funciones que nos ofrece, se puede decir que igualmente se ha incrementado el número de usuarios que trabajan con computadoras, no sin antes destacar él Internet; una vía de comunicación efectiva y eficaz, donde nos une a todos por medio de una computadora.

Utilizando la Red de Area Local en una estructura interna y privada en una organización, seguidamente se construye usando los protocolos TCP/IP. Permite a los usuarios trabajar de una forma sencilla y efectiva, al mismo tiempo brinda seguridad en cuanto a la información ya que esta protegida por un firewall.

Por otra parte el Intranet nos permite trabajar en grupo en proyectos, compartir información, llevar a cabo conferencias visuales y establecer procedimientos seguros para el trabajo de producción.

La Intranet es una red privada, aquellos usuarios dentro de una empresa que trabajan con Intranet pueden acceder a Internet, pero aquellos en Internet no pueden entrar en la Intranet de dicha empresa. El software que se utilizan en los Intranets es estándar: software de Internet como él Netscape Navigator y los Navegadores Explorer para Web de Microsoft, facilitan los intercambios de información entre varios departamentos para poder llevar a cabo sus objetivos. Los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el guión de C.P.I. (Interfase Común de Pasarela) permitiendo hacer negocios en línea, la información enviada a través de una Intranet alcanza su lugar exacto mediante los enrutadores.

Construyendo los protocolos TCP/IP (son los que diferencian a la Intranet de cualquier otra red privada) los cuales trabajan juntos para transmitir datos. (TCP: Protocolo de Control de Transmisión y el I.P: Protocolo de Internet), estos protocolos manejan el encadenamiento de los datos y asegura que se envían al destino exacto, funciona conjuntamente y se sitúan uno encima de otro en lo que se conoce comúnmente Peta de Protocolo, esta formatea los datos que se están enviando para que la pila inferior, la de transporte, los pueda remitir.

Cuando hay una gran cantidad de tráfico en una Red de Area Local, los paquetes de datos pueden chocar entre ellos, reduciendo en eficacia de la Red. Por tal motivo se utilizan combinaciones de Hardware y Software denominados Puentes que conectan con enrutadores en un solo producto llamado brouter, que ejecuta la tarea de ambos. Los enrutadores son los que aseguran que todos los datos se envíen donde se supone tienen que ir y de que lo hacen por la ruta más eficaz, desviando el trafico y ofreciendo rutas, cuentan con dos más puertos físicos. Los de recepción (de entrada) y los de envío (de salida), cada puerto es bidireccional y puede recibir o enviar datos.

Saliendo un poco en cuanto a Procesamiento de Datos podemos destacar dentro del Intranet el Uso de Correo Electrónico, utilizando a la vez el Protocolo Simple de Transmisión de Correo (CMTP), emplea una arquitectura cliente / servidor; el receptor del correo puede utilizar ahora un agente usuario de correo para leer el mensaje, archivarlo y responderlo.

Frecuentemente el correo electrónico generado por Intranet no se entregará a una computadora de la Intranet, sino a alguien en Internet, en otra Intranet. EL mensaje deja la Intranet y se envía a un enrutador Internet. EL enrutador examina la dirección, determina donde debería mandarse el mensaje, y después lo pone en camino.

El motivo por el cual que una Intranet es porque la Web facilita la publicación de la información y formularios usando el Lenguaje de Hipertexto (HTML), permite también la creación de paginas iniciales multimedia, que están compuestas por textos, video, animación, sonido e imagen.

Los programadores pueden vincular datos corporativos desde una Intranet, permitiendo el uso de sistemas patrimoniales como base de datos en el Java, el cual es similar al lenguaje informático C++, es compilado, lo que significa que después de que el programa Java se escribe, debe ejecutarse a través de un compilador para transformar el programa en el lenguaje que pueda entender la computadora.

La Intranet se puede subdividir en varios niveles al momento de sobrepasar su tamaño y al ser difícil de manejar, para resolver el problema se crean subsecciones de una Intranet que las hacen más fáciles de hoslid: los bits que se usan para distinguir subredes se llaman números de subred.

Finalmente podemos decir que las Intranets permiten a los empresarios que a sus empleados trabajen en grupo, tal motivo se debe al extenso aportado de programas para trabajo en grupo y admite que los usuarios empleen la conferencia visual, compartan documentos, participen en discusiones y trabajen juntos de otro modo, no solo para coordinar negocios y hacerlos más eficaces, sino también como un lugar para hacerlo recibir y rellenar pedidos de bienes y servicios.

GLOSARIO DE TÉRMINOS.

2B+D.- Codificación de línea: 2B1Q.

2B+D.- Canales B, B y D.

ACK.- Acuse de Recibo, *(Acknowledgement)*.

ARQ.- Requerimiento de Repetición Automático, *(Automatic Repeat Request)*.

ASCII.- Código Estándar Americano para el Intercambio de Información, *(American Standard Code for Information Interchange)*.

ATM.- Modelo de Transferencia Asíncrono, *(Asynchronous Trabsfer Mode)*.

BER.- Tasa de Errores de Bit *(Bit Error Rate)*.

BOOTP.- *Bootstrap Protocol*.

CCITT.- Comité Consultivo Internacional de Telegrafía y Telefonía, *(Committee Consultative Internacional for Telegraphy and Telephony)*.

CIB.- Bit Indicador de CRC 32, *(CRC 32 Indicator Bit)*.

COCF.- Función de Convergencia Orientada a Conexiones, *(Connection-Oriented Convergente Function)*.

COM.- Continuación del Mensaje *(Continuation of the Message)*.

CRC.- Verificación de Redundancia Cíclica *(Cyclic Redundancy Check)*.

CSMA/CD.- Acceso Múltiple por Detección de Portadora/Detección de Colisiones, *(Carrier Sense Multiple Access/Collision Detect)*.

CSTA.- Aplicaciones Telefónicas Soportadas por ordenador, *(Computer Supported Telephony Applications)*.

CSU.- Unidad de Servicio de Canal, *(Channel Service Unit)*.

DNS.- Sistema de Nombres de Dominio, *(Domain Name System)*.

DP.- Punto de Detección, *(Detection Point)*.

DPDU.- PDU de Capa de Enlace de Datos, *(Data Link Layer PDU)*.

DPSK.- PSK Differential, *(Differential PSK)*.

DSI.- Interpolación Digital de Voz, *(Digital Speech Interpolation)*.

DSP.- Parte Específica para el Dominio, *(Domain Specific Part)*.

DSU.- Unidad de Datos de Servicio, *(Data Service Unit)*.

DTE.- Equipo Terminal de Datos, *(Data Terminal Equipment)*.

DTI.- Departamento de Comercio e Industria, *(Department of Trade and Industry)*.

DTMF.- Tono Dual, Múltiple Frecuencia, *(Dual Tone Multiple Frecuency)*.

DNA.- Arquitectura Digital de Red, *(Digital Network Architecture)*.

EC.- Comisión Europea, *(European Commission)*.

ECMA.- Asociación de Fabricantes de Equipo de Cómputo Europea, *(European Computer Manufacturers Association)*.

ECSA.- Asociación de Normas Portadoras de Intercambio, *(Exchange Carriers Standards Association)*.

EOM.- Fin del Mensaje, *(End of Message)*.

ETSI.- Instituto de Normas de Telecomunicaciones Europeas, *(European Telecommunications Standard Institute)*.

FCC.- Comisión Federal de Comunicaciones, *(Federal Communications Commission)*.

FDDI.- Interfase de Datos Distribuida por Fibra, *(Fiber Distribuited Data Interface)*.

FEC.- Control de Errores hacia Adelante, *(Forward Error Control)*.

FEC.- Corrección de Errores hacia Adelante, *(Forward Error Correction)*.

FECN.- Bit de Notificaciones Explícita de Congestionamiento hacia Adelante, *(Forward Explicit Congestion Notification Bit)*.

FRF.- Foro de Frame Relay, *(Frame Relay Forum)*.

FTP.- Protocolo de Transferencia de Archivos, *(File Transfer Protocol)*.

GSM.- Grupo Especial Móvil, *(Groupe Speciale Mobile)*.

GUI.- Interfase Gráfica de usuario, *(Graphical User Interface)*.

HCS.- Secuencia de Verificación de Encabezado, *(Header Check Sequence)*.

HDCL.- Control de Enlace de Datos de Alto Nivel, *(High Level Data Link Control)*.

HDSL.- Línea de Suscriptor Digital con Alta Tasa de Bits, *(High Bit-Rate Digital Subscriber Line)*.

HTTP.- Protocolo de Transferencia de Hipertexto, (*Hyper Texte Transfer Protocol)*.

ICF.- Función de Convergencia Isócrona, *(Isochronous Convergence Function)*.

ICI.- Interfase de Portadora de Intercambio, *(Interchange Carrier Interface)*.

ICIP.- Protocolo ICI, *(ICI Protocol)*.

IEEE.- Instituto de Ingenieros en Electricidad y Electrónica, *(Institute of Electrical and Electronic Engineers)*.

IGMP.- *Internet Group Multicast Protocol.*

IKE.- *Internet Key Exchange.*

IMPDU.- Unidad de Datos de Protocolo MAC Inicial, *(Inicial MAC Protocol Data Unit)*.

IP.- Protocolo de Internet, *(Internet Protocol)*.

IPv4.- Protocolo de Internet Versión 4, *(Internet protocol Version 4)*.

IPv6.- Protocolo de Internet Versión 6, *(Internet protocol Version 6)*

ISDN.- Red Digital de Servicios Integrados, *(Integrated Services Digital Network)*.

ISO.- Organización Internacional de Normas, *(Internacional Standards Organization)*.

ISP.- *Internet Service Provider.*

ISUP.- Parte de usuario de ISDN, *(ISDN User Part).*

ITU.- Unión Internacional de Telecomunicaciones, *(Internacional Telecommunications Union).*

LAN.- Redes de Área Local, *(Local Area Networks).*

LAPB.- Procedimiento de Acceso a Enlaces Balanceado, *(Link Access Procedure Balanced).*

LAPD.- Procedimiento de Acceso a Enlaces para el Canal D, *(Link Access Procedure for the D Channel).*

LT.- Terminación de Línea, *(Line Termination).*

MAN.- Red de Área Metropolitana, *(Metropolitan Area Network).*

MIB.- Base de Información de Gestión, *(Management Information Base).*

MID.- Identificador de Mensaje, *(Message Identifier).*

MMDS.- Servicio de Distribución Multipunto Multicanal, *(Multipoint Multichannel Distribution Service).*

MPLS.- *Multi Protocol Laber Switching.*

MSU.- Unidad de Señal de Mensaje, *(Message Signal Unit).*

MTP.- Parte de Transferencia de Mensajes, *(Message Transfer Part).*

N-ISDN.- ISDN de Banda Angosta, *(Narrowband ISDN).*

NAK.- Acuse de Recibo Negativo, *(Negative Acknowlegment).*

NEI.- Identificador de Entidad de Red, *(Network Entity Identifier).*

NIU.- Unidad de Interfase de Red, *(Network Interface Unit).*

MNS.- *Network Management System.*

NNI.- Interfase Red-Nodo *(Network-Node Interface).*

NNI.- Interfase Red-Red, *(Network-to-Network Interface).*

NOC.-*Network Operations Center.*

OSPF.- Abrir Primero el Trayecto más Corto, *(Open Shortest Path First).*

PABX.- *Private Automatic Branch Exchange.*

PBX.- *Private Branch Exchange.*

PCI.- *Protocol Control Information.*

PCM.- Modulación por Código de Pulso, *(Pulse Code Modulation).*

PCMCIA.- *Personal Computer Memory Card Internal Associated.*

PHY.- Capa Física, *(Phisical Layer).*

PPTP.- *Poin-to-Point Tunneling Protocol.*

PRI.- Interfase de Tasa primaria, *(Primary Rate Interface).*

PSK.- Modulación por Desplazamiento de Fase, *(Phase Shift Key).*

PSTN.- *Public Switched Telephone Network.*

PT.- Tipo de carga Útil, *(Payload Type).*

PTT.- Protocolo para Telefonía y Telegrafía.

PVC.- Circuito Virtual Permanente, *(Permanent Virtual Circuit).*

PVN.- Red Virtual Permanente, *(Private Virtual Network).*

QAM.- Modulación de Amplitud y Cuadratura, *(Quadrature Amplitude Modulation).*

QoS.- Calidad de Servicio, *(Quality of Service).*

QPSK.- Modulación de Cuadratura y Desplazamiento de Fase, *(Quadrature Phase Shift Keyed).*

RQ.- Contador o Temporizador de Solicitudes, *(Request Timer).*

SAP.- Punto de Acceso al Servicio, *(Service Access Point).*

SAPI.- Identificador de Punto de Acceso al Servicio, *(Service Access Point Identifier).*

SDDI.- Especificación de Par trenzado Blindado.

SDH.- Jerarquía Digital Síncrona, *(Synchronous Digital Hierachy).*

SIR.- Tasa de Información Sostenida, *(Sustained Information Rate).*

SNMP.- Protocolo Simple de Gestión de Redes, *(Simple Network Management Protocol).*

SONET.- Red Óptica Síncrona, *(Synchronous Optical Network).*

SPVC.- Circuito Virtual Semipermanente, *(Semipermanent Virtual Circuit).*

SQL.- *Standard Query Language.*

STDM.- Multiplexor Estadístico por División en el Tiempo, *(Statistical Time Division Multiplexer).*

SVC.- Circuito Virtual Conmutado, *(Switched Virtual Circuit).*

TCP.- Protocolo de Control de Transmisión, *(Transmisión Control Protocol).*

TDM.- Multiplexión por División en el Tiempo, *(Time Division Multiplexing).*

TDMA.- Acceso Múltiple por División del Tiempo, *(Time Division Multiple Access).*

TELNET.- Protocolo TELNET.

ToS.- Tipo de Servicio, *(Type of Service).*

TTY.- Teletipo.

UI.- Información no Numerada, *(Unnumbered Information).*

UDP.- *User Datagram Protocol.*

ULP.- Protocolos de Capa Superior, *(Upper Layer Protocols).*

UTP.- Par Trenzado no Blindado, *(Unshielded Twisted Pair).*

VC.- Canal Virtual, *(Virtual Channel).*

VCC.- Conexión de Canal Virtual, *(Virtual Channel Connection)*.

VLAN.- *Virtual LAN.*

VPC.- Conexión de Trayectoria Virtual, *(Virtual Path Connection)*.

VPN.- Red Privada Virtual, *(Virtual Private Network).*

WAN.- Red de Área Amplia o Extensa, *(Wide Area Network).*

WLAN.- *Wireless LAN.*

BIBLIOGARFÍA

Banke, A. y Badrinath, B. (1995). **I-TCP: Indirect TCP for Mobile Hosts.** New York: Prentice-Hall.

Barlow, J. P. (1995). **Property and Speech: Who Owns Whay You Say in Cyberspace.** USA: Commun of the ACM, vol. 38.

Bates, R. J. (1994). **Wireless Networked Communications.** New York: Mc Graw-Hill.

Beltrao, A. (1998). **Redes de Computadoras. Protocolos y Prestaciones.** México: Mc Graw-Hill. Primera Edición.

Bertsekas D. y Gallager R. (1997). **Data Networks.** New Jersey: Prentice-Hall, Englewood Cliffs.

Black, U. D. (1994). **Emerging Communication Technologies.** New Jersey: Prentice-Hall, Englewood Cliffs.

Black, U. D. (1995). **TCP/IP and Related Protocols.** New York: Mc Graw-Hill.

Black, Ulysees. (1999). **Redes de Computadoras: Protocolos, Normas e Interfases**. México: Mc Graw-Hill.

Carl-Mitchell, S. y Quarterman, J. S. (2001). **Practical Internetworking with TCP/IP and UNIX.** New Jersey: Addisson Wesley.

Clark, D. (1998). **Window and Acknowledgement Strategy in TCP.** New Jersey: Prentice Hall, Englewood Cliffs.

Comer D. E. (1995). **Internetworking with TCP/IP.** New Jersey: Prentice-Hall, Englewood Cliffs.

Comer, D. (1996). **Redes Globales de Información con Internet y TCP/IP: Principios Básicos, Protocolos y Arquitectura.** México: Pearson-Prentice Hall.

Conant, G. E. y Wecker, S. (1996). **DNA: An Architecture for Heterogeneous Computer Networks.** Toronto: ICCC.

De Prycker, M. (1993). **Asynchronous Transfer Mode Solution for Broadband ISDN.** UK: Ellis Horwood, Second Edition.

De Prycker, M. (1993). **Asynchronous Transfer Mode.** New York: Ellis Horwood. Second Edition.

Deening, P. J. (1989). **The Science of Computing: Worldnet.** USA: In American Scientist, 432-434.

Deering, S y Cheriton, R. (2000). **Multicast Routing in Datagram Internetworks and Extended LAN's.** New Jersey: Prentice- Hall.

Fischer, W et al. (1994). **Data Communications Using ATM: Architectures, Protocols and Resource Management.** IEEE Magazine, vol. 32.

Floyd, S. y Jacobson, V. (1993). Random Early Detection Gateways for Congestion Avoidance. **IEEE/ACM Transactions on Networking**, I(4).

Frank, H. y Chiou, W. (1991). **Routing in Computer Networks.** New Jersey: Prentice Hall.

Frank, H. y Frish, J. (1991). **Communicion, Transmission and Transportation Networks.** Massachusetts: Addison-Wesley.

Gerla, M. y Kleinrock, I. (1998). **Flow Control: A Comparative Survey.** *IEEE Transactions on Communications.* USA: IEEE.

Giozza, W.; De Araújo, J. y Moura, J. (1996). **Redes Locales de Computadores: Aplicaciones y Tecnologías.** México: Mc Graw-Hill.

González, Néstor. (1999). **Comunicaciones y Redes de Procesamiento de Datos**. México: Mc Graw-Hill.

Green, Paul. (1992). **Computer Network Architectures and Protocols.** New York: Plenum Press, Second Edition.

Huitema, C. (1995). **Routing in the Internet.** New Jersey: Prentice-Hall, Englewood Cliffs.

International Organization for Standarization. (1987a). Information Processing Systems –Open Systems Interconnection- **Specification of Basic Specification of Abstract Syntax Notation One (ASN.1).** International Standar number 8824, ISO, Switzerland.

International Organization for Standarization. (1987b). Information Processing Systems –Open Systems Interconnection – **Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).** International Standard number 8825, ISO, Switzerland.

International Organization for Standarization. (1988a). Information Processing Systems –Open Systems Interconnection- **Management Information Protocol Definition, Part 2: Common Management Information Protocol.** Draft International Standard number 9596-2.

Latif, A., Rowlance, E. J. y Adams, R. H. (1992). **The IBM LAN Bridge.** IEEE Network Magazine.

Laudon, K. C. (1995). "Ethical Concepts and Information Technology". ***Comun of the AMC***, vol. 38. pp. 33-39, Dec. 1995.

Madrón, A. (1997). **Redes de Computadoras.** México: Mc Graw-Hill.

Menascé, D. A. y Schwabe, D. (1994). **Redes de Computadoras.** Buenos Aires: Ed. Campus.

Milenkovic, Anton. (1998). **Sistemas Operativos**. México: Mc Graw-Hill.

Novel, Inc. (1995). **Introducción a Novel: Manual de Referencia.** México: Novel Incorporation.

Perlman, R. (1992). **Interconnections: Bridges and Routers.** New Jersey: Addisson Wesley.

Rose, M. (1993). **The Internet Message.** New Jersey: Prentice Hall, Engewood Cliffs.

Rosenthal, R. (Ed.). **The Selection of Local Area Computer Networks.** USA: National Bureau of Standards Special Publications.

Santifaller, M. (1994). **TCP/IP and ONC/NFS.** New Jersey: Addisson Wesley.

Schwartz, M. y Stern, T. (1999). **IEEE Transactions on Communications.** USA: COM-28 (4), 539-552.

Sipior, J. C. y Ward, B. T. (1995). « The Ethical and Legal Quandary of E-mails Privacy ». ***Comun of the AMC***, vol. 38, pp. 48-54, Dec. 1995.

SNA, (1995). **IBM System Network Architecture – General Information.** North Carolina: IBM System Development Division, Publications Center Department.

Stallings, W. (1995a). **ISDN and Broadband ISDN with Frame Relay and ATM.** New Jersey: Prentice Hall.

Stallings, W. (1995b). **Network and Internetwork Security.** New Jersey: Prentice Hall.

Stallings, W. (1995c). **Protect your Privacy: The PGP User's Guide.** New Jersey: Prentice Hall.

Stallings, W. (1999). **Data and Computer Communications.** New York: Macmillan Edition.

Tanembaum, Andrews. (1997). **Redes de Computadoras.** México: Pearson/Prentice-Hall. Tercera Edición.

Tanenbaum, A. (1981). **Computer Networks: Toward Distributed Processing Systems.** New Jersey: Prentice-Hall, Englewood Cliffs.

Tanenbaum, A. S. (1991). **Computer Networks.** New Jersey: Prentice Hall, Ebglewood Cliffs.

Villamizan, C. y Song, C. (1995). **High Performance TCP in ANSNET.** USA: Mc Graw-Hill.

Yeh, H., Hluchyj, M y Acampora, A. (1997). **The Knockout Switch: A Simple, Modular Architecture for High-Performance Packet Switching.** USA: IEEE Edition.

INDICE