26.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

REESTRUCTURACION DE LAS REDES DE DATOS Y COMUNICACIONES DE LA COMISION NACIONAL BANCARIA Y DE VALORES PARA HACER EFICIENTES LOS PROCESOS DE REGULACION DEL SISTEMA FINANCIERO MEXICANO

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N :

CRUZ AQUINO ANABELL

MENDOZA CONTRERAS JOSE ALFREDO

MORA ZAFRA ERASMO ALEJANDRO

PIEDRA PEÑA HECTOR ALFONSO

SANCHEZ MEZA RICARDO ANGEL

DIRECTOR DE TESIS:

FIS. RAYMUNDO HUGO RANGEL GUTIERREZ

MEXICO, D. F. MARZO, 2000

A mi madre,

Por su ayuda incondicional, por su amor infinito, gracias por creer en mi.

A mi hermana Andrea,

Quien es la persona mas importante en mi vida y que es mi orgullo y un gran ejemplo a seguir.

A Mariha Elena,

Mi alma gemela, quien recuerdo como la mejor de las amigas, gracias por todo lo vivido. Siempre te llevo en el corazón.

A la quintilla de ases,

Dios los hace y ello se unen. Por todas las cosas buenas y malas que vivimos.
Siempre los recordaré.

A mi padre,

Gracias por estar conmigo en la buenas y en las malas y por respetar y aceptar mis decisiones con amor.

A Alfredo,

Por permitirme ser parte de su vida, por toda su ayuda desinteresada y por ser mi amigo.

Al veracruzano,

Quien me enseñó la otra cara de la moneda. Y esa forma tan especial de luchar por un sueño.

A la vida,

Que día a día me recuerda que lo mas importante es el amor.

A todos aquellos que a lo largo del camino me dieron su amistad y ayuda sin ningún interés,
Mil gracias por estar justo en el momento en que los necesité.

ANABELL

A mis padres

Por enseñarme el camino de la responsabilidad, el trabajo y la rectitud. Gracias por todos sus esfuerzos para que pudiera alcanzar esta meta. Este logro constituye la herencia más valiosa que pueda recibir.
Con amor, respeto y admiración.

A la familia Mendoza Pérez

Siempre les viviré agradecido por las atenciones que tuvieron conmigo. Gracias por todo el apoyo y comprensión que me brindaron.

A mis compañeros de tesis

Por la aventura que iniciamos y terminamos juntos. Nunca los olvidaré.

A mis hermanos Norma y Carlos

Porque forman parte de una gran familia que me apoya y motiva siempre.
Los quiero mucho.

A Kenya

Gracias por permitirme compartir tu vida con la mía. Con tu apoyo y confianza he logrado alcanzar esta meta. Espero sea la primera de muchas.
Te amo.

A Anabell

Una amiga inolvidable que siempre me contagia las ganas de vivir.

Gracias a todos los seres que han compartido conmigo cada momento de mi vida. Gracias por su energía, enseñanza y orientación transmitida. Gracias por su tiempo y por su espacio.

ALFREDO

A mi padre José Luis,

Una pequeña muestra de agradecimiento para un hombre excepcional.

A mi novia Alejandra,

Con todo mi cariño: tu amor, ternura, paciencia y motivación alegran mi vida. Te amo.

A mis hermanos José Luis, Juan de Dios, Carlos Eduardo, Ligia Lenny, Jorge Alejandro,

Mi vida no sería la misma sin ustedes, los amo...

Al Director de nuestra Tesis,

Por su apoyo y comprensión, suerte.

A mi madre Ligia Leny,

Una luchadora incansable.

Los amo a los dos, gracias por estar siempre conmigo y por su apoyo incondicional.

A mis compañeros de Tesis Alejandro, Alfredo, Anabell, Ricardo,

No solo compartimos la tesis, también maravillosas experiencias.

A la UNAM,

Gracias por ayudarme a ser lo que soy. Espero pronto sanen las heridas, y resulte fortalecida.

A todos los soñadores,

Soñar es el primer paso, la perseverancia es el segundo...

HÉCTOR

A mis padres,

Por todo el apoyo, comprensión e impulso que me brindaron durante el desarrollo de mi carrera y que el día de hoy se ve consumado todo este gran esfuerzo.

A Argelia

Por todo el tiempo y las alegrías que hemos compartido.

A José Juan (q.e.p.d.),

El ser que a pesar de vivir una vida muy difícil, la enfrentó con entereza y siempre fue para mí un ser que me estimuló para afrontar los problemas de frente y nunca retroceder ante ellos.

A mis Hermanos,

Que con sus palabras de aliento me han permitido alcanzar una de las metas más importantes en mi vida.

A mis compañeros Anabell, Alfredo, Héctor y Ricardo,

Gracias por todo este tiempo, experiencias y amistad que compartimos, que me han brindado durante el desarrollo de este gran proyecto.

A la U.N.A.M.

Eternamente agradecido por toda la preparación y formación que me has dado.

Cada uno y todos en su conjunto me han dado un panorama diferente para crecer como ser humano y ser más productivo.

A L E J A N D R O

Gracias a mis padres,

Por su dedicación y apoyo en la vida.

Gracias a mis compañeros de tesis,

Alfredo por su liderazgo y experiencia.
Anabell para quién todo es posible, por su motivación y comprensión.
Alejandro por su constancia y empeño.
Héctor por su búsqueda de nuevas ideas.

Gracias a mis amigos y compañeros de DGSCA,

Por su maravillosa amistad y colaboración, y enseñarme que todos los objetivos son alcanzables con esfuerzo y dedicación.

RICARDO

INDICE

Capítulo 1

Introducción.

La naturaleza de las organizaciones tradicionales cambia y simplemente ya no funciona. Se requiere una transformación de los negocios apoyada en la información para ser competitivos en el nuevo ambiente que se ha generado. Las empresas modernas son dinámicas y capaces de responder rápidamente a las condiciones cambiantes de los mercados. Su estructura es más homogénea y orientada al trabajo en equipo eliminando toda jerarquía. Se basa en compromisos, en lugar de controles y sus procesos se alinean a productividad y calidad, llevándolas a ser totalmente abiertas e interactivas.

Mientras tanto, la tecnología de la información se encamina a una segunda etapa. Al igual que las empresas, es abierta e interactiva. Con sus partes intercambiables, se vuelve modular y dinámica. Incrementa el poder en los usuarios proporcionándoles conocimiento informático y poder de decisión. Trabaja integrando datos, texto, voz e imágenes en diversos formatos y puede proveer un canal de flujo entre los grupos de trabajo.

La magnitud del volumen de información creó la necesidad de agilizar el flujo de la misma. Los requerimientos de ancho de banda y velocidad han provocado el surgimiento de nuevas tecnologías que permiten la transmisión de grandes cantidades de información en forma rápida y eficiente, rompiendo con las barreras geográficas. Estas tecnologías están convergiendo para poder hacer realidad las nuevas formas de comunicación.

Enlaces satelitales, frame relay, ATM (Asynchronous Transfer Mode), modo de transferencia asíncrona; RDSI (Red Digital de Servicios Integrados), la tecnología celular; son solo algunos ejemplos de estas nuevas formas de comunicación que, en forma aislado o conjunta, han dado lugar a una nueva etapa en el área de las telecomunicaciones.

Esto ha permitido la generación de nuevos servicios de comunicación tales como la videoconferencia, internet, correo de voz, etc. que unidos formarán la llamada *supercarretera de la información*, revolucionando el concepto de comunicación e intercambio de información.

Por su parte, con el desarrollo de nuevos productos como *bridges* (puentes), *gateways* (puertas), *routers* (enrutadores), *multiplexores*, etc., la red de área local (LAN) rebasó el concepto de *local*, de tal manera que con estos instrumentos, combinados con un módem y una línea telefónica, fue factible la interconexión de redes remotas, lo cual dio origen a las llamadas redes de área amplia o Wide Area Network (WAN).

Este desarrollo representa una nueva dimensión de manejo y proceso de comunicación, la distancia y el tiempo se redujeron prácticamente a cero, el concepto de interoperabilidad cobro una fuerza inusitada.

En México las redes hicieron su aparición alrededor del primer lustro de la década de los ochenta, al igual que en todo el mundo y debido a sus ventajas, su popularidad fue creciendo de manera notable.

Uno de los primeros sectores que se vio inmerso en estas tecnologías fue el financiero. Los bancos empezaron a llevar sus movimientos en una computadora que estaba conectada en red a un equipo central, para posteriormente procesarlos y emitir estados financieros. Posteriormente surgieron los cajeros automáticos, comunicados entre sí vía módem, y que era una extensión del banco para ciertas operaciones. Por su parte, las casas de bolsa se mantienen en línea con sus corredores en el piso de remates de la Bolsa Mexicana de Valores, a través de una computadora y un módem.

Como se ve, el desarrollo y modernización de los mercados económicos, trajo consigo nuevas y más extensivas necesidades en materia de equipos y sistemas computacionales, en donde el uso cotidiano de sistemas automatizados de información se ha constituido en una constante.

A escala internacional es clara la tendencia hacia la globalización y la integración de los mercados internacionales, tendencia de la cual no se podrán apartar nuestros mercados financieros, haciéndose necesario que se adecuen.

En el caso particular de la Comisión Nacional Bancaria y de Valores (CNBV), institución desconcentrada de la Secretaría de Hacienda y Crédito Público (SHCP) reguladora y supervisora del mercado financiero nacional, es de vital importancia contar con un sistema de comunicaciones y una infraestructura de cómputo eficiente para realizar sus funciones.

La CNBV, surgió a raíz de la consolidación de dos antiguas Comisiones; la Comisión Nacional de Valores y la Comisión Nacional Bancaria, en un solo organismo.

Independientemente de los cambios administrativos y de funciones, también los hubo en el ámbito informático. Las plataformas de hardware y software de ambas Comisiones, hasta hoy existentes, son muy distintas. Cada red local (LAN) tiene características muy diferentes a la otra. En la siguiente tabla se resumen algunas de ellas:

COMISIÓN NACIONAL BANCARIA Y DE VALORES

CARACTERÍSTICAS	LAN C.N.V.	LAN C.N.B.
Ubicación Física	Edificio Torre Sur	Edificio Torre Norte
No. PCs en red	600	450
Sistema operativo de red	NetWare 3.11	Unix HP-UX 10.20
Protocolo	IPX/SPX	TCP/IP
Cómputo central	AS400	HP9000
Topología	Token Ring	Ethernet
Medios de transmisión	líneas conmutadas, privadas y RDI	Líneas privadas
Otras instituciones con comunicación activa	Bolsa Mexicana de Valores, NAFIN, SHCP y todas las casas de Bolsa	Banco de México
Motor de Base de Datos	SQL Windows	Sybase
Oficinas regionales	Ninguna	31
Redes remotas	4	3

Tabla 1.1. Características generales de las redes de datos de C.N.V y C.N.B.

Nota : Ninguna de las oficinas regionales y redes remotas está actualmente enlazada a las oficinas centrales.

Esta tesis trata de proponer soluciones a:

- ☑ La integración de ambas plataformas en una sola, manteniendo las topologías, protocolos y sistemas existentes, mediante una red de área local (LAN) y un eficiente medio de transmisión entre ellas, a través de una columna vertebral de fibra óptica (backbone) y utilizando tecnologías de redes de alta velocidad: FDDI, frame relay, fast ethernet, gigabit ethernet, etc. Además de la incorporación de las redes remotas y oficinas regionales con que se cuenta para la creación de una red de área amplia (WAN).

- ☑ Dado que actualmente, cada una de las redes locales se basa en grupo de macrocomputadoras (mainframes); AS/400 y HP 9000, se debe implementar el modelo cliente / servidor en las aplicaciones de misión crítica, para reducir el tráfico de la red y aprovechar en forma óptima los recursos informáticos con que cuenta la CNBV. Esto a través del análisis en los siguientes rubros:

  - ⇒ Separación de tareas.
  - ⇒ Comportamiento de periféricos.
  - ⇒ Comportamiento de herramientas.
  - ⇒ Acceso a la información.

- ☑ Implementación de una LAN robusta y eficiente para dar servicio a más de 1200 empleados que laboran en la CNBV y que requieren el manejo de grandes bases de datos, información en línea, soporte técnico, etc.

- ☑ La incorporación de la WAN de la CNBV a la red financiera mexicana, utilizando tecnología de punta y contando con respaldo suficiente para los puntos críticos.

☑ Equipar a la CNBV con una estructura de telecomunicaciones sólida y capaz de dar soporte a los nuevos servicios que aparecen día a día en el mercado: Internet, videoconferencia, correo electrónico, etc.

En conclusión, se trata de realizar la consolidación de las dos plataformas informáticas existentes en la CNBV, utilizando tecnología de punta y optimizando la infraestructura instalada.

El contenido de esta Tesis inicia en el capítulo 2 con el estado actual de los sistemas de información y comunicaciones en el ámbito financiero en México, los organismos e instituciones que lo conforman y su estructura actual.

En el tercer capítulo, nos adentramos en la problemática real y actual de la red de datos y comunicaciones de la Comisión Nacional Bancaria y de Valores, analizando su infraestructura informática, topologías, servicios, puntos críticos y aspectos que nos ayuden a tener una idea clara del problema a solucionar.

Basándonos en lo anterior, en el capítulo cuatro, proponemos y analizamos alternativas de solución para estructurar una red local de datos y comunicaciones para la CNBV, que le permita integrarse a la red financiera Mexicana en forma eficiente

Finalmente, en el capítulo cinco, definimos las etapas de implementación y los beneficios que se obtendrán al término de cada una de ellas.

Adicionalmente, incluimos apéndices en los que revisamos las normas y estándares para cada uno de los medios y sistemas de comunicación existentes y que se encuentran vigentes en México; sus velocidades, rendimiento, costos y la legislación que existe sobre ellos. Damos un panorama general del concepto de conectividad, modos y códigos de transmisión.

Investigamos conceptos generales de los componentes que intervienen en una WAN, el modelo de referencia OSI, estándares, características de los principales sistemas operativos de red, protocolos de comunicación, conectividad avanzada y administración de redes.

Capítulo 2

El Sistema Financiero Mexicano: Estado Actual de las Telecomunicaciones y los Sistemas de Información en el Ámbito Financiero.

2.1. El Sistema Financiero en México.

2.1.1. Sistema Financiero.

Se puede definir como el conjunto de intermediarios entre ahorradores e inversores cuya función principal es canalizar el ahorro hacia la inversión, ofreciendo a los ahorradores condiciones satisfactorias de seguridad, liquidez y rendimiento y a los inversores condiciones adecuadas de cantidad, plazo y precio. Y de esta forma resulte provechoso el proceso de producción y distribución de bienes y servicios.

En términos generales, el sector financiero de la economía incluye a los mercados bursátiles, monetario, crediticio y cambiario. Las transacciones en estos mercados influyen y a su vez se ven afectadas por lo que ocurre con la oferta y demanda de bienes y servicios en el país.

Las necesidades financieras y motivaciones de inversores y ahorradores son muy distintas, por lo que los intermediarios que forman el Sistema Financiero ofrecen diversos productos y servicios acordes a las exigencias de unos y otros.

Todo sistema financiero persigue tres objetivos fundamentales:

- ☑ Fomento del ahorro privado.
- ☑ Asignación eficaz de los recursos financieros con el fin de obtener la utilidad más eficiente posible del capital existente.
- ☑ Flexibilidad y adaptación de las instituciones, instrumentos y mercados a los cambios necesarios para llegar a los dos primeros objetivos.

El sistema financiero de un país es de vital importancia para su desarrollo económico, ya que representa la existencia de un cuadro institucional, dentro del cual hay una estructura capaz de ejercer control y coordinar las actividades económicas.

2.2. Organismos e Instituciones que integran el Sistema Financiero Mexicano.

En esta sección se presenta una visión esquemática del sistema financiero de México, las instituciones que lo integran y su operación.

En la Figura 2.1.. se presenta la organización actual del sistema financiero. Como puede apreciarse en el diagrama los organismos supremos son la Secretaría de Hacienda y Crédito Público y el Banco de México.

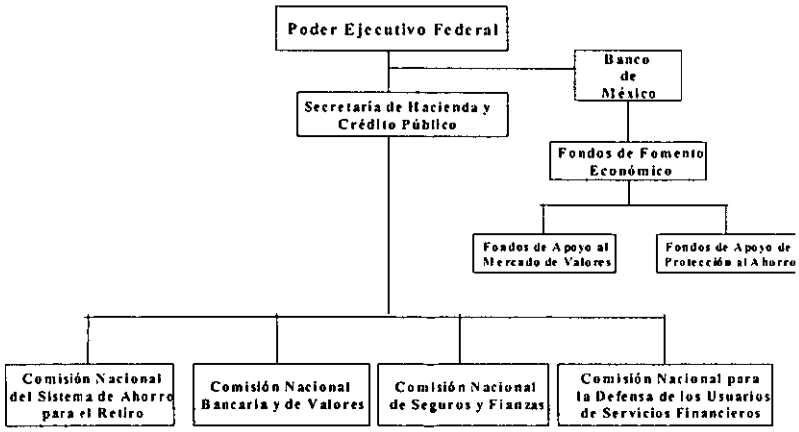


Figura 2.1. Autoridades Financieras Mexicanas.

2.2.1 Secretaría de Hacienda y Crédito Público (SHCP).

Le corresponde la función regulatoria de todo el sistema financiero, para lo cual se vale de dos organismos desconcentrados que son la Comisión Nacional Bancaria y de Valores y la Comisión Nacional de Seguros y Fianzas.

2.2.2 Comisión Nacional Bancaria y de Valores (CNBV).

Esta Comisión surgió el 28 de abril de 1995, a raíz de la consolidación de la Comisión Nacional de Valores y la Comisión Nacional Bancaria en un solo organismo.

El objetivo principal de la nueva entidad, así como sus derechos y obligaciones, están descritos en la Ley de la Comisión Nacional Bancaria y de Valores, y es la supervisión y regulación, en el ámbito de su competencia, de las entidades financieras, a fin de procurar su estabilidad y correcto funcionamiento, así como mantener y fomentar el sano y equilibrado desarrollo del sistema financiero en su conjunto, en protección de los intereses del público.

2.2.3. Comisión Nacional de Seguros y Fianzas (CNSF).

Se creó como un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público mediante un decreto publicado el 3 de enero de 1990, surgiendo de la extinta Comisión Nacional Bancaria y de Seguros.

Su objetivo fundamental, consiste en "garantizar al público usuario de los seguros y las fianzas, que los servicios y actividades que las instituciones y entidades realizan, se apeguen a lo establecido por las leyes".

2.2.4. Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR).

La coordinación, regulación, supervisión y vigilancia de los sistemas de ahorro para el retiro están a cargo de la Comisión Nacional del Sistema de Ahorro para el retiro, que surge en 1994 como órgano administrativo desconcentrado de la SHCP, dotado de autonomía técnica y facultades ejecutivas, con competencia funcional propia en los términos de la ley de los sistemas de ahorro para el retiro.

2.2.5. Comisión Nacional para la Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

Es una institución que tiene como actividad básica la protección y defensa de los derechos e intereses del público usuario de los servicios financieros, para este propósito le asesora y defiende ante cualquier abuso o anomalía.

La creación de la CONDUSEF va aunada al nacimiento de la ley de Protección y Defensa al servicio de los usuarios Financieros, publicada el 18 de enero de 1999 en el Diario Oficial de la Federación y que entró en vigor el 18 de abril de 1999.

2.2.4. Banco de México.

Le compete realizar las funciones de banca central, tales como regular las políticas, monetaria y cambiaria; así como otras funciones de importancia, como: prestatario de servicios de tesorería para el Gobierno Federal, fija tasa de intereses, realiza operaciones de mercado abierto, determina los requerimientos de encaje, interviene en los mercados cambiarios y realiza el manejo de la reserva internacional.

2.3. Caso de Estudio: La Comisión Nacional Bancaria y de Valores.

2.3.1. Antecedentes.

Los antecedentes de este Organismo los encontramos en la Comisión Nacional Bancaria y la Comisión Nacional de Valores creadas, respectivamente, por decretos del Ejecutivo Federal del 24 de Diciembre de 1924 y del 11 de febrero de 1946, como Órganos desconcentrados de la Secretaría de Hacienda y Crédito Público, para supervisar a las entidades del sector Bancario y del sector Bursátil.

2.3.2. Creación.

El 28 de abril de 1995 fue publicada en el Diario Oficial de la Federación la Ley de la Comisión Nacional Bancaria y de Valores con vigencia a partir del 10 de Abril de ese mismo año por virtud de la cual se crea la Comisión Nacional Bancaria y de Valores (CNBV), con autonomía técnica y facultades ejecutivas en los términos de esa Ley.

En la exposición de motivos de la iniciativa se establece que:

> "...La nueva Comisión Nacional Bancaria y de Valores tendría por objeto supervisar y regular, en el ámbito de su competencia, a las entidades financieras, a fin de procurar su estabilidad y correcto funcionamiento, así como mantener y fomentar el sano y equilibrado desarrollo del sistema financiero en su conjunto, en protección de los intereses del público.

Esta nueva Comisión aglutinaría las funciones y facultades que actualmente corresponden a la Comisión Nacional Bancaria y a la Comisión Nacional de Valores y comprendería en su esfera de atribuciones a todas las Instituciones del sistema financiero, excepción hecha de las correspondientes al sector asegurador y afianzador, que por sus particularidades y especialización es conveniente mantenerlas bajo la vigilancia de otro órgano supervisor..."

2.3.3. Facultades y Obligaciones.

La creación de la Comisión Nacional Bancaria y de Valores tuvo como propósito consolidar en un solo órgano las funciones y facultades que en materia de supervisión, de manera principal, anteriormente correspondían a la Comisión Nacional Bancaria y a la Comisión Nacional de Valores y su conformación no implica redistribución alguna de competencia con las demás autoridades financieras, pues se preservan inalterables las atribuciones que ya tenían a las citadas Comisiones como son, sólo a manera de ejemplo, las siguientes:

Supervisión: Supervisar a las entidades, personas físicas y demás personas morales cuando realicen actividades previstas en las leyes relativas al Sistemas Financiero, a fin de procurar su estabilidad y correcto funcionamiento, así como mantener y fomentar el sano y equilibrado desarrollo de dicho Sistema Financiero en su conjunto, en protección de los intereses del público.

Regulación: Emitir de conformidad con lo que establezcan las leyes relativas al Sistema Financiero, regulación prudencial orientada a preservar la liquidez, solvencia y estabilidad de las entidades financieras; además, estudia y propone a la Secretaría de

Hacienda y Crédito Público tesis y criterios de aplicación general en materia de política financiera.

Opinión y Consulta: La Secretaría de Hacienda y Crédito Público, antes de ejercer varias de sus facultades en materia financiera, solicita la opinión de la Comisión Nacional Bancaria y de Valores como del Banco de México.

Autorización: Autorizar la constitución y operación, así como determinar el capital mínimo de aquellas entidades que señalan las leyes; asimismo, autorizar, suspender o cancelar la inscripción de Valores y Especialistas Bursátiles en el Registro Nacional de Valores e Intermediarios, así como suspender la citada inscripción por lo que hace a las Casas de Bolsa. También, autorizar o aprobar los nombramientos de consejeros, directivos, comisarios y apoderados de las entidades, en los términos de las Leyes respectivas y determinar o recomendar que se proceda a la amonestación, suspensión, veto o remoción y, en su caso, inhabilitación de los consejeros, directivos, comisarios, delegados fiduciarios, apoderados, funcionarios y demás personas que puedan obligar a las entidades, de conformidad con lo establecido en las leyes que las rigen.

Imposición de Sanciones: Cuando las entidades o sujetos de aplicación de la Ley no respetan las normas a que la misma los obliga, la Comisión Nacional Bancaria y de Valores interviene para hacer respetar la norma violada, mediante la aplicación de sanciones pecuniarias o administrativas, como son la imposición de multas, o la remoción, suspensión o inhabilitación de sus funcionarios.

Protección de los Intereses del Público: La Comisión Nacional Bancaria y de Valores actúa como conciliador y, en su caso, como árbitro en estricto derecho y amigable composición, en las reclamaciones que presenten los usuarios de los servicios financieros; con excepción de las compañías de seguros.

Ejecución: Las facultades de ejecución comprenden aquellas atribuciones que le concede la Ley o le delega la Secretaría de Hacienda y Crédito Público para autorizar, aprobar o revocar la realización de determinadas operaciones. Como ejemplo de este concepto se encuentra la atribución de otorgar autorización para operar a las Uniones de Crédito y, en su caso, revocárselas.

Suspensión de Operaciones: La Ley por la cual se creó la CNBV, complementa las atribuciones que ya tenían la Comisión Nacional Bancaria y la Comisión Nacional de Valores, con la de suspender todas o algunas de las operaciones de las entidades financieras por violaciones graves o reiteradas a la legislación que les resulte aplicable, así como a las disposiciones que emanen de ella.

Intervención: Intervenir administrativa o gerencial a las entidades con objeto de suspender, normalizar o resolver las operaciones que pongan en peligro su solvencia, estabilidad o liquidez, o aquellas violatorias de las leyes que las regulan o de las disposiciones de carácter general que de ellas deriven, en los términos que establecen las propias leyes.

2.3.4. Ámbito de Supervisión.

La supervisión que le corresponde ejercer a la CNBV, abarca a las siguientes entidades:

Con base en la Ley de Instituciones de Crédito:

- ☑ Instituciones de banca múltiple.
- ☑ Instituciones de banca de desarrollo.
- ☑ Sociedades financieras de objeto limitado.
- ☑ Oficinas de representación de entidades financieras del exterior.

- ☑ Sucursales de bancos extranjeros.
- ☑ Filiales de instituciones financieras del exterior.
- ☑ Patronato del Ahorro Nacional.
- ☑ Fondos y fideicomisos de fomento constituidos por el Gobierno Federal.
- ☑ Instituto del Fondo Nacional de la Vivienda para los Trabajadores (Infonavit), Fondo de la Vivienda para los Militares en Activo (Fovimi), etc.

Con Base en la Ley del Mercado de Valores y en la Ley de Sociedades de Inversión:

- ☑ Casas de bolsa.
- ☑ Especialistas bursátiles.
- ☑ Bolsas de Valores.
- ☑ Filiales de instituciones financieras del exterior.
- ☑ Emisores de valores inscritos en el Registro Nacional de Valores e Intermediarios, sólo respecto de las obligaciones que impone la Ley del Mercado de Valores.
- ☑ Sociedades de Inversión.
- ☑ Sociedades operadoras de sociedades de inversión.
- ☑ Instituciones para el Depósito de Valores.
- ☑ Empresas calificadoras de riesgo.

Con Base en la Ley para Regular las Agrupaciones Financieras:

- ☑ Sociedades controladoras de grupos financieros, excepto cuando la supervisión de la entidad preponderante del grupo corresponda a la Comisión Nacional de Seguros y Fianzas.

- ☑ Sociedades controladoras de grupos financieros, filiales de Instituciones financieras del exterior.
- ☑ Sociedades de información crediticia.

Con Base en la Ley General de Organizaciones y Actividades Auxiliares del Crédito:

- ☑ Almacenes generales de depósito.
- ☑ Empresas de factoraje financiero.
- ☑ Arrendadoras financieras.
- ☑ Uniones de Crédito.
- ☑ Sociedades de ahorro y préstamo.
- ☑ Casas de cambio (las que se dedican a operaciones de mayoreo).
- ☑ Filiales de entidades financieras del exterior.

Otras Entidades:

- ☑ Sociedades inmobiliarias, tanto bancarias como bursátiles y, además, empresas de servicios complementarios o conexos.
- ☑ Sociedades inmobiliarias y empresas de servicios complementarios o conexos a filiales de entidades financieras del exterior.

2.4. Estructura Actual de las Telecomunicaciones en el Sector Financiero Mexicano.

2.4.1. La red financiera.

Actualmente, las diversas entidades que conforman el Sistema Financiero Mexicano funcionan en forma independiente, utilizando diversos protocolos, topologías, sistemas y medios de enlace y transmisión.

Cada una mantiene una red de área local (LAN) para dar soporte a cada una de las áreas que la conforman, existiendo comunicación con otras dependencias a través de enlaces punto a punto, utilizando líneas privadas a velocidades de 56000 bps. y, en casos muy especiales, utilizando la Red Digital Integrada de Telmex.

La conectividad entre estas entidades se lleva a cabo con enlaces punto a punto, generando un esquema similar al que se muestra en la Figura 2.2.

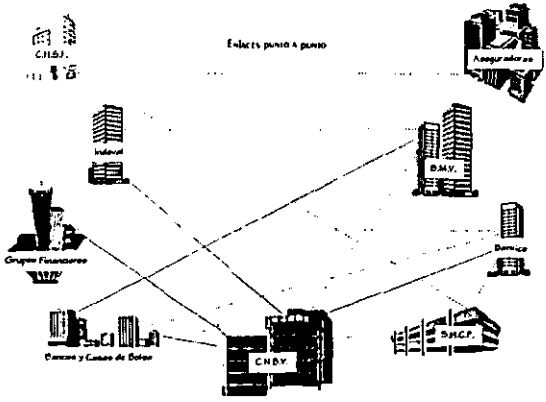


Figura 2.2. Conectividad del Sector Financiero en México.

Como se puede observar, el intercambio de información se realiza en forma desordenada y poco eficiente, utilizando diversos medios de enlace y solo con algunos de los participantes del medio financiero.

Actualmente, se está estudiando la incorporación de todas las instituciones que conforman este sistema, a una red de alta velocidad Frame Relay (Fig. 2.3.); con lo cual se mejorarían tiempos de respuesta, intercambio de información, introducción de nuevos servicios tales como: correo de voz, videoconferencia, etc. para así tener un sistema de telecomunicaciones más eficiente y adecuado a las necesidades actuales de información en el sector financiero y mantener un mejor control y vigilancia del mercado.

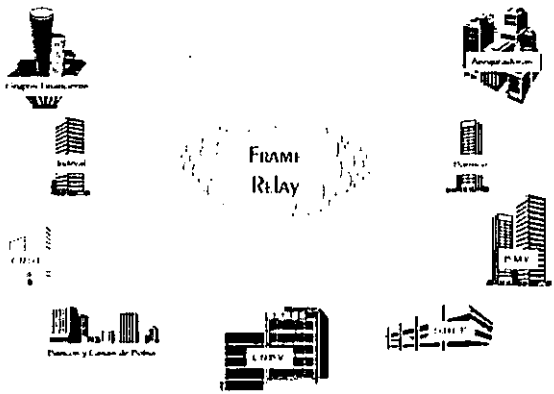


Figura 2.3. Estructura Futura de Telecomunicaciones para el Sector Financiero en México.

Bajo este esquema, se hace necesario implementar la infraestructura suficiente en cada institución para dar soporte estas a nuevas tecnologías.

Capítulo 3

Análisis de la problemática actual de las redes de datos y comunicaciones de la CNBV.

3.1. Problemática.

La Comisión, al ser un órgano regidor, impulsa la confianza y tranquilidad al inversionista dentro de los mercados financieros, por lo que es una vía para estimular la economía nacional a través de la inversión en el mercado financiero. Está encargada de supervisar de que no se cometan irregularidades en la compraventa de acciones, en algunos fondos, en algunas sociedades de inversión, en bancos, etc. Es decir, vigila y promueve el desarrollo del mercado financiero; sugiere acerca de como hacer mejor las cosas, tomando medidas correctivas dentro de los regímenes que le otorga la ley.

Por la incesante dinámica de estos y la importancia de su correcta operación para la sanidad económica nacional, esta institución debe recibir, integrar, procesar y enviar información en segundos. Como herramienta central para el logro de estos objetivos, se ha optado por implementar un sistema de red de datos tanto local como con puntos de enlace remotos a través de los distintos medios de enlace. Adicionalmente, es necesario incorporarla a la red global del sistema financiero, para así compartir información con los demás participantes de dicha red.

El fenómeno nacional de desarrollo económico necesariamente ha venido aparejado de un crecimiento financiero, y como consecuencia de esto, se tiene una mayor demanda de servicios informáticos en los que se requiere de mayor rapidez en el intercambio de información y confiabilidad en las operaciones. La necesidad de contar con mayor información y en forma cada vez más oportuna por parte de las distintas áreas de la CNBV, la ha llevado a crecer en recursos y sistemas de automatización. En el presente capítulo analizaremos las razones para ello, así como las características de éstas. Además de dar el antecedente y la misma evolución tecnológica en esta materia.

La red local de la Comisión Nacional Bancaria y de Valores, nace de la fusión de dos plataformas distintas. Con esto, surge la necesidad de interconectar las redes, para poder compartir recursos e información entre ellas.

En un principio, se mantuvieron ambas plataformas, conviviendo en un ambiente abierto de multiprotocolos. Este arreglo funcionó, pero tenía el inconveniente de consumir muchos recursos de memoria RAM y espacio en disco duro en la estación en donde se instalaba. Además el tráfico en el medio que enlaza a ambas torres, se vio incrementado notablemente, al trasmitir paquetes de IPX/SPX (red Novell), TCP/IP (red Unix) y manejar velocidades variables de 4, 16 y 10 Mbps al utilizar topologías Token-Ring y Ethernet.

Actualmente, este esquema ya no es suficiente, es necesario eficientar las velocidades de respuesta y transferencia de la red de datos de la CNBV. Se debe realizar la consolidación de plataformas tecnológicas. Esto con el fin de poder dar un mejor servicio a los usuarios finales.

3.1.1. Objetivos.

- ☑ Disponer de una base tecnológica sólida que nos sirva para determinar soluciones y servicios acordes a las funciones de los usuarios y a las tendencias de la informática institucional de la CNBV.

- ☑ Garantizar, mediante las pruebas correspondientes, la compatibilidad e interoperabilidad de todos y cada uno de los elementos que se integren al esquema tanto de la red de datos como la de comunicaciones, para garantizar su adecuado funcionamiento así como tener una buena aproximación a las posibles fallas o requerimientos de mantenimiento tanto preventivo como correctivo de todos estos elementos.

3.1.2. Estrategia.

Dada la dinámica característica de las necesidades tanto de información como de servicios de la CNBV y el incesante cambio tecnológico, es importante considerar en la evolución de los servicios de cómputo y las comunicaciones, el crecimiento y la afinación de la plataforma instalada, tanto en sus componentes de hardware y software como en los niveles de habilidades del personal, con el fin de que dicha evolución se dé, en la medida de lo posible, con transparencia respecto al usuario.

Deberemos establecer el marco de referencia identificando la situación actual y final, así como el establecimiento de la ruta crítica de actividades-tiempos-recursos necesarios.

Se identificarán las tareas prioritarias, así como sus relaciones de dependencia, secuencia y sus controles correspondientes.

Necesitaremos contar con el mejor conocimiento de las estrategias y del modelo tecnológico, así como de los procesos involucrados, para responder adecuadamente a los requerimientos de las distintas áreas de la CNBV y brindar un servicio de la completa satisfacción de los usuarios.

Consideraremos, dentro de la arquitectura global de la red de la CNBV, el modelo de las aplicaciones e información tanto en su forma actual como en previsión a las futuras, así como brindar soporte técnico de la misma estructura, puntualizando nuestro enfoque de área de servicio y ocupándonos de contar con las herramientas y el apoyo necesario para dicha tarea.

3.2. Análisis de la Red Local (LAN).

Es necesario determinar los elementos que intervienen en ambas topologías, el software y sistemas operativos utilizados en cada una, así como los sistemas, procesos y aplicaciones que corren en ella.

Adicionalmente, las actividades de seguimiento y análisis de la información financiera, constituyen la base de la supervisión de los mercados financieros. Es fundamental que la CNBV busque fortalecer la coordinación y el intercambio de información entre las actividades de inspección y las de seguimiento y análisis, a efecto de que la evaluación que se lleve a cabo de las entidades supervisadas sea más completa, óptima, profunda y objetiva y permita un mejor conocimiento de la situación financiera de cada institución.

La información financiera proveniente de las instituciones supervisadas llega a la CNBV, en la mayoría de los casos, a través de la ventanilla única de recepción de información financiera. Cada una de las instituciones de los diferentes sectores supervisados envía la información requerida de sus operaciones a la CNBV en distintos formatos preestablecidos y en el medio determinado para dicho formato: electrónico, diskette, vía módem, fax, etc. En el caso de otras autoridades y organismos financieros como Banco de México o la SHCP, se tiene acuerdos mediante los cuales cada entidad recopila la información que a ellos concierne y posteriormente se intercambia y cruza para complementarla y validarla; esto con el propósito de evitar que distintos organismos soliciten a la institución, la misma información.

La información recibida por diferentes medios, se carga en bases de datos temporales para que se apliquen diversos procesos de validación, en los que se verifica su confiabilidad y congruencia, para integrarlas a las bases de datos definitivas.

El proceso de validación se realiza mediante la comparación entre los diversos reportes que envían las instituciones y los generados por el Banco de México y la Bolsa Mexicana de Valores.

Actualmente se dedican demasiados esfuerzos a la recepción, validación e integración de la información a las bases de datos, ya que se manejan distintos esquemas de recepción. Por otra parte, existen diferentes procesos, manuales y automáticos, para validar e integrar.

Con el esquema actual, se reciben diariamente múltiples documentos de las instituciones que componen el sector financiero. Estos documentos pueden presentar problemas como: virus, insuficiencia en la información, formato incorrecto, información inválida o duplicada entre otros. Cuando los documentos son incorrectos, la CNBV notifica a las instituciones o a las áreas responsables para que vuelva a enviar la información, lo que provoca retrasos en los procesos.

Este esquema de acopio y validación de información provoca que se tengan problemas como:

- Rezago en la entrega de información.
- Falta de consistencia en los formatos de la información.
- Equipo dedicado al envío y recepción de información.
- Diversidad en los medios de recepción.

3.2.1. Plataforma Informática Instalada.

Topologías, protocolos, sistemas operativos y distribución geográfica.

En las Figuras 3.1 y 3.2 se muestran la topología de la red de datos. A continuación se enumeran las características de cada una de ellas:

Torre Sur.

- ☑ Topología : Token-Ring.
- ☑ Windows 95.
- ☑ Sistema operativo de red: Novell NetWare V3.11.
- ☑ Protocolos utilizados: IPX/SPX, SNA, y TCP/IP.
- ☑ Backbone de fibra óptica multimodo instalada en todo el edificio con una velocidad de 16 Mbps.
- ☑ La red se encuentra segmentada en cinco anillos distribuidos en el edificio, con lo cual se da servicio a 610 computadoras personales pentium a 100 MHz conectadas a la red y 200 equipos 486.
- ☑ En cada anillo existe un servidor conectado, respetando la filosofía del sistema operativo Netware de contar con al menos un servidor en cada segmento.
- ☑ Cada anillo llega a un concentrador a través de cableado niveles 3 y 5.
- ☑ Los concentradores se interconectan al backbone a través de un bridge que se encarga de pasar de 16 Mbps a 4 Mbps a través de 2 tarjetas Token Ring.
- ☑ El anillo con mayor tráfico es el 3, ya que en él convergen todos los servidores y servicios de red.
- ☑ Se cuenta con una macrocomputadora AS/400.

Torre Norte.

- ☑ Topología : Ethernet.
- ☑ Windows 95.
- ☑ Sistema operativo de red: Unix HPUX-9000.
- ☑ Protocolo utilizado: TCP/IP.
- ☑ Vertical de fibra óptica multimodo instalada en todo el edificio con una velocidad de 10 Mbps colapsada en un switch.
- ☑ La red se encuentra segmentada en seis partes distribuidos en el edificio, con lo cual se da servicio a 460 computadoras personales pentium a 100 MHz conectadas a la red y 90 equipos 486.
- ☑ Cada segmento se colapsa en un Switch ubicado en el piso 5.
- ☑ El segmento con mayor tráfico es el 5, ya que a él llegan todos los servidores del sistema HP-9000, el switch y todos lo sistemas de monitoreo y estaciones de trabajo.

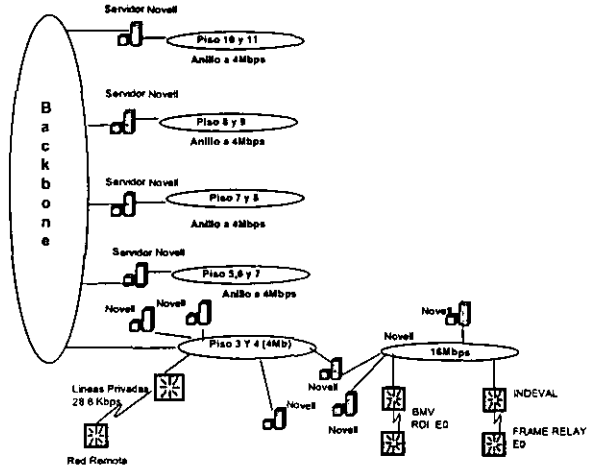


Figura 3.1. Topología de la red de datos Torre Sur.

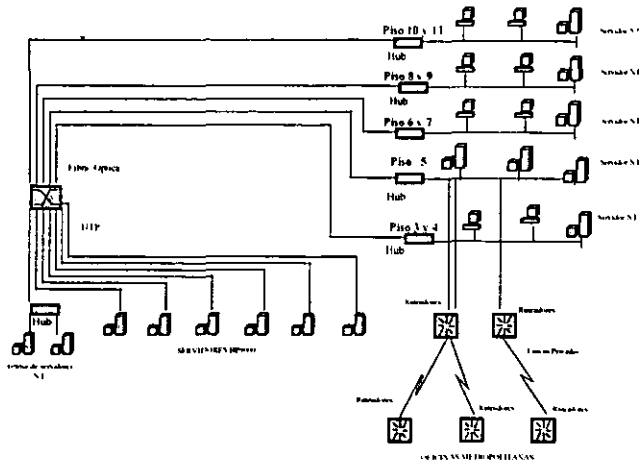


Figura 3.2. Topología de la red de datos Torre Norte.

3.2.2. Sistemas en Operación.

En la Tabla 3.1 se resumen los sistemas, software y aplicaciones utilizadas en cada ambiente.

SISTEMAS, SOFTWARE Y APLICACIONES	TORRE SUR	TORRE NORTE
Automatización de oficinas	Microsoft Office '95 Windows 95 Sin correo electrónico	Microsoft Office '95 Windows 95 Microsoft Exchange
Motor de Bases de Datos	Sqlbase	Sybase
Software de desarrollo	Visual Basic V4	Visual Basic V4
Sistemas de seguridad	El propio de redes Novell	El propio de redes UNIX
Sistemas de respaldo	DDS	DLT

Tabla 3.1. Sistemas, software y aplicaciones en Torre Sur y Torre Norte.

3.2.3. Equipamiento Personal.

Existen necesidades de servicios de red hacia las áreas usuarias para el apoyo y cumplimiento de las funciones de normatividad, supervisión y vigilancia del sector financiero.

Actualmente la CNBV cuenta con 290 equipos personales 486 obsoletos para el tipo de aplicaciones y servicios estándar en la Comisión, los cuales incluso resulta infructuoso mantener en buen estado funcional. Si a esto sumamos que los requerimientos de las distintas áreas en cuanto a equipamiento de cómputo como herramientas para el acceso y explotación de los sistemas de información de la CNBV, y para incrementar la productividad del personal mediante el uso de los distintos servicios que pueden ofrecerse con y a través de estas, asciende a más de 160 equipos, resulta imperativo dotar de más infraestructura de cómputo personal a la Comisión. De ahí que sea necesario la adquisición de un total de 400 computadoras personales que actualicen este lote de equipo y satisfagan la demanda interna, redistribuyéndolos de acuerdo a necesidades específicas del personal de la CNBV.

Otro rubro importante y que se ha incrementado en función de los servicios de red es el de impresión, para el cual se requiere adquirir 50 impresoras de tipo láser, a efecto de satisfacer la demanda, incrementar la productividad del personal y equipos, sustitución de equipo obsoleto imposibilitado de una conexión a red y brindar una óptima calidad de impresión, logrando con esto incrementar el número de usuarios que concurren en dicho servicio.

Por otra parte, el equipo destinado a la labor de supervisión in-situ esta limitado a unos cuantos, lo que repercute directamente en dicha función, sin mencionar que además es pilar del "Programa Institucional 1999-2000". Comparativamente, el número de computadoras portátiles es inferior en un 60% aproximadamente respecto al número de supervisores o personal que requiere de esta clase de equipos, por lo que se hace necesario acercar a dicho personal a este tipo de tecnologías, fortificando la labor de supervisión mediante la designación de recursos informáticos que permitan el acceso a información y sistemas de la CNBV de manera remota, con la facilidad de la portabilidad que estos ofrecen, por lo que es necesario ampliar el número de computadoras portátiles en 80 para dotar de equipo a más supervisores y personal que se encarga de la labor de supervisión in-situ.

3.2.4. Equipamiento central.

El nivel de almacenamiento y procesamiento del equipo actual de la marca HP para la recepción electrónica de información financiera se encuentra próximo a la saturación, si a esto sumamos el aumento de información que los supervisados enviarán a la CNBV así como también el incremento de instituciones que se enlazarán por este medio, se hace necesario tomar las medidas pertinentes para ampliar dichas capacidades.

Por otra parte y dando continuidad a la actualización del equipo en los centros de cómputo por falta de capacidad, limitación en su crecimiento y posibilidades de integración al ambiente CNBV en un 100%, se requiere actualizar la estación de trabajo dedicada a funciones de administración y monitoreo.

Como consecuencia de los nuevos sistemas administrativos, el servicio de impresión requiere integrarse a los servicios de red, sustituyendo la impresión directa desde Unix que es como se venía ofreciendo, lo que permitiría en su momento incluso descentralizar esta labor hacia las áreas usuarias.

3.2.5. Servidores departamentales.

Actualmente los servicios de red que se proporcionan en las oficinas centrales (Plaza Inn) corren en una plataforma de sistema operativo heterogénea (Novell Netware y Windows NT), lo cual implica administrar configuraciones diferentes en computadoras personales de los usuarios para el acceso a los distintos servidores para realizar su trabajo; en oficinas metropolitanas se tienen solo algunos servicios, mientras que en las oficinas estatales no se cuenta con infraestructura de red (actualmente el intercambio de información se realiza mediante fax), esta situación trae consigo la siguiente problemática:

- No existe homologación de servicios de red en ambas torres, ya que unos utilizan procesador de texto (Word), hojas electrónicas de cálculo (Excel) y herramientas de presentación (Powerpoint) de la red. En cambio otros tienen instaladas estas herramientas en su propia computadora personal, además de manejar versiones diferentes de tales productos.
- No se cuenta con una plataforma homogénea de cómputo, como computadoras con muy poca capacidad de procesamiento, almacenamiento y memoria (ejemplo: microcomputadoras 486).
- No existe una estrategia definida para ubicar servicios, de que manera y a quienes se les debe proporcionar correo, fax, acceso a aplicaciones que manejan bases de datos tanto institucionales como departamentales, etc.

- No se puede ofrecer servicios adicionales a la mayoría de los usuarios con la infraestructura actual, tales como: fax, actualización automatizada de versiones de paquetería, bases de datos departamentales, entre otros, ya que la capacidad de los equipos tanto en procesamiento como en almacenamiento no les daría soporte.
- Se cuenta con una infraestructura informática obsoleta con relación a las necesidades de la institución, se tienen operando servidores con escasas capacidades de cómputo (servidores Pentium a 100 MHz) cuando algunos usuarios ya cuentan con computadoras personales con capacidades mayores a nuestros propios servidores, con lo cual la respuesta del servidor se toma más tiempo en procesar que la petición de la computadora personal del usuario.
- No se cuenta con infraestructura de red en todas las oficinas de la institución, y por lo tanto, de servicios de red, tanto en automatización de oficinas como en acceso las aplicaciones de la institución.
- La plataforma de servidores se encuentra dispersa en diferentes ubicaciones, algunos servidores se encuentran repartidos entre los pisos con la consecuente problemática de monitoreo constante de los mismos.
- Carencia de espacio físico para ubicar nuevos servidores; actualmente los centros de cómputo están saturados y requieren ampliarse para dar cabida a los nuevos equipos, que satisfagan eficientemente los requerimientos de los usuarios, en los servicios de red.

3.2.6. Administración y monitoreo.

Actualmente la CNBV cuenta con una plataforma de administración y monitoreo escasa, ya que todos los productos que se utilizan son obsoletos o no se han terminado de implementar (NetMetrix, OpenView, Optivity, Lattisnet, LanAnalizer, Monitor de Sybase, Sheils diseñados, entre otros). Bajo este esquema, se detectan fallas en forma aislada

dentro de la Institución, es decir, no existe una integración de los recursos para llevar a cabo esta tarea y así poder prevenir los contratiempos que se puedan presentar. A continuación se muestran algunos de los puntos que creemos más relevantes:

- ✓ Falta una homologación en los servicios.
- ✓ Se cuenta con distintas plataformas de operación.
- ✓ No existe una estrategia definida para administrar y monitorear los recursos de la Institución.
- ✓ No se pueden ofrecer servicios adicionales (atención a usuarios, distribución de software, configuraciones remotas) por falta de recursos.
- ✓ La infraestructura se encuentra atrasada con relación al avance tecnológico (switches, ATM, frame relay, fast ethernet).
- ✓ Integración de las herramientas en una sola plataforma.
- ✓ Crecimiento desmesurado y falta de planeación.

3.2.7. Internet.

Los procesos de trabajo de la Comisión Nacional Bancaria y de Valores, tienen la necesidad de gestión de información para atender los requerimientos propios del trabajo de las diferentes áreas. Para sistematizar en forma integral la administración de información, la Comisión con una visión de informática de usuario final, ha previsto un proyecto que incluye como parte inicial, un estudio del medio de comunicaciones e información vía Internet, con objeto de cubrir la demanda de información y comunicación del organismo.

Internet es el conjunto de redes de computadoras (interconectadas) más grande del mundo. El valor de esta red radica en los servicios de información a los que se podrá acceder el personal autorizado de la Comisión, a cualquier parte del mundo; servicios tales

como: consultas a bancos de datos, correo electrónico, noticias, intercambio de información entre oficinas regionales y dependencias e implícitamente otras instituciones, incluso sesiones o conexiones remotas a aplicaciones o programas de la Comisión.

Dada la necesidad de búsqueda de información a través de Internet, del intercambio de correo electrónico, de consultas a bancos de información en el extranjero, entre otras, algunas áreas de la CNBV han requerido contratar servicios de enlace a Internet a través de una compañía privada llamada "compuserve"; los cuales se obtienen mediante el uso de líneas telefónicas conmutadas (enlaces "dial-up"). Si bien ésta ha sido una buena solución para algunos usuarios, la mayoría requiere de un mejor tiempo de respuesta, facilidad de manejo y disponibilidad del enlace en cualquier momento. Además se requiere de nuevos servicios como tener intercambio de información con las delegaciones regionales evitando el costo de llamadas de larga distancia.

3.3. Análisis de la Red de Área Amplia (WAN).

La WAN de la Comisión se compone de las siguientes oficinas:

Oficinas Centrales:

- ☑ Torre Sur.
- ☑ Torre Norte.

Oficinas metropolitanas:

- ☑ Insurgentes Sur.
- ☑ Pensilvania.
- ☑ Ogazón.

Oficinas estatales:

- ☑ Una en cada capital de estado de la República Mexicana.

Cada una con la necesidad de interconexión con las oficinas centrales (Fig. 3.3.).

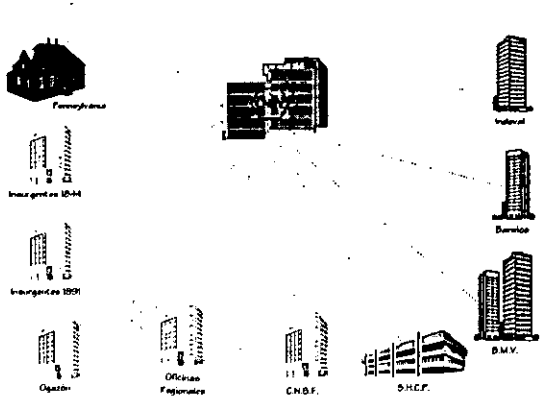


Figura 3.3. Esquema General de Interconexión requerido para la CNBV.

3.3.1. Infraestructura Actual.

En las Figuras 3.4, 3.5, 3.6 y 3.7., se muestra el diagrama actual de la red de servicios de cómputo y comunicaciones de la CNBV y cada una de las oficinas externas con las que cuenta.

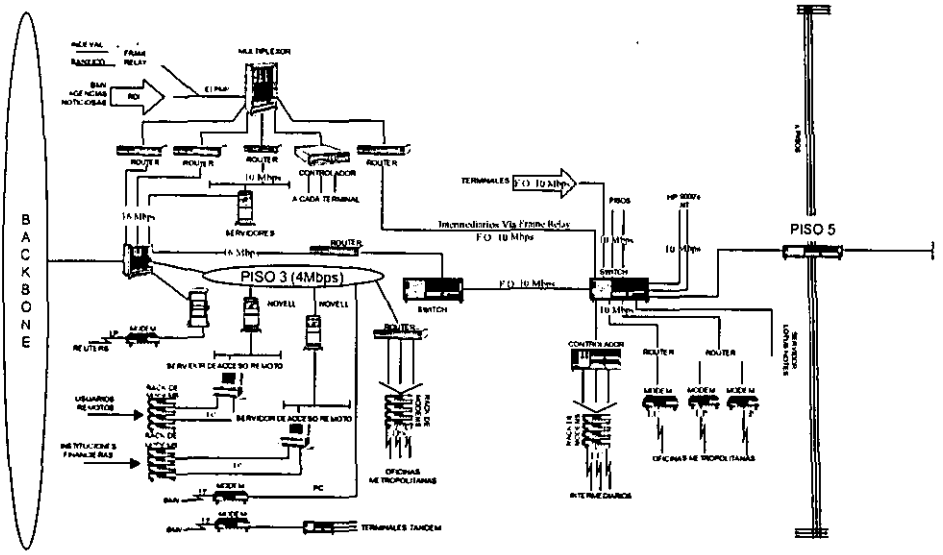


Figura 3.4. Diagrama general de comunicaciones.

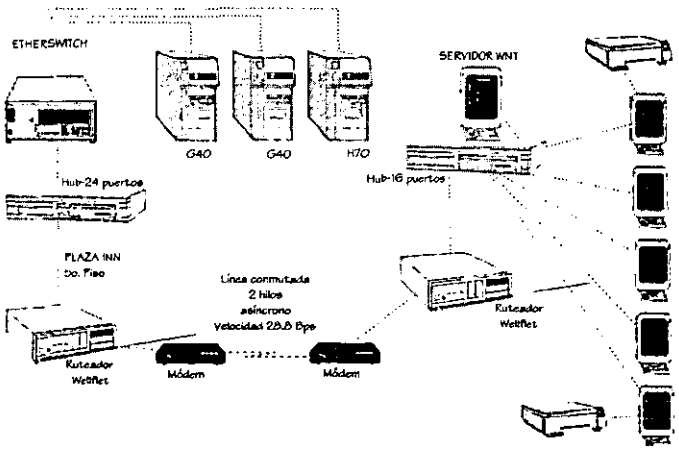


Figura 3.5. Esquema actual de enlace edificio Pennsylvania.

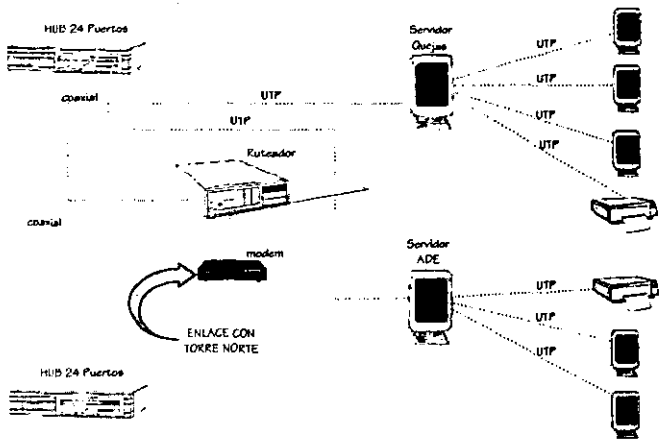


Figura 3.6. Esquema actual de enlace edificio Insurgentes 1844.

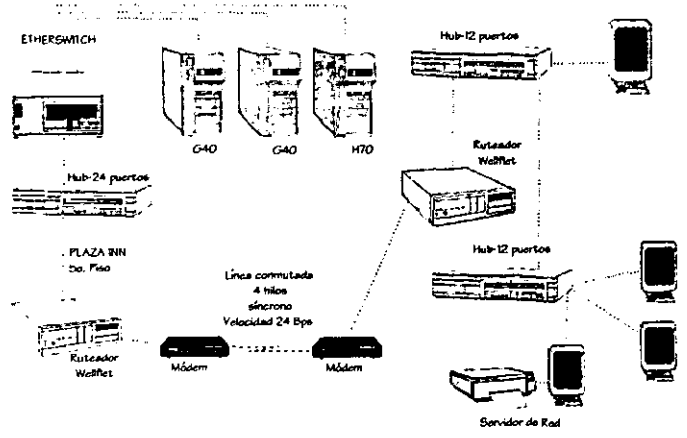


Figura 3.7. Esquema actual de enlace edifico Ogazón.

3.3.2. Problemática.

La infraestructura instalada presenta algunas limitaciones en cuanto a seguridad en el acceso de información.

Las actuales necesidades de comunicación y acopio de información que la CNBV mantiene con las entidades financieras en su carácter de institución supervisora ha puesto al límite los dispositivos de enlace y comunicación de la red externa, también a esto podemos sumar requerimientos de usuario como son: aumentar las capacidades de los enlaces con las oficinas metropolitanas, contar la infraestructura que nos permita soportar los futuros enlaces con las oficinas estatales, que los supervisores y personal de la institución pueda comunicarse desde cualquier línea telefónica a la red, así como la ampliación del servicio de internet, todos estas demandas de requerimientos y servicios hacen imperante el actualizar y ampliar la actual infraestructura de red externa.

La creciente demanda de envío - recepción de información a través de medios electrónicos para la comunicación de datos, ha hecho que las capacidades de los equipos destinados a ello empiecen a verse rebasadas y con la imposibilidad de ampliarlas dadas las características propias de estos equipos. Aunado a esto, el servicio de interconexión entre instituciones y CNBV se ha incrementado, lo que ocasiona sobrecarga a determinadas horas y/o días y, por ende, molestia entre los usuarios del servicio, ya que su transmisión se vuelve lenta o bien tienen que esperar a que algún medio este disponible para poder realizarla.

Así mismo existen servicios de interconexión entre la CNBV y las oficinas metropolitanas como con algunas autoridades financieras como Banco de México y la S.H.C.P. y varios servicios de información importantes para el seguimiento de los mercados. Esto complica la prestación de este servicio a las diversas instituciones del

sistema financiero ya que la obsolescencia y falta de capacidad para crecer en su configuración y equipamiento impide contar con un conexión transparente y natural con la nueva infraestructura de la red de cómputo de la CNBV.

Adicionalmente, se pretende contar con la infraestructura para tener enlaces directos con cada una de las oficinas estatales que componen a la Comisión. Obviamente, los equipos actuales no tienen capacidad para ello.

Como puede observarse, los esquemas en las oficinas metropolitanas son muy similares y, salvo algunas modificaciones y actualización de equipo, las redes locales de cada punto funcionan en forma satisfactoria ya que los flujos de información son pequeños.

Por otra parte, analizando el esquema general de comunicaciones, se observó lo siguiente:

- ☑ El medio de enlace son líneas conmutadas utilizando módems de 56 Kbps.
- ☑ Los protocolos de ruteo y de red son: el Point to Point Protocol (PPP) y TCP/IP con lo cual se asegura una total compatibilidad con los protocolos utilizados en oficinas centrales.
- ☑ La cantidad de información transferida y el tiempo de conexión es bastante entre cada oficina externa y la central, ya que existe una transferencia de datos continua.
- ☑ Solo existe transferencia de datos.
- ☑ Al tratarse de enlace vía telefónica, es necesario que en las oficinas centrales con equipo y líneas telefónica suficientes para recibir cada enlace.

3.3.3. Expectativas de Crecimiento.

Se planean introducir servicios de consulta en línea de algunos tópicos financieros: índices, monitoreo, tasas, noticias bursátiles, reglamentos, leyes, etc. Todo esto con un enfoque cliente/servidor.

En cuestión de personal, no se tiene contemplado un gran incremento y se piensa que la estructura actual en cada oficina externa es suficiente.

Los flujos de información se mantendrán en los mismos niveles. Sin embargo, ocasionalmente, se requerirá un medio de comunicación de las oficinas centrales hacia las regionales para difundir comunicados o documentos en forma global.

3.3.4. Red financiera.

Actualmente, las diversas entidades que conforman el Sistema Financiero Mexicano funcionan en plataformas de telecomunicaciones propias, utilizando diversos protocolos, topologías, infraestructura y medios de enlace. Cada una mantiene una red local (LAN) para dar soporte a sus áreas internas, existiendo comunicación con otras dependencias a través de enlaces punto a punto, utilizando líneas privadas a velocidades de 56 Kbps. y, en algunos casos, utilizando la Red Digital Integrada de Telmex o servicios de Frame Relay público.

La diversidad en la infraestructura utilizada para la transmisión de datos, ha provocado que cada institución requiera de varios enlaces y equipos para comunicarse con las otras entidades financieras. Adicionalmente la falta de "estándares " en este proceso, ha provocado que se utilicen diversas configuraciones, protocolos y esquemas de seguridad.

Considerando el fuerte intercambio de información que existe entre autoridades e instituciones financieras y su continuo incremento, se hace vital contar con un inventario de equipos de comunicación, tecnologías utilizadas, medios de transmisión y sistemas de información que intervienen en este proceso.

Adicionalmente se requiere un estudio de las diversas opciones de conectividad que existen actualmente en el mercado, y su factibilidad de implementación en todo el sector financiero. Se debe considerar el manejo de voz, datos e imagen y contar con una cobertura en las principales ciudades de la República Mexicana. Debe permitir un acceso rápido y eficiente, integrando a cualquier institución financiera del país y contar con esquemas de alta disponibilidad y alta seguridad. También se debe considerar el soporte y/o actualización a nuevas tecnologías de transmisión.

Capítulo 4

Desarrollo para la reestructuración de las redes de datos y comunicaciones de la CNBV.

4.1. Antecedentes y Propuesta.

La red de la Comisión Nacional Bancaria y de Valores ha venido presentado una serie de cambios, entre los cuales destacan:

- Fusión de las Instituciones con diferentes estándares de infraestructura informática, que ha traído consigo las siguientes implicaciones:

  - ✓ Al existir diferentes plataformas de cómputo (dispositivos de comunicación y concentración) no se ha logrado que todos los usuarios puedan tener acceso a los diferentes servicios de automatización de oficina y consulta de información de las bases de datos institucionales.

  - ✓ Por otro lado al no tener un estándar unificado, esto ha obligado a poner soluciones temporales a través de gateways (dispositivos conformados por un software y un hardware que nos permiten que dos plataformas de cómputo diferentes se puedan "platicar") que no son la mejor opción ya que restan eficiencia y calidad en el servicio de red.

- Los dispositivos de concentración actual no tienen capacidad para conectar a más usuarios en red.

- Redes con diferentes tecnologías de acceso a la información (token ring y ethernet), lo cual provoca que algunas aplicaciones (sociedades de inversión, padrón bursátil, entre otros), solo puedan ser utilizadas por algunos usuarios, es decir, aquellos usuarios que se encuentran con la opción de token ring (torre sur) son lo únicos que pueden acceder dichos sistemas.

- Los usuarios actualmente están demandando accesar cualquier servicio de red ya sea de automatización de oficina (fax, paquetería, correo electrónico, impresión en red, etc.) y/o de acceso a la base de datos institucional; con la infraestructura actual no es posible ofrecer este requerimiento.

- Infraestructura limitada (velocidades de transmisión de datos y soporte para nuevas aplicaciones con mayor demanda de tráfico en la red), con lo cual no es posible ofrecer el servicio a todos los usuarios para las nuevas aplicaciones que se están desarrollando tales como: Ventanilla Única, Control de Gestión, Jurídico (información de imágenes), Publicación de Información Institucional para el área de la Coordinación General de Normatividad (internet / Intranet).

Dada la problemática anteriormente descrita es necesario hacer un cambio total de infraestructura de la Red Local en las *Oficinas Centrales*.

La reestructuración de las redes de datos y comunicaciones de la CNBV, la hemos dividido en los siguientes rubros:

- ☑ Red de área local (LAN).
- ☑ Red de área amplia (WAN).
- ☑ Equipamiento personal.
- ☑ Equipamiento central.
- ☑ Servidores departamentales.
- ☑ Base de datos institucional.
- ☑ Plataforma de administración y monitoreo.
- ☑ Intranet/Internet.
- ☑ Seguridad.
- ☑ Help Desk.

4.2. Red de Área Local (LAN).

4.2.1. Alcance.

☑ Implementar una infraestructura estándar de red local en toda la Institución que mejore los accesos a los diferentes servicios de red y fuentes de información, sin importar la localización física del usuario debiendo ser transparente y fácil de administrar.

☑ Ofrecer un alto desempeño de la red y disponibilidad de los servicios con una administración flexible, dinámica, centralizada y planeada conforme a las necesidades de la Institución.

☑ Contar con esquemas de seguridad que garanticen la integridad de la información que fluye a través de la red local de datos.

4.2.2. Diseño.

La infraestructura de la CNBV esta compuesta por dos edificios: Torre Norte y Torre Sur, en los cuales se propone instalar soluciones idénticas (una plataforma estándar).

La solución esta dividida en tres partes:

- Centro de cómputo Central.
- Dispositivos para pisos.
- Cableado estructurado.

Centro de cómputo Central

Para el enlace entre torres se tendrá un dispositivo central (switch), el cual nos permitirá tener una comunicación entre torres más eficiente, contará con redundancia, es decir, en caso de ocurrir alguna falla, existirán varios enlaces de tal forma que si uno de éstos llega a dañarse la información que está viajando por estos medios tome otra ruta para hacer llegar los datos a la torre correspondiente.

Por otro lado los enlaces contarán con mayor velocidad y confiabilidad en la transmisión de la información al utilizar fibra óptica.

Dispositivos para pisos

Se tendrá un dispositivo (switch) por cada dos pisos (del piso 3 al 11) con los cuales se busca mejorar la calidad de los servicios de red (automatización de oficina y bases de datos institucional) ya que son equipos que entre otras bondades proporcionan un incremento bastante significativo en la velocidad de transmisión de datos, funcionalidad y confiabilidad de la entera operación de la red.

Cableado estructurado

Se propone garantizar a la CNBV una solución integral a sus sistemas de comunicación mediante la instalación de un cableado estructurado que permita la unificación de las torres (torre norte, torre sur).

Actualmente la CNBV en las dos torres: Norte y Sur, cuenta con cableados independientes uno del otro, haciendo dos especies de redes (LAN), las cuales están armadas con diferentes tipos de cables, Coaxial, UTP nivel 3, nivel 5, etc. En una forma no administrable, y sin posibilidad de crecimiento a futuro. No se encontró ningún elemento de

administración, y por ende no cumple con las normas para poder elaborar una certificación ya que no cuenta con las características de un cableado estructurado.

Las adecuaciones y condiciones existentes también son un punto importante ya que son los medios de distribución a cada estación de trabajo, en esto recae: ductos, canalizaciones, pasos de cable, etc. ya que no se cuenta con estos medios ideales para una instalación de la red. No existen los ductos apropiados, así como los pasos de comunicación entre pisos que son fundamentales en una red.

Por tal motivo la selección del cable apropiado y del equipo de conexión para la red es importante, porque el rendimiento total del sistema esta determinado por el componente de rendimiento más débil. Por ejemplo, un sistema de cableado que utiliza coaxial, UTP nivel 3, solamente tendrá el rendimiento de categoría 3. Por lo tanto, cada componente deberá ser de la misma categoría o superior de rendimiento para lograr el rendimiento deseado del sistema.

Para asegurar aún más la totalidad de su red, las características eléctricas de cada componente individual se miden en atenuación (perdida de fuerza de señal) y en aislamiento diafónico cerca del extremo. Cuando se considera cada componente en la red en relación con estas dos características, se determina el margen de señal a diafonía (crosstalk) del sistema de cableado, lo que es un indicador del rendimiento total del mismo. A mayor crosstalk y amplitud de la frecuencia probada, mejor será el rendimiento y capacidad de ancho de banda.

Dentro de la etapa que corresponde al cableado estructurado se harán las adecuaciones necesarias para la buen conducción de cada uno de los servicios a instalar en los pisos que lo requiera. Esto se logrará por medio de canaleta, tubería de diferentes diámetros, o escalerilla dentro de cada una de las torres a cablear.

Cada servicio de datos tendrá las adecuaciones necesarias para poder implementar voz y/o video dentro de esta misma salida de información. El cableado tendrá una certificación que garantice el ancho de banda hasta por 155 MBPS y esta garantía tendrá una validez de hasta 15 años.

El número de nodos a cablear es de 2160 nodos (tomando en cuenta que la máxima instalación por piso que aproximadamente es de 120 nodos, esto multiplicado por las salidas correspondientes a voz y/o video, multiplicado por la cantidad de 18 pisos) quedando sujeto a las necesidades y requerimientos del cliente. Se tenderán cables de fibra óptica con la finalidad de contar con un respaldo del cableado que une ambas redes. Este cableado que cumple con las normas esta previsto para acomodar una amplia variedad de aplicaciones de sistemas (por ejemplo, voz, fax, módem, macrocomputadora y video) utilizando un esquema de cableado universal.

El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se están apoyando las necesidades actuales sino también cuando se anticipan las necesidades del mañana. Hacer esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del sistema de cableado.

La integración de los servicios de voz, datos, así como video, son parte de la plataforma de comunicaciones que el cableado permitirá. El sistema de cableado estructurado podrá permitir el crecimiento y el decremento de los servicios de video, voz y datos de una forma ordenada.

Al término del proyecto el proveedor deberá entregar memoria técnica descriptiva del trabajo realizado en el proyecto. En este, se describen los servicios instalados en el cableado estructurado de la CNBV, la cual contempla: tabla de distancias por nodo,

descripción de cada uno de los materiales instalados, planos, esquemas, rutas de tubería, códigos internacionales que aplican en el cableado, lista de materiales en su composición, así como el diagrama esquemático de la red y planos en general.

4.2.3. Beneficios a obtenerse.

Una infraestructura de red local totalmente nueva con los siguientes atributos:

- Cualquier usuario podrá acceder con mejor tiempo de respuesta y eficiencia a los servicios de automatización de oficina y acceso a la base de datos institucional.
- Poder dar soporte a las nuevas tecnologías de información que los usuarios actualmente están demandando como es el caso de internet / intranet.
- Poder conectar a cualquier usuario que necesite servicios de red.
- Una comunicación segura, eficiente y rápida en el enlace entre torres.
- Sistema redundante (que minimice impactos de servicio cuando algún componente de la red y/o de la instalación eléctrica falle) que permite una alta disponibilidad de los servicios.
- Lograr que no existan barreras de formas de acceso a la información, para que cualquier usuario pueda acceder sin restricción los servicios de red que él desee.
- Eliminación de soluciones temporales (gateways) al contar con una sola plataforma estándar de red local (ethernet / fastethernet).
- Mayor rendimiento y control de tráfico en la red.
- Administración simplificada de la red.

- Planeada para proporcionar una sólida y segura inversión, ya que estos equipos nos permitirán ir creciendo de acuerdo a nuestras necesidades de expansión y capacidad.

4.3. Red de Área Amplia (WAN).

La CNBV, en su calidad de organismo supervisor y regulador del sistema financiero, requiere que las instituciones del sector la provean de la información necesaria para llevar a cabo dicha función. Para esto, las instituciones se apoyan en los medios de transmisión de datos existentes para hacer llegar su información por estas vías. Por tal motivo, la Comisión debe contar con una infraestructura de comunicaciones robusta y diversificada para cumplir eficientemente con esta parte del proceso de supervisión y análisis.

La demanda de comunicación y acopio de información es cada vez mayor y con un número más grande de instituciones, lo que le permitirá a la CNBV ampliar sus posibilidades de supervisión y análisis del sistema financiero siempre que cuente con la infraestructura para ello.

4.3.1. Alcance.

☑ Garantizar la confidencialidad de la información que es enviada a la CNBV por parte de la entidades supervisadas del sistema financiero nacional.

☑ Apoyar las labores de supervisión del sector financiero, al establecer la tecnología y medios electrónicos para la transmisión de datos que permitan interconectar la totalidad de los intermediarios financieros con la CNBV.

- ☑ Garantizar el intercambio electrónico de información optimizando la plataforma y medios de comunicación entre los organismos participantes del sector financiero.

- ☑ Asegurar el acceso a la red de cómputo de la CNBV mediante metodologías y herramientas necesarias que prohíban a personas no autorizadas hacer uso de este servicio.

4.3.2. Diseño.

Se planean introducir servicios de consulta en línea de algunos tópicos financieros: índices, monitoreo, tasas, noticias bursátiles, reglamentos, leyes, etc. Todo esto con un enfoque cliente / servidor.

- ☑ La estructura actual en cada oficina externa es suficiente.
- ☑ Los flujos de información se mantendrán en los mismos niveles y, solo en caso excepcional, se incrementarán los tiempos de conexión a las oficinas centrales.
- ☑ Solo se requiere de un incremento en el ancho de banda en los enlaces que se tienen con las oficinas metropolitanas y hacia otros organismos financieros.
- ☑ Se requerirá un medio de comunicación de las oficinas centrales hacia las regionales para difundir comunicados o documentos en forma global.

Se propone:

1. Para el caso de oficinas metropolitanas, establecer enlaces a través de la Red Digital Integrada (RDI) mediante servicios DSO a 64 Kbps.

2. La instalación de un servidor de Internet para proporcionar estos servicios a las oficinas regionales.
3. Contratar servicios de Internet en cada una de las oficinas regionales.

El esquema se muestra en la Figura 4.1.:

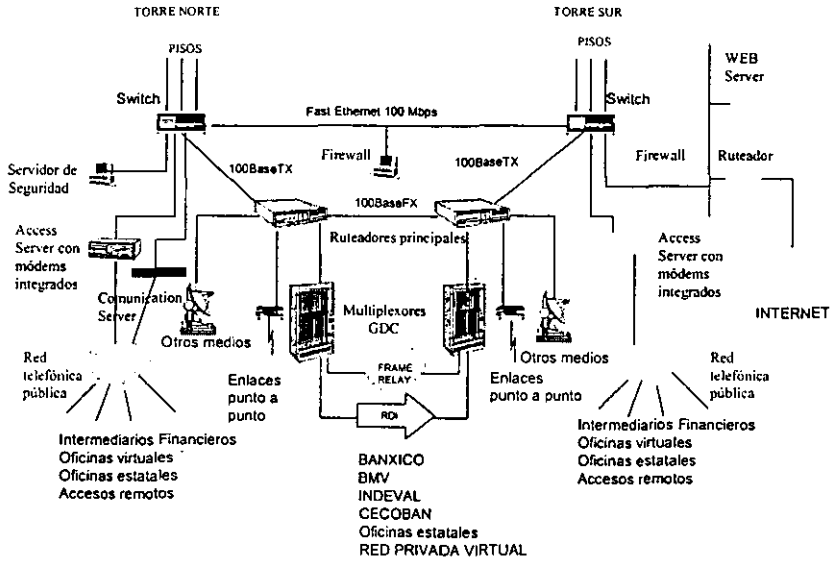


Fig. 4.1. Propuesta de estructura de Comunicaciones para la C.N.B.V

Con este diseño se pretende contar con una infraestructura actualizada y completa que cumpla con las actuales demandas de comunicación con las entidades financieras así como de personal que realiza las labores de supervisión *in situ*, para que desde cualquier línea telefónica se conecta a la red de la CNBV y pueda acceder a los sistemas de análisis financiero y catálogos bancarios, está infraestructura contará con las siguientes características:

- Una comunicación más eficiente con la oficinas metropolitanas, además de sentar las bases para poder comenzar a soportar a las oficinas estatales.
- Ampliar las capacidades de acceso para poder atender a más instituciones supervisadas y así cumplir con el objetivo de llegar a supervisar al 100% de las mismas.
- Se mejorarían los procesos de envío y recepción de información con otras entidades.
- Para la parte de los enlaces contaremos con esquemas de seguridad y redundancia en los medios, es decir, existirían canales por diferentes rutas, de tal manera que si alguno llegará a tener alguna falla habría una ruta alterna que daría la disponibilidad del servicio. De lado de seguridad tendremos software especializado para proteger a la red interna de intrusos y tener un estrecha vigilancia de quienes accedan nuestra red.

4.3.3. Beneficios a obtenerse.

Minimización de riesgos por el acceso no autorizado a la red de cómputo de la CNBV al contar con los mecanismos adecuados para asegurarlos.

Eficientar los procesos de envío y recepción de información con las instituciones financieras, logrando optimizar el apoyo que requiere el proceso de supervisión y análisis.

Garantizar la compatibilidad e interoperabilidad de todos y cada uno de los elementos que se integren al esquema de comunicaciones con la red de cómputo de la CNBV, posibilitando la extensión de los servicios de esta última a usuarios que remotamente requieran conectarse.

Establecimiento de esquemas de redundancia en los medios de enlace.

Contar con una infraestructura con capacidad suficiente para enlazar a las oficinas metropolitanas, estatales (en un futuro y considerando que los equipos nuevos se podrán ampliar para ello), otras autoridades, agencias noticiosas, intermediarios financieros, etc.

Diversificar la plataforma de comunicaciones para tener acceso a las nuevas tecnologías que en materia de comunicación van surgiendo en el mercado nacional e internacional.

4.4. Equipamiento Personal.

4.4.1. Alcance.

☑ Dotar a la CNBV con equipo de cómputo que permita una alta disponibilidad de los servicios de red que ofrece la Dirección General de Informática.

☑ Actualizar todo el equipo obsoleto de cómputo personal, con equipo que soporte los requerimientos actuales y nuevos de sistemas de información y servicios de automatización de oficina.

☑ Preparar la infraestructura hacia la nueva generación de aplicaciones (plataforma de 32 bits).

☑ Llegar con servicios de red a todo usuario que cuente con una microcomputadora.

☑ Proveer de servicios de impresión en red a todos los usuarios.

☑ Proveer de equipo de cómputo portátil a toda el personal que realiza funciones de supervisión in situ.

4.4.2. Diseño.

Se debe adquirir, a través de una licitación pública internacional, el equipo de cómputo personal y portátil con las características de almacenamiento, procesamiento y comunicaciones que garanticen la operación y sistematización de las actividades de las áreas usuarias.

Bajo las consideraciones de compatibilidad tecnológica, se optimizaran los recursos obviando necesidades de capacitación y soporte técnico especializado en distintas arquitecturas, facilidades de escalabilidad, requerimientos de stock de partes y componentes, y garantías inclusive con equipos de respaldo con características y posibilidades iguales a los que sustituyen.

Un dato adicional es el que muestra el parque instalado de 1200 equipos personales en la CNBV, de los cuales 900 son de la marca Hewlett Packard, sin considerar el equipo por sustituir, lo que representa más del 70% a nivel Comisión. Esto es un punto muy relevante en el aspecto de mantenimientos preventivo y correctivo a los equipos, ya que el contar con un solo proveedor que respalde estos servicios, facilita el control y administración de los mismos.

Solicitar los servicios de mantenimiento para una diversidad de equipos con el aseguramiento de la calidad necesaria (que el proveedor sea centro autorizado de soporte de cada uno de los fabricantes de los equipos en cuestión), y además sea proporcionado por un solo proveedor; debe resultar más costoso debido a la especialización que requieren los técnicos de cada uno de los equipos. Así mismo el mantener un stock de partes para una diversidad de equipos resulta un mayor costo para el proveedor, por consiguiente se refleja en el costo total del servicio.

El modificar la configuración inicial de un equipo requiere de un procedimiento específico, que en muchos de los casos es diferente al tratarse de equipos de varios fabricantes, razón por la cual sería necesario capacitar o contar con personal que tuviera el perfil técnico necesario para poder solucionar cualquier falla y/o actualización a la configuración que se requiera para dar soporte a los requerimientos de las nuevas aplicaciones.

Adquirir por el mismo procedimiento, impresoras tipo láser, con características de ser incorporadas a la red de cómputo de la CNBV, permitiendo establecer grupos de impresión por piso o por área usuaria, lo que nos permitirá optimizar el servicio de impresión en la cantidad y calidad necesaria para la emisión de reportes y documentos generados por el personal en sus actividades cotidianas.

4.4.3. Beneficios a obtenerse.

- ☑ Equipo de cómputo con capacidad de almacenamiento y procesamiento acorde a las necesidades de las áreas usuarias.
- ☑ Apoyo al personal de supervisión y vigilancia, al contar con equipo portátil con facilidades de comunicación y trasferencia de información no importando el lugar donde se encuentren, lo cual ayudará a agilizar las actividades que estas áreas realizan.
- ☑ Garantizar el acceso remoto por las capacidades propias del equipo portátil implementando el concepto de oficina virtual, una vez que los medios de acceso así lo permitan.
- ☑ Ampliar los beneficios del servicio de impresión en red a más usuarios, optimizando a la vez los recursos y bienes informáticos de la CNBV.
- ☑ Incrementar la productividad en la CNBV, al proporcionarle a los usuarios los medios de acceso, explotación y trabajo de oficina sobre todos los servicios de cómputo que se otorgan, y que por sus necesidades específicas requieran.

4.5. Equipamiento central.

4.5.1. Alcance.

☑ Cubrir las necesidades de las áreas usuarias (administrativos, sistemas, usuarios, etc) con una infraestructura robusta en cuanto a capacidades de almacenamiento, desempeño de los equipos ,esquemas de respaldo con alta disponibilidad, tolerantes a fallas en cuanto a equipo y servicio.

☑ Implementar un esquema de redundancia entre los diferentes equipos para poder asegurar los servicios continuos en la Institución.

☑ Cubrir las necesidades de los centros de cómputo en cuanto a mobiliario, instalaciones eléctricas, respaldos de energía, control ambiental de temperatura, para mantener la operación de los equipos centrales, a fin de garantizar la prestación de servicios.

☑ Incrementar la capacidad de almacenamiento y procesamiento del equipo central, requerida por el aumento de procesos y flujo de información que las diferentes áreas usuarias requieren para llevar a cabo sus labores de supervisión y vigilancia del sector financiero nacional.

☑ Contar con la infraestructura adecuada para la implementación de una arquitectura de base de datos institucional, necesaria para el almacenamiento de información que todas las entidades supervisadas envían la CNBV.

4.5.1. Diseño.

Con este proyecto se pretende crear una infraestructura que nos permita operar en forma continua durante los 365 días de año por 24 hrs. Se podrá aprovechar las características de los equipos como son: el multiprocesamiento, la velocidad de acceso e incrementar la capacidad de almacenamiento entre otras. Contar con la capacidad de estar preparados en caso de contingencias, además de facilitar la administración de los servidores de misión crítica. Es decir, implantar una configuración tolerante a fallas con equipos HP-9000, con capacidad de proceso al menos tres veces superior al actual, y una disponibilidad de 99.999% (5 minutos de falla no planeada al año).

Acondicionar los centros de cómputo con mobiliario, instalaciones eléctricas, de aire, respaldos de energía, para poder solventar la operación de cualquier clase de equipo que opere dentro de ellos.

Actualmente se cuenta con una infraestructura poco robusta para soportar las cargas de trabajo dentro de los equipos centrales, ya que el crecimiento en cuanto a requerimientos y necesidades se ha ido incrementando de una manera acelerada. Los equipos se encuentran a un 90% de su capacidad y con pocas opciones para incrementar los recursos debido a que la vida útil de los equipos es de 5 años y varias máquinas están por terminarla, de tal forma que cualquier situación ordinaria ó extraordinaria podría afectar el funcionamiento de los servicios.

Por lo anterior, la tecnología utilizada para realizar tareas de respaldo es obsoleta y por lo tanto se hace necesario buscar nuevas herramientas que nos permitan tener un mayor desempeño en esta área.

Aunado a esto los equipos no cuenta con la capacidad de ser tolerantes a fallas, y las aplicaciones y requerimientos que actualmente se maneja en la Institución requieren tener este tipo de servicios.

Otro factor determinante en este proyecto es la migración de aplicaciones, debido a la fusión de las Instituciones.

Debido a la fusión de Instituciones, se hace un factor determinante la migración de aplicaciones para homologar las tecnologías de bases de datos, ya que anteriormente cada una se manejaba independientemente.

Es necesario considerar un crecimiento en los centros de cómputo, ya que sus capacidades para albergar nuevos equipos (Comunicaciones, Equipo Central, Servidores de correo, etc) ha sido sobrepasada, como podemos observar dentro de los Centros de Cómputo.

De acuerdo a los recursos establecidos, se han venido implementado los sistemas desarrollados en Sybase, los servidores de Lotus-Notes, aplicaciones administrativas, hasta el punto de contar con equipo en préstamo; sin embargo la demanda de requerimientos por parte de las diferentes Direcciones se hacen cada día mas constantes.

El nivel de almacenamiento y procesamiento del equipo actual de la marca HP para la Recepción Electrónica de Información Financiera se encuentra próximo a la saturación, si a esto sumamos el aumento de información que los supervisados enviarán a la CNBV así como también el incremento de instituciones que se enlazarán por este medio, se hace necesario tomar las medidas pertinentes para ampliar dichas capacidades.

Por otra parte y dando continuidad a la actualización del equipo en los centros de cómputo por falta de capacidad, limitación en su crecimiento y posibilidades de integración al ambiente de la CNBV en un 100%, se requiere actualizar la estación de trabajo dedicada a funciones de administración y monitoreo.

Como consecuencia de los nuevos Sistemas Administrativos, el servicio de impresión requiere integrarse a los servicios de red, sustituyendo la impresión directa desde Unix que es como se venía ofreciendo, lo que permitiría en su momento incluso descentralizar esta labor hacia las áreas usuarias.

4.5.1. Beneficios a obtenerse.

Al tener esta infraestructura nos ayudara a mantener un servicio de óptima calidad que se verá reflejada en el aprovechamiento por parte de los usuarios de los equipos. Además se podrá garantizar el crecimiento homogéneo entre las necesidades de la Institución y la capacidad de cómputo central. Homologación dentro de los equipos para las aplicaciones que se esperan introducir en este año como son: Sistema de Análisis Financiero, Sistema de Administración y Sociedades de Inversiones entre otros. Por otro lado se podrá contar con un esquema de redundancia entre servidores y centros de cómputo.

Se mantendrá un balanceo de cargas adecuado para no saturar la capacidad de los equipos, introducir nuevas tecnologías en las aplicaciones como son: Sybase, Lotus Notes y la versión de sistema operativo HP-UX. Ampliar la capacidad física de los centros de cómputo para poder alojar una mayor cantidad de equipo y hacer una reorganización de los equipos existentes.

Contaremos con la capacidad de proceso y almacenamiento adecuado para los requerimientos de manejo de grandes volúmenes de información, necesarios en las tareas de recepción y carga de información que se realizan como parte del proceso de supervisión del sector financiero nacional.

La operación y el servicio serán continuos para las aplicaciones de recepción y carga de información financiera en beneficio de las áreas usuarias, al contar con las características de tolerancia a fallas y respaldo de información automática, complementando la compra hecha con recursos propios.

Se obtendrá trasparencia en la migración de las aplicaciones de recepción y carga de información actuales a lo nuevos equipos, en beneficio de los las actividades de las diferentes áreas usuarias de la CNBV.

4.6. Servidores Departamentales.

4.6.1. Alcance.

Actualmente los servicios de red que se proporcionan en las *Oficinas Centrales (Plaza Inn)* corren en una plataforma de sistema operativo heterogénea (Novell Netware y Windows NT); en *Oficinas Metropolitanas* se tienen solo algunos servicios, mientras que en las *Oficinas Estatales* no se cuenta con infraestructura de red, esta situación trae consigo la siguiente problemática:

- No existe homologación de servicios de red en ambas torres.
- No se cuenta con una plataforma homogénea de cómputo.
- No existe una estrategia definida para ubicar servicios.

- No se puede ofrecer servicios adicionales con la infraestructura actual, tales como: fax, actualización automatizada de versiones de software, bases de datos departamentales, entre otros.
- Se cuenta con una infraestructura informática obsoleta con relación a las necesidades de la Institución.
- No se cuenta con infraestructura de red en todas las oficinas de la Institución.
- La plataforma de servidores se encuentra dispersa en diferentes ubicaciones.
- Carencia de espacio físico para ubicar nuevos servidores.

Los alcances de este estudio es el siguiente:

☑ Definir, desarrollar e implantar la infraestructura de Cómputo Distribuido (Servidores departamentales) de la CNBV, que garantice la oportuna y ágil respuesta a la demanda de servicios de información, apoyando con ello a los usuarios en las labores de supervisión y vigilancia del sector financiero.

☑ Proporcionar una plataforma común de servicios de red, administrada, robusta, segura y flexible que responda oportunamente a los requerimientos y necesidades de los usuarios y por ende al organismo.

☑ Apoyar en el incremento de la productividad del personal de CNBV, ofreciendo herramientas para la Automatización de Oficinas, manejo electrónico de información, administración y soporte de las aplicaciones y recursos informáticos que faciliten y den valor agregado al trabajo diario del personal.

4.6.2. Diseño.

Una infraestructura de cómputo distribuido de las *Oficinas Centrales* y *Oficinas Metropolitanas* consistente de servidores que ofrezcan servicios de *automatización de oficina* tales como: paquetería, impresión, aplicaciones, archivos compartidos, administración de la infraestructura de cómputo personal (inventario de equipo, distribución de software, soporte remoto), fax en red, publicación de información institucional y bases de datos departamentales.

4.6.3. Beneficios a obtenerse.

- ☑ Una administración centralizada, que facilitará un mejor control del servicio en la atención de usuarios.
- ☑ Una distribución eficiente de los recursos de red, permitirá un mejor aprovechamiento de la misma.
- ☑ Se tendrá una infraestructura actualizada de acuerdo a las necesidades de la Comisión.
- ☑ La distribución de los servicios permitirá una mayor seguridad y control en el manejo de la información.
- ☑ Aumento en la productividad de los usuarios mediante la disposición de nuevas herramientas.
- ☑ Se contará con un inventario al día de los equipos de cómputo personal, así como la actualización de nuevas versiones de software de manera automatizada.
- ☑ Se optimizará el espacio físico en los centros de cómputo.

4.7. Base de Datos Institucional.

4.7.1. Alcance.

Implementar una infraestructura a nivel base de datos donde se desarrollen sistemas en diferentes plataformas y sistemas operativos.

Homologar la plataforma de base de datos.

Contar con una plataforma de servidores de bases de datos homogénea para la administración de la información en la institución.

Desarrollar un esquema de documentación técnica y de procesos de cambios de las bases de datos y de sus componentes.

Normar, estandarizar y controlar los esquemas operativos y de administración de bases de Datos para garantizar el control, disponibilidad, integridad y confiabilidad de la información de CNBV.

Separar los ambientes desarrollo y de producción para optimizar la liberación de nuevas aplicaciones y elaborar una adecuada política de respaldos.

4.7.2. Diseño.

A la fecha no se cuenta con una instalación confiable, ni homogénea de la versión del SQL server de Sybase (ASE 11.5) lo que origina el no poder garantizar un funcionamiento, servicio y soporte por parte del proveedor. Esto no permite tener una

compatibilidad entre las estructuras de las bases de datos y la información de cada uno de los servidores de la CNBV.

No existe una compatibilidad al 100% entre las plataformas de los servidores en cuanto a estructuras y componentes lo cual no permite la migración transparente de estructuras y datos entre ellas, para eventos de liberación de un ambiente de desarrollo a producción o bajo algún esquema de contingencia.

Se deberá crear un ambiente de producción en el que los desarrolladores a lo mas puedan consultar la información pero no la puedan modificar de manera que los servidores de producción no se vean impactados por las cargas de trabajo del área de Desarrollo manteniendo la seguridad e integridad de la información. Así mismo deberá proveer a los desarrolladores de un ambiente en el que sean libres de modificar tanto la estructura de la base, como los datos, con la capacidad de poder contar con la información real cuando esto sea necesario.

El ambiente de pruebas de preproducción permitirá evaluar las aplicaciones, tanto por parte del usuario en su funcionalidad y tiempos de respuesta, así como el impacto en el performance del servidor.

A la fecha no se cuenta con una documentación de los esquemas de instalación, configuración y componentes de los servidores y de las bases de datos, así como la clasificación y tipos de información residente en el DBMS lo que origina no garantizar la información necesaria para auditorias, planes de contingencia, esquemas de seguridad, etc.

La solución se llevara a cabo a través propuestas de políticas a los involucrados que deberán acordar conjuntamente su aprobación e implementación. Se propone la creación de un comité de normatividad conformado por las direcciones involucradas para la aprobación de las políticas que se citan.

- Se establecerán y definirán la clasificación y tratamiento de la Información almacenada en los servidores de Bases de Datos.
- Se establecerá y definirá la normatividad de los indicadores de control y administración de los servidores y bases de datos, así como la correlación con la Dirección de Desarrollo de Sistemas.
- Se normarán los elementos y ambientes de las definiciones de la residencia de servidores de bases de datos Sybase para determinar las estrategias de avance tecnológico.
- Se definirá la normatividad de las responsabilidades y procedimientos de los servicios prestados.
- Se definirá la normatividad de los esquemas de seguridad de las bases de datos para su difusión junto con la Dirección de Desarrollo de Sistemas.
- Se definirá la normatividad para la implementación y modificaciones de los sistemas en producción .

Se utilizará Sybase v 11.5.2 como manejador de la base de datos considerando que gran parte de los sistemas actuales están desarrollados en esa plataforma y solo se tendrían que migrar algunos desarrollados en el manejador Gupta.

Sybase es una serie de componentes que proporcionas soluciones a empresas para un gran rango de aplicaciones de bases de datos incluyendo almacenamiento de datos, procesamiento de transacciones en línea, sistemas de soporte de decisión y despliegue de volúmenes. Trabaja de igual manera sobre una variedad de plataformas desde laptops hasta sistemas de mainframes.

En los últimos años el modelo Cliente/ Servidor ha sido la "nueva tendencia" desde computadoras en red como en modelos tradicionales. Este modelo divide el procesamiento

en "aplicaciones clientes" y "aplicaciones servidor" que cooperan a realizar tareas para una aplicación total.

Las aplicaciones cliente hacen la solicitud para el servicio, las aplicaciones servidor reciben la solicitud y responde a través de un dato, con otra información o tomando alguna acción.

Con este manejador de base de datos, el servidor SQL corre todos los sistemas actuales de manejadores de base de datos, esto es todos los procesamientos asociados con acceso de base de datos. El servidor de base de datos lleva a cabo las tareas iniciadas por el cliente requeridas directamente a la base de datos. Su arquitectura asegura la integridad de los datos, el control concurrente y la habilidad para recuperar las fallas. El servidor de base de datos también mantiene el diccionario de base de datos la cual define la estructura y contenido de la base de datos.

El "servidor de base de datos" es el SQL server y el "cliente base de datos" es cualquier cliente software que puede interactuar con el SQL server. El SQL, es una aplicación cliente que interactúa con el SQL server para ejecutar y realizar tareas.

4.7.3. Beneficios a obtenerse.

- Simplificar la interacción entre la computadora y el usuario ya que el cliente puede tener una interfaz gráfica en la workstation y aplicaciones en multimedia. El costo para el desarrollo de aplicaciones que usa este tipo de interfaz es económica comparada con las aplicaciones para los servidores en macrocomputadora.

- Reducir el tráfico en la red, el cual mejora el rendimiento, ya que el modelo cliente / servidor requiere muy pocos eventos de red.

- Facilitar la implementación de sistemas abiertos porque esta basada en el modelo ISO para sistemas de redes. Este modelo especifica se basa en la interfaz entre capas la cual oculta lo complejo de los bajos niveles de software, haciendo esto fácil para agregar nuevo hardware y aplicaciones.

- Estandarización en las instalaciones de los servidores de la CNBV.

- Contar con información estadística relacionada con versiones y licencias del producto y seguridad en la integridad de la información.

- Evitar cualquier tipo de irregularidad en la información de producción y tener un mejor control sobre la creación de objetos y accesos en producción.

- Poder medir el impacto de las aplicaciones sobre el ambiente de producción antes de que estas sean liberadas.

- Dar mayor libertad a los desarroiladores, pues al no tener que probar en producción ellos son libres de manejar sus ambientes como mejor les convenga

4.8. Plataforma de Administración y Monitoreo.

4.8.1. Alcance.

☑ Definir, desarrollar e implementar la infraestructura de administración y monitoreo centralizado de la CNBV; que nos permita no solo prevenir, localizar y aislar fallas de cualquier índole, sino también planear, integrar y controlar los servicios en una sola plataforma robusta que nos permita incrementar la calidad y continuidad de los servicios. Además de contribuir en optimizar el desempeño de la infraestructura informática que demandan los usuarios de los servicios para cumplir con las responsabilidades de supervisión del entorno financiero que la ley le otorga a la Comisión Nacional Bancaria y de Valores.

☑ Esta plataforma administrará los siguientes recursos informáticos:

- ✓ Equipo de comunicaciones y red local.
- ✓ Equipo de cómputo central, distribuido y personal.
- ✓ Sistemas de misión crítica.
- ✓ Aplicaciones.
- ✓ Accesos, privilegios y servicios de los usuarios.
- ✓ Seguridad.
- ✓ Bases de datos.

4.8.2. Diseño.

HP OpenView es un administrador e integrador de redes, sistemas, aplicaciones y bases de datos en varios ambientes de cómputo.

La solución consiste de un grupo de productos de administración y servicios que ayudan a monitorear cada uno de los elementos que integran una red de datos. Los principales son los siguientes:

- ✓ Interfaz de usuario.
- ✓ Administración de eventos.
- ✓ Descubrimiento.
- ✓ Administración de bases de datos (almacenamiento de datos en la red).
- ✓ Infraestructura de comunicación.
- ✓ Administración de nodos.

Interfaz de usuario

La interfaz de usuario más común es el mapa, el cual proporciona un punto de vista de la red para todas la aplicaciones de monitoreo. El mapa debe permitir al usuario el paso a través de la red en una jerarquía de vistas representando subredes y elementos de red básicos. Estos componentes son usualmente representados en el mapa por iconos. El mapa también debe enviar información a los administradores acerca de cambios en el estado de su red.

Descubrimiento

Antes de que un dispositivo se encuentre el mapa de administración, la plataforma debe percatarse de su presencia en la red. El proceso de encontrar un dispositivo de red y entonces desplegarlo en un mapa es llamado "descubrimiento".

Las herramientas de descubrimiento pueden solo ver y descubrir tipos de los dispositivos que este conoce.

Administración de eventos

Una vez descubiertos, el software que presenta estos dispositivos en la red deben notificar a las aplicaciones acerca de eventos específicos. Los eventos son notificados enviando al administrador de la red permite conocer de ciertas ocurrencias con el dispositivo. Estas ocurrencias deben ser notificaciones de rutinas ocurridas, advertencias de problemas inminentes o notificaciones de catástrofes ocurridas con el dispositivo. El manejo de estos eventos es conocido como "administración de eventos".

Administración de bases de datos

Es el depósito central para almacenar los datos de administración de la red. Varias aplicaciones de administración incluyen sus bases de datos propietarias, pero la tendencia se mueve a un modelo de datos abiertos permitiendo a los usuarios emplear las bases de datos de su elección.

Una efectiva administración debe basarse en el análisis de información en tiempo real e histórica. Estas bases de datos de administración son usadas para contener justo esta clase de información. Una vez reunida, las aplicaciones deben tener acceso a la información para graficar y analizarla y generar reportes.

Infraestructura de comunicación

Capacidades tales como realizar el descubrimiento de dispositivos, solicitando información de agentes en dispositivos y recibiendo reportes de eventos requiere una infraestructura de comunicación por dos razones a) soportar varios protocolos y b) facilitar la conexión entre aplicaciones y los objetos administrados. El protocolo estándar para comunicar información de administración de red es SNMP.

Administración de Nodos

El número de nodos administrados puede ser confuso. Las soluciones de administración de red deben ser capaces de descubrir y prepararlo en un mapa gráfico, un cierto numero de dispositivos de red o nodos. Estos son típicamente grandes números. Los dispositivos descubiertos incluyen ruteadores, bridges, switches, servidores, PCs, impresoras, etc.

Respaldos

La herramienta para realizar los respaldos será Omniback II. Es posible seleccionar desde un respaldo de filesystem total/incremental o respaldo en línea. Las cintas de respaldos existentes pueden ser copiadas local o remotamente siguiendo un sofisticado proceso de valuación.

4.8.3. Beneficios a obtenerse.

- ✓ Administración y monitoreo estandarizado conforme a políticas.
- ✓ Optimizar el desempeño de los recursos informáticos.
- ✓ Elevar la disponibilidad y calidad de los servicios .
- ✓ Prevenir, localizar y aislar fallas de cualquiera de los componentes de red.
- ✓ Obtención de información histórica del desempeño de los recursos.
- ✓ Planeación de crecimientos.
- ✓ Configuraciones de los dispositivos de red.
- ✓ Infraestructura de Administración y Monitoreo abierta, escalable para los nuevos requerimientos de servicios informáticos.
- ✓ Reducir los tiempos de respuesta en la atención a usuarios ya que se contará con una administración centralizada, que facilitará un mejor control del servicio red, tales como soporte técnico desde una consola, mediante la cual se podrá

actualizar paquetería, modificar las configuraciones la instalación o actualización de aplicaciones del usuario en forma remota así como un manejo mas eficiente de la información almacenada en los servidores como bases de datos y archivos compartidos.

- ✓ Aumento en la productividad de los usuarios mediante la disposición de nuevas herramientas, como fax de red, internet, intranet, versiones de paquetería actualizadas y un ambiente que permita la implementación de nuevos requerimientos que faciliten las labores del día de los usuarios.
- ✓ Contar con un inventario al día de los equipos de cómputo personal, y de las últimas versiones de software de manera automatizada con las características de estas herramientas se tendrá un mejor control de los bienes informáticos de cómputo personal para las áreas de Contraloría, Adquisiciones e Inventarios.

4.9. Intranet / Internet.

4.9.1. Alcance.

☑ Eficientar las labores de supervisión del sector financiero, estableciendo la tecnología y medios electrónicos que permitan interconectar al 100% de los intermediarios financieros con la CNBV.

☑ Establecer la plataforma de cómputo necesaria y suficiente que permita incrementar el intercambio y publicación electrónica de información entre las instituciones supervisadas y la CNBV.

☑ Garantizar la confidencialidad de la información que viaja por medios electrónicos, estableciendo las metodologías y herramientas necesarias que eviten el acceso no autorizado a dicha información.

☑ El proyecto de servicios Internet, busca dotar al Organismo con un sistema basado en la plataforma tecnológica que actualmente opera en la Comisión, el cual proporcione con oportunidad y al mejor costo, información suficiente para la efectiva toma de decisiones, cubriendo las necesidades de gestión de información que requiere la dinámica actual de las labores, mediante la interconexión a redes y lograr redes de área amplia necesarias a nivel nacional, con enlaces a nivel mundial.

☑ Publicación en Internet de las diferentes áreas de la CNBV que requieran comunicarse e intercambiar información con las entidades supervisadas y se ubiquen en los edificios centrales (Plaza Inn).

4.9.2. Diseño.

Intranet

Una intranet es una red privada empresarial que utiliza las tecnologías y los productos de Internet. Los intranets pueden estar protegidos de usuarios externos (de la Internet) a través de barreras (firewalls) o simplemente no conectándose al mundo exterior.

Existen algunas características que les son distintivas:

- Utilizan el protocolo de transmisión de información TCP/IP tanto para área local como para área amplia.
- Usan HTML, SMTP y otros estándares abiertos de Internet como medio para mover información de clientes a servidores.

- Son propiedad de la empresa y no necesariamente accesibles para el público en general.
- El acceso de los usuarios a los documentos en el servidor Web emplea el protocolo HTTP.

Una de las grandes virtudes de un intranet es la estandarización. En el pasado, cada área contaba con una aplicación determinada basada en distintas plataformas y con distintas interfases de usuario. Luego vino el tener un solo sistema para todos los empleados y se construyeron aplicaciones en Powerbuilder o Visual Basic.

Usar el navegador como cliente universal es muy económico, y un salto muy importante en la tecnología de información ya que obliga a repensar la manera en que se construyen las aplicaciones.

Este servicio de intranet se depositará en un servidor totalmente aislado del acceso a la Internet para mantener su confidencialidad y que sea accesado únicamente por empleados de la propia Comisión a través de la red interna.

Internet

Debido a que el los servicios que se pretenden montar en el servidor Internet de la CNBV tienen que ver tanto con envío como con recepción de información, se debe de contar con un mecanismo de seguridad que aísle la red de la CNBV de posibles "ataques" por terceros. De esta forma, el esquema de solución se basa en colocar el servidor de internet de la CNBV en un segmento aislado de la red interna con el fin de aprovechar el servicio de seguridad que proporcionaría el firewall, (Figura 4.2).

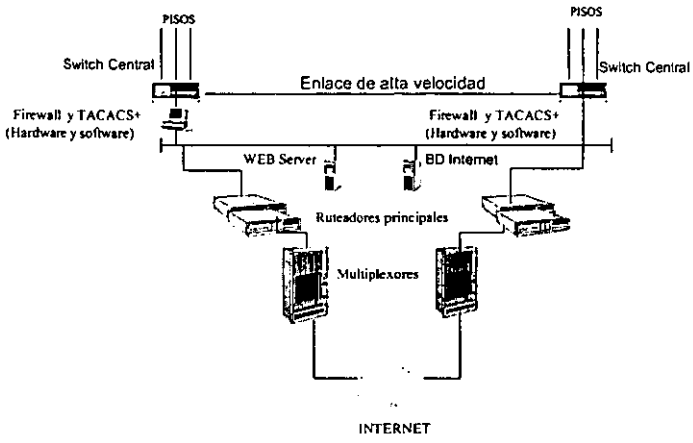


Fig. 4.2. Implementación de servicios de internet a través del firewall.

4.9.3. Beneficios a obtenerse.

Eliminación del contrato cuentas dial-up. Ahorro de teléfono por la cuentas dial-up.

Acceso corporativo de más de 100 usuarios.

Consulta e intercambio de documentos con entidades financieras.

Comunicación efectiva con las entidades supervisadas.

Publicación a nivel mundial de información de la CNBV.

Desarrollo de aplicaciones independientes del sistema operativo, hardware y ubicación física.

4.10. Seguridad.

4.10.1. Alcance.

☑ El objetivo principal es definir un modelo de seguridad informática que permita garantizar la confidencialidad, privacía, disponibilidad e integridad de la información, así como la autenticación y comprobación de la fuente generadora de dicha información, optimizando la relación costo / beneficio de la inversión en seguridad.

☑ Proponer e implantar un plan estratégico de seguridad informática, el cual garantice la disponibilidad, integridad y confidencialidad de la información.

4.10.2. Diseño.

Dado que en México no se cuenta aún con una guía de lineamientos generales de seguridad informática en el ámbito federal contra la cual medir la posición actual de la CNBV, se buscó este tipo de referencias a nivel internacional. .

A lo largo del presente estudio se hacen referencia a dichos organismos reguladores o emisores de guías, normas, estándares, etc. de varios países como son los Estados Unidos de Norte América, y Gran Bretaña entre otros.

Los organismos (NIST, que es el National Institute of Standards and Technology; BSI, el British Standards Institution; NCSC, que es el National Computer Security Center, etc.) encargados de la definición de estándares de seguridad en dichos países, llevan a cabo foros de discusión entre usuarios y proveedores, grupos de trabajo de usuarios gubernamentales, financieros y comerciales con el fin de definir los lineamientos, normas,

guías, recomendaciones y estándares a seguir dentro de las prácticas de seguridad diarias de los participantes.

En México existen pocos grupos que han hecho algunos avances en materia de estándares y legislación a nivel informática que pueden ser tomados en cuenta para alguno de los componentes.

Este estudio se enfoca principalmente a la seguridad física y lógica de los bienes y servicios informáticos con relación a los componentes que integran la red de área local y la red de comunicaciones de la Comisión.

Políticas de Seguridad

Las políticas de seguridad son instrucciones indicando las intenciones de la gerencia sobre las operaciones de una organización. Son aseveraciones de alto nivel que proveen una guía a los empleados para la toma de decisiones.

Las políticas son mandatorias dada la importancia que tiene el que sean obedecidas para cumplir con la seguridad deseada.

Empleo de Arquitecturas Confiables

Actualmente la mayoría de los proveedores de hardware y software ofrecen soluciones basadas en arquitecturas ya probadas que garantizan en la mayoría de los casos buenos resultados siempre y cuando la implementación se realice adecuadamente. Existen arquitecturas "fault-tolerance", de redundancia, de espejeo, que brindan una nivel de seguridad a la continuidad del servicio. La seguridad debe seguir a los cambios tecnológicos. Hasta cierto punto se recomienda que sea de manera conservadora ante tecnologías no maduras y debe evitarse el elegir tecnologías obsoletas.

Certidumbre en la Distribución

Es más reconfortante el saber que la información que viaja por medio electrónico, ya sea simples documentos o aplicaciones, se encuentre íntegra al momento de recibirle. Por lo mismo, sumas binarias o firmas y certificados electrónicos brindan un seguro de que no fue alterada en el camino. El empleo de software anti-virus da tranquilidad al ser empleado para la verificación de software proveniente de fuentes poco confiables.

Aseguramiento en la Operación

El enfoque en este punto se concentra ya no en los elementos de seguridad incorporados en un sistema, si no más bien en los elementos técnicos de los sistemas y si son seguidos o bien son evadidos en el uso diario del sistema.

Existen dos métodos principales:

Auditorias del Sistema; llevadas a cabo una sólo vez o bien periódicamente para evaluar la seguridad. Puede ser a nivel de todo el sistema o bien para evaluar algún punto específico que indique alguna anomalía.

Monitoreo; actividad constante que verifica al sistema, sus usuarios o el ambiente en el que opera (por ejemplo, la revisión diaria o semanal de intrusos en la red).

Métodos de Auditorias

Para la auditoria periódica o monitoreo de sistemas en específico, existen actualmente en el mercado herramientas de software que facilitan la tarea de los auditores y que se configuran de acuerdo a los lineamientos y políticas de seguridad de cada organización.

Herramientas automatizadas

El empleo de herramientas automatizadas para auditar sistemas es ampliamente recomendable dada la labor que implica una auditoria.

Existen dos tipos de herramientas: Las activas, que encuentran vulnerabilidades al estar continuamente tratando de explotarlas, y las pasivas, que examinan el sistema y reportan la existencia de anomalías al comparar el estado del sistema.

Varios proveedores ofrecen en el mercado soluciones de este tipo como por ejemplo Network Associates (NAI) o Internet Security Systems (ISS) entre los más conocidos.

Este tipo de Sistemas de Monitoreo y Administración de la Seguridad se adaptan a los sistemas de red y seguridad existentes en una organización.

La arquitectura básica se caracteriza por el empleo de agentes que monitorean servidores de información crítica, sistemas de seguridad (firewalls), ruteadores, etc. levantando información sobre todo lo que ocurre en la red. De encontrar discrepancias en las políticas de seguridad establecidas a nivel componente o bien vulnerabilidades, amenazas o desconfiguración de algún sistema, se previene al administrador y se inician acciones preventivas y correctivas según se establezca.

Con el fin de garantizar la privacía de esta información, el monitoreo debe realizarse de manera cifrada.

Este tipo de herramientas complementan el monitoreo y auditoria de los sistemas al recabar información importante sobre riesgos y vulnerabilidades tales como control de acceso, o configuración del control de acceso, passwords débiles, falta de integridad del

software de los sistemas o aspectos como versiones de sistema operativo obsoletas o falta de parches recomendados. Este tipo de herramientas son empleadas por los hackers para irrumpir en los sistemas. El empleo de éste tipo de herramientas apoyan a los administradores de la seguridad a tener las mismas "armas" en la lucha por proteger sus sistemas.

Herramientas Automatizadas para el Monitoreo

Algunas de las herramientas empleadas en el monitoreo cotidiano de los sistemas con mayor aceptación en la actualidad son:

Escáneres de virus; que verifican la existencia de programas extraños que pudieran afectar a los sistemas y a la información que ellos manejan. Su modo de empleo ha variado acorde a las nuevas prácticas de trabajo.

"Checksums": Es un método de comprobar que un documento o programa no ha sido afectado. Compara sobre la base de una suma de bits el estado de un programa con el fin de verificar su integridad. Éste método es adecuado para identificar la presencia de virus, Caballos de Troya, cambios accidentales en los archivos causados por fallas en el hardware, etc. Su inconveniente reside en que puede ser alterado fácilmente por algún intruso al sistema. En este caso se recomienda el empleo de firmas electrónicas.

Firmas y Certificados Electrónicos: Con la creciente actividad de negocios a través del Internet, la necesidad de crear mecanismos seguros de intercambio de información entre partes ha llevado al empleo de firmas y certificados electrónicos.

Herramientas de Ruptura de Passwords: La base de éste tipo de herramientas reside en la comparación de un password con una lista o diccionario de passwords conocidos o bien comparando variantes o combinaciones del identificador del usuario.

Desempeño del Sistema: Su función es la de monitorear el desempeño normal de un sistema verificando, según los parámetros de operación normal, cambios en la rapidez de procesamiento o de la red, posibles fallas de hardware o software, etc. que pudiesen comprometer la disponibilidad del servicio.

Detectores de Intrusos: Las mismas herramientas empleadas en la auditoria pero usadas de manera cotidiana para rastrear entradas ilegales o anormales al sistema, conexiones no autorizadas (ej. Empleo de módems personales para servicios de Internet vía los enlaces conmutados de la organización).

Controles técnicos

Corresponden a todos aquellos controles que ejecutan los sistemas de cómputo propiamente. La implementación requiere de importantes consideraciones operacionales, y debe ser consistente con la administración de la seguridad de la organización.

- ✓ Identificación y Autenticación.
- ✓ Control de Acceso Lógico.
- ✓ Rastros de Auditoría.
- ✓ Criptografía.

Inventario de Activos

Uno de los principales pasos al inicio de cualquier plan de seguridad es el saber qué es lo que se quiere proteger.

Cada uno de los activos deben de ser debidamente identificados, así como su dueño o responsable y su nivel de seguridad definido.

Dentro de los sistemas de información podemos notar los siguientes activos a clasificar:

- ✓ Activos de Información: Bases de datos, y archivos de información, documentación de los sistemas, manuales de usuarios, material de capacitación, procedimientos de operación o soporte, planes de continuidad.
- ✓ Activos de software: Aplicaciones, sistemas operativos, herramientas de desarrollo, utilerías.
- ✓ Activos Físicos: Equipos de cómputo y comunicaciones, medios magnéticos (discos, cintas), otros equipos técnicos (aire acondicionado, fuentes de poder, etc.) mobiliario, instalaciones.
- ✓ Servicios: Servicios de cómputo y comunicaciones, iluminación, energía, aire acondicionado, etc.

Actividades Básicas de Administración

Con esto intentamos mantener la integridad y disponibilidad de los servicios de informática.

Los respaldos periódicos de los datos e información crítica deben hacerse regularmente. Se tiene que garantizar la recuperación de los respaldos de datos y software en caso de un desastre de cómputo o falla de la media. A nivel individual de cada sistema se deben considerar los siguientes lineamientos:

- ✓ Un nivel mínimo de información respaldada, junto con registros confiables de su contenido, los respaldos deben ser almacenados en sitios remotos en el evento de un desastre a las instalaciones del sitio principal. Por lo menos tres generaciones de los respaldos deben ser conservados para las aplicaciones más críticas.

- ✓ Los datos de respaldos deben de guardarse con un mínimo de protección física y ambiental consistente con los estándares del sitio principal.

- ✓ Los respaldos deben ser probados periódicamente con el fin de asegurar la recuperación de la información en el momento necesario.

- ✓ Los dueños de los sistemas deben de especificar los períodos de retención de los respaldos sobre todo de los sistemas más críticos.

Administración de la Red

Los administradores de la red deben garantizar la seguridad de los datos que viajan por la red implantando controles adecuados que incluso eviten las conexiones no autorizadas.

- ✓ La operación de las redes debe ser independiente de la operación de los sistemas de cómputo.

- ✓ Se deben establecer responsabilidades y procedimientos para el manejo de equipo remoto, incluso en áreas de usuarios.

- ✓ Controles específicos deben ser implantados para salvaguardar la confidencialidad e integridad de la información que viaja por redes públicas y proteger a los sistemas conectados.

- ✓ Las actividades de administración tanto de los sistemas de cómputo como de las redes deben ser coordinada con el fin de optimizar el servicio y que las medidas de seguridad son aplicadas de manera consistente en toda la infraestructura informática.

Control de Acceso a Redes

Los servicios de cómputo y red que pueden ser accesados por un usuario individual o desde un equipo en particular deberán ser consistentes con la política de control de acceso de la organización.

Ruta Forzada

El propósito de limitar rutas es el de evitar que los usuarios tengan acceso a servicios para los cuales éste no fue autorizado. Esto implica la ubicación de controles a lo largo de la ruta, como podrían ser:

- ✓ Asignación de líneas dedicadas o números telefónicos.
- ✓ Conexión automática de puertos a sistemas específicos o a gateways de seguridad.
- ✓ Limitación de opciones en menús y submenús.
- ✓ Prevenir el paseo ilimitado por la red.

Autenticación de usuarios y nodos remotos

Cualquier conexión vía redes públicas o externas a la organización deberá ser autenticada.

Protección de puertos de diagnóstico remotos. Deben existir controles estrictos para asegurar estos puertos, debiendo garantizar que serán accesados únicamente cuando sea acordado entre el Responsable del área y el personal de soporte de hardware o software.

Segregación en Redes. Conforme aumenta el tamaño de las redes en las organizaciones, y se extienden los accesos más allá de la propia organización se incrementan los riesgos de accesos no autorizados a aquellos sistemas de alto grado de sensibilidad. Un método para

lograr esto, consiste en la creación de diferentes dominios y perímetros de seguridad, pudiéndose controlar los accesos entre los diferentes dominios.

Control de conexión a redes.

Como soporte a las políticas de control de acceso de ciertas aplicaciones, puede llegar a ser necesario incorporar controles de acceso para restringir las capacidades de conexión de los usuarios, tales como el permitir el uso de correo electrónico únicamente; transferencia de archivos en un sentido; restricciones por fecha y hora, etc. Tales controles pueden implementarse por medio de gateways que filtren el tráfico por medio de reglas predefinidas.

Control de ruteo en redes.

Algunas redes compartidas pueden requerir la incorporación de controles de ruteo como garantía de que los flujos de información y las conexiones no vayan en contra de las políticas de control de acceso.

4.11. Atención a usuarios (help desk).

Atención a usuarios es una función que es una interfaz entre el área de informática y los usuarios finales. Esta acepta y registra llamadas de usuarios, da seguimiento a problemas y da al usuarios el status del trabajo, y en caso de ser necesario escala los incidentes a manejo de problemas para su resolución.

Los beneficios de soporte a usuarios son:

- ✓ Mayor productividad de los usuarios.
- ✓ Menos incidentes y problemas en la utilización de aplicaciones.

- ✓ Reducción en el tiempo de resolución de incidencias.
- ✓ Un solo dueño del problema reportado.
- ✓ Seguridad de que los problemas que han sido reportados fueron registrados y se esta trabajando sobre ellos.

4.11.1. Alcance.

El alcance de esta etapa es el de diseñar e implementar un servicio de atención a usuarios en donde, a través de un centro de llamas (call center) y con el apoyo de personal de soporte capacitado, se proporcione ayuda y capacitación a los usuarios de la red de datos y servicios informáticos que la componen.

4.11.2. Diseño.

Un centro de atención a usuarios comprende varias actividades que a continuación se definen:

Manejo de problemas.

Es un proceso encargado de la prevención y resolución de problemas y consiste en políticas, estándares y tecnología enfocada en evitar los problemas y resolverlos, registrar los errores conocidos, y proveer a la gerencia con reportes.

Los beneficios del manejo de problemas son:

- ☑ Mayor eficacia para el manejo de problemas que se refleja en una mejora de los servicios.
- ☑ Reducción del número de problemas.

- ☑ Tener una bitácora de soluciones a problemas.
- ☑ Poder dar seguimiento y correlacionar errores, determinar tendencias y evitar problemas de forma proactiva.

Control e implantación de infraestructura.

El control e implantación de infraestructura es una función que está encaminada al empaquetamiento y distribución de software y hardware.

Los beneficios son:

- ☑ La habilidad de monitorear y controlar licencias y versiones de software.
- ☑ La habilidad de empaquetar y distribuir software eficientemente.
- ☑ La habilidad de responder rápidamente a los requerimientos de clientes de nuevo o modificadas configuraciones de hardware PC, estaciones de trabajo y servidores.

Funciones de help desk

- ✓ Coordinar las actividades para la recepción e instalación y cambios de PCs y software en la compañía.
- ✓ Mantener el inventario de equipo y programas actualizado.
- ✓ Atender los requerimientos de los usuarios y asesorarlos en la definición de los mismos.
- ✓ Proporcionar las claves de acceso (passwords) a bases de datos y aplicaciones.
- ✓ Dar solución y seguimiento a problemas reportados por el usuario y mantener en buen funcionamiento el equipo de PCs y sus periféricos instalados.
- ✓ Asesorar a usuarios en la planeación de sus metas y presupuestos de gastos relacionados con sistemas, así como en convenios con clientes y proveedores.

- ✓ Difundir la cultura informática, implementar herramientas de usuario final y capacitarlos en su uso.
- ✓ Dar atención personalizada para la evaluación de requerimientos y optimización y aprovechamiento de los recursos instalados.

Todo esto con la finalidad de mejorar el servicio al cliente, centralizando y dando seguimiento a los reportes cotidianos de los usuarios.

Help desk requiere también de fuentes de información, por los tanto, para las externas se tiene:

- ✓ Internet.
- ✓ Proveedores externos.
- ✓ Revistas y diarios especializados en informática.

De las fuentes internas de información se tiene a:

- ✓ Los usuarios de todos los departamentos de la compañía.
- ✓ Las gerencias de sistemas.
- ✓ Las necesidades detectadas cuando se realiza consultoría.

Help desk requiere también de los sistemas de recursos humanos para la administración de su personal y del sistema de presupuesto de gastos para el estudio de factibilidad de proyectos.

Capítulo 5

Implementación

5.1. Red de área local (LAN).

A través de esta propuesta se busca una infraestructura que cumpla con los siguientes puntos:

- Implantar un estándar de red en toda la institución.
- Homologar los accesos a las diferentes fuentes de información sin importar la localización física del usuario debiendo ser transparente y sin necesidad de ninguna adecuación la consulta de la misma.
- Ofrecer un alto desempeño de la red de datos.
- Brindar una alta disponibilidad de servicios.
- Administración centralizada y dinámica.
- Planeación y crecimiento conforme a una tendencia tecnológica.

5.1.1. Cableado estructurado.

Como se puntualizó en la parte de análisis, se requiere una estrategia definida para lograr un máximo rendimiento en la operación de la red, tal estrategia se define a partir de los siguientes puntos:

- ☑ Levantamiento técnico.
- ☑ Reconocimiento.
- ☑ Levantamiento de Información.
- ☑ Visita Técnica.
- ☑ Diseño.
- ☑ Implementación.
- ☑ Instalación de ductos.

- ☑ Instalación de cable UTL nivel 5.
- ☑ Instalación de los elementos de conectividad.
- ☑ Pruebas.
- ☑ Diseño.
- ☑ Cierre del Proyecto.

Para la comunicación entre edificios se propone un enlace doble a través de fibra óptica multimodo, como se muestra en la Figura 5.1.

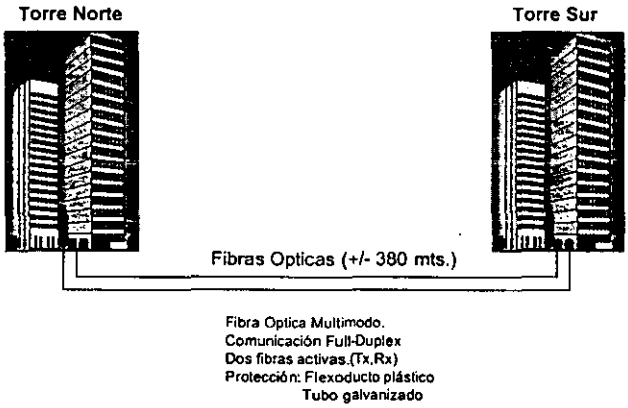


Figura 5.1. Enlace entre edificios centrales.

Para el cableado estructurado proponemos la instalación de fibras ópticas multimodo de cada uno de los armarios de telecomunicaciones hacia los equipos de concentración ubicados en los centros de cómputo de cada edificio para generar una arquitectura de columna vertebral (backbone) colapsada como se muestra en la Figura 5.2.

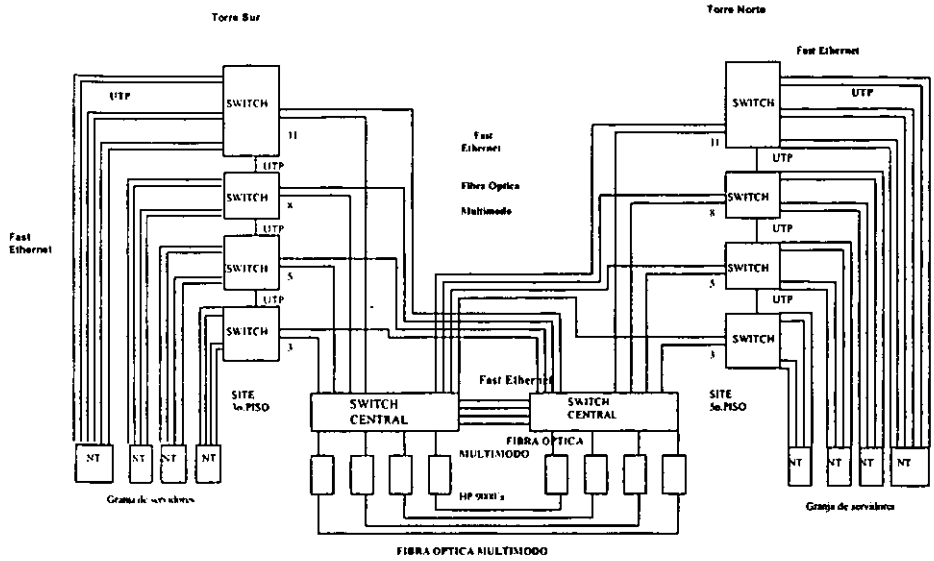


Figura 5.2. Cableado estructurado y dispositivos de concentración.

Adicionalmente, los equipos de concentración (switches) de cada piso tendrán conexión a ambas torres para contar con redundancia en la conectividad. La granja de servidores NT se concentraran el los centros de cómputo que contarán con servicios de corriente ininterrumpida (UPS), aire acondicionado, sistemas contra incendio y todas las restricciones de acceso necesarias para estos equipos. También los equipos HP9000 estarán instalados en este lugar.

Para realizar una red que asegure plenamente un buen funcionamiento de la misma es necesario tener medios de distribución como armarios de telecomunicaciones o ascendentes existentes. Con espacios suficientes para la instalación del equipo de red y de comunicaciones.

La distribución del cableado se realizará con canales de metal por lo perimetral de las oficinas que correrán a lo largo, pasando de oficina a oficina. Dichos canales permitirán un fácil acceso del cable usándose en áreas pequeñas en las cuales la mayoría de las tomas se colocarán en las paredes, donde la cubierta frontal del canal perimetral será removible, y donde las tomas podrán instalarse en cualquier lugar a lo largo del canal.

Este método que va desde el armario de telecomunicaciones a las tomas en las áreas de trabajo es económico y ofrece la mayor flexibilidad para la distribución de los cables.

Adicionalmente se realizará la perforación de paso con tuberías, o bien cualquier otro elemento para la guía del cable, lo que implica la perforación de piso, permitiendo el paso de los cables por dicho orificio hasta el espacio en el techo del nivel inferior, y/o superior, este método es utilizado para la interconexión de dos pisos.

Se realizará la instalación de ductos bajo piso para la comunicación (interconexión) entre edificios, de esta manera se hará el tendido de la fibra óptica para interconectar los diferentes closets que se crearán en los diferentes edificios, o en los diferentes pisos a conectar.

El tendido de la fibra óptica es un sistema de distribución autónomo que integrará los servicios de datos dentro de un conjunto de edificios (campus). El plan de distribución, incorporará el uso de equipos de conexión cruzada con subsistemas de fibra óptica como elementos primarios del sistema de distribución de un edificio.

Los elementos utilizados para distribución de fibra óptica son los siguientes:

Para conexiones:

- ✓ Conectores ST II y SC.

Para transmisiones:

- ✓ Cables de Interconexión de fibra (jumpers).

Para administración de circuitos:

- ✓ Unidades de conexión cruzada óptica.
- ✓ Unidades de interconexión óptica.
- ✓ Paneles de conectores de fibra óptica.
- ✓ Puentes de fibra simples.

Realizando el tendido de la fibra se procederá a interconectar entre sus extremos, las unidades de interconexión de fibra (LIU), que son el equipo estándar de conexión cruzada óptica las cuales están diseñadas para cables trenzados y de puentes, así como también empalmes al conector.

El cable de conexión cruzada nos permitirá conectar cada fibra entrante con una fibra saliente mediante un cable de puente de casquillo a casquillo (patch cord de fibra), el campo de conexión cruzada constará de un solo módulo, en donde cada módulo terminarán 6 fibras.

La longitud recomendada para el cable de interconexión de fibra usado como puente al módulo de conexión de fibra será de tres metros.

Los sistemas de fibras ópticas ofrecen lo más avanzado en canales de comunicaciones de datos. Esta tecnología ha demostrado ser extremadamente confiable para transmitir grandes cantidades de datos a largas distancias con costos

relativamente bajos. Además de su extraordinaria capacidad para transmitir datos, los sistemas de fibra óptica ofrecen la inmunidad a EMI (interferencia electromagnética) y a RFI (interferencia de radiofrecuencia).

Descripción para voz y datos.

Las configuraciones típicas de conexión cruzada incluyen las descripciones de los equipos a utilizar, así como la alternativa más apropiada para satisfacer las necesidades, tales como las aplicaciones, velocidad, tráfico y el lugar físico de la instalación.

Por lo que debemos considerar que las tomas (rosetas) situadas en el área de trabajo de los usuarios y en otras salas, terminan al subsistema de cableado horizontal brindando un punto universal de acceso para conectar los servicios de voz y datos o video para terminar en el sistema de distribución.

La ubicación y el tipo de equipos usados para construir campos de conexión cruzada, influyen directamente en la forma en que el sistema de distribución se administra con la capacidad de realizar cambios fácilmente en respuesta a las necesidades de reubicación de personal o equipos dentro de un edificio, este punto es cada vez más importante puesto que los costos de efectuar estos cambios aumentan constantemente. Una manera de reducir los costos, consiste en eliminar las necesidades de diversos tipos de medios de transmisión desde el armario de telecomunicaciones hasta el área de trabajo mediante el uso uniforme de UTP de 4 pares y fibra óptica.

El equipo de conexión cruzada es el que se instalará para el armario de telecomunicaciones de cableado ascendente y las terminales de la sala de equipos.

Para el tendido de cable de cobre UTP sus componentes típicos de un sistema son los siguientes:

Sistemas verticales

- ☑ Cable UTP nivel 5 para datos y voz.
- ☑ Cable de Fibra Óptica de 12 hilos de 62.5/125 micras.
- ☑ Racks de Distribución, paneles conmutadores y cajas de terminación.
- ☑ Cables de Puenteo y cables de conexión temporales.

Sistemas Horizontales

- ☑ Cables horizontales.
- ☑ Paneles de Parcheo y cajas de terminación.
- ☑ Blocks 110 para ponchado para voz con soportes de montaje.
- ☑ Paneles de parcheo para Datos sin soportes de montaje.
- ☑ Salidas información multimedios.
- ☑ Conjunto de cables para puenteo y cables de parcheo temporales.

Conectores

- ☑ Tipo ST.
- ☑ Jacks tipo nivel 5.
- ☑ Capaz de hacer conexión de una o varias salidas.
- ☑ Capaz de acoplarse y desacoplarse más de 200 veces.

Equipos de conexión

- ☑ Para el montaje en las paredes, en los bastidores o en otros tipos de cuadros de distribución.

- ☑ Proporcionar un medio para interconectar corridas de cables con los de puenteo de interconexión.
- ☑ Permite una buena administración de los cables de puenteo.
- ☑ Poseen elementos de protección a las conexiones.

De esta forma se reducen los costos que permiten hacer cambios de circuitos en el campo de conexión cruzada sin necesidad de herramientas especiales o técnicos altamente entrenados. Con esto se cubren las necesidades actuales y futuras descansando sobre un sistema de cableado organizado, pertinentes de la industria.

Normativa utilizada (EIA/TIA 568)

Las normas vigentes y los productos que se utilizarán, se basan en cableado de par trenzado, sin blindar de 4 pares. Los requisitos de categoría 5 se especifican en la norma EIA/TIA 568 /Julio 1991) y se aplica en:

- ☑ Arquitectura de cableado en general.
- ☑ Cables (cordones).
- ☑ Accesorios de conexión.

El estándar EIA/TIA-568 requiere de una topología física en estrella. Los elementos del sistema de cableado incluyen:

- ☑ El cableado horizontal.
- ☑ El cableado de "backbone".
- ☑ El área de trabajo.
- ☑ Los armarios de telecomunicaciones.
- ☑ Las salas de equipo.
- ☑ Los puntos de administración.
- ☑ La infraestructura de entrada.

Las distancias máximas de cable especificadas por el estándar EIA/TIA-568 para UTP se indican a continuación:

- ☑ Cableado horizontal: 90 m.
- ☑ Cableado de "backbone": 800 m.
- ☑ Área de Trabajo: 3 m.

Clóset de telecomunicaciones

- ☑ Terminación de horizontal: 7 m.
- ☑ Del horizontal al "Backbone": 6 m.
- ☑ Salas de equipos: 20 m.
- ☑ Puntos de administración.
- ☑ Conexión cruzada principal (MC): 20 m.
- ☑ Conexión cruzada intermedia (IC): 20 m.

Método Técnico para la Instalación de Canalizaciones

Ductos - Los tramos de ducto no deben tener más de 30 m de longitud ni más de dos codos de 90° entre los puntos o cajetes de acceso. El radio interno de los codos debe ser por lo menos 6 veces el diámetro del conducto. En el caso de ductos de más de 50 mm (2 pulgadas) este radio debe ser por lo menos 10 veces el diámetro del ducto. Con el fin de minimizar la tensión del cable y evitar que éste se deteriore o rompa, es importante emplear los equipos adecuados y seguir los procedimientos correctos.

Distribución en el techo - Por encima de cielos rasos pueden colocarse ductos, escalerillas porta cables y cualquier otro medio que se emplee como trayecto para los cables, pero lo más frecuente es que el cable cuelgue libremente. En este último caso, se requieren accesorios de soporte apropiados (ganchos en J, anillos etc.).

Los cables no deben tenderse directamente sobre las planchas, los rieles o los soportes del techo, a menos que éstos hayan sido diseñados específicamente para servir de apoyo a los cables.

En el sistema de cableado estructurado de la CNBV, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella, facilitando la interconexión y la administración del sistema. Esta disposición permite la comunicación con virtualmente cualquier dispositivo, en cualquier lugar y en cualquier momento.

En la Figura 5.3. se muestra la estructura actual del cableado y en las Figuras 5.4 y 5.5. la esperada al finalizar la instalación del cableado estructurado.

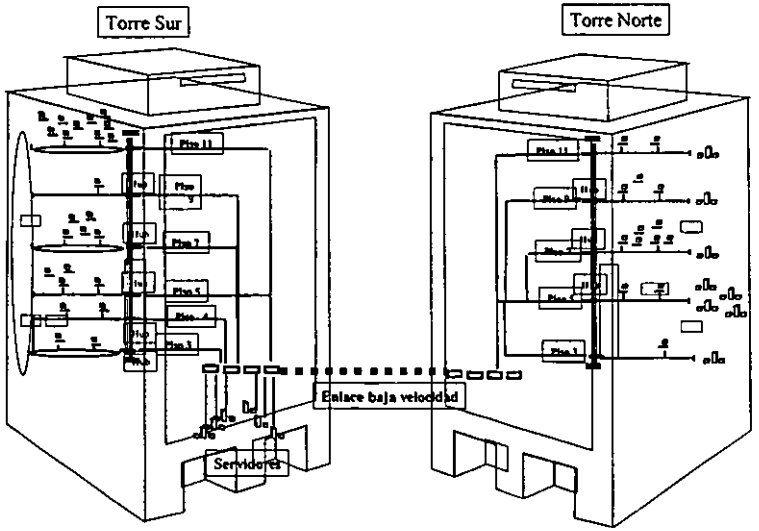


Figura 5.3. Estructura de red actual.

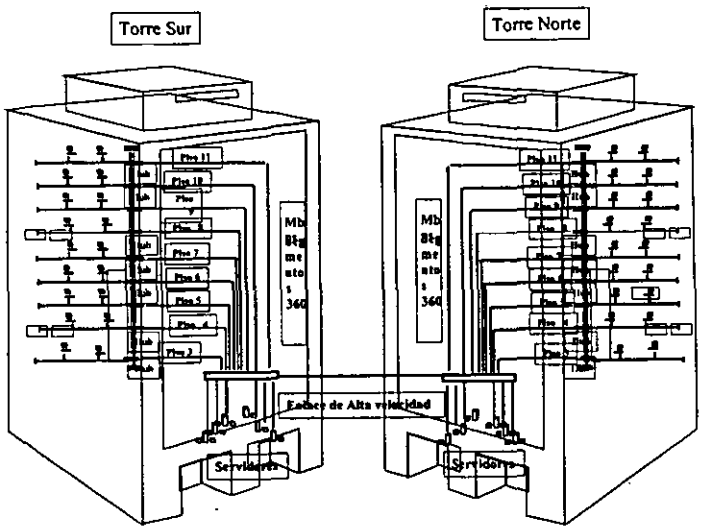


Figura 5.4. Vista física de la estructura de red a obtener.

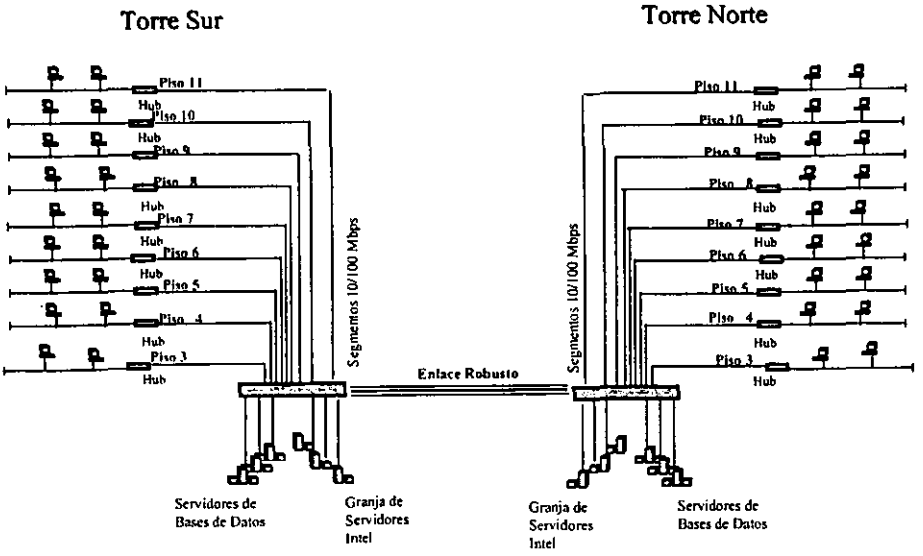


Figura 5.5. Vista lógica de la estructura de red a obtener.

5.1.2. Topología y equipo activo.

Se propone la siguiente topología y estructura informática:

Torre Norte: Continuar con la topología Ethernet para los servicios a usuarios.

Torre Sur: Migrar de Token Ring a Ethernet (10BaseT).

Enlace entre Torres: Modificar el actual enlace Ethernet a Fast Ethernet (100BaseT).

Servidores Unix y NT: Incorporarlos a Fast Ethernet.

Requerimientos :

Torre Sur

Partiendo de que se tiene instalado cableado estructurado, rosetas y jacks nivel 5 en todo el edificio, se propone la siguiente estructura y equipamiento:

- ☑ Cambio de topología token ring a ethernet.
- ☑ Instalación de módulos Ethernet en el switch de Token Ring.
- ☑ Conversión del backbone de fibra óptica a vertical colapsada de fibra óptica.
- ☑ Implantación de un sistema de redundancia en la red.

Equipamiento necesario

- ☑ Módulos Ethernet para concentrador Synoptics.
- ☑ Switch Ethernet y Fibra óptica (para realizar bus colapsado) con 2 puertos 100BaseT.
- ☑ Un ruteador capaz de soportar puertos 10baseT y 100baseT y Token Ring para la migración de usuarios y servicios.

Torre Norte

En Torre Norte existe vertical de fibra óptica, 10 hubs instalados (5 en cada nivel), un switch que maneja puerto 10BaseT, se propone la siguiente estructura y equipamiento:

- ☑ Cambio del switch con puertos 10BaseT a uno que de soporte a puertos 100BaseT.
- ☑ Reubicación del switch para realizar tareas de segmentación de la red.
- ☑ Implantación de un sistema de redundancia en la conexión entre hubs y el switch.

Equipamiento necesario

- ☑ 1 Switch Ethernet y Fibra óptica (para realizar la concentración de las redes de los pisos) con 2 puertos 100BASET.
- ☑ Un ruteador capaz de dar soporte a puertos Ethernet y FastEthernet.

Etapas

Cambio del actual enlace entre torres a través de un puerto LAN Ethernet que corre a 10 Mbps a dos de Fast Ethernet. Para lo cual es necesario:

- ☑ Tendido de una segunda fibra óptica que una ambas torres.
- ☑ Enlace de 2 ruteadores (uno en cada torre) a través de Fast Ethernet utilizando ambas fibras. Para no cortar el servicio, se empezaría con la nueva fibra, se realizarían pruebas y en cuanto quedara lista se cambiará la conexión de torres a ésta, para realizar el cambio con la fibra actualmente en operación.

Cambio de switch de torre Norte a uno que dé soporte a puertos 100baseT.

- ☑ Esto se podría realizar en forma paulatina y por segmentos.
- ☑ Redundancia a través de servidores. Cada servidor tendrá dos tarjetas de red: una irá al hub central y la otra irá a un hub de otro nivel.

Funcionamiento de ambas topologías en torre Sur.

- ☑ Cambio de módulos Token Ring a Ethernet en los concentradores de cada segmento.
- ☑ Instalación del switch.
- ☑ Cada nivel se conectará al switch a través de cable UTP nivel 5.
- ☑ El switch se conectará a un puerto del ruteador que hará la conversión de Token Ring a Ethernet.
- ☑ Poco a poco se irán cambiando las tarjetas de la red de Token Ring a Ethernet y cambiando su acceso del switch de Token Ring al módulo de Ethernet.
- ☑ Al finalizar la tarea anterior, se procederá a convertir el backbone de fibra óptica a vertical de fibra óptica.
- ☑ Finalmente, los switches se interconectarán a través de la vertical de fibra óptica y se generará la redundancia a través de los servidores.

Futuro :

La emigración de toda la red a nuevas tecnologías tales como :Fast Ethernet, ATM o Gigabit Ethernet, para lo cual será necesario cambiar todas las tarjetas de red instaladas, más no el cableado.

5.2. Red de área amplia (WAN).

La infraestructura instalada presenta algunas limitaciones en cuanto a capacidad y seguridad en el acceso de información.

La creciente demanda de envío-recepción de información a través de medios electrónicos para la comunicación de datos, ha hecho que las capacidades de los equipos destinados a ello empiecen a verse rebasadas y con la imposibilidad de ampliarlas dadas las características propias de estos equipos.

Aunado a esto, el servicio de interconexión entre instituciones y CNBV se ha incrementado, lo que ocasiona sobrecarga a determinadas horas y/o días y, por ende, molestia entre los usuarios del servicio, ya que su transmisión se vuelve lenta o bien tienen que esperar a que algún medio este disponible para poder realizarla.

Así mismo existen servicios de interconexión entre la CNBV y las oficinas metropolitanas como con algunas autoridades financieras como Banco de México y la S.H.C.P. y varios servicios de información importantes para el seguimiento de los mercados (Reuters, Infosel, Bloomberg, Bolsa Mexicana de Valores, etc.). Esto complica la prestación de este servicio a las diversas instituciones del sistema financiero ya que la obsolescencia y falta de capacidad para crecer en su configuración y equipamiento impide contar con un conexión transparente y natural con la nueva infraestructura de la red de cómputo de la CNBV.

Adicionalmente, se pretende contar con la infraestructura para tener enlaces directos con cada una de las oficinas estatales que componen a la Comisión. Obviamente, los equipos actuales no tienen capacidad para ello.

5.2.1. Propuesta de solución.

Se debe adquirir el equipo de comunicaciones necesario que permita contar con una infraestructura actualizada y completa, que satisfaga las demandas actuales de comunicación con las entidades financieras así como con el personal que realiza la supervisión in-situ, para que desde cualquier punto y con los medios necesarios (líneas telefónicas, RDI, Frame Relay, etc.) logre conectarse a la red de cómputo de la CNBV de manera segura y transparente.

En la tabla 5.1. se muestran las características generales de los equipos de comunicaciones.

EQUIPO	CARACTERÍSTICAS
Servidores de acceso remoto	Soporte de al menos 100 usuarios concurrentes. Distribuidos en ambas Torres. Configurables por puerto: velocidad, protocolo, norma, etc. Esquemas de seguridad en el acceso: Radius o TACACS. Multiprotocolo: PPP, SLIP, etc. Protocolos de red : TCP/IP e IPX. Puertos LAN : Etnernet
Módems	Soporte de las siguientes normas : Datos : ITU-T V.34, V.32 bis, V.32, V.23, V.22 bis, V.21, Bell 212 A , Bell 103 ITU-T V.42/V.42 bis y MNP 2 al 5, V.42/V.42 bis para la corrección de errores. Compresión de datos para alcanzar 115.2 Kbps MNP del 2 al 5 Operación full-duplex asíncrona/síncrona a 2 hilos. Compatible con Hayes Velocidad 56 Kbps. Soporte de comandos AT Interfase digital : conforme a EIA-232D e ITU-T V.24

Tabla 5.1. Especificaciones técnicas de los equipos de comunicaciones.

EQUIPO	CARACTERÍSTICAS
Ruteadores principales	Distribuidos en ambas torres. Tolerantes a fallas. Puertos WAN configurables. Protocolos de ruteo : RIP, OSPF, EGP, etc. Circuitos : Frame Relay, X.25, Ethernet, Token Ring, Point to Point, PPP,SMDS, etc. Equipado con los siguientes puertos: 4 accesos a LAN Ethernet (TCP/IP e IPX). 10 puertos seriales

Tabla 5.1. Especificaciones técnicas de los equipos de comunicaciones (continuación).

Con esto se permitirá el enlace de las oficinas metropolitanas y demás servicios para autoridades y servicios de información a la red de cómputo de la CNBV, aprovechando las características de la nueva red e interconectándose de manera natural y 100% integrada y segura.

Este proyecto contempla la utilización de diversas opciones para el adecuado funcionamiento de la estructura final de comunicaciones. Por un lado se requiere homologar y fortalecer el equipamiento hacia la tecnología actual y utilizar los "estándares" establecidos en el Sector Financiero Mexicano. Para esto existen diversos fabricantes que ofrecen soluciones integrales. La solución a implementar debe considerar los siguientes puntos:

- Equipamiento de ruteo: puertos seriales y de red.
- Equipamiento de acceso remoto: módems, líneas telefónicas y puertos en equipo.
- Medios de transmisión adecuados a los servicios que serán proporcionados.
- Redundancia y/o equipos de respaldo.
- Alta disponibilidad.
- Capacidad de actualización a nuevas tecnologías.

Adicionalmente, se requiere implementar un sistema de seguridad integral de acceso que abarque a cualquier tipo de transmisión que se realiza desde o hacia instituciones, proveedores o cualquier tipo de servicio remoto. En este rubro se debe contar con sistemas de protección tales como: firewall, servidor con seguridad TACACS+ o RADIUS para controlar el acceso remoto vía módem, listas de acceso en ruteadores y filtros en equipos de comunicaciones. Estos deben contar con la característica de ser redundantes y suficientemente robustos para atender la demanda de acceso.

Finalmente se debe contar con una plataforma de administración y monitoreo general para la detección oportuna de fallas y/o alarmas en la infraestructura de comunicaciones.

La estructura de comunicaciones propuesta es la que se muestra en la Figura 5.6.

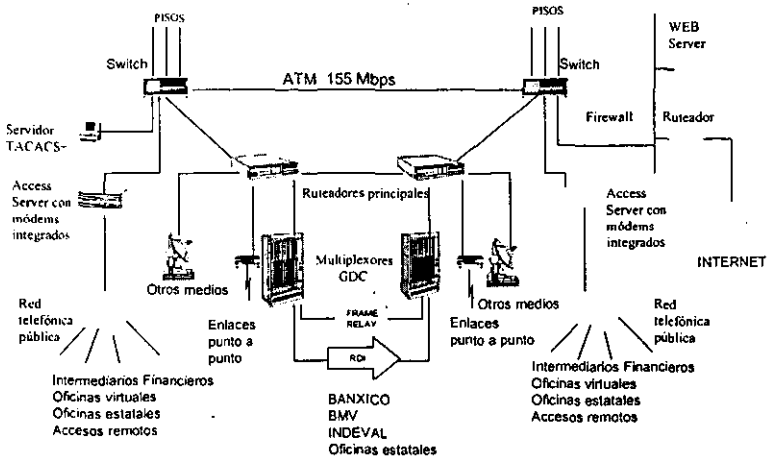


Figura 5.6. Estructura de comunicaciones propuesta.

Este proyecto contempla el incremento de líneas telefónicas en los equipos Access Server de las torres norte y sur a fin de hacer un total de 120 puertos disponibles para la conexión vía módem hacia la Comisión. Debemos incrementar la seguridad en este acceso para garantizar la confidencialidad e integridad de la información recibida. Esto se logrará a través de los perfiles de usuarios remotos, permisos, tiempos de conexión y su adecuada autentificación. Adicionalmente, debemos estudiar la posibilidad de utilizar otras herramientas de seguridad tales como tokens cards, a fin de reforzar la seguridad.

Por otro lado, requerimos homologar la plataforma de administración y monitoreo del equipo de comunicaciones con la de la infraestructura de red interna, a fin de centralizarla y utilizar herramientas similares y/o compatibles. Se debe capacitar al área de Operación en estas herramientas porque, al final, ellos realizarán este monitoreo. La generación de procedimientos de operación y escalación de fallas, facilitará el correcto funcionamiento de la infraestructura de comunicaciones.

Finalmente, es necesario segmentar lógicamente la red a través de hardware (firewall) y utilizando direccionamiento IP diferente, a fin de mejorar la seguridad en los accesos y evitar intrusiones. En la Figura 5.7. se muestra la propuesta para esta segmentación.

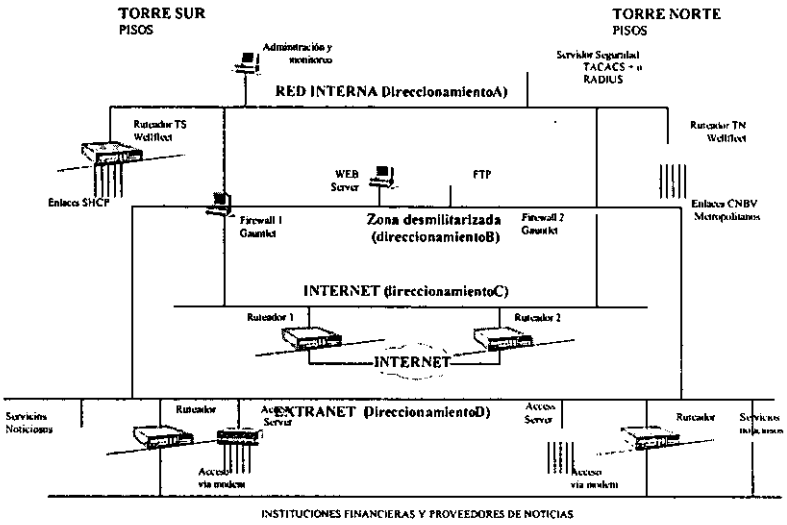


Figura 5.7. Estructura lógica y segmentación de la red de comunicaciones.

5.2.2. Características de la red de Comunicaciones.

☑ Frente común de comunicaciones con soporte a servicios a través de:

Acceso remoto vía dial-up para soportar al menos 120 usuarios concurrentes.

Enlaces vía líneas privadas, RDI, Frame Relay y ATM.

Interconexión de alta velocidad con oficinas metropolitanas y estatales.

Soporte a nuevas tecnologías.

- ☑ Redundancia de enlaces y equipo de comunicaciones.

  Respaldo en los enlaces externos.

  Balanceo de cargas en el acceso remoto.

  Redundancia en el equipo front-end de comunicaciones.

  Switcheo automático en caso de fallas.

  Flexibilidad para incrementar los anchos de banda de cada enlace de acuerdo a necesidades.

- ☑ Alta seguridad en el acceso a la LAN de la CNBV.

- ☑ Optimización de recursos y anchos de banda de cada enlace.

5.2.3. Red de telecomunicaciones del sistema financiero mexicano.

La actual red de telecomunicaciones del sistema financiero mexicano (Figura 5.8.), tiene las siguientes características:

- Diversidad de redes de Comunicaciones: BANXICO, BMV, TEI, INDEVAL, etc.
- Falta de estandarización.
- Cada institución debe contar con un enlace hacia cada una de las redes de Comunicaciones a la cual quiere tener acceso.
- Cada red proporciona diversos servicios a diferente número de usuarios.
- Diversidad en equipos de comunicaciones.

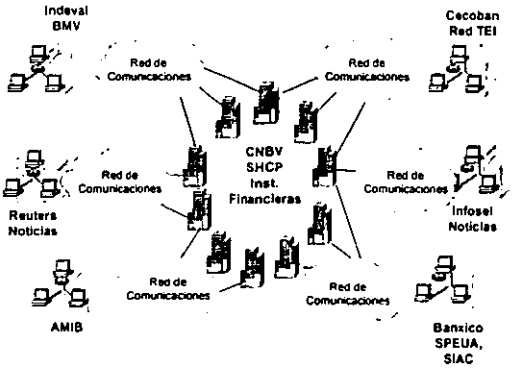


Figura 5.8. Actual red de telecomunicaciones del sistema financiero mexicano

Existe el proyecto de integrar cada una de las redes locales de cada institución, organismo o proveedor financiero en una gran red financiera de alta velocidad, probablemente a través de Frame Relay o ATM.

Esta red reunirá a todas las entidades financieras del país, así como proveedores de servicios, como se muestra en la Figura 5.9.

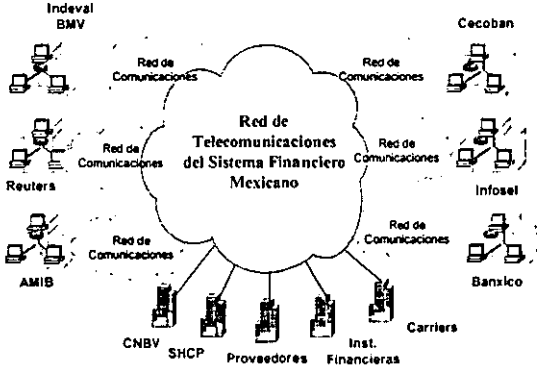


Figura 5.9. Futura red de telecomunicaciones del sistema financiero mexicano

Todos los participantes estarán interconectados a través de una red de telecomunicaciones de alta velocidad lo que asegurará una comunicación eficiente y de alta disponibilidad.

Esta tecnología permitirá el tráfico simultáneo de voz, video y datos (Figura 5.10.). Esto significa que, además de poder acceder a los diversos sistemas en tiempo real, los usuarios de la red podrán establecer comunicación telefónica y realizar sesiones de videoconferencia; todo operando en una sola plataforma de comunicaciones.

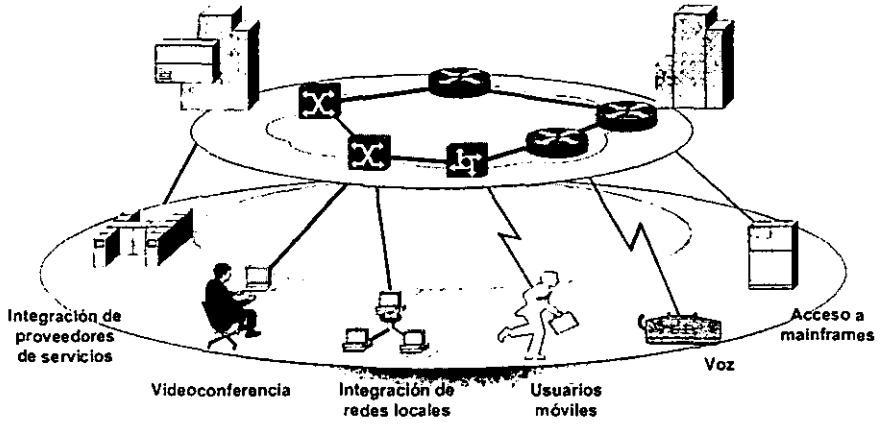


Figura 5.10. Servicios que proporcionará la red de telecomunicaciones del sistema financiero mexicano

Algunos beneficios serán los siguientes:

- Red Privada de Telecomunicaciones que permita el tráfico de video, voz y datos, entre todas las instituciones que conforman el Sistema Financiero Mexicano.

- Promover una mejor integración de las instituciones que participan en el mercado financiero.
- Permitir el acceso rápido y eficiente de los proveedores de servicios financieros.
- Unificar políticas, usuarios e infraestructura en una plataforma de Telecomunicaciones eficiente.
- Proveer una comunicación ágil, sencilla y económica entre los participantes del mercado financiero.
- Correo electrónico integral.
- Alta disponibilidad al contar con un servicio funcionando las 24 horas del día los 365 días del año.
- Alta Seguridad y un sistema de redundancia en los medios de transmisión.
- Utilización de la tecnología más moderna e infraestructura 100% digital.

5.3. Equipamiento personal.

Actualmente la CNBV cuenta con 290 equipos personales obsoletos para el tipo de aplicaciones y servicios estándar, los cuales incluso resulta infructuoso mantener en buen estado funcional. Si a esto sumamos que los requerimientos de las distintas áreas en cuanto a equipamiento de cómputo como herramientas para el acceso y explotación de los sistemas de información, y para incrementar la productividad del personal mediante el uso de los distintos servicios que pueden ofrecerse con y a través de estas, asciende a más de 160 equipos, resulta imperativo dotar de más infraestructura de cómputo personal a la Comisión.

Es necesario la adquisición de un total de 400 computadoras personales que actualicen este lote de equipo y satisfagan la demanda interna, redistribuyéndolos de acuerdo a necesidades específicas del personal.

Otro rubro importante y que se ha incrementado en función de los servicios de red es el de impresión, para el cual se requiere adquirir 45 impresoras de tipo láser, a efecto de satisfacer la demanda, incrementar la productividad del personal y equipos, sustitución de equipo obsoleto imposibilitado de una conexión a red y brindar una optima calidad de impresión.

Por otra parte, el equipo destinado a la labor de supervisión in-situ (laptops), esta limitado a unos cuantos. Comparativamente, el número de computadoras portátiles es inferior en un 60% aproximadamente respecto al número de supervisores o personal que requiere de esta clase de equipos, por lo que se hace necesario acercar a dicho personal a este tipo de tecnologías, fortificando la labor de supervisión mediante la designación de recursos informáticos que permitan el acceso a información y sistemas de la CNBV de manera remota, con la facilidad de la portabilidad que estos ofrecen, por lo que es necesario ampliar el número de computadoras portátiles en 50 objeto de esta justificación, para dotar de equipo a más supervisores y personal que se encarga de la labor de supervisión in-situ.

5.3.1. Especificaciones de la propuesta.

Se deben adquirir el equipo de cómputo personal y portátil con las características de almacenamiento, procesamiento y comunicaciones que garanticen la operación y sistematización de las actividades de las áreas usuarias.

Un dato adicional es el que muestra el parque instalado de 1200 equipos personales en la CNBV, de los cuales 900 son de la marca Hewlett Packard, sin considerar el equipo por sustituir, lo que representa un 70% a nivel Comisión.

También se debe considerar la adquisición de impresoras tipo láser, con características de ser incorporadas a la red de datos, permitiendo establecer grupos de impresión por piso o por área usuaria, lo que nos permitirá optimizar el servicio de impresión en la cantidad y calidad necesaria para la emisión de reportes y documentos generados por el personal en sus actividades cotidianas.

Los equipos a adquirir deberán tener mínimo, las siguientes características:

- Computadora Personal Pentium II a 400 MHz, 64 MB de RAM, 4 GB en disco duro, con USB (Universal Serial Bus) tarjeta de red Ethernet 10/100 Mbps y accesorios multimedia.
- Impresora Láser capacidad de impresión de 24 ppm, procesador a 40 MHz RISC, 12 MB de RAM, resolución 600 dpi, 3 alimentadores de hojas con capacidad combinada de 1100 hojas.
- Computadora Portátil Pentium II 366 MHz, 64 MB de RAM, 4 GB en disco duro, unidad de CD 6x tarjeta de red, fax módem V.90 y accesorios.
- Digitalizador de Imágenes carga automática de hojas, capacidad de 8 hojas ppm,

5.4. Equipamiento central.

5.4.1. Actualización de Centros de Cómputo.

Actualmente se cuenta con una infraestructura poco robusta para dar soporte a las cargas de trabajo dentro de los equipos centrales, ya que el crecimiento en cuanto a requerimientos y necesidades se ha ido incrementando de una manera acelerada. Los equipos se encuentran a un 90% de su capacidad y con pocas opciones para incrementar los recursos debido a que la vida útil de los equipos es de 5 años y varias máquinas están por cumplirla.

Por lo anterior, la tecnología utilizada para realizar tareas de respaldo es obsoleta y por lo tanto se hace necesario buscar nuevas herramientas que nos permitan tener un mayor desempeño en esta área.

Adicionalmente existen dos plataformas de cómputo central: AS400 de IBM con protocolo SNA y equipo HP9000 de Hewlett Packard con protocolo TCP/IP y sistema operativo Unix.

Aunado a esto los equipos no cuenta con la capacidad de ser tolerantes a fallas, y las aplicaciones y requerimientos que actualmente se maneja en la Institución requieren tener este tipo de servicios.

Otro factor determinante en este proyecto es la migración de aplicaciones, debido a la fusión de las Instituciones. Por esta razón es determinante la migración de aplicaciones para homologar las tecnologías de bases de datos, ya que anteriormente cada una se manejaba independientemente.

Es necesario considerar un crecimiento en los centros de cómputo y sus capacidades para albergar nuevos equipos (Comunicaciones, Equipo Central, Servidores de correo, etc) ha sido sobrepasada, como podemos observar dentro de los Centros de Cómputo.

De acuerdo a los recursos establecidos, se han venido implementado los sistemas desarrollados en Sybase, los servidores de Lotus-Notes, aplicaciones administrativas, hasta el punto de contar con equipo en préstamo; sin embargo la demanda de requerimientos por parte de las diferentes usuarias se hacen cada día mas constantes.

Se debe considerar la adquisición de un servidor Unix que se integre de manera natural y transparente al esquema de prevención de fallas, capacidad de multiprocesamiento, respaldo de información en línea, información espejeada, etc., que se ha armado con el proceso de licitación de recursos propios, y sobre el cual se implementaría el proceso de Intercambio Electrónico de Información Financiera por una parte, y por otra se balancearían aún más las cargas operativas cotidianas resultado de los sistemas CNBV.

La actualización de la estación de trabajo ampliando su capacidad de proceso y almacenamiento es algo vital para optimizar las labores de operación, administración y monitoreo que se efectúan en el centro de cómputo.

5.4.2. Beneficios a obtenerse.

Al tener esta infraestructura nos ayudara a mantener un servicio de óptima calidad que se verá reflejada en el aprovechamiento por parte de los usuarios de los equipos. Además se podrá garantizar el crecimiento homogéneo entre las necesidades de la Institución y la capacidad de cómputo central. Homologación dentro de los equipos para

las aplicaciones que se esperan introducir en este año. Por otro lado se podrá contar con un esquema de redundancia entre servidores y centros de cómputo.

Mantener un balanceo de cargas adecuado para no saturar la capacidad de los equipos, introducir nuevas tecnologías en las aplicaciones como son: Sybase, Lotus Notes y la versión de sistema operativo HP-UX. Ampliar la capacidad física de los centros de cómputo para poder alojar una mayor cantidad de equipo y hacer una reorganización de los equipos existentes.

Contar con la capacidad de proceso y almacenamiento adecuado para los requerimientos de manejo de grandes volúmenes de información, necesarios en las tareas de recepción y carga de información que se realizan como parte del proceso de supervisión del sector financiero nacional.

Operación y servicio continuos para las aplicaciones de recepción y carga de información financiera en beneficio de las áreas usuarias, al contar con las características de tolerancia a fallas y respaldo de información automática, complementando la compra hecha con recursos propios.

Trasparencia de la migración de las aplicaciones de recepción y carga de información actuales a lo nuevos equipos, en beneficio de los las actividades de las diferentes áreas usuarias de la CNBV.

5.4.3. Alta disponibilidad.

Para implementar esquemas de alta disponibilidad en cómputo central, existen dos soluciones principales:

Instalación con EPS:

Ventajas:

a) Redundancia entre equipos.

b) Utilización de arreglos de discos.

c) Tolerante a fallas.

d) Instalación en un solo centro de cómputo.

e) Distribución de carga en los equipos.

Desventajas:

a) Supeditado a una sola tecnología FDI.

b) Redundancia a través de dispositivos externos en la misma tecnología.

c) No tiene espejeo entre servidores.

d) No realiza monitoreo de los recursos.

e) Capacidad de 2,500 transacciones.

Instalación con Clusters:

Ventajas:

a) Redundancia de información.

b) Monitoreo de los recursos.

c) Espejeo de información.

d) Asignación dinámica de recursos.

e) Tolerante a fallas.

f) Adaptable a cualquier tecnología.

g) Capacidad de 8,000 transacciones.

h) Desempeño en red adaptable a la tecnología.

Desventajas:

a) Introduce tráfico dentro de la red.

b) Distancia entre clusters limitada.

c) Redundancia de equipo a un costo elevado.

Solución Propuesta:

La propuesta que resulta más viable es a través de clusters, ya que permite asignar recursos dinámicamente, además de tener una redundancia entre equipos a través de un arreglo de discos de alta disponibilidad. Por otro lado tiene una disponibilidad de casi el 100 %.

La propuesta puede ser modificada, de tal forma de que en vez de que sean cuatro equipos de las mismas capacidades, se puede llegar a manejar una máquina robusta que cumpla con los requerimientos para crear el centro de cómputo alterno. En caso de contingencias, los equipos pueden ser conmutados de uno a otro, en situación de pérdida del cluster principal, entraría en operación el cluster redundante.

En la fig. 5.11. se muestra un esquema de la solución.

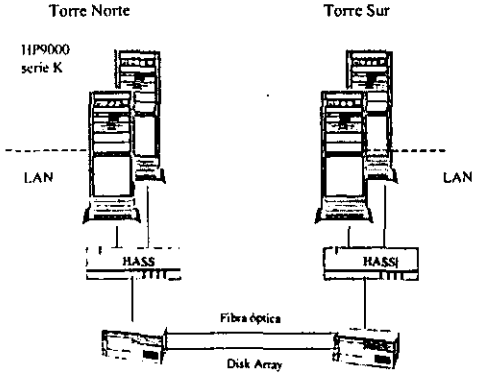


Figura 5.11. Cluster entre equipos centrales HP900 y arreglo de discos Hass.

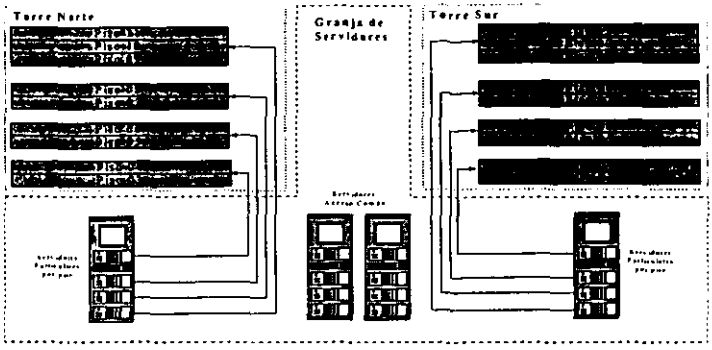
5.5. Servidores departamentales.

5.5.1. Implementación.

Se propone implementar una solución basada en una estrategia desarrollada por el personal de la CNBV y con el apoyo de proveedores externos que permita cubrir los requerimientos de los usuarios. Esta infraestructura esta pensada para ser vigente cuando menos en un lapso de 3 años y aún venciendo éste plazo permita ser actualizada.

Una infraestructura de cómputo distribuido (granja de servidores) de las *oficinas centrales* y *oficinas metropolitanas* (fig. 5.12.), consistente de servidores que ofrezcan servicios de *automatización de oficina* tales como: paquetería (word, excel, powerpoint), servidores de impresión, aplicaciones propias, archivos compartidos, administración de la infraestructura de cómputo personal (inventario de equipo, distribución de software, soporte remoto), fax en red, publicación de información institucional (servidor para intranet e internet) y bases de datos departamentales.

Oficinas Centrales (Plaza Inn)



Oficinas Metropolitanas

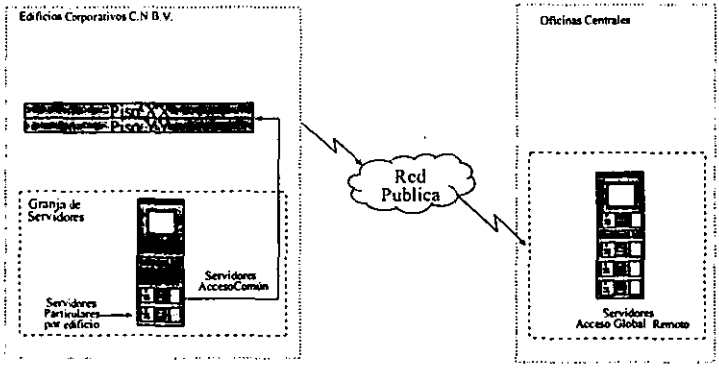


Figura 5.12. Modelo propuesto para la implementación de una granja de servidores departamentales.

Especificaciones físicas

Servidores Particulares.- Es el servidor que dará servicio por segmento (cada 2 pisos), proporcionando la facilidad de trabajar con aplicaciones particulares por piso y que no son aplicaciones de acceso común:

- Servicio de impresión.
- Aplicaciones propias de cada área de la CNBV.
- Administración de cómputo personal (distribución de software).

Servidores de acceso común.- Son los servidores que proporcionarán servicios de acceso general.

- Transferencia electrónica de información.
  - Correo electrónico.
  - Formas Electrónicas.
  - Conectividad con Internet.
- Fax.
- Archivos compartidos
- Administración de cómputo personal.
  - Distribución de software.
  - Inventario de equipo y aplicaciones.
  - Herramientas de Soporte.
- Publicación de información institucional interna.
- Bases de datos departamentales.
- Respaldo y pruebas.

Oficinas Centrales (Plaza Inn)

- ✓ Servidores centralizados bajo el concepto de granja.
- ✓ 8 Servidores particulares por torre distribuidos como se muestra en la tabla 5.2.

UBICACIÓN	NO. DE SERVIDORES PARTICULARES	PISOS
	1	3,4
Torre	1	5,6
Norte	1	7,8
	1	9,10,11
	1	3,4
Torre	1	5,6
Sur	1	7,8
	1	9,10,11

Tabla 5.2. Distribución de servidores particulares.

✓ 10 Servidores de acceso común brindando servicios de acuerdo a la tabla 5.3.

NO. DE SERVIDORES	SERVICIOS
2	Transferencia electrónica de información
1	Fax en red
2	Archivos compartidos (File Sharing)
1	Distribución de software
1	Publicación de información institucional interna
2	Bases de datos departamentales
1	Respaldo y pruebas

Tabla 5.3. Distribución de servidores comunes.

Oficinas Metropolitanas

- ✓ Servidores centralizados bajo el concepto de granja.
- ✓ 1 servidor particular por edificio proporcionado servicio de impresión y aplicaciones propias de la oficina; así como servicios para uso de intranet, paquetería y administración de cómputo personal.
- ✓ 1 servidor de acceso común brindando los siguientes servicios:

  Transferencia electrónica de información.

  Compartir información (file sharing).

  Base de datos departamentales

5.5.2. Requerimientos Hardware.

Servidores Oficinas centrales

- ✓ Servidores particulares con arquitectura de rack con las características que se muestran en la tabla 5.4.

CARACTERÍSTICAS	VALOR
Tolerancia a fallas	Fuentes de poder redundante Tarjeta de red redundante Tarjeta de Arreglo de Discos Bus interno redundante
Procesadores	2 Pentium Xeon 500 MHz
Almacenamiento	Arreglo de 3 discos de 8 GB en raid 5
RAM	128 MB (mínimo)
Memoria cache	1 MB
Multimedia	Unidad de CD 24X (mínimo)
Interfaz de red	2 Ethernet 10/100
Video	Monitor SVGA
Capacidad de procesadores	8

Tabla 5.4. Características de los servidores particulares.

Nota: Para los servidores particulares de los pisos 9,10 y 11 deberán llevar 3 tarjetas de red.

✓ Servidores de acceso común con arquitectura de rack con las características generales que se muestran en la tabla 5.5.

CARACTERÍSTICAS	VALOR
Tolerancia a fallas	Fuentes de poder redundante Tarjeta de red redundante Tarjeta de arreglo de discos Dos procesadores Bus interno redundante
Procesador	Dual Pentium Xeon 500 MHz
RAM	128 MB
Memoria cache	1 MB
Multimedia	Unidad de CD 24X (mínimo)
Interfaz de red	Ethernet 10/100
Video	Monitor SVGA
Capacidad de procesadores	4

Tabla 5.5. Características generales de los servidores de acceso común.

Nota: Se debe considerar el equipamiento adicional que se muestra en la tabla 5.6. para cada uno de los servicios que van a proporcionar los servidores de acceso común.

SERVIDOR	CARACTERÍSTICAS	VALOR
Transferencia electrónica de información	Almacenamiento	Arreglo de 4 discos de 8 GB en raid 5
Fax en red	Manejo de faxes	Tarjeta multipuerto serial (Digiboard)
	Almacenamiento	Arreglo de 3 discos de 8 GB en raid 5
Publicación de información institucional interna	Almacenamiento	Arreglo de 2 discos de 8 GB en raid 1
Base de datos departamental	Almacenamiento	Arreglo de 3 discos de 8 GB en raid 5
Archivos compartidos (file sharing)	Almacenamiento	2 unidades de almacenamiento externo de 7 bahías con 3 discos de 8 GB.
Distribución de software	Almacenamiento	2 unidades de almacenamiento externo de 7 bahías con 3 discos de 8 GB
Respaldo y pruebas	Almacenamiento	Arreglo de 3 discos de 8 GB en raid 5

Tabla 5.6. Características adicionales de cada servidor de acceso común dependiendo del servicio que proporcionará.

Servidores Oficinas Metropolitanas

Las características técnicas de cada uno de los servidores a instalar en las oficinas metropolitanas se muestran en la tabla 5.7.

TIPO DE SERVIDOR	CARACTERÍSTICAS	VALOR
SERVIDORES PARTICULARES	Tolerancia a fallas	Fuentes de poder redundante Tarjeta de red redundante Tarjeta de Arreglo de Discos Bus interno redundante
	Procesador	Pentium Xeon 500 MHz
	Almacenamiento	Arreglo de 3 discos de 8 GB en Raid 5
	RAM	128 MB
	Memoria cache	512 (mínimo)
	Multimedia	Unidad de CD 24X
	Interfaz de red	Ethernet 10/100
	Capacidad de procesadores	2
SERVIDORES DE ACCESO COMÚN	Tolerancia a fallas	Fuentes de poder redundante Tarjeta de red redundante Tarjeta de Arreglo de Discos Bus interno redundante
	Procesador	Dual Pentium Xeon 500 MHz
	RAM	128 MB
	Memoria cache	512 (mínimo)
	Almacenamiento	2 cajas de almacenamiento externo de 7 bahías con 3 discos de 8 GB.
	Multimedia	Unidad de CD 24X
	Interfaz de red	Ethernet 10/100
	Capacidad de procesadores	4

Tabla 5.7. Características de servidores en oficinas metropolitanas.

Servicios a instalar en todos los servidores departamentales.

- Sistema Operativo : Windows NT Server 4.0.
- Service Pack 5.
- OpenClient de Sybase como manejador de base de datos.

Riesgos involucrados en caso de no contar con los servicios:

- Los requerimientos de servicios de red actuales, no podrán ser satisfechos a corto plazo. La demanda de procesamiento de las aplicaciones de los usuarios, instaladas en los servidores, es cada vez es mayor y la respuesta de los mismos mas lenta, la generación de datos históricos necesarios para los usuarios exceden la capacidad de almacenamiento de los servidores, los cuales contienen solo datos de fechas recientes dificultando a los usuarios los análisis históricos.

- La infraestructura actual (tecnológicamente incompatible e insuficiente), no podrá cubrir la demanda en instalación de aplicaciones y servicios de automatización de oficina, ya que la instalación de nuevos paquetes y aplicaciones demandan mayor capacidad de procesamiento y almacenamiento que algunos servidores no pueden cubrir.

- Se verá limitado el desarrollo de nuevas aplicaciones, ya que las nuevas tecnologías en desarrollo, requieren de una infraestructura más versátil y robusta, los requerimientos de las nuevas aplicaciones de los usuarios, demandan nuevas herramientas de desarrollo, las cuales a su vez requieren de mayor procesamiento y almacenamiento y una infraestructura de servidores que las contengan. Con la que se cuenta actualmente no podrá ser parte de una solución.

- No se tendrían disponibles los servicios de red en forma integral (el usuario debe tener siempre la posibilidad de contar con cualquier servicio de red y/o información), con la infraestructura actual no se pueden consolidar las aplicaciones y el ambiente de red por problemas de incompatibilidad en el manejo de las plataformas (Netware Novell y Windows NT).

5.6. Base de datos institucional.

5.6.1. Características.

El objetivo del área de base de datos es la de salvaguardar y administrar la información que la CNBV maneja, así como clasificarla de acuerdo a los requerimientos de los distintos departamentos que la rigen.

La información que reside en las distintas bases de datos es considerada de alta sensibilidad, por lo que la protección debe ser prioritaria. Pérdidas de la información manejada en este componente generarían una interrupción en los servicios con repercusiones graves a todos los niveles, pudiendo engendrar problemas de confiabilidad, afectar a la reputación de la CNBV o incluso una falsa evaluación de la situación financiera de las instituciones controladas.

La plataforma en la cual estarán montadas las bases de datos Sybase es bajo UNIX (HP-UX), de la cual se tendrá una redundancia a través de dispositivos de conexión en cluster, de acuerdo a la propuesta de cómputo central que se mencionó en este capítulo.

Importancia de la continuidad en la Operación de los sistemas de misión crítica de la organización.

Es prioritario mantener la información disponible de la cual la CNBV depende para realizar funciones primarias.

El problema crítico con esta área reside en su relación con el área de desarrollo, al no existir un lineamiento en el desarrollo de aplicaciones con respecto a las bases de datos.

Existe una proposición no formal hacia el área de desarrollo para el control de cambios y pruebas, sin embargo se necesita más elaboración de documentos que contengan la información de los lineamientos por parte de Bases de Datos (BD).

Vulnerabilidades Contempladas.

El administrador de bases de datos tendrá que generar políticas en función a los riesgos identificados. Dichos puntos cubrirán lo siguiente:

- Discos: espacios contemplados para el desarrollo de los distintos proyectos.
- Memoria: rangos y parámetros de tolerancia para el desempeño de las aplicaciones.
- Espacio en desarrollo: que implica limitantes de recursos para el desarrollo de las aplicaciones, estas limitantes ponen en peligro la integridad de datos.
- Cambios en las cuentas de los usuarios: permisos en las cuentas de los usuarios las cuales están restringidas sin embargo los datos son reales.
- Atributos dados a las distintas clases de cuentas.
- Restringir el acceso a aplicaciones según el nivel de acceso de los usuarios.

- Controlar el acceso indebido a los servidores de bases de datos mediante el uso de herramientas de control de usuarios.
- Implantar un ambiente de pruebas, y que los desarrolladores no tengan acceso a datos de producción durante las pruebas y el desarrollo.
- No existe una certificación por cada aplicación que se monta en producción, ni un método de liberación de sistemas.
- La falta de un proceso de reingeniería a las antiguas aplicaciones que en la actualidad no cumplen con ciertas expectativas.
- Seguridad de Información.
- Conexiones seguras entre aplicaciones, BD y administración.
- Encriptación de Información.
- No existe documentación para peticiones de permisos.
- No existen formatos de reportes.

5.6.2. Requerimientos.

Para los lineamientos de las bases de datos, es importante la forma en la cual se protegerá la Integridad de la Información, por lo cual damos los puntos específicos que políticas y procedimientos internacionales plantean:

1. Definición formal de ambientes de producción y de desarrollo o pruebas.
2. Controles de accesos para los usuarios finales en la restauración de los procesos.
3. Notificación formal y detallada de cambios a las bases de datos, para la administración así como para las áreas involucradas.
4. Control de creación de cuentas a usuarios de bases de datos, así como fijar perfiles de los mismos y sus atributos.
5. Definir y clasificar los niveles de información.
6. Definir qué tipos de datos se respaldarán y cuál es la mínima frecuencia de respaldo.

7. Cifrado de los medios de almacenamiento para los respaldos.
8. Obtener siempre en base a la clasificación, dos copias de información sensible, crítica y valorada.
9. Fijar los requerimientos para el cambio de información sensible, crítica y valorada.
10. Especificar formalmente, y con consentimiento de otras áreas afectadas, el proceso de respaldo y su frecuencia.
11. Tener fuera del centro de cómputo copias de respaldos para contingencias.
12. Situar los medios de almacenamiento en zonas de fuego distintas de la máquina de origen.
13. Fijar de manera formal un periodo mínimo de retención del almacenamiento.
14. Limpieza regular de información, la cual es necesario retener por largos lapsos de tiempo.
15. Dar un lineamiento para formalizar la destrucción de la información y disponibilidad de los sistemas de información.
16. Definición de la organización de retención de datos almacenados y archivados.
17. Definir responsabilidades para la organización de retención de datos almacenados.
18. Definir medios de almacenamiento de datos aceptables.
19. La administración debe notificar los fallos en la integridad de la información en tiempo real.
20. Suprimir o clasificar bajo estudio los niveles de información incompleta u obsoleta.
21. Verificar que las transacciones de entrada en producción lleven un número secuencial.
22. Cifrar todas las comunicaciones remotas a la base de datos.
23. Asegurar las conexiones que administren vía remota la base de datos.
24. Exigir que las aplicaciones de las bases de datos pasen por un nivel de liberación y certificación antes de situarlas en producción.
25. Evitar el acceso a la información a personal externo, o sólo bajo supervisión del administrador.

5.6.2. Plan de implementación.

En las tablas 5.8. y 5.9. se definen los planes de implementación general y de políticas para optimizar y asegurar el uso, actualización y acceso a las bases de datos institucionales de la CNBV.

TAREA	OBJETIVO	ENTREGABLE
Auditar las aplicaciones de bases de datos para localizar los riesgos de seguridad	Implementar los requerimientos de seguridad en las aplicaciones que se ejecutan en los servidores de DB.	Analizar características de seguridad en las aplicaciones.
Incluir en las bases de datos las limitantes de acceso que el RDBMS permite.	Restringir acceso a información.	Crear perfiles de usuarios para adjudicar permisos a módulos.
Restringir el acceso a aplicaciones a las cuales no se tiene derecho.	Controlar el acceso a información.	Situar privilegios de acuerdo a usuarios.
Implantar una política más estricta en el manejo de los passwords.	Evitar acceso a información no permitida.	Utilización de passwords personalizados y herramientas de autenticación como tokens cards.
Controlar el acceso indebido a los servidores de Bases de Datos para consultas de datos sin un control por medio del uso de herramientas no permitidas a ciertos usuarios.	Evitar el descontrol en uso de herramientas.	Auditar conexiones remotas y cerrar puertos inservibles.

Tabla 5.8. Plan de implementación.

TAREA	OBJETIVO	ENTREGABLE
Implantar un ambiente de pruebas, y que los desarrolladores no acceden datos de producción para pruebas y desarrollo.	Proteger la integridad de los datos así como el funcionamiento de los servidores de producción.	Crear un laboratorio de desarrollo y pruebas.
Implementar un proceso de certificación por cada aplicación que se monte en producción, ni un método de liberación de sistemas.	Garantizar la producción del procesamiento de datos y la integridad de los mismos.	Crear documento oficial de liberación de aplicaciones.
Implantar un proceso de reingeniería a las antiguas aplicaciones que en la actualidad no cumplen con ciertas expectativas.	Evitar el uso innecesarios de recursos, además de garantizar la veracidad de los resultados esperados.	Analizar todas las aplicaciones implementadas, su historial y en base a su funcionalidad aplicar reingeniería en las que aplique.

Tabla 5.8. Plan de implementación (continuación).

TAREA	OBJETIVO	ENTREGABLE(S)
Separación de instalaciones de desarrollo y operación.	Salvaguardar la integridad de los servicios así como las bases de datos.	Crear lineamientos de aceptación de nuevos sistemas los cuales estarán debidamente establecidos y documentados, además de crear pruebas adecuadas y satisfactorias.
Auditorias y revisiones de la administración de usuarios.	Tener control sobre datos y manejo en las cuentas de los usuarios.	Realizar revisiones imprevistas sobre cuentas de usuarios.

Tabla 5.9. Implementación de estándares.

TAREA	OBJETIVO	ENTREGABLE(S)
Asegurar el acceso a terceros	Mantener la seguridad en las instalaciones organizacionales y de los bienes informáticos accesados por terceros.	Documento oficial que contenga las condiciones de seguridad necesarias para asegurar el cumplimiento con las políticas y estándares organizacionales
Revisiones anuales de los sistemas de Bases de Datos por los proveedores del sistema.	Tener información de status de la Integridad del sistema de Base de datos.	Adquirir planes de soporte para análisis de "Performance & Tuning", mantenimientos preventivos, consultoría de integridad de la base de datos.
Etiquetado de activos	Intercambiar o restringir a la información, así como al impacto de un acceso o alteración de la Información no autorizada.	Dentro del clasificado etiquetar todos los activos según el nivel de: Confidencialidad. Integridad Disponibilidad.
Implementar un plan de respuestas ante incidentes.	Minimizar el daño por incidentes de seguridad o mal funcionamiento.	Implementación de una metodología de levantamiento de reportes en cada proyecto, los cuales incluirán : Incidentes de seguridad. Debilidades de seguridad. Funcionamiento inadecuado de software.
Detección de actividades no autorizadas o ilegales.	Evitar un mal uso de recursos que pongan en riesgo la integridad de los datos.	Revisiones periódicas de fases o módulos de proyectos.

Tabla 5.9. Implementación de estándares (continuación).

TAREA	OBJETIVO	ENTREGABLE(S)
Definición de planes de contingencia.	Protección de la integridad de activos.	En base al clasificado de activos crear planes de contingencia o métodos alternos en caso de pérdida de información o mal uso de ella.
Analizar requerimientos de seguridad de SW.	Asegurar la incorporación de mecanismos de seguridad en la operación de los sistemas y aplicaciones.	Auditar que todos los requerimientos de seguridad especificados por aplicaciones y procesos de desarrollo se cumplan e incorporen.

Tabla 5.9. Implementación de estándares (continuación).

5.7. Plataforma de administración y monitoreo.

5.7.1. Implementación.

Considerando que la infraestructura de cómputo central está basada en equipos HP9000, la plataforma natural de administración y monitoreo es OpenView. El esquema propuesto es el que se muestra en la Figura 5.13.

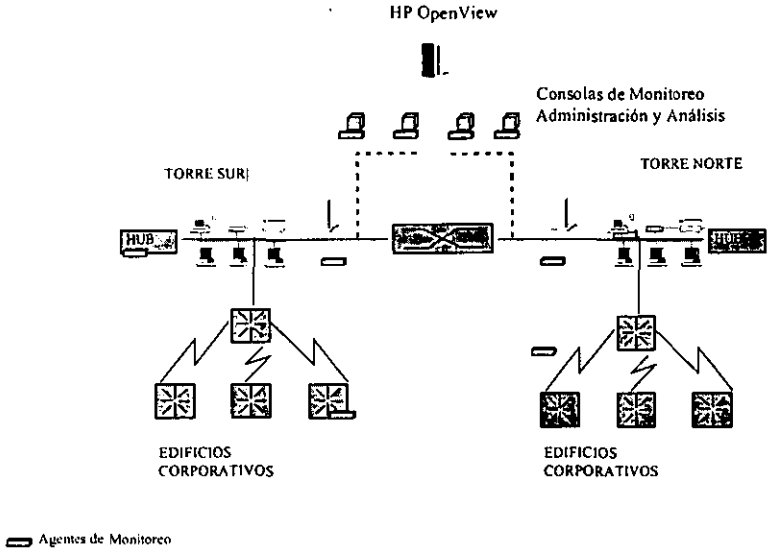


Figura 5.13. Plataforma de administración y monitoreo propuesto.

5.7.2. Características.

- ✓ Plataforma basada en HP OpenView centralizado en el edificio sede (Plaza Inn) y agentes distribuidos en cada componente para su monitoreo y desempeño.
- ✓ Contempla las 7 capas del modelo OSI.

- ✓ Permite la configuración, administración y monitoreo de los dispositivos de red bajo estándares: SNMPI y II, RMON, RPCs, entre otros.
- ✓ Permite la configuración de umbrales de alertamiento, notificación a consolas y pagers.
- ✓ Ejecuta eventos o programas con base a umbrales.
- ✓ Cuenta con una base de datos de históricos de desempeño y problemas de todos los componentes.
- ✓ Dispositivos de monitoreo distribuido, con capacidades de procesamiento y almacenamiento internos y que permitan el optimo uso de ancho de banda.
- ✓ Inteligencia en la localización y aislamiento de fallas.
- ✓ Plataformas de administración de los diferentes dispositivos integrables a la plataforma HP OpenView.
- ✓ Infraestructura abierta y escalable.

Productos a instalar en la plataforma central de administración y monitoreo.

- Sistema de respaldo: Omniback II.
- Herramienta de descubrimiento de la red: Network Node Manager.
- Agentes de monitoreo y reporteador : Perfview y MeasureWare..
- Umbrales de alertamiento y notificación a consolas: IT/O (Information Technology Operation).

HP OpenView. IT (Information Tecnology).

Las herramientas de administración son un componente importante para proporcionar servicios de información a la CNBV. OpenView proporciona las herramientas que se requieren para unir las expectativas de los usuarios y proporcionar IT de calidad y soluciones de costo / beneficio.

Las herramientas de administración HP OpenView están diseñadas para administrar aspectos específicos de la infraestructura de cómputo como son sistemas, redes, performance, costos, inventarios, etc. Estas herramientas están organizadas entorno a procesos específicos y áreas operacionales.

Características y Beneficios

El concepto IT/Operation

OpenView IT/Operation es una solución de software distribuida cliente / servidor en el servidor es una consola central de administración y los clientes son "agentes inteligentes". Desde la consola de administración central, se tiene el control total de los recursos distribuidos a través de la red, identificando problemas potenciales antes de que ocurran y resolviéndolos antes de que los usuarios finales sean afectados. Los agentes también pueden preconfigurarse para resolver problemas inmediatamente sin interactuar con la consola de administración central.

IT/Operation proporciona vista punto a punto de todo el ambiente administrado. Por tener la ventaja de una interfaz común, se puede verificar inmediatamente el estado de los sistemas de misión critica, infraestructura de red (incluyendo intranets), y aplicaciones de negocios críticos como son bases de datos, servidores internet, correo electrónico, etc. Los datos de red y rendimiento del sistema, almacenamiento y respaldo de información de la empresa, inventario de hardware y software, perfiles de usuario final, etc. puede ser consultada y usada para administrar más efectivamente el ambiente de cómputo.

La CNBV demanda mejor confiabilidad y desempeño de sus ambientes de cómputo. Al tener la ventaja de acciones autónomas de IT/Operation y capacidad de administración de eventos inteligentes, los problemas complejos pueden identificarse, correlacionados y resueltos antes de ser afectados los usuarios finales.

Por usar bases de datos integradas, la historia de eventos puede ser analizada para predecir y prevenir futuros problemas, además de proporcionar un estatus inmediato del ambiente de cómputo para continuar obteniendo el nivel de servicio esperado.

Con esta plataforma no solo se administran aplicaciones y bases de datos, también puede manejar el sistema operativo Unix y servidores Windows NT que componen a la red interna.

Network Node Manager.

Network Node Manager colecciona y presenta datos para ayudar a encontrar las necesidades de configuración, desempeño y administración. Automáticamente descubre cada uno de los dispositivos que integran a la red, generando una presentación precisa de la topología. También recolecta eventos a través de toda la empresa que puedan indicar problemas potenciales.

HP PerfView y MeasureWare.

Software de administración centralizada para análisis, monitoreo y planeación de recursos para sistemas y ambientes distribuidos. La integración con OpenView corre en estaciones de trabajo y servidores HP 9000, usa medidas proporcionadas a través de agentes de MeasureWare corriendo en los equipos a administrar.

El análisis gráfico de la tendencia de datos históricos medidos se genera en tres niveles:

- ✓ Procesos.
- ✓ Aplicaciones (definido como un grupo de uno o más procesos).
- ✓ Niveles global (sistema).

OmniBack.

OmniBack II proporciona protección de datos sin interrumpir las operaciones del sistema.

El respaldo de datos se proporciona a través de la red con dispositivos de almacenamiento tales como DDS y DLTs. Puede realizarse en forma local o remota desde un punto de administración central. Es posible seleccionar desde un respaldo de file system total/incremental o respaldo en línea. Las cintas de respaldos existentes pueden ser copiadas local o remotamente siguiendo un proceso de valuación.

Con esta plataforma se pueden realizar respaldos completos de todos los servidores que componen la red de la CNBV, incluyendo UNIX, Windows NT y NetWare desde un sistema central. Toda la información relevante acerca de sesiones de respaldo individual, incluyendo archivo y medio de información, son administrados a través de una base de datos.

5.7.3. Requerimientos de Hardware.

- o Estación de trabajo con sistema operativo Unix HP-UX v10.20.
- o Agentes externos compatibles con plataforma base (Measureware).
- o Interfaz de red 100BaseT.
- o Interfaz de comunicación.
- o Unidades de respaldo DDS y DLT.

5.8. Intranet / Internet.

5.8.1. Implementación

Esta propuesta busca que el personal de la CNBV pueda hacer uso de los servicios a través de Internet bajo un enlace corporativo en función al análisis que se realizó en el capítulo 4.

Las etapas que se contemplará serán las siguientes:

- Establecer un enlace dedicado hacia un proveedor de servicios de Internet. Este enlace será digital aprovechando la infraestructura de comunicaciones con la que cuenta la Comisión. La propuesta es que se utilice un canal de 2 Mbps (E1) para dar servicio a 500 usuarios a través de la red interna.
- Desarrollo, publicación y mantenimiento de la página de la CNBV en Internet.
- Establecimiento de los servicios de correo electrónico, transferencia de archivos, web, enlaces remotos, etc. a través

Esquema prototipo para el desarrollo del proyecto Internet/Intranet

La figura 5.14. muestra la arquitectura hardware necesaria para el desarrollo del proyecto Internet / Intranet en la Comisión Nacional Bancaria y de Valores.

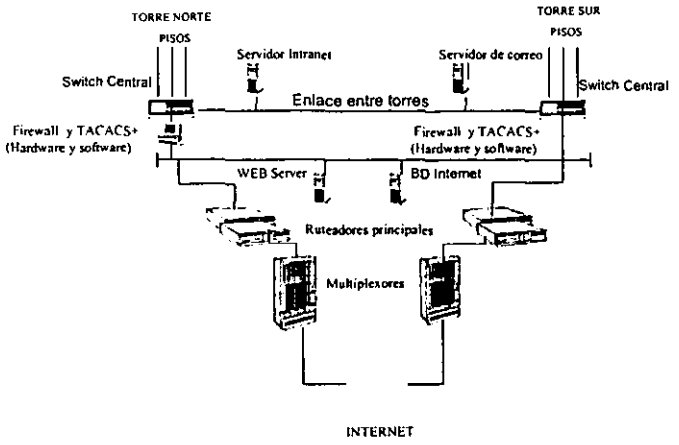


Figura 5.14. Plataforma tecnológica para el servicio de Internet / Intranet.

La arquitectura contempla los siguientes componentes de equipamiento:

- ✓ Un servidor dedicado para el web-site de la CNBV y del DNS.
- ✓ Un firewall en cada edificio para la protección de los recursos de la red de la CNBV y contar con un esquema de redundancia.
- ✓ Un servidor interno dedicado de Intranet.
- ✓ Un servidor para el correo electrónico, la transferencia de archivos, etc.
- ✓ Una estación para el desarrollo del web site de la CNBV y de Intranet con herramientas de autoría para HTML, CGI's, Java, JavaScript y otras.

Bajo este esquema, las oficinas virtuales (oficinas regionales, gente de supervisión, empleados con máquinas portátiles fuera de la red de la CNBV) podrían conectarse vía dial-up a través del mismo proveedor de servicios.

- Las características generales de los equipos para dar soporte al servicio debe ser: Sistema Operativo UNIX de 64 bits.

- Estación de trabajo con procesador RISC de 64 bits, escalable, que cuente con herramientas de autoría para páginas web, etc.

Dada la importancia de los recursos que operan en la red de la CNBV debe contemplarse un equipo para la seguridad de los mismos, capaces de controlar estrictas políticas de autorización para el acceso a la red, así como facilidad de administración, configuración e instalación.

Un punto importante a considerar es la capacitación en las herramientas para la instalación, desarrollo, y mantenimiento de los equipos (software y hardware).

5.9. Seguridad.

5.9.1. Manejo de Información Electrónica Seguro.

El presente modelo tiene por objeto garantizar la privacia y seguridad de la información que viaja por la red local o remota de la CNBV.

Dicho modelo cubre aspectos del tipo Infraestructura de llaves públicas, infraestructura de firewalls y redes virtuales privadas, así como también la administración automatizada de dichas herramientas y el monitoreo constante de posibles violaciones a la seguridad de los sistemas permitiendo tomar medidas preventivas y correctivas a tiempo.

Los componentes de una política de seguridad se muestran en la Figura 5.14.

Figura 5.14. Componentes de una política de seguridad.

En la identificación, el sistema de seguridad debe realizar tres preguntas:

¿ Quién es?

¿De dónde es?

¿Qué permisos debe tener?

La etapa de integridad debe considerar los siguientes elementos:

- Seguridad Física.
- Seguridad de configuraciones.
- Seguridad actualización de rutas.
- Seguridad de transferencia de información.
- Firewalls.

Finalmente, el registro de eventos deberá tener estricto control sobre los siguientes rubros:

- Servidor de actividad.
- Políticas.
- Seguridad.
- Reportes.
  - Errores.
  - Recursos Accesados.
  - Anomalías.

5.9.2. Implementación de seguridad en las redes de datos y comunicaciones.

Infraestructura de Llaves Públicas (PKI).

Partiremos del principio de que toda la información que viajará por la red de la CNBV es clasificada como confidencial (fig. 5.15). Por lo mismo el modelo debe contemplar no solo mecanismos de privacia a nivel comunicaciones sino también mecanismos de certificación de autenticidad, integridad confidencialidad de la información. También deberá autenticar y certificar que dicha información proviene de la persona quien dice emitirla, vía mecanismos de firmas y certificados electrónicos.

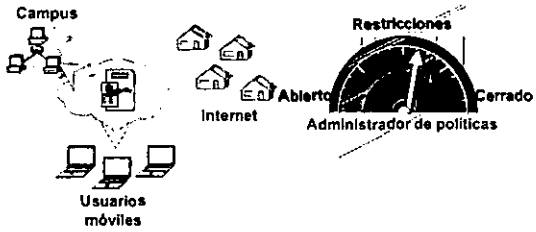


Figura 5.15. Implementación de políticas de seguridad.

A este tipo de soluciones se les conoce como infraestructura de llaves públicas (public key infrastructure).

Para que dicho modelo funcione, debe existir una autoridad certificadora (AC) que garantice la autenticidad de firmas y documentos. Comparable a un notario pero electrónico en este caso, donde por cada mensaje que se envíe vía la red firmado por el emisor, la AC firme a su vez el mensaje declarando que dicha firma y mensaje provienen de la persona quien dice enviarlos.

En el caso de la CNBV, ella será su propio AC pero podría, en un momento dado, convertirse en el AC para todas las Agencias Financieras de México dado su papel dentro del Mercado Financiero Mexicano.

Seguridad a nivel de comunicaciones.

La Seguridad en Comunicaciones es una colección de componentes, que colectivamente tienen las siguientes propiedades:

- Todo el tráfico de entrada-salida debe pasar a través de ella.
- Solamente tráfico autorizado debe poder transmitirse a través de la WAN, siguiendo las políticas definidas.
- La seguridad, por sí misma, debe ser inmune a los intentos de ataques por parte de hackers.

A nivel comunicaciones la infraestructura de redes virtuales privadas y firewalls brindan protección a la información que viaja de una oficina a otra o de una oficina a un cliente remoto. Dicha información viaja cifrada minimizando los riesgos de que su privacia

sea violada. Adicionalmente se protegen las redes internas de tentativas de acceso por parte de redes o usuarios externos no autorizados como sería el caso del Internet.

Una de las herramientas ya empleadas en la CNBV es el Gauntlet Internet Firewall (Firewall a nivel aplicación) considerado de los más seguros por su diseño.

Una vez establecido el perímetro de seguridad de la red, se debe garantizar la privacia de las comunicaciones, aún bajo el empleo de enlaces privados dedicados. La cifrado a nivel IP ha demostrado ser una manera eficaz de lograr dicho objetivo. Existen soluciones en el mercado basadas en software únicamente o combinadas con hardware, las cuales brindan un mejor desempeño dado que se dedica un procesador únicamente a cifrar y descifrar la información que pasa por él. Sin embargo, su "ownership cost" (costo de administración) es mucho más elevado además de no garantizar la compatibilidad con otros equipos.

El empleo de algoritmos de cifrado dura (DDE, 3DES, RSA, etc.) garantizan un nivel de privacia robusto, además de que no requiere de hardware adicional ya que corre sobre el mismo equipo firewall.

Los cuellos de botella en la cifrado y descifrado de la información en el firewall pueden ser controlados con un buen dimensionamiento del hardware empleado.

Una red privada virtual global (fig. 5.16.), global virtual private network (GVPN), puede establecerse entre firewalls remotos de oficinas regionales, y con equipos clientes móviles (laptops). Una vez establecida dicha infraestructura, el PKI puede encargase de realizar las tareas de autenticación y control de acceso a este tipo de servicios para la gente autorizada.

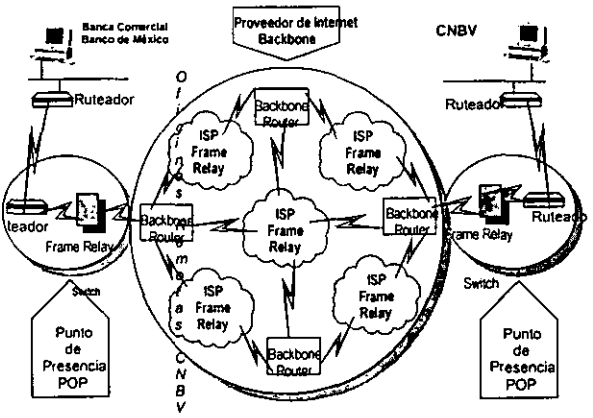


Figura 5.16. Diagrama típico de una Global Virtual Private Network (GVPN).

5.9.3. Monitoreo, Auditorías y Detección de Intrusos

Una vez establecidas las infraestructuras de llaves públicas y de seguridad de comunicaciones, el tercer elemento de la solución se basa en sistemas de monitoreo y administración de la seguridad que se adapte a los sistemas de red y seguridad existentes en una organización.

Dicha arquitectura se caracteriza por el empleo de agentes que monitorean servidores de información crítica, sistemas de seguridad (firewalls), ruteadores, etc. levantando información sobre todo lo que ocurre en la red. De encontrarse discrepancias en las políticas de seguridad establecidas a nivel componente o bien vulnerabilidades, amenazas o desconfiguración de algún sistema, se previene al administrador y se inician acciones preventivas y correctivas según se establezca.

Autenticación y el Proceso de Single Sign-on

En un ambiente distribuido, los usuarios se conectan a varios sistemas disponibles por la red, donde cada sistema cuenta con su propia identificación de usuario y password. Los usuarios deben recordar en un mismo momento un gran número de identificaciones y passwords lo cual los incita a escribir ésta información sensible para cuando se les ofrezca, creando un problema grave de seguridad. Las tendencias actuales para resolver este tipo de problemas son el Modelo de Single Sign-On (SSO).

El modelo de SSO permite a los usuarios acceder a todos los sistemas y aplicaciones requeridas con una sola identificación y password sin comprometer la seguridad. Una vez autenticados los usuarios pueden tener acceso a todos los servicios asegurados por este sistema y a los cuales tengan derecho.

Se busca proteger una red distribuida proveyendo autenticación segura, intercambio seguro de mensajes e integridad de los datos. El programa cliente al iniciar la sesión de Log-in al sistema automáticamente asigna credenciales a los usuarios las cuales empleará posteriormente para la autenticación a nivel aplicaciones y servicios. Del lado de las aplicaciones, es necesario realizar ciertas modificaciones que empleen el modelo de SSO cómo su autenticador.

Los protocolos empleados para este tipo de funciones se basan en estándares de seguridad de redes tipo Kerberos.

Kerberos, originalmente desarrollado en el MIT bajo el proyecto de Athena, provee autenticación segura en ambiente de redes, sin el riesgo de que los passwords sean vistos (sniffer) mientras viajan por la red. Adicionalmente el protocolo ofrece los mecanismos de cifrado necesarios para verificar y resguardar la integridad y privacía de la información.

En bases de datos como Sybase, se ha desarrollado una capa llamada Secure Control Layer (SCL) que brinda la posibilidad de adoptar una interfaz uniforme de seguridad hacia las aplicaciones y servidores. Dicha SCL provee una arquitectura consistente de seguridad que soporta una gran variedad de servicios de autenticación.

Políticas

Se sugieren las siguientes políticas:

- ✓ Mantener en sobre cerrado todos los passwords de cada equipo.
- ✓ Mantener la capacitación tanto del área de operación como de soporte técnico.
- ✓ Identificar todos los equipos involucrados en el área de comunicaciones.
- ✓ Mantener actualizado los diagramas físico de la topología de la red de comunicaciones.
- ✓ Implementación de enlaces alternos para servicios críticos.
- ✓ Procedimientos para el switcheo a canales alternos, en caso de que no sea automático.
- ✓ Mantener el directorio de proveedores de servicios (carriers) y su escalonamiento de fallas.
- ✓ Actualizar los diagramas físicos y lógicos de topología, proveedor y velocidad de cada enlace.
- ✓ Habilitación de cifrado en los enlaces críticos.
- ✓ Generación de listas de acceso en ruteadores.
- ✓ Implementación de rutas estáticas y evitar la conectividad entre segmentos de redes locales y externas.
- ✓ Capacitación de personal de operación en el uso, configuración y actualización del servidor de seguridad.
- ✓ Implementación de un estándar para habilitar servicios de SNMP en equipos activos.
- ✓ Continua verificación de la operación de equipos y servidores de seguridad para afinar su correcta operación (tunning).

Procedimientos de monitoreo

Se lleva a cabo un monitoreo para vigilar el funcionamiento de los equipos activos a través de los servicios de SNMP, además de contar con OpenView para el monitoreo de los ruteadores. En caso de existir una alarma o problema en algún enlace se reporta al encargado del área de comunicaciones o a Telmex.

Procedimientos para la operación y mantenimiento de los equipos y monitoreo.

En algunos equipos se implementa la redundancia tanto en tarjetas como en fuentes de poder, además de contar con UPS y plantas de luz.

Respaldo periódico de la configuración de equipos activos

Periódicamente se lleva a cabo un respaldo de todas las configuraciones de cada equipo. Ya sea por actualización o por haber realizado un cambio.

Estándar de Seguridad

Una adecuada seguridad en una sistema requiere de una apropiada combinación de políticas de seguridad y procedimientos, controles técnicos, entrenamiento de usuarios y concientización, y un plan de contingencia. Todas estas áreas son críticas para proveer una adecuada protección.

Mecanismos para asegurar los servicios de un sistema

Se debe contar con los medios de autenticación necesarios para llevar a cabo la identificación y autenticación de los administradores de los equipos y usuarios externos ya sea cisco secure, servidor de Tacacs +, secure Id, radius, medidas biométricas etc.

Deberá de contarse con medios de control de acceso que garanticen la seguridad física y lógica de los equipos activos. Los controles pueden ser tarjetas inteligentes, medidas biométricas etc.

Para contar con integridad y confiabilidad se deberá hacer uso de cifrado en todos los enlaces.

Deberá llevarse a cabo un monitoreo constante para vigilar el funcionamiento de los equipos y enlaces de comunicaciones,

Se deberán generar bitácoras que lleven el historial, tanto de los cambios realizados en las configuraciones como del comportamiento de los equipos.
Se debe crear un directorio de proveedores que contenga teléfonos y contratos.

Red Interna

Administrar y monitorear la base instalada de switches con el software de administración de OpenView, a fin de detectar y solucionar de forma oportuna, y basándose en los niveles de servicio establecidos, cualquier anomalía en el rendimiento de la red o problemas que se presenten en dicha infraestructura, así como el acceso a servidores.

Procedimiento de reporte de errores o mal funcionamiento de los sistemas

El monitoreo se lleva a cabo a través de OpenView. En caso de detectar alguna falla, es corregida por gente del área y si se trata de algún problema físico o de mal funcionamiento del equipo se contacta con el proveedor de servicios.

Mecanismos para asegurar los servicios de un sistema

- ✓ Se debe contar con los medios de autenticación necesarios para llevar a cabo la identificación y autenticación de los administradores.
- ✓ La identificación y la autenticación permite asegurar que el acceso sea único para el personal autorizado.
- ✓ Deberá de contar con medios de control de acceso que garanticen la seguridad física y lógica de los equipos activos. Los controles pueden ser: Tarjetas Inteligentes, medidas Biométricas etc.
- ✓ El control de acceso permite asegurar que los recursos están siendo utilizados por el personal autorizado. Este servicio protege contra el uso no autorizado de los recursos.
- ✓ Se debe contar con equipos de monitoreo y de combate contra incendios en todos los lugares donde se encuentren los equipos.
- ✓ Debe existir redundancia en todos los enlaces críticos.
- ✓ Debe llevarse acabo un respaldo de las configuraciones de los equipos.
- ✓ Debe existir un servidor de FTP que contenga las configuraciones de los equipos.
- ✓ Debe realizarse un control de cambios para la configuración de los equipos y las nuevas aplicaciones.
- ✓ Para contar con integridad y confiabilidad se deberá hacer uso de cifrado en todos los enlaces.

- ✓ Deberá llevarse a cabo un monitoreo constante para vigilar el funcionamiento de los equipos y enlaces de comunicaciones.
- ✓ Se deberán generar bitácoras que lleven el historial, tanto de los cambios realizados en las configuraciones como del comportamiento de los equipos.
- ✓ Para contar con integridad y confiabilidad, se deberá hacer uso de cifrado en todos los enlaces.
- ✓ La confidencialidad de mensajes y datos permite asegurar que los datos, software y mensajes no sean revelados a personal o dependencias no autorizados.
- ✓ La confidencialidad de mensajes y datos, puede ofrecer protección incorporando mecanismos de criptografía.
- ✓ Deberá de llevarse a cabo un monitoreo constante para vigilar el funcionamiento de los equipos activos.
- ✓ Se deberán generar bitácoras que lleven el historial tanto de los cambios realizados en las configuraciones como del comportamiento de los equipos.
- ✓ Se debe crear un directorio de proveedores que contenga teléfonos y contratos.
- ✓ Comparación.
- ✓ Siguiendo los mecanismos de seguridad descritos anteriormente, no se encontraron políticas ni procesos que regulen la identificación y autenticación para la administración y monitoreo de los equipos.

Firewalls

Los firewalls se encuentran instalados sobre dos servidores HP con el sistema operativo HP-UX versión 10.20, que ya cuenta con los parches para el año 2000. El esquema de conexión se muestra en la Figura 5.17.

El software instalado para esta labor es el Gauntlet Internet Firewall.

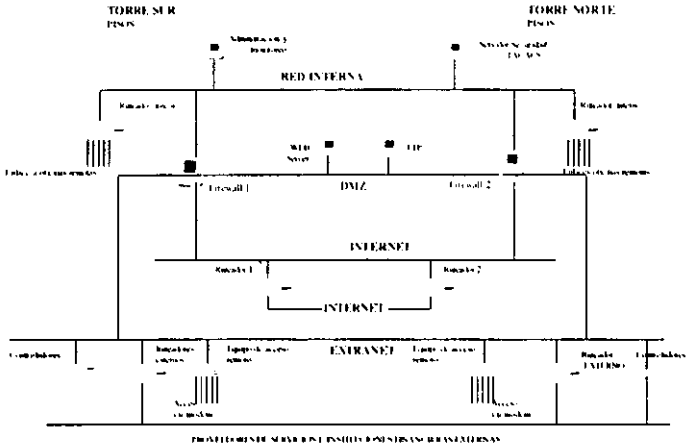


Figura 5.17. Configuración de la seguridad a través de los firewalls.

Cuentan con cuatro flancos, es decir cuatro enlaces, con direccionamiento IP independiente y protegidos a través del firewall de cada torre:

- ✓ Proveedor de Internet. Será por donde se establezca el enlace hacia internet.
- ✓ Extranet. En esta zona se conectarán los bancos y otras instituciones financieras y bursátiles, además de algunos proveedores de servicios.
- ✓ Red interna. Es la conexión hacia la red local de datos.
- ✓ DMZ (Zona desmilitarizada). Será un área en donde se establezcan todos los servicios de internet que sean públicos: web server, servicios de ftp, etc.

El firewall es el encargado de permitir o denegar los accesos entre los cuatro flancos, con los que tiene conexiones la CNBV. Está configurado para que los usuarios internos tengan acceso hacia los distintos flancos de seguridad, dependiendo de las necesidades de cada uno de ellos. También ofrece servicios de consulta hacia su Web, no importando que la petición llegue por cualquiera de sus flancos.

Cabe señalar que si los firewalls no están en servicio la CNBV no queda desprotegida, ya que éstos son los encargados de brindar la conectividad entre la CNBV y sus enlaces.

Virtual Private Networks (VPN)

Las VPNs permiten la comunicación segura de dos redes confiables a través de un medio inseguro como podría ser una red publica (Internet). Algunos firewalls proveen esta capacidad dentro de sus características generales de configuración. Cualquier conexión entre firewalls sobre una red publica deberá usar cifrado para garantizar la privacía e integridad de los datos que viajan a través de ella.

Toda conexión que use una VPN deberá ser revisada y supervisada por los administradores del firewall.

Los medios para la distribución de llaves y su mantenimiento deberán ser establecidas con anterioridad antes de establecer cualquier enlace por VPN.

DNS

Algunos firewalls pueden configurarse para ejecutar funciones de DNS como un primario, secundario, o cache.

La decisión de cómo administrar o llevar un DNS no es generalmente una decisión que comprometa la seguridad. Muchas organizaciones delegan responsabilidades a terceros como podría ser su proveedor de Internet. En este caso, el firewall puede ser usado como DNS cache, mejorando así su rendimiento ya que no requiere de dar soporte a su base de datos del DNS.

Si la organización decide dirigir su propia base de datos de DNS, el firewall puede actuar como el servidor de DNS. Si el firewall es configurado como un servidor de DNS (primario, secundario, o cache), es necesario tomar las precauciones de seguridad necesarias. Una ventaja de implementar el firewall como un servidor de DNS es que se puede configurar para ocultar la información interna de los hosts. En otras palabras, con el firewall actuando como un servidor de DNS, los hosts internos consiguen una vista sin restricciones de ambos flancos tanto el interno y externo. Los hosts externos, por otra parte, no tienen acceso a la información sobre máquinas internas. Para el mundo externo, todas las conexiones a cualquier host en la red interna parecerán tener origen en el firewall. Con la información del host oculta desde fuera, un atacante no sabrá cuales son las direcciones y nombres de los hosts internos que ofrecen sus servicios al Internet.

Una política de seguridad para DNS: Si el firewall se está ejecutando como un servidor de DNS, entonces el firewall debe configurarse para ocultar información sobre la red interna para que los hosts no sean anunciados al mundo exterior.

Perímetros de Seguridad

La seguridad total debe estar basada en varios perímetros de seguridad.

El primer perímetro se sugiere para crear una división entre la LAN y el Extranet e Internet.

El segundo perímetro interno, se sugiere para dividir a la LAN de los servidores de aplicación ya que no se puede garantizar que no pueda existir un ataque interno, particularmente si la mayoría de los ataques reportados provienen precisamente de usuarios internos.

Ventajas de tener un segundo perímetro de seguridad:

- ✓ Se puede implementar y robustecer el control de acceso a los servidores más fácilmente.
- ✓ El análisis de bitácoras se hace de una forma independiente.
- ✓ Típicamente el tráfico es menor.
- ✓ La vigilancia se puede concentrar en cada perímetro.
- ✓ El mundo exterior (Extranet e Internet), se encuentra más distante.

MENSAJERÍA ELECIRÓNICA

Proporcionar la infraestructura, para brindarle a la CNBV un medio de mensajería electrónico rápido y eficiente.

PERSONIFICACIÓN

La personificación puede ser anulada al utilizar algoritmos de cifrado para firmar digitalmente el mensaje de correo electrónico. Un método popular usado es con criptografía de llave publica. Un número de dispersión (hash) calculado para cada mensaje se cifra utilizando la llave publica del remitente. El receptor usa su llave privada para descifrar el número de dispersión, y entonces verifica el número que calculó contra el que contenía el mensaje recibido. Esto asegura que el mensaje realmente fue escrito por el remitente, y que el mensaje no ha cambiado en el tránsito. El Gobierno Federal DE EE.UU. requiere que se utilice el Algoritmo Seguro de hash (SHA) y la Norma Numérica de Firma, donde sea aplicable. Los programas de computación comercial más populares usan RSAS RC2, RC4, o RC5 como algoritmos de hash.

Recomendaciones Específicas

- ✓ Toda información que viaje hacia el exterior debe ser cifrada para poder ser enviada.
- ✓ Un programa para cifrar correos de una forma muy sencilla y confiable es el PGP.
- ✓ La recepción de attachments debe ser estudiada, ya que es un riesgo potencial de que a la CNBV lleguen virus o posibles programas con caballos de Troya.
- ✓ Se debe estudiar la posibilidad de que el servidor de Exchange pueda estar revisando los correos ya sea para evitar virus o posibles ataques con software.
- ✓ El envío de correos que contienen attachment hacia el exterior, se debe analizar con mucho cuidado ya que es un riesgo potencial.
- ✓ Se debe contar con PKI, para que toda la información viaje cifrada y firmada. Con esto se evitaría la repudiación de cualquier información transmitida.
- ✓ Se debe contar con mecanismos automatizados, que verifiquen que absolutamente todos los correos sean enviados cifrados, y en caso de que se detecte alguno que no cumpla los requisitos, sea rechazado.

En la Figura 5.18. se muestra el esquema global de seguridad propuesto.

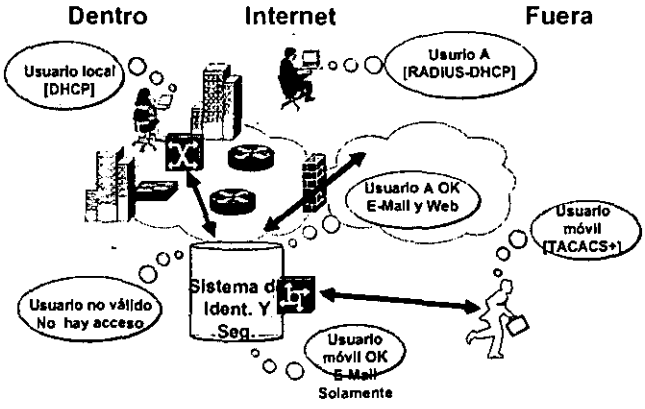


Figura 5.18. Funcionalidad integral de la seguridad.

5.10. Help Desk.

5.10.1. Funciones

Es un departamento para asesoría a usuarios y tendrá las siguientes funciones primordiales:

- Optimizar el uso de recursos de cómputo.
- Personalizar la atención a los usuarios.
- Atender fallas del hardware y software.
- Realizar mantenimiento preventivo y correctivo.
- Realizar procedimientos de configuración de software y hardware.
- Llevar a cabo control de inventarios.
- Coordinación de recursos de Outsourcing.
- Evaluación de nuevas tendencias informáticas.

5.10.2. Soporte a Usuarios

En muchas organizaciones, el soporte a los usuarios tiene lugar mediante un Help Desk. Pueden dar soporte a una organización entera, un departamento, un sistema específico, o una combinación de estos. El soporte a usuarios debe vincularse estrechamente a la capacidad de la organización de manejar incidentes. En muchos casos, el mismo personal desempeña estas funciones.

Una consideración importante de seguridad para el soporte a usuarios, es si el personal está siendo capaz de reconocer si el problema (reportado por el usuario) se relaciona con la seguridad. Por ejemplo, la incapacidad de algunos usuarios de registrarse en un sistema computacional puede resultar en la inutilización de sus cuentas debido a demasiados intentos fallidos de acceso. Esto podría indicar la presencia de hackers tratando de adivinar las contraseñas de los usuarios.

En general, el staff para el soporte a sistemas y operación debe ser capaz de identificar problemas de seguridad, responder adecuadamente, e informarlo a la persona apropiada. Existe una amplia gama de posibles problemas de seguridad. Algunos serán internos debido a aplicaciones propias, mientras otros aplican a productos externos. Por demás, los problemas pueden ser basados en software o hardware. Los sistemas pequeños son especialmente susceptibles a los virus, mientras las redes son particularmente susceptibles a ataques de hackers. El personal de soporte debe ser capaz de reconocer ataques y saber cómo responder.

El sistema más efectivo e inteligente de soporte es que se provea el menor soporte a usuarios informalmente. El soporte que proveen los otros usuarios es importante, pero ellos no pueden estar conscientes de las posibles complicaciones que se tengan en cuanto a la seguridad.

5.10.3. Implementación del helpdesk.

En CNBV, el área de helpdesk tendrá la responsabilidad de mantener en óptimo estado el equipo PC de todas las áreas que le corresponden, en un horario de atención de 8:30 a 19:00 hrs. Dicha actividad comprenderá el mantenimiento preventivo y correctivo de los equipos, e instalación de software, así como hacer efectivas las garantías de éstos, si así se requiere. Aunado a ello, tendrá el deber de realizar cada mes una auditoria al software y hardware que está instalado en cada PC.

También brindará soporte a los usuarios on-site, así como asignará peticiones de los usuarios, tales como dar de alta, baja y cambios en cuentas en los servidores NT, el servicio de E-mail e Internet, a los departamentos que le competan.

Deberá definir, ofrecer administrar, y regular los servicios de cómputo a los usuarios de la CNBV. Se generaran documentos de difusión, manuales del usuario, entrenamiento, etc., sobre nuevos servicios y soluciones para los usuarios de la CNBV.

Auditorias.

Cada mes realizará una auditoria al software y hardware que está instalado en cada PC, por medio de un software que realiza inventario y distribución de software a través de la red, llamado SMS. Cabe señalar que el helpdesk solo lo puede utilizar para realizar consultas.

Seguridad en los Datos

Trabajará con tres bases de datos:

Base de datos de inventarios informáticos.

Base de datos de Bodega.

Base de datos del Helpdesk.

Parte de la información que manejan las bases de datos, utilizadas por el sistema de helpdesk, será confidencial, pero no es vulnerable ya que solo personal autorizado hará uso de ellas para consultas de datos, tales como nombre y número de identificación de usuarios, etc. Por otro lado, la información recopilada al realizar el inventario de software y hardware en las PCs le será útil a este departamento y al de contraloría, y nadie más puede verla.

Importancia de los sistemas y el impacto en la organización.

Se requiere que los sistemas que utilizan para las consultas estén disponibles, ya que de éstos depende el funcionamiento de este departamento. De no ser así, no se podrá atender adecuadamente a los usuarios teniéndose como resultado un tiempo de respuesta mayor al establecido y por lo tanto un acumulamiento mayor de reportes en cola de espera. Esto ocasionaría que los usuarios paren su producción por falta de atención del Helpdesk.

En resumen, se atenderán a los siguientes equipos y sistemas:

- Un número aproximado de 1,200 equipos PC.
- 75 paquetes comerciales con licencias.
- 115 aplicaciones registradas que han sido creadas en el área de desarrollo.

Organización y reporte jerárquico incluyendo la separación de deberes.

El departamento estará conformado por:

- Un líder encargado de guiar y supervisar que se cumplan todos los servicios que brinda el Helpdesk.
- Cinco técnicos que atiendan los reportes de los usuarios vía telefónica, y de ser necesario en el lugar donde se encuentre el equipo.
- Dos personas más que generen estadísticas de los resultados obtenidos del trabajo de esta área.

Manejo y distribución de reportes de Servicios que brinda el Helpdesk.

Los reportes de servicios serán manejados por los técnicos, quienes al realizar el servicio, deberán llenarlos con los datos correspondientes, y deben ser firmados por los usuarios de conformidad con el servicio. Posteriormente, entregarán un reporte de las labores realizadas durante el día a su superior.

En la tabla 5.10. se muestra en plan de implementación.

TAREA	OBJETIVO	ENTREGABLE(S)
Capacitación del personal del helpdesk para identificar problemas de seguridad.	Que dicho personal cuente con los conocimientos necesarios para poder identificar problemas de seguridad.	Que el personal cuente con la pericia técnica, necesaria para enseñar a los usuarios como asegurar sus sistemas.
Capacitación del personal del helpdesk acerca de la organización en el manejo de incidentes.	Que dicho personal cuente con los conocimientos necesarios para reaccionar adecuadamente ante estos incidentes.	Evaluación del personal

Tabla 5.10. Plan de implementación del Help Desk.

TAREA	OBJETIVO	ENTREGABLE(S)
Capacitación del personal del helpdesk acerca de como responder ante un problema de seguridad acecuadamente, e informarlo a la persona apropiada.	Que dicho personal cuente con los conocimientos necesarios para que el soporte y las operaciones sean fundamentadas en procedimientos de seguridad.	Que todos los incidentes sean documentados y ser utilizados como la DB de conocimientos
Probar e inspeccionar el software antes de que se cargue.	Determinar compatibilidad con aplicaciones o identificar otras interacciones imprevistas.	Documentar, indicando quien evalúa el software, así como anotando todas las ventajas y desventajas que proveerá dicho software
Se deberá tener especial cuidado en la configuración y uso de utilerías poderosas para cualquier sistema.	Evitar comprometer la integridad de los sistemas activos y controles lógicos de acceso.	Documentar, indicando la capacidad de los sistemas así como la configuración realizada.
Formalizar los procedimientos y prácticas operacionales con detalle	Eliminar seguridad caduca y vigilar que el personal reciba instrucciones suficientemente detalladas. También permiten garantizar que se provea un servicio de calidad y seguro, de tal manera que las operaciones se desempeñarán correcta y eficientemente	Documentación de los procedimientos determinados y manuales operacionales de los sistemas
Formalizar y estandarizar el proceso de instalación y actualización de software por cada una de las plataformas y/o usuarios	Que el usuario no sea el responsable de la actualización del software y el área tenga mayor control de esto. Facilitar el proceso de capacitación de nuevo personal	Documentación de cada una de las instalaciones del software, incluyendo los posibles percances.

Tabla 5.10. Plan de implementación del Help Desk (continuación).

TAREA	OBJETIVO	ENTREGABLE(S)
Supervisión del personal del Helpdesk	Impedir algunos problemas, tales como "curioseando alrededor" del área física. Sin embargo, una vez que alguien tiene acceso al sistema, es muy difícil para la supervisión el impedir daño hecho mediante el proceso de mantenimiento.	Reporte del responsable de como desempeñan sus tareas.
Establecer las sanciones a las que se harán acreedores los usuarios por averías o robos, ya sea parciales o totales de sus equipos, o componentes de los mismos, de los cuales estén a su cargo	Erradicar estos incidentes que causan perdidas a la CNBV y por otro lado que los usuarios tomen todas las medidas necesarias para evitarlas.	Tabulador de las sanciones según el daño causado, así como el tiempo que tiene para cumplir con ellas.
Formalizar políticas y procedimientos para el manejo de respaldos en esta área las cuales incluyan calendarización.	Que el área cuente con los medios necesarios para que, en caso de pérdida de la información esta sea momentánea y no permanente.	Documentación de tiempos y contenidos de dichos respaldos
Se deben crear procedimientos que indiquen cómo revisar un equipo que sale de la CNBV, ya sea para la realización de alguna demo o junta, ya que puede contener software o documentación confidencial	Garantizar que no salgan equipos e información no permitidos por la CNBV.	Documentación del procedimiento para la revisión de los equipos que salen de la CNBV.

Tabla 5.10. Plan de implementación del Help Desk (continuación).

5.11. Plan y costos generales de implementación.

En la implementación de cada una de las fases que propone esta tesis, deberá seguirse un plan estricto para evitar dejar fuera de operación las actividades cotidianas de la institución.

En la Figura 5.19. y en la tabla 5.11. se propone un proceso y calendario de implementación que no impactaría en forma importante al servicio proporcionado por el área de Informática.

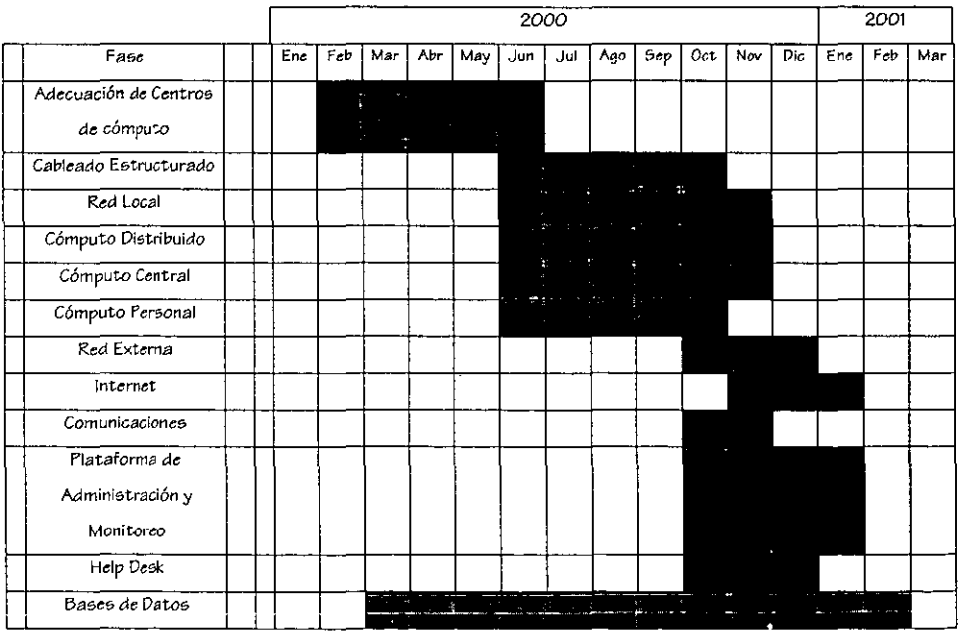


Tabla 5.11. Calendario de implementación.

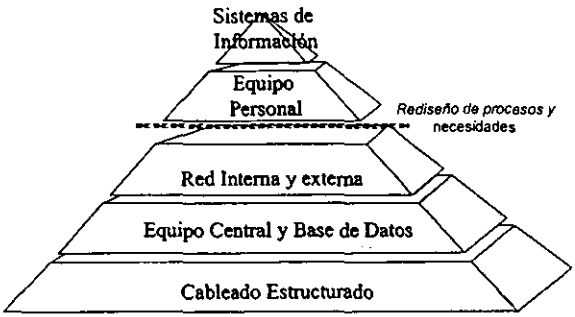


Figura 5.19. Etapas de implementación.

5.11.1 Plan de inversión.

En la tabla 5.11. se muestra un resumen de los costos para el desarrollo de cada proyecto que compone esta tesis. Los precios son aproximados y tratan de englobar el costo total de implementación.

PROYECTO	REQUERIMIENTOS	COSTO (M.N)
BASE DE DATOS INSTITUCIONAL	Adquisición de los derechos para uso de la herramienta (Base de Datos Sybase) . Software de Administración de Base de Datos Consultoría para implementación y funcionamiento de la herramienta, así como para la transferencia de conocimientos.	$3'560,000
ATENCION DE USUARIOS (Help Desk)	Centro de ayuda que abarcará todas las oficinas de la CNBV Oficinas Centrales (Plaza Inn). Oficinas Metropolitanas. 31 Oficinas en todo el interior de la República.	$1,350,000

Tabla 5.11. Costos aproximados de implementación de cada proyecto.

PROYECTO	REQUERIMIENTOS	COSTO (M.N)
INFRAESTRUCTURA	4 equipos y accesorios para cómputo central (Memoria, disco y procesadores). Se solicita actualización de dos equipos HP9000. 2 equipos HP9000 K4XX con 2 procesadores y capacidad de crecer a 4, 2GB RAM capacidad de crecer a 3.4 MB Adquisición de 2 arreglos de discos Symmetrix. 2 dispositivos de respaldo en cinta para servidores UNIX y NT (dlt). Adecuación de centros de cómputo de ambas torres (aire acondicionado, sistema contra incendio, etc.). 15 Servidores con arquitectura CISC (Intel) con las siguientes características generales: Procesador dual pentium Xeon 500 MHz. 128 MB RAM. 1 MB de memoria caché. Unidad de CDROM 24x. Tarjeta de red 10/100 Mbps. 400 computadoras personales. 66 computadoras portátiles. 60 impresoras láser. 3 digitalizadores de imágenes (scanners). Accesorios HW y SW (memoria, discos, etc.). 1500 licenciamientos de software (licencia por nodo). Plataforma de administración y monitoreo. Metodología de administración.	$48'125,000

Tabla 5.11. Costos aproximados de implementación de cada proyecto (continuación).

PROYECTO	REQUERIMIENTOS	COSTO (M.N)
INFRAESTRUCTURA PARA LA RED LOCAL (LAN)	Sistema de cableado estructurado para 1500 nodos. Se incluye voz y datos. Enlace entre edificios y backbone en pisos con fibra óptica. Cable UTP categoría 5 al usuario. Incluye enlace redundante entre torres y equipos centrales. Certificación a 15 años 2 Equipos de comunicación central (switch central). Enlace entre edificios y Backbone con FastEhernet 18 Equipos de comunicación para grupos de usuarios (switches de piso). 250 Tarjetas de red (Ethernet). 2 Estaciones de trabajo para monitoreo.	$20,670,000
PROYECTO	REQUERIMIENTOS	COSTO (M.N)
INFRAESTRUCTURA PARA LA RED DE COMUNICACIONES (WAN).	2 ruteadores centrales con interfaz FastEthernet. 8 ruteadores para grupos de usuarios con interfaz Ethernet. 2 servidores de acceso remoto con capacidad de 120 usuarios concurrentes. 1 software para seguridad en el acceso remoto (TACACS+). 4 enlaces de datos de alta velocidad (&4 Kbps.) 2 Firewalls. 1 servidor Web. Servicio de internet. Costo instalación del enlace dedicado al proveedor Renta mensual de enlace. Mantenimiento de dominio.	(4'644,900)

Tabla 5.11. Costos aproximados de implementación de cada proyecto (continuación).

Conclusiones.

Considerando que actualmente la infraestructura de cómputo y comunicaciones en la Comisión Nacional Bancaria y de Valores es heterogénea debido a la fusión de la Comisión Nacional Bancaria y la Comisión Nacional de Valores, los componentes informáticos que la conforman están llegando a su límite de capacidades de crecimiento y funcionalidad, también se carece de una falta de metodología para administrarla y además la plataforma actual no permite dar una respuesta ágil a las nuevas necesidades de sistemas de información.

Con la propuesta que realizamos en esta tesis, se tendrá una infraestructura actualizada de acuerdo a las necesidades de la CNBV, con la cual esta institución tendrá la capacidad de dar cualquier servicio informático a todo usuario interno que lo requiera: acceso a Internet, intranet, fax de red, correo, acceso a bases de datos a través de los diversos sistemas desarrollados.

Los objetivos alcanzados con esta tesis fueron los siguientes:

- Definir, diseñar y planear una infraestructura de cómputo y comunicaciones para la CNBV, que garantice la oportuna y ágil respuesta a los cambios tecnológicos que demandan la continua actualización tecnológica del medio financiero.

- Brindar servicios informáticos con la calidad y oportunidad requerida por los usuarios apoyando con ello las labores de supervisión financiera responsabilidad de la CNBV.

- Proporcionar elementos y juicios para la definición de políticas, estándares y procedimientos de operación de cada una de las áreas que administran y monitorean cada elemento de las redes de datos y comunicaciones de la CNBV.

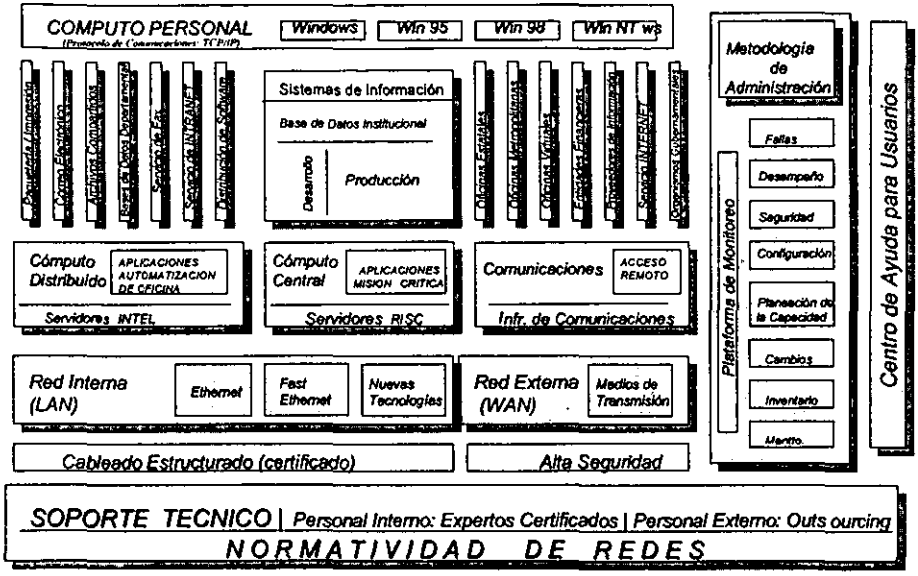
- Integrar a la CNBV a la red financiera en forma eficiente para realizar todo el intercambio de información en forma confiable y segura con cada uno de los participantes del sector.

Con la distribución de los servicios que propone este trabajo, se logrará una mayor seguridad y control en el manejo de la información, ya que algunos servicios se accederán por piso y otros serán de acceso común, de acuerdo a los requerimientos y necesidades definidos por el perfil de cada usuario.

También se mantendrá una distribución eficiente de los recursos de red, permitirá un mejor aprovechamiento de los mismos, con servidores de acceso particular por piso y servidores de acceso común, controlados y administrados desde el centro de cómputo de cada torre u oficina metropolitana.

Se optimizará el espacio físico en los centros de cómputo, ya que se implementará el apilamiento de varios servidores, manejados y controlados por una sola consola de administración y monitoreo.

Con la distribución de áreas que proponemos para dar solución a cada elemento que compone la infraestructura de cómputo de la CNBV, logramos obtener e implantar el modelo de arquitectura tecnológica que se muestra en al siguiente figura:



Se definieron y diseñaron las estructuras, características, especificaciones técnicas y modo de implementación de cada componente a través de una normatividad de redes, logrando las siguientes características:

- Una red externa (WAN) eficiente, flexible, escalable y segura con ágil respuesta para apoyar la función de supervisión y regulación de las entidades financieras.
- Utilizar la arquitectura Ethernet para las red local de datos y FastEthernet para el backbone.
- Una red interna (LAN) robusta, versátil y escalable con la característica de ser confiable en los servicios de red

- Utilizar parte de la infraestructura existente para evitar gastos innecesarios.
- Obtención de un cableado estructurado y un backbone de fibra óptica certificado que cumpla con las normas internacionales de instalación y funcionamiento.
- Procesamiento de cómputo modular clasificado en:

  Central.- Para Misión Crítica (Bases de Datos).

  Distribuido.- Para Automatización de Oficinas.

  Personal.- Para Usuario Final.

  con lo cual obtendremos una mejor calidad y eficiencia de los servicios de red
- Sistema de administración y monitoreo centralizado.
- Se contempló capacidad de crecimiento en hardware y software a futuro.
- Conexión a las oficinas regionales.
- Una plataforma escalable que soporte la nueva tecnología para la publicación de información institucional tanto interna como externa (Internet / Intranet).
- Centro de cómputo central acondicionado.
- Base de datos Institucional integral, fácil de explotar y administrar.
- Servidores departamentales.
- Migración de aplicaciones con una arquitectura cliente-servidor.
- Paquetería estándar para automatización de oficinas.
- Administración simplificada de la red mediante una metodología de informática

Esta tesis representa la planeación de cada componente para lograr una infraestructura de cómputo estable y eficiente.

Apéndice A.

Códigos para la comunicación de datos.

Codificación de datos.

El objetivo del presente apéndice es orientar en el estudio de la codificación de datos que se efectúa durante la transmisión de la información, ya sea de una manera local o remota.

Entendiendo por codificación de datos a la transformación desarrollada de ésta en forma binaria. Para ello se utilizan los códigos que correspondan a cada carácter, entiéndase letras, números, caracteres especiales y de control, que son una serie precisa de elementos binarios.

Dos son las convenciones de codificación de datos que expondremos:

- La primera se refiere a la codificación de datos que se realizan en las PCs y máquinas grandes (mainframes), conocido como lenguaje de máquina.

- La segunda representa la codificación en línea que se efectúa durante el proceso de transmisión de datos.

A continuación se describen dos de los principales códigos ASCII y EBCDIC, de los cuales se expondrá sus características y aplicaciones más importantes.

> Código ASCII (American Standard Code for Information Interchange: código americano estandarizado para el intercambio de información), también conocido como CCITT No 5, Alfabeto Internacional No. 5 (véase Figura A1) . Es un código de 8 bits o niveles, consiste de 7 niveles de información más un nivel de chequeo de paridad, la cual es una técnica de detección de errores.

Siete bits de información nos permiten una combinación de 2 a la 7 =128* combinaciones.

Un número de caracteres de control están incluidos en ASCII y son usados para iniciar otras funciones del dispositivo, diferentes a la impresión de caracteres. Algunos de los más importantes caracteres de control son:

POSICION DE BITS:				0	0	0	0	1	1	1	1
				0	0	1	1	0	0	1	1
7				0	1	0	1	0	1	0	1
,6											
,5											
,4											
|	3	2	1								
|	|	|	|								
0	0	0	0	NUL	DLE	SP	0	@	P	`	p
0	0	0	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	STX	DC2	"	2	B	R	b	r
0	0	1	1	ETX	DC3	#	3	C	S	c	s
0	1	0	0	EOT	DC4	$	4	D	T	d	t
0	1	0	1	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	ACK	SYN	&	6	F	V	f	v
0	1	1	1	BEL	ETB	./	7	G	W	g	w
1	0	0	0	BS	CAN	(	8	H	X	h	x
1	0	0	1	HT	EM	)	9	I	Y	i	y
1	0	1	0	LF	SUB	*	:	J	Z	j	z
1	0	1	1	VT	ESC	.+	;	K	[	k	{
1	1	0	0	FF	FS	,	<	L	\	l	,
1	1	0	1	CR	GS	.-	.=	M	]	m	}
1	1	1	0	SO	RS	.	>	N	^	n	. ~
1	1	1	1	SI	US	./	?	O	_	o	del
				|	|			EJEMPLO:			
				CARACTERES DE CONTROL				0110000=0 (Cero)			

Figura A 1 Código ASCII

* NOTA: ACTUALMENTE SE USA UN CÓDIGO ASCII AMPLIADO QUE INCLUYE CARACTERES INTERNACIONALES COMO LA "Ñ" Y LAS VOCALES ACENTUADAS, CARACTERES GRIEGOS, MATEMÁTICOS Y GRÁFICOS.

•ACK. (Acknowledge) Reconocimiento positivo, transmitido por un receptor como una respuesta afirmativa al que envía.

•NAK. (Negativa Acknowledge) Reconocimiento negativo, transmitido por un receptor como una respuesta negativa al que envía.

•ENQ. (Enquire) Consulta, este carácter se usa siempre como una petición de respuesta desde una estación remota

•SOH. (Start of Heading) principio de encabezado. Aparece como primer carácter de la información de un mensaje.

•STX. (Start of Text) Principio de texto, aparece como primer carácter a continuación del encabezado. Identifica, a todos los caracteres que le siguen como texto.

•ETX. (End of Text) Fin de texto, usado para terminar un texto.

•EOT. (End of Transmission) Fin de transmisión, usado para indicar la conclusión de la transmisión de uno o más textos. En procedimientos de control se utiliza como primer carácter en la, rutina Poll-Select.

•BCC. (Block Character Control) Carácter para verificar por bloque. Este carácter se envía con todos los mensajes de datos y se emplea para detectar errores en dichos mensajes.

•ETB. (End of Transmission Block) Usado para indicar el fin de un bloque de transmisión de datos.

•SYN (Synchronous) Carácter que provee un patrón de bits requeridos para la sincronización de la estación receptora.

Código EBCDIC. (Extended Binary Coded Decimal Interchange Codo: código de intercambio de codificación binaria decimal extendida). Este es un código de nivel 8, con características similares al código ASCII. El número de posibles combinaciones es de (2a la 8 = 256), lo que le da mucha flexibilidad y poder en el manejo de la información. En la actualidad junto con el código ASCII, son los más usados como códigos entre sistemas procesadores de información. A pesar de que muchas de las posibles combinaciones de este código quedan de momento sin utilizar, es posible verificar paridad, efectuar reconocimiento de transmisión, inicio y final de transmisión, etcétera. La Figura A2 muestra la arquitectura de este código.

		VALOR EQUIVALENTE DE LOS 4 ELEMENTOS BINARIOS DE PESOS MAYORES															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	NUL	DLE	DS		blanc	&	.-									0
OS	1	SOH	DC1	SOS				/		a	j			A	J		1
AR	2	STX	DC2	FS						b	k	s		B	K	S	2
DEN	3	ETX	DC3		SYN					c	l	t		C	L	T	3
TOS	4	PF	RES	BYP						d	m	u		D	M	U	4
MEN	5	HT	NL	LF	PN					e	n	v		E	N	V	5
ELE	6	LC	BS	EOB	RS					f	o	w		F	O	W	6
4	7	DEL	IDL	PRE	UC					g	p	x		G	P	X	7
LOS	8		CAN		EOT					h	q	y		H	Q	Y	8
DE	9		EM							i	r	z		I	R	Z	9
TE	10	SMM	CC	SM		C	!		:								
LEN	11	VT					$	.	#								
NA	12	FF	IFS		DC4	<	*	%	@								
EQU	13	CR	IGS	ENQ	NAK	(	)	-	'								
OR	14	SO	IRS	ACK		+	;	>	=								
VAL	15	SI	IUS	BEL	SUB	|	¬	?	"								

Figura A2 CÓDIGO EBCDIC

Códigos de línea.

La modulación por pulsos codificados consiste básicamente en convertir una señal de tipo analógico a una señal digital. La señal generada, es unipolar sin retorno a cero (NRZ) y debido a su unipolaridad tiene la característica de contar con un componente de corriente directa, por lo que no es posible transmitir esta señal por los medios de comunicación usualmente utilizados, debido a que los regeneradores de señal cuentan con un acoplamiento de transformadores. Para solucionar este y otros factores la señal es modificada por medio de un código de línea.

Código de inversión de marcas alternadas (AMI)

Existen diferentes códigos de línea siendo el más sencillo el código de inversión de marcas alternadas AMI (véase Figura A3), el cual consiste en invertir la polaridad de los pulsos "unos"(marcas) alternadamente, convirtiendo la señal en forma unipolar.

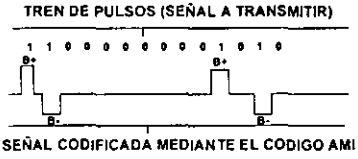


Figura A3 Código AMI

De esta manera se elimina el problema de la componente de corriente directa, sin embargo, en las secuencias largas de ceros no hay inversión de polaridad, por lo que existe el riesgo de perder la sincronía de la señal.

Código de alta densidad de orden tres (HDB3)

Otro código de línea es el HDB3 (High Density Bipolar de Degree 3: alta densidad de orden tres), es similar al código AMI, sin embargo, este código no permite más de tres ceros consecutivos, cada vez que se presenta una secuencia prolongada de ceros se divide en bloques de cuatro ceros, estos bloques se reemplaza por 00V ó B00V donde 'V' designa una violación de bipolaridad y "B " es un signo de bipolaridad suplementaria.

Existen dos posibilidades para la codificación del primer cero del bloque.

- La primera se refiere a que el primer cero de un bloque se codifica como cero si la marca que le precede de la señal HDB3 tiene una polaridad opuesta a la polaridad de violación que le precede.

- La segunda posibilidad es que el primer cero de un bloque se codifica como marca, si la marca que le precede de la señal HDB3 tiene la misma polaridad de la violación que le precede. Ver Figura A4.

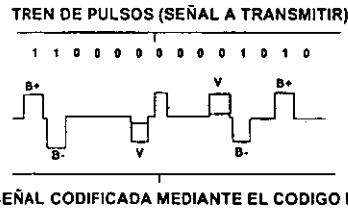


Figura A4 Código HDB3

Código de inversión de marca codificada (CMI)

El código CMI (Coded mark inversion: inversión de marca codificada), es un código de 2 niveles, sin retorno a cero en el cual el cero binario se codifica de manera que los dos niveles de amplitud, Al y A2, se obtienen consecutivamente, cada uno durante un periodo igual a la mitad de un intervalo unitario (T/2), como se ilustra en la Figura A5.

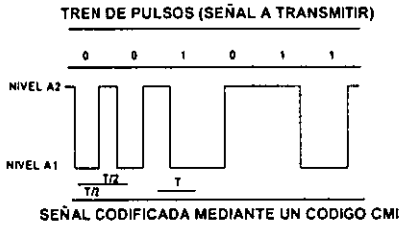


Figura A5 Código CMI

El uno binario se codifica de modo que los dos niveles de amplitud Al y A2, se obtienen alternativamente cada uno durante un periodo igual a un intervalo unitario completo (T).

Para el uno binario:

- Existe una transición positiva al comienzo del intervalo de tiempo unitario binario si el nivel precedente era Al.

- Existe una transición negativa al comienzo del intervalo de tiempo unitario binario si el último uno binario estaba codificado en el nivel A2.

- Para el cero binario, existe siempre una transición positiva en el punto medio del intervalo de tiempo unitario binario.

Apéndice B.

Características de los Sistemas de Comunicación, Normas y Estándares en México.

Sistemas de Comunicación.

La red de telecomunicaciones es un sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario.

Telefonía Convencional: Línea Conmutada y Punto a Punto.

Para disponer de un enlace permanente entre un punto y otro a través de la red telefónica, el usuario puede escoger entre adquirir una línea privada o una línea con dedicación exclusiva, (las líneas privadas también pueden conmutarse, a través de centros privados de conmutación, o centralistas). Las líneas privadas no conmutadas suelen ser de gran utilidad para aquellos usuarios que no puedan permitirse el retardo que supone establecer una conexión, o que no puedan tolerar que la llamada se bloquee si todas las líneas están ocupadas. Además, los usuarios cuyo tráfico ocupa varias horas diarias de enlace, pueden ahorrar bastante dinero utilizando una línea con dedicación exclusiva.

A continuación se definen las principales diferencias de ambos sistemas:

SERVICIOS	VENTAJAS:	DESVENTAJAS
Conmutados	▪ Flexibilidad. ▪ Economía si el volumen de tráfico es pequeño.	▪ Lentitud de respuesta ▪ Posibilidad de Bloqueo (señal de comunicado) ▪ Baja calidad ▪ Elevado costo si el tráfico es intenso
No Conmutados	▪ Da soporte a un mayor volumen de tráfico. ▪ Posibilidad de obtener una mayor calidad. ▪ Libre de bloqueos (señales de comunicado).	▪ Costo elevado si el tráfico es pequeño. ▪ Escasa flexibilidad.

Tabla B1 Esquema comparativo líneas Conmutadas y No Conmutadas.

Red Digital Integrada (RDI)

Una Red Digital Integrada (RDI) proporciona conectividad de extremo a extremo para una amplia variedad de servicios. En esencia, todos los tipos de información (voz, datos, televisión, facsímil, etc.) se transmiten mediante tecnología digital. Los objetivos principales de la RDI son cinco:

1. Ofrecer una red digital uniforme a escala mundial que proporcione una amplia gama de servicios y que emplee las mismas normas en todos los países.
2. Ofrecer un conjunto uniforme de normas para la transmisión digital entre redes.
3. Proporcionar una interfaz de usuario estándar para la conexión a la RDI, con el fin de que los cambios internos de la red no afecten al usuario final.
4. Proporcionar independencia de la aplicación con el usuario final; para la RDI no tienen relevancia las características de la misma.
5. Ofrecer portabilidad a las aplicaciones y usuarios.

La RDI se basa en tres aspectos fundamentales:

1. Normalización de los servicios que se ofrecen a los abonados, con el fin favorecer la compatibilidad internacional.
2. Normalización de la interfaz entre el usuario y la red, con el objeto de promover el desarrollo de terminales y equipos de red por parte de fabricantes independientes.
3. Normalización de las posibilidades de la red, con el fin de favorecer las comunicaciones entre usuarios y entre redes.

La RDI ofrece un pequeño conjunto de interfaces compatibles que pretende dar soporte de forma económica a una amplia variedad de aplicaciones de usuario. En la propia norma se reconoce que aplicaciones con distintas necesidades requieren velocidades de transmisión diferentes.

Enlace Satelital.

En comunicaciones vía satélite se emplean antenas de microondas para recibir las señales de radio procedentes de las estaciones emisoras en la Tierra y para devolver estas señales a otras estaciones terrenas. En la Figura B1 se ilustra este proceso. El satélite sirve de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (canal de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B, mediante una frecuencia distinta (canal de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión.

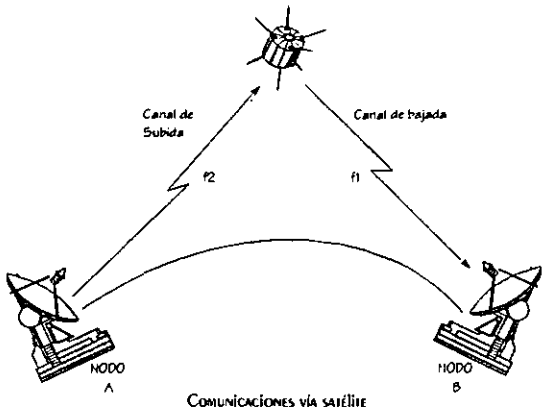


Figura B1. Comunicación vía Satelital.

Las comunicaciones por satélites presentan varias características muy atractivas. En primer lugar, los satélites poseen una enorme capacidad de transmisión. Al trabajar en la amplia banda de los Gigahertzios, cada satélite es capaz de dar soporte a varios miles de canales telefónicos.

Por otra parte, los satélites proporcionan una cobertura territorial muy amplia. Esta característica tiene un gran atractivo para las empresas muy esparcidas a lo largo de un país o con muchas sucursales o filiales en todo el mundo. Pero esta amplia cobertura plantea también serios problemas de seguridad, ya que cualquier estación puede captar las transmisiones de una empresa con sólo sintonizar la frecuencia del satélite.

El costo de una transmisión es independiente de la distancia entre las dos estaciones terrestres. Da igual que estén separadas diez o varios miles de kilómetros, el costo permanece constante, ya que las señales transmitidas desde éste pueden ser captadas por todas las estaciones, cualquiera que sea la distancia a que se encuentren.

Los satélites de comunicaciones permiten tener redes conmutadas sin necesidad de conmutadores físicos. Esta capacidad de difusión conlleva una considerable reducción de costos en comparación con las redes terrestres, que manejan innumerables líneas físicas y equipos de conmutación.

Microondas.

El objetivo de los sistemas de comunicación de microondas es transmitir información de un lugar a otro sin interrupción y una reproducción limpia en el receptor. Los canales de voz, video y datos son entrelazadas por una técnica conocida como multiplexaje que produce una señal BB. Esta señal es modulada en frecuencia a una IF y entonces convertida a RF para su transmisión a través de la atmósfera. El proceso inverso ocurre en el receptor. Las frecuencias de transmisión de microondas se encuentran en el rango de 2 a 24 GHz.

Normas y estándares.

El modelo de referencia OSI (Open System Interconection, interconexión de Sistemas Abiertos) se ha estado gestando durante varios años. Este estándar es apoyado por los principales organismos de normalización, administraciones de telecomunicación y empresas. En la Figura B2 aparece la estructura de las entidades reguladoras más importantes.

El Comité Consultivo Internacional de Telefonía y Telegrafía (CCITT) es miembro de la Unión Internacional de Telecomunicaciones (ITU), organismos de cooperación internacional fundado en 1865. ITU es hoy un cuerpo especializado dentro de las Naciones Unidas. El CCITT ha apoyado numerosos estándares, sobre todo en el campo de las redes de comunicación de datos, conmutación telefónica, sistemas digitales y terminales. El Departamento de Estado es el organismo norteamericano con voto en el CCITT.

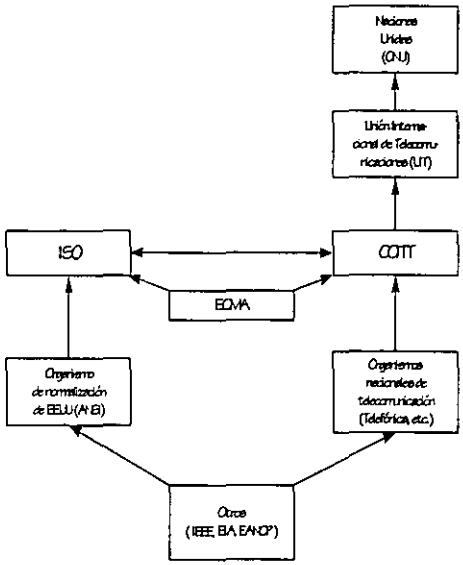


Figura B2. Estructura de las Organismos de Normalización.

La Organización Internacional de Normalización (ISO) es un cuerpo voluntario. Está integrado por los organismos normalizadores de los diferentes países miembros. En ISO intervienen principalmente los comités de usuarios y los fabricantes, a diferencia del CCITT, en el que están representadas mayoritariamente las compañías telefónicas. El ANSI (American National Standards Institute) es la principal organización americana representada en ISO.

La Asociación Europea de Fabricantes de Computadoras (ECMA) se dedica a desarrollar estándares aplicables a las tecnologías informáticas y de telecomunicaciones. No es una organización comercial, como el nombre parece sugerir, sino un grupo de normalización y estudios técnicos. Algunos subcómites de ECMA colaboran activamente con el CCITT y con ISO.

ANSI es un ente que intenta coordinar y clarificar los estándares que se aplican, de forma voluntaria, en Estados Unidos. Además de ser miembro de ISO, ANSI trabaja activamente en el desarrollo de normas para la comunicación de datos según el modelo ISO, y también en el campo de los sistemas criptográficos.

La Asociación de Industrias Electrónicas (EIA) es una asociación comercial americana que lleva muchos años desarrollando estándares. El EIA publica sus propias normas, y también envía al ANSI propuestas de normas para todo el territorio americano.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés) también tiene un larga trayectoria en al concepción de estándares. Se trata de una conocida sociedad profesional con representaciones en todo el mundo. Sus esfuerzos más recientes en el sector de las redes locales han sido objeto de gran atención. Además de las redes locales, el IEEE interviene en muchos otros estándares.

Algunas organizaciones gubernamentales han desempeñado papeles destacados en el desarrollo de normas internacionales. Como comentábamos anteriormente, el Departamento de Estado Norteamericano tiene voto en el CCITT. El NCS (National Communications System) es un consorcio de agencias federales con un gran peso en el sector de las telecomunicaciones. El NCS colabora muy estrechamente con otros organismos como EIA, ISO y CCITT. Uno de sus objetivos es potenciar el peso de estas entidades federales en las decisiones de los organismos normalizadores internacionales. La organización NBS (National Bureau of Standards) también es muy activa en los comités internacionales. En la actualidad interviene en la especificación de los niveles superiores del modelo OSI.

Estado Actual y Tendencias de las Telecomunicaciones.

Durante algún tiempo se consideraba a la inversión en infraestructura de telecomunicaciones tanto para empresas como para países como una necesidad exclusiva de las entidades más avanzadas. Recientemente hemos vivido un cambio mundial en la manera de obrar y competir que nos enfrentan a una nueva realidad. Las telecomunicaciones no son ya privilegio de unos cuantos, sino necesidad de todo país o empresa que desee participar en el cambio hacia un nuevo orden mundial.

Infraestructura Tecnológica.

La tecnología puede ser medida en dos ambientes diferentes: uno es el "estado del arte" (state of the art), que normalmente se utiliza para designar el último adelanto tecnológico recién salido del laboratorio, y otro que se denomina "infraestructura tecnológica". El primero indica lo que la tecnología es capaz de lograr y adelanta el futuro de la aplicación masiva; y el segundo señala lo que la industria ha logrado aplicar en volumen de aplicaciones confiables y el grado de avance en diversas industrias, países o regiones.

Necesariamente la tecnología de telecomunicaciones se encuentra ligada a la tecnología de computación, ya que es el adelanto de esta última el que impulsa su desarrollo.

En Francia el gobierno ha invertido fuertemente desde los '70s en infraestructura de comunicaciones, fundamentalmente alrededor de un sistema llamado Minitel que a la fecha ofrece más de 13,000 servicios de información a empresas y al público en general.

Inglaterra introdujo en 1984 la primera versión de la Red Digital de Servicios Integrados (ISDN) que es una red de telecomunicaciones pública capaz de transmitir voz, datos, música de calidad digital, textos e imágenes a muy alta velocidad y que constituye el fundamento de la nueva generación de redes de valor agregado.

Japón la ofreció en 1988 y Francia en 1989 a la fecha todas las ciudades de Inglaterra, Francia y Japón tienen acceso a una Red Digital de Servicios Integrados.

En México, Teléfonos de México introdujo una versión recortada de la ISDN denominada Red Digital Integrada (RDI) en Enero de 1991. A la fecha tiene conectados 3,000 nodos del tipo denominado E1 con grandes usuarios corporativos.

En el área de infraestructura de telecomunicaciones algunos logros se han obtenido recientemente. La contratación y el lanzamiento de la nueva generación de satélites de telecomunicaciones Solidaridad 1 y 2, ofreciendo además una vida útil de 14 años en lugar de 8, con una cobertura continental y no sólo nacional. También Telmex firmó el inicio de la construcción del cable transatlántico de fibra óptica Columbus que unirá nuestro país con Europa.

Sin embargo el ritmo de inversión en otros países más avanzados es tan abrumadoramente mayor, que es fácil entender que en vez de acercarnos tecnológicamente la diferencia en infraestructura será cada vez mayor. Ya hay indicativos en el sentido de que nuestro gobierno paulatinamente está entrando en un proceso de apertura al consignar a iniciativa privada de los servicios de proveedor transporte masivo de voz, datos y, recientemente, larga distancia. En el principio sólo para redes privadas y en el futuro, cuando el contrato de Telmex así lo permita, también a redes de servicio público.

Conectividad e Interoperabilidad.

Es fácil imaginarse que la reciente carrera por lograr la conectividad, local y remota ha logrado poner en contacto a una gran diversidad de equipo de cómputo. Desgraciadamente muchos de estos equipos no fueron originalmente concebidos para interactuar transparentemente en un ambiente de conectividad total.

A pesar del gran despliegue técnico y publicitario por lograrlo, la realidad actual es que ni los equipos se conecten eficientemente, sin problemas, ni los usuarios muestran un grado aceptable de confianza en las redes de computadoras.

La tendencia no puede ser más clara: Durante los siguientes años deberemos exigir y ofrecer mucha mayor interoperabilidad.

Existen diversas definiciones que integran este concepto:

- ☑ Utilización de toda la base instalada de computadoras del usuario sin importar la marca de fabricante o el sistema operativo que utiliza.
- ☑ Acceso instantáneo y transparente a toda la información disponible en la organización sin importar su localización geográfica.
- ☑ Eliminación de redundancias en el procesamiento o almacenamiento de la información. Una determinada base de datos debe existir sólo en un lugar en la organización y un determinado proceso de la información debe ocurrir sólo una vez en el sistema.

Interoperabilidad es lograr que los equipos y los sistemas trabajan eficientemente entre sí evitando redundancias en la organización. Es permitir que un usuario de la red tenga todos los recursos informáticos de la organización a su alcance sin importar que pantalla se encuentre viendo. Interoperabilidad nos da la oportunidad de reducir nuestros

presupuestos de compra de equipo al lograr una utilización máxima de la tecnología evitando su obsolescencia prematura.

La interoperabilidad resuelve el reto de ver a una red como un solo sistema y no como un grupo de sistemas conectados. La tendencia de los siguientes dos y tres años es ver a los sistemas de diversas compañías interactuando entre sí como si fueran un solo sistema.

A menudo se escucha sobre proyectos que intentan conectar los sistemas de diversas compañías, clientes y proveedores para lograr procesos de satisfacción total, bajar inventarios, aumentar eficiencias, reducir al mínimo su tiempo de respuesta a las necesidades de los clientes. Pero en esos momentos es viable preguntarse cómo será posible lograrlo si no es con un muy alto grado de interoperabilidad.

En el futuro la búsqueda de la interoperabilidad forzará inevitablemente el crecimiento de los sistemas abiertos, de las plataformas compatibles, esto propiciará más funciones y adquisiciones de compañías anteriormente rivales. Se verá con gusto el desarrollo de más software de comunicación global como sistemas operativos de múltiples servidores, programas de localización mundial de usuarios de la red (Global Naming) y hará que los participantes del mercado se posicionen cada vez más en el ofrecimiento de valores agregados y menos en la diferenciación tecnológica.

Los Usuarios Móviles siempre en contacto.

Uno de los conceptos que se encuentra tomando apenas forma es el de los usuarios móviles. Hace dos años se afirmó que todas las computadoras de escritorio tendrían tarde o temprano que terminar conectadas a una red y que las computadoras portátiles (laptops) serían las únicas que continuarían siendo computadoras personales (PCs) en el estricto sentido de la palabra. Esta aseveración continua siendo cierta, con

una variación: Cada vez más veremos que el usuario de computadoras portátiles también debe tener acceso a la red.

Esto se logrará básicamente a través de dos modalidades. Por un lado la tecnología que se podría llamar "red desconectada", en la que el usuario móvil realiza tareas de comunicación tales como captura de información para una base de datos, o envío de correo electrónico cuando su computadora no se encuentra en la red. Al llegar a su base de operaciones, típicamente en su oficina, se conecta momentáneamente y se realiza operaciones automáticas de entrega y recibo de información dándole el acceso deseado a la información procesada durante el periodo en que la computadora se encontró desconectada de la red.

Por otro lado, la tecnología de conectividad inalámbrica (wireless networks) permitirá al usuario móvil acceso instantáneo y regular a su red. Actualmente existen ya implantaciones de esta modalidad tanto en LANs (WaveLan de NCR) como en WANs (radiomodems) sin embargo el estado actual de la tecnología no ofrece aún una alternativa en confiabilidad y velocidad similar a las redes vía cable.

Apéndice C.

La red de área local: Normatividad y Estándares.

Red de área local.

La habilidad para transportar datos de una manera rápida, flexible y económica es requerimiento esencial de una red de información efectiva. Dentro de un área geográfica limitada, una red LAN (Local Area Network, red de área local), provee un medio común para interconectar e integrar elementos heterogéneos utilizando un sistema de comunicaciones compartido.

Una LAN incluye las siguientes especificaciones:

1. Un medio de comunicaciones a través del cual los datos pasan de un dispositivo a otro.
2. Adaptadores de red (también conocidas como tarjetas de red), que proveen un dispositivo con una interfaz al medio de comunicación.
3. Una topología física a través de la cual el medio es extensivo a los demás adaptadores.
4. Un protocolo de acceso que asegura un orden y un uso adecuado del medio.
5. Un formato lógico de los datos para transmitir a través del medio.
6. Una especificación eléctrica de la codificación de datos a ser transmitidos.

Los puntos a considerar en el diseño de la red son:

1. Accesibilidad. Puntos de conexión, los cuales pueden ser fácilmente extendidos en cualquier otra ubicación dentro del edificio.
2. Capacidad. La red puede proveer a cada usuario con el suficiente ancho de banda para que pueda realizar todas sus operaciones.

3. Seguridad en su funcionamiento. Tolerancia a fallas en elementos individuales de la red, y proveer un nivel de servicio consistente con su papel de controlador de la red.
4. Administración. La red ofrece un medio de administración de su configuración y crecimiento, de control de acceso a la red y del flujo del tráfico.
5. Mantenimiento. Reparaciones, actualizaciones, expansiones y cambios pueden ser realizados con un impacto mínimo sobre la mayoría de los usuarios de la red.
6. Compatibilidad. Estándares y protocolos que permiten que varios tipos de equipo se puedan conectar a la red.
7. Economía. La red provee conexiones a un costo efectivo.

Tipos de cableado.

Cable par trenzado.

Uno de los medios de transmisión más antiguo, y todavía uno de los más ampliamente usados es el par trenzado. Un cable par trenzado consiste de alambres de conductores (por lo general, de cobre de 1 mm. de espesor) aislados individualmente y cubiertos por una protección común. Los alambres se entrelazan de manera helicoidal. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor (dos cables paralelos constituyen una antena simple, en tanto que un par trenzado no).

La aplicación más común del par trenzado es el sistema telefónico. La distancia que pueden recorrer estos cables es de varios kilómetros sin necesidad de amplificar señales, pero sí es necesario incluir repetidores en distancias más largas. Cuando hay

muchos pares trenzados colocados paralelamente que recorren distancias considerables, como podría ser el caso de los cables de un edificio de departamentos que se dirigen a la oficina de teléfonos, estos se agrupan y se cubren con una malla protectora. Los pares dentro de estos agrupamientos podrían sufrir interferencias mutuas si no están correctamente entrelazados.

El par trenzado se puede utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios megabits por segundo (Mbps), en distancias de pocos kilómetros. Debido a su adecuado comportamiento y bajo costo, los pares trenzados se utilizan ampliamente y es probable que su presencia permanezca por muchos años.

El cable multipar es extensamente utilizado en redes de telecomunicaciones. Recientemente, el cableado existente ha sido adaptado para usarse en redes de área local digitales, esta claro que el cable multipar tendrá una fuerte influencia en el desarrollo de servicios digitales futuros que se construirán tomando como base una red telefónica.

Par trenzado sin blindar

Actualmente, se utilizan dos tipos básicos de cable trenzado, uno de ellos es el conocido como UTP (UTP=*Unshielded Twisted Pair*), es el tipo de cable de cobre de menor costo. UTP consiste de dos alambres de cobre trenzados y recubiertos por una delgada capa de plástico.

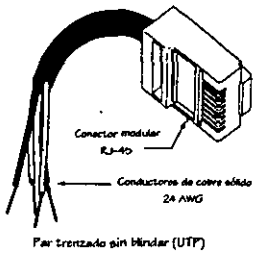


Figura C1. Cable UTP con conector RJ-45.

Este tipo de cable es muy utilizado en cableado telefónico, lo cual constituye una ventaja. En muchos edificios se emplean cuatro cables UTP, de los cuales el teléfono requiere dos, y los otros se dejan libres para servicios especiales telefónicos, o bien para datos.

Los más comunes estándares de red, tales como Ethernet y Token-Ring, requieren dos pares trenzados, uno para transmitir y otro para recibir. Con la excepción del cable coaxial, los conductores en un cable de datos deben estar trenzados juntos; la función del trenzado es el de eliminar las posibles interferencias eléctricas entre ellos, además ayuda contra la interferencia externa y atenúa el ruido de radiofrecuencias. En la práctica, es difícil eliminar las interferencias de manera completa, y de hecho en algunos edificios esto puede convertirse en un verdadero problema si existen dispositivos eléctricos muy cercanos al cable, como por ejemplo, un elevador.

A continuación se enumeran las ventajas y desventajas de UTP:

Ventajas:

- ☑ Relativamente barato.
- ☑ Los accesorios son también relativamente baratos.
- ☑ Fácil de trabajar con él (manejable).
- ☑ Tecnología bien establecida y bien definida.
- ☑ Muchos edificios están cableados con UTP.

Desventajas.

- ☑ Ancho de banda limitado.
- ☑ Susceptible a interferencia magnética.

Par trenzado blindado.

Mejor conocido como STP (STP=*Shielded Twisted Pair*). A diferencia de UTP, los alambres de cobre de par trenzado están individualmente blindados con una coraza de aluminio. La coraza esta aterrizada y previene la interferencia y radiación de señales. Como cada par en un cable multipar esta protegido, la interferencia no es un problema en STP.

Como consecuencia STP cubre una distancia mayor que UTP. Por ejemplo, La distancia máxima entre una estación y un *hub* es de 300 metros para STP, mientras que es de sólo 100 metros para UTP.

La mayoría de las redes que emplean este tipo de cable son el estándar IEEE 802.5 Token-Ring. Las ventajas de STP son:

Ventajas:

- ☑ Cubre una distancia mayor que UTP.
- ☑ Gran resistencia a la interferencia.

Desventajas.

- ☑ Más caro que UTP e incluso que algunas variedades de cable coaxial.
- ☑ Es más grueso que UTP y muchas variedades de coaxial, por los que no es muy manejable.

Cable Coaxial.

El cable coaxial, es otro típico medio de transmisión. Un cable coaxial consiste en un alambre conductor centrado (núcleo), el cual se encuentra rodeado por un material aislante. Este material esta a su vez, rodeado por un conductor cilíndrico compuesto por un aislador en su parte interna y por material que sirve como protección y conductor en su parte externa. Los dos conductores son aislados de otros usando varios materiales dieléctricos, incluyendo plástico y gas. El conductor externo puede consistir de una o más capas de metal trenzado, cuando se necesita flexibilidad, o tubo de metal sólido, cuando gran protección o rigidez es requerida. En las Figuras C2., C3. y C4. se muestran las características de este tipo de medio.

Hay dos tipos de cable coaxial que se utilizan ampliamente, uno de ellos es el cable de 50 ohms, que se utiliza en la transmisión digital; el otro tipo, es el cable de 75 ohms, que se emplea en la transmisión analógica.

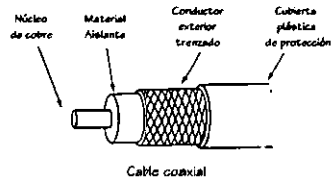


Figura C2. Cable coaxial.

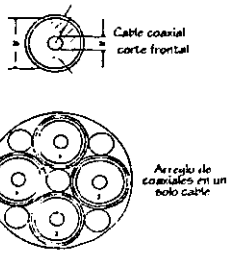


Figura C3. Cable coaxial y cable multicoaxial.

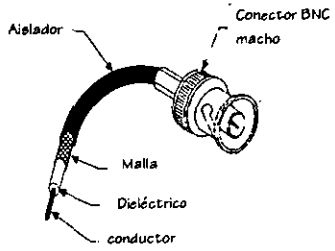


Figura C4. Ejemplo de cable coaxial con conector BNC.

El cable coaxial tiene un gran número de ventajas como medio de transmisión. La construcción del cable coaxial provee una buena combinación de un gran ancho de banda y una excelente inmunidad al ruido; lo que permite una gran confiabilidad en la transmisión y poca pérdida de datos a altas frecuencias. El cable coaxial puede ser usado para transmitir un gran número de conversaciones telefónicas, alta velocidad de datos, y un gran número de canales de televisión. Se emplea en redes como columna vertebral (backbone) en el cableado cuando se requiere un gran ancho de banda para soportar a varias computadoras.

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

El cable coaxial ha sido ampliamente utilizado en redes de área local, para transmisiones de larga distancia del sistema telefónico, en redes en ciertas porciones de alta densidad de tráfico, también es empleado en zonas de congestión de radiofrecuencias. También se emplea continuamente en sistema de televisión por cable.

A continuación se enumeran las ventajas y desventajas del cable coaxial:

Ventajas:

- ☑ Fácil de trabajar con él (manejable).
- ☑ Resistente a las interferencias.
- ☑ Gran ancho de banda.
- ☑ Tecnología bien respaldada.
- ☑ El empleo común de cable coaxial en edificios.

Desventajas:

- ☑ Más caro que el par trenzado
- ☑ No es soportado para algunos estándares de redes, como Token-Ring

Fibras Ópticas.

El desarrollo de la tecnología óptica ha hecho posible la transmisión de información mediante pulsos de luz. Un pulso de luz puede utilizarse para indicar un valor 1; la ausencia de pulso indicará la existencia de valor 0. La luz visible tiene una frecuencia de alrededor de 0^8 MHz, por lo que el ancho de banda de un sistema de transmisión óptica presenta un potencial enorme.

Un sistema de transmisión óptica consta de tres componentes: el medio de transmisión, la fuente de luz y el detector. El medio de transmisión consiste de un muy fino cilindro de vidrio o silicio fundido, llamado el núcleo; rodeado de una capa concéntrica también de vidrio, llamada cubierta. La fuente de luz puede ser un LED (diodo emisor de luz), o un diodo láser; cualesquiera de los dos emite pulsos de luz cuando se le aplica una corriente eléctrica. El detector es un fotodiodo que genera un pulso en el diodo láser en el extremo de una fibra óptica, y un fotodiodo lo recibe en el otro extremo. Se tiene una transmisión de datos unidireccional que acepta una señal eléctrica, la convierte y la transmite por medio de pulsos de luz y, después, reconvierte la salida en una señal eléctrica, en el extremo receptor.

El vidrio en la cubierta tiene un índice de menor refracción que el vidrio en el núcleo (la luz viaja más lentamente en el núcleo que en la cubierta). Cuando un rayo de luz pasa de un medio con alto índice de refracción a un medio con menor índice de refracción, el rayo es dirigido en dirección al medio original. De aquí que, si un rayo de luz es lanzado dentro del núcleo de la fibra óptica en un ángulo lo suficientemente oblicuo, este es reflejado de regreso al núcleo por la cubierta. El proceso es repetido y así es como viaja el rayo a través de la fibra. En otras palabras, la diferencia entre los índices de refracción entre los dos materiales guían la luz de un extremo al otro.

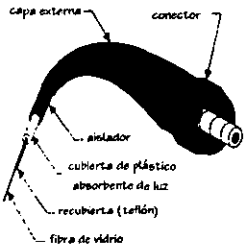


Figura C5. Construcción de cable de fibra óptica.

Fibra multimodo.

La luz es introducida en una gran variedad de ángulos. En algunos ángulos, la luz escapa de la fibra y es absorbida por la cubierta. En otros ángulos, la luz es continuamente reflejada y se repite el proceso. La fibra multimodo tiene el menor ancho de banda de los tres tipos, y soporta anchos de banda hasta de 200 MHz/km.

Multimodo con índice graduado.

Utiliza fibra de vidrio en la cual el índice de refracción es variado. La luz permanece más coherente, por lo que el ancho de banda es mayor. Este tipo de fibra óptica es el más

empleado en redes de área local; da soporte a anchos de banda en un rango de 100 MHz/km. a 3 GHz (giga o billones de hertz).

Ya que las señales de luz pueden seguir diferentes trayectorias a través del cable multimodo, las señales pueden tomar entonces diferentes caminos hasta llegar al receptor.

Modo sencillo.

Tiene el mayor ancho de banda. En este tipo de cable, el diámetro de la fibra de vidrio es reducido hasta que sólo una señal pueda ser transmitida. Esto elimina las reflexiones de los cables multimodo, e incrementa en gran medida el ancho de banda. Soporta hasta 50 MHz/km. Algunos diámetros comunes son: 50, 62.5, y 100 micrones. Por ejemplo, la de 62.5 micrones es la más común; es el estándar para FDDI.

El tamaño tan pequeño trae como consecuencia una dificultad, los extremos de las fibras deben estar cuidadosamente alineadas.

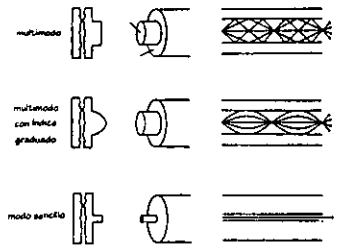


Figura C6. Fibra óptica; multimodo, multimodo con índice graduado y modo sencillo.

Los enlaces de fibra óptica están siendo empleados en diferentes países en la instalación de líneas telefónicas de larga distancia, y esta tendencia seguramente

continuará en las siguientes décadas, y será cada vez mayor la sustitución del cable coaxial por fibras, en un número cada vez más grande de aplicaciones.

Una razón importante para utilizarla es el gran ancho de banda al que le da soporte, dependiendo de la distancia y del tipo de fibra. Teóricamente, en un kilómetro de largo, puede alcanzar velocidades del orden de 100 Mbps, a medio kilómetro alcanza aproximadamente los 200 Mbps. El ancho de banda esta especificado en términos de megahertz por kilómetro (MHz/km.).

Las velocidades actuales están limitadas por el tipo de red. Ethernet por ejemplo es una red de 10 Mbps. Hay versiones de 4 Mbps y 16 Mbps de Token-Ring. FDDI (la veremos posteriormente) tiene un límite teórico de 100 Mbps, Fast Ethernet a 100 Mbps y ATM que actualmente maneja 155 Mbps. Es posible combinar múltiples señales de red en una sola, mediante una técnica llamada *multiplexaje*. Una fibra, puede utilizando esta técnica, transmitir las señales de 10 Ethernet separadas entre dos edificios; de cualquier forma cada Ethernet individual sigue funcionando a una razón de 10 Mbps.

Un tipo de red en especial es la Interfaz para Distribución de Datos a través de fibra, más conocida como FDDI (*Fiber Distributed Data Interfaz*) fue diseñada para aprovechar el cableado por fibra óptica. Sin embargo también puede utilizarse en otros tipos de red como: Ethernet, Token-Ring, ARCnet, Fast Ethernet y ATM.

Ventajas:

- ☑ El mayor ancho de banda.
- ☑ Tiempo de vida muy largo.
- ☑ Más pequeño y más ligero que el cobre.

Desventajas:

- ☑ Costo inicial muy alto.
- ☑ Más difícil y tiempo de instalación más lento que la tecnología del cableado de cobre.

Modelo de Referencia OSI.

En la Figuras C1 se muestra el modelo de referencia OSI, basado en la propuesta desarrollada por la Organización Internacional de Normas más conocida por sus siglas en inglés ISO (International Standard Organization), como un primer paso hacia la normalización internacional de varios protocolos. A este modelo se le conoce como Modelo de Referencia OSI (Open System Interconnection), interconexión de sistemas abiertos de la ISO, porque precisamente se refiere a la conexión de sistemas heterogéneos, es decir, a sistemas dispuestos a establecer comunicación con otros distintos. En forma abreviada, lo llamaremos sencillamente modelo OSI.

Capas del Modelo OSI.

El modelo OSI tiene siete capas. Por sí mismo no es una arquitectura de red, dado que no especifica, en forma exacta, los servicios y protocolos que se utilizarán en cada una de las capas. Sólo indica lo que cada capa deberá hacer. Sin embargo, la ISO también ha generado normas para todas las capas, aunque éstas, estrictamente hablando, no forman parte del modelo.

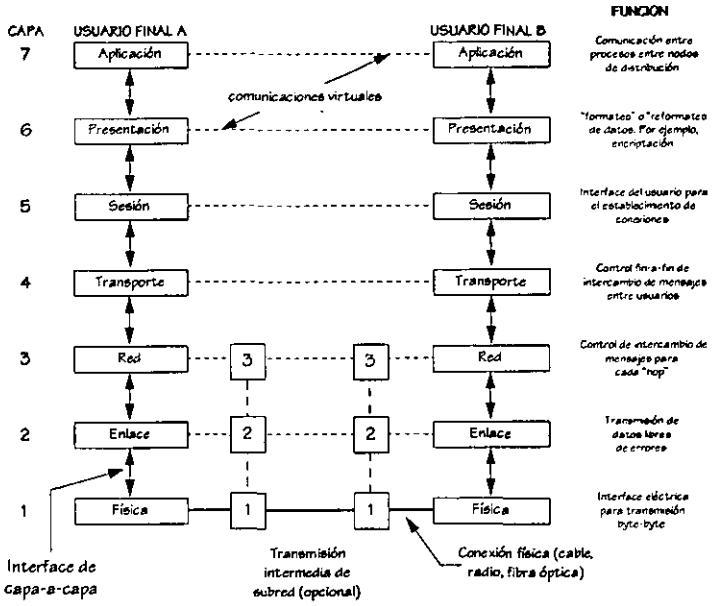


Figura C1. Modelo OSI de ISO.

- La información pasa físicamente sólo a través de la capa 1.

  Las capas superiores se conectan a través de conexiones lógicas virtuales

Capa física.

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación.

Capa de enlace.

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

tramas de datos (típicamente constituidas por algunos cientos de octetos), y las transmita en forma secuencial y procese las tramas de asentimiento, devueltas por el receptor.

Capa de red.

La capa de red se ocupa del control de la operación. Un punto de suma importancia en su diseño, es la determinación sobre cómo encaminar los paquetes del origen al destino.

Capa de transporte.

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de la red y asegurar que todos ellos lleguen correctamente al otro extremo, de tal forma que aísle la capa de sesión de los cambios inevitables a los que está sujeta la tecnología de hardware.

Capa de sesión.

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se utilizan en algunas aplicaciones.

Capa de presentación.

La capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

Capa de aplicación.

Los protocolos de la capa de aplicación verifican la semántica de la información recibida y enviada a través de las capas inferiores del modelo OSI.

Arquitectura de Redes de Cómputo.

La instalación y la operación de una red de cómputo depende totalmente de su arquitectura, la cual define la forma en que están conectados los nodos, la velocidad en que se puede transmitir la información y la seguridad de la misma. Es importante dejar bien definidos cada uno de los conceptos y elementos que intervienen en la configuración de una red de trabajo sea de forma local o amplia.

Topologías.

La configuración de una red suele conocerse como topología de la misma. La topología describe la forma de conexión de los equipos, es decir la forma física de interconexión de los equipos de cómputo que conforman la red.

Así pues, tenemos las topologías de red más comunes que se describen a continuación:

- ☑ Topología árbol (jerárquica).
- ☑ Topología horizontal (bus).
- ☑ Topología estrella.
- ☑ Topología anillo.
- ☑ Topología en malla.

Topología de Árbol.

La estructura tipo árbol (jerárquica) es una de las más extendidas en la actualidad. El software que controla la red es relativamente simple, y la topología proporciona un punto de concentración de las tareas de control y de resolución de errores. En la mayoría de los casos, la estación de trabajo situada en el nivel más elevado de la jerarquía es la que controla la red, Figura C2.

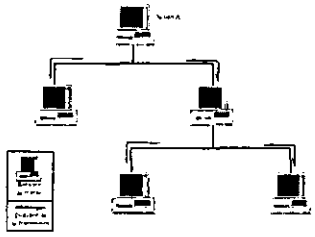


*Figura C2. **Topología de Árbol (jerárquica).***

Aunque la topología árbol resulta interesante por ser fácil de controlar, puede presentar ciertos problemas en cuanto a la posibilidad de aparición de cuellos de botella.

Topología Bus.

En la Figura C3 se ilustra la topología horizontal o en bus. Esta estructura es frecuente en las redes de área local. Es relativamente fácil controlar el flujo de tráfico entre las distintas estaciones de trabajo, ya que el bus permite que todas las estaciones reciban todas las transmisiones, es decir, una estación puede difundir la información a todas las demás.

La principal limitación de una topología horizontal está en el hecho de que suele existir un solo canal de comunicaciones para todos los dispositivos de la red. En consecuencia, si el canal de comunicaciones falla, todas la red deja de funcionar.

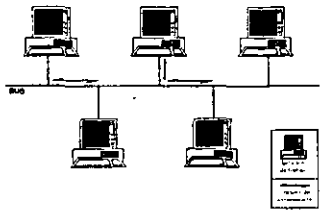


*Figura C3. **Topología de Bus (Horizontal).***

Topología Estrella.

La topología en estrella es una de las más empleadas en los sistemas de comunicación de datos. Todo el tráfico emana del núcleo de la estrella, que en la Figura C4. es el nodo central, marcado como "A". El nodo "A" es por lo general una computadora que posee el control total de las estaciones de trabajo conectadas a ella. La configuración en estrella es, por tanto, una estructura muy similar a la de la topología jerárquica, aunque su capacidad de procesamiento distribuido es limitada.

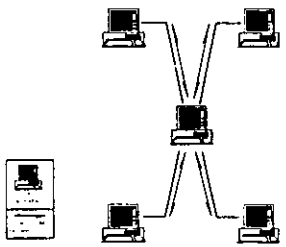


*Figura C4. **Topología estrella.***

Topología Anillo.

La estructura en anillo es otra configuración bastante extendida. Mostrada en la Figura C5, la topología anillo se llama así por el aspecto circular del flujo de datos. Los

datos fluyen en una sola dirección, y cada estación recibe la señal y la transmite a la siguiente del anillo. La organización en anillo resulta atractiva porque con ella son bastante raros los embotellamientos, tan comunes en los sistemas estrella o árbol. Cada miembro sólo ha de llevar acabo una serie de tareas muy sencillas: aceptar los datos, enviarlos a la estación de trabajo conectada al anillo o retransmitirlos al próximo miembro del mismo. El inconveniente en esta configuración es que todos los elementos del anillo están unidos por el mismo canal. Si falla el canal entre dos nodos toda la red se interrumpe. Por lo que algunos fabricantes construyen conmutadores que dirigen los datos automáticamente, evitando el nodo afectado.

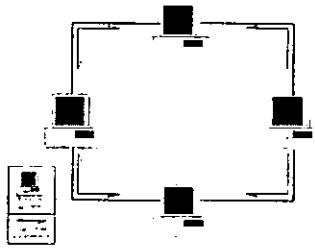


Figura C5. ***Topología Anillo.***

Topología en malla.

La topología en malla, representada en la Figura C6, se ha venido empleando durante los últimos años. Es atractiva por su relativa inmunidad a los problemas de embotellamiento y averías. Todo debido a la variedad de rutas factibles a través de distintas estaciones de trabajo y equipos de conmutación de datos, es posible orientar el tráfico por rutas alternativas, en el supuesto caso de que algún nodo esté averiado u ocupado. A pesar de que la realización de este método es compleja y costosa, muchos usuarios la prefieren entre otras alternativas. Además, para proporcionar dichas funciones, la lógica de control de los protocolos de una red tipo malla puede llegar a ser extremadamente complicada.

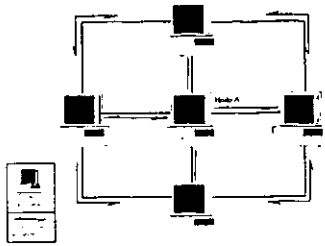


Figura C6. ***Topología en malla.***

Consideraciones en el diseño de una topología.

Una vez definidos los diferentes tipos de red, es importante considerar que a la hora de establecer la topología de la misma, el diseñador ha de plantearse tres objetivos principales:

1. Proporcionar la máxima fiabilidad posible, para garantizar la recepción correcta de todo el tráfico (encaminamiento alternativo).
2. Encaminar el tráfico entre la estación de trabajo transmisora y la receptora a través del camino más económico dentro de la red (aunque, si se consideran más importantes otros factores, como la fiabilidad, este camino de costo mínimo puede no ser el más conveniente).
3. Proporcionar al usuario final un tiempo de respuesta óptimo y un caudal eficaz máximo. Para reducir al mínimo el tiempo de respuesta hay que acortar el retardo entre la transmisión y la recepción de los datos de una estación de trabajo a otra.

Redes Locales de Alta Velocidad.

Cuando se requiere de una red de alta velocidad para distancias cortas, es recomendable utilizar la tecnología de fibra óptica, la cual posee un gran ancho de banda. A continuación revisaremos algunas de las tecnologías empleadas en redes LAN de alta velocidad:

FDDI

FDDI (Fiber Distributed Data Interfaz), o bien Interfaz para la Distribución de Datos a través de Fibra; es una red LAN del tipo *Token-Ring* de alto rendimiento basada en fibra óptica la cual corre a velocidades por encima de los 100 Mbps hasta una distancia de 200 Km., y soporta hasta 1000 estaciones. Puede ser utilizada en la misma forma que cualquier otra red LAN 802, pero su ancho de banda es mucho mayor, otro uso común es el de columna vertebral (*backbone*), para enlazar a otras LANs de menor tamaño. Tal como se muestra en la Figura C7.

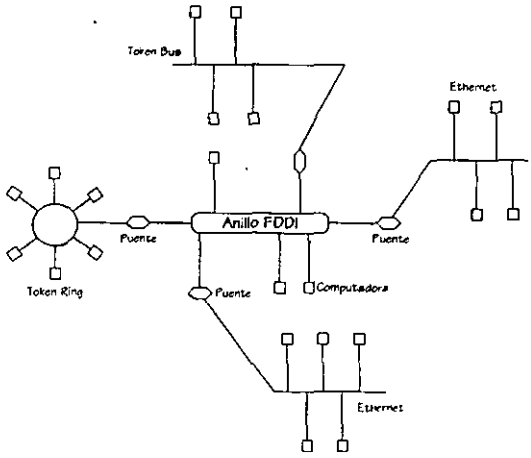


Figura C7. Un anillo FDDI utilizado como backbone *para interconectar otras LAN's.*

FDDI utiliza fibra óptica multimodo (para que la velocidad sea de 100 Mbps), también emplea LED's en lugar de láser, no sólo por el costo sino porque en ocasiones se conecta directamente a la estación del usuario. La especificación de diseño de FDDI determina un margen de error de 1 en 2.5×10^{10} bits. Aunque algunas implementaciones pueden mejorarlo.

El cableado de FDDI consiste de dos anillos de fibra óptica, uno transmitiendo por pulsos de reloj, el otro por un contador de pulsos de reloj, si uno de falla, el otro puede ser usado como respaldo. Si ambos fallan al mismo tiempo, los dos cables pueden ser unidos y forman un anillo de aproximadamente la mitad del tamaño.

Fast Ethernet

Una propuesta de la IEEE del comité 802.3 fue la de crear una red LAN que mantuviera el estándar de Ethernet, pero más rápida, esto creó otro comité denominado 802.12.

La idea fundamental detrás de Fast-Ethernet fue sencilla: mantener todos los viejos formatos, interfaces, y reglas de procedimientos; pero reduciendo el tiempo entre bits de 100 ns a 10 ns. Técnicamente era posible emplear 10Base-5 o 10Base-2 y aún detectar colisiones simplemente reduciendo el tamaño máximo del cable entre un factor de 10 (Ten-Factor). De cualquier forma la ventajas del cableado 10Base-T esta basado enteramente en este diseño. Todos los sistemas de Fast-Ethernet usan *hubs*; no son permitidos cableados con conectores BNC.

Medidas del funcionamiento de una red

Tres medidas efectivas del funcionamiento de una red son:

1. **Fiabilidad.** La probabilidad de que un componente del sistema no falle. Esto comúnmente se expresa como *tiempo entre falla* (MTBF=mean time between failures).
2. **Disponibilidad.** La probabilidad de que los servicios del sistema estén disponibles en cualquier instante de tiempo, a pesar de la demanda. A nivel de usuario, esto se expresa como la disponibilidad de la línea, o la probabilidad de que la petición de servicio de un usuario sea atendida.
3. **Calidad de servicio.** La rapidez con que el sistema puede ser reparado en caso de una falla eventual. Esto se expresa frecuentemente como *tiempo en ser reparado* (MTTR=mean time to repair).

Protocolos de Comunicación

Un protocolo de comunicación es en su forma más simple, la forma en que dos o más equipos de cómputo intercambian su información. En computación, un protocolo es necesario para que dos ETDs tengan un método a través del cual envíen y reciban información. Podemos ver una primera representación física y lógica del protocolo de la siguiente manera:

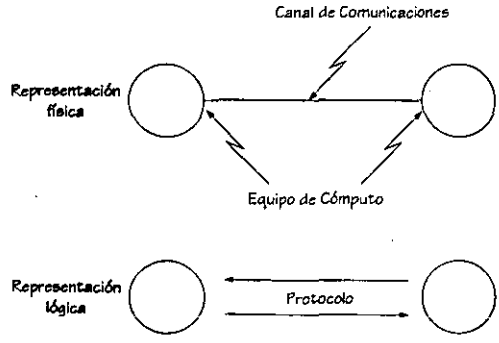


Figura C8. ***Representación física y lógica de un protocolo.***

El protocolo es, en otras palabras, la abstracción lógica del proceso que permite que dos diferentes máquinas compartan información. Son tres las funciones fundamentales que un protocolo debe realizar:

1. El establecimiento de las convenciones necesarias para intercambiar información.
2. El establecimiento de un canal (o ruta) de comunicación estándar.
3. El establecimiento de un elemento de datos estándar.

Un protocolo de comunicación se encarga de asegurar la correcta secuencia e integridad de los datos transmitidos entre un emisor y un receptor.

TCP/IP (Transport Control Protocol/Internet Protocol)

El Protocolo Controlador de Transporte / Protocolo de interconexión de redes de trabajo conocido como TCP/IP, es un conjunto de protocolos que permiten que diversos dispositivos se puedan comunicar entre sí y poder compartir recursos en un ambiente heterogéneo. Esta diseñado para establecer comunicación entre redes e implementar el concepto de interred "internetwork", llamado ARPAnet que más tarde se convertiría en Internet.

La red concebida por DARPA, e instalada con la serie de protocolos TCP/IP, es una red de conmutación de paquetes. Se llama así a la red que transmite información de la red en pequeños segmentos, llamados paquetes. Los protocolos TCP/IP definen el formato de estos paquetes incluyendo el origen, destino, tamaño y tipo, así como la forma en que las redes deben recibir y retransmitir paquetes cuentas veces sea necesario.

La serie de protocolos TCP/IP definen formatos y reglas para la transmisión y recepción de información independientemente del tipo de red o el hardware que se utilice.

Aún cuando los protocolos fueron desarrollados para Internet, también son aplicables para otros casos donde se necesite conectar redes.

Relación de TCP/IP con el modelo **OSI** y transferencia de información

Los protocolos de la serie TCP/IP no corresponden totalmente con el modelo de comunicaciones entre redes, definido por la Organización Internacional de Estándares (ISO). en la Figura C9. se ilustran las siete capas del modelo OSI y algunos de los protocolos más comunes dentro de la serie TCP/IP, los servicios que proveen y la relación entre los protocolos TCP/IP y las capas del modelo OSI.

Las aplicaciones desarrolladas para TCP/IP generalmente utilizan varios de los protocolos de la serie. La suma de las capas de la serie de protocolos es también conocida como la pila de protocolos. Las aplicaciones de los usuarios se comunican con la última capa de la serie de protocolos. Esta última capa en la computadora origen pasa información a capas inferiores de la pila, que a su vez la dirige a la red físicamente. La parte física de la red transfiere la información a la computadora destino. Las capas inferiores de la computadora destino pasan esta información a capas superiores, y finalmente se obtiene la aplicación destino.

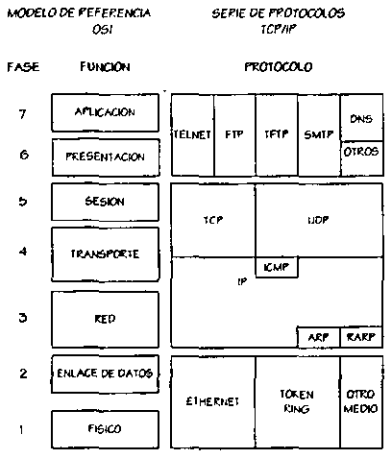


*Figura C9. **Relación de TCP/IP con el modelo OSI***

Los nodos que usan los protocolos TCP/IP traducen la dirección destino IP a direcciones físicas. Por esto, que se requiere una dirección IP para que un nodo se pueda comunicar con otros que emplean la serie TCP/IP, incluyendo a nodos en otras redes privadas así como a los que estén en Internet. Cada dirección IP de 4 bytes está dividida en dos partes: una porción de red, que identifica a la red, y una porción de anfitrión, que identifica a un nodo en particular. Esta división puede caer en una de tres localidades dentro de la dirección de 32 bits. Estas divisiones corresponden a tres clases de direcciones IP: clase A, clase B y clase C. Sin importar la clase de dirección todos los nodos de una red comparten la misma porción de red, todos los nodos tienen una porción de anfitrión única.

SNA (Sistema de Arquitectura de Redes).

El Sistema de Arquitectura de Redes (SNA: System Network Arquitecture) de IBM es el protocolo que adopta esta organización para crear un ambiente de conectividad entre sus distintos equipos. Más que ser un protocolo como tal, son todas las herramientas

necesarias que IBM proporciona para la integración de sistemas, terminales y periféricos para configurar e instalar una red. Este tipo de arquitectura de red tiende a ser propietaria, por lo cual no se puede definir como una topología abierta. SNA es una estructura jerárquica que consiste de siete niveles bien definidos, con similitud al modelo OSI. Cada nivel en la arquitectura desarrolla una función específica. En la Figura C10. se identifican los siete niveles y sus funciones.

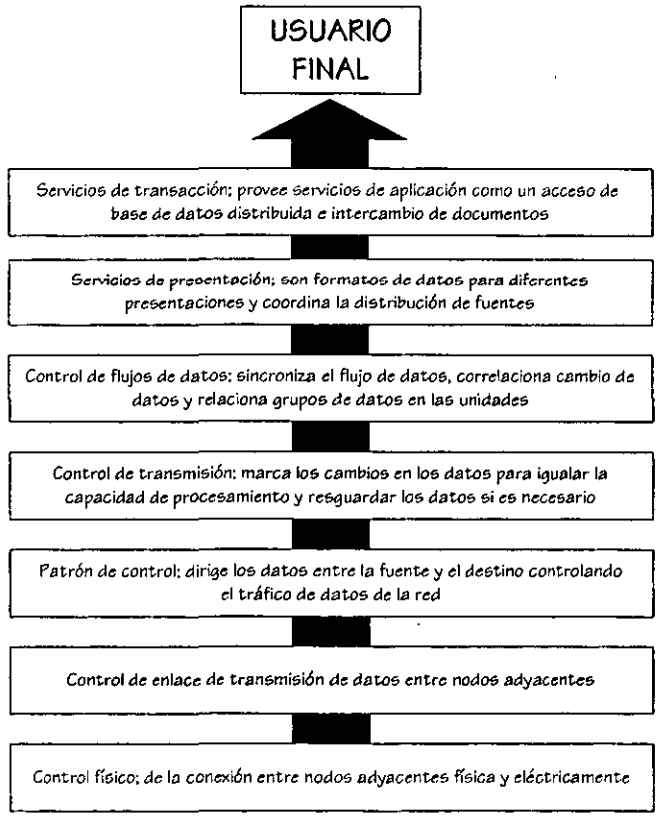


*Figura C10. **Niveles y funciones de SNA.***

Componentes de la red SNA.

Los componentes de hardware y software implementan las funciones de los siete niveles de la arquitectura. Los componentes de hardware incluyen procesadores, controladores de comunicaciones, controladores de terminales, estaciones de trabajo e impresores. El software tiene como componentes para la implementación del SNA funciones tales como los métodos de acceso a las telecomunicaciones, subsistemas de aplicación, y los programas de control de la red. En la Figura C11. se ilustra una configuración de este tipo de red.

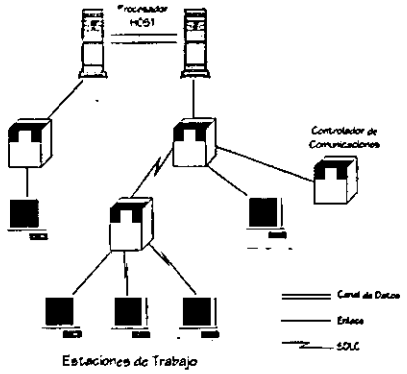


*Figura C11. **Configuración de red SNA.***

HDLC (High-Level Data Link Control)

HDLC (Control de enlace de datos de alto nivel), es una norma publicada por ISO. HDLC proporciona una amplia variedad de funciones y cumple un amplio espectro de aplicaciones, Se considera en realidad como un ámbito que engloba a muchos otros protocolos. Las opciones que permite HDLC, hacen que algunas partes del protocolo resulten una especie de híbrido entre los esquemas primario/secundario puros y los esquemas homogéneos.

El protocolo HDLC puede instalarse de muy diversas maneras. Admite transmisión dúplex y semidúplex, configuraciones punto a punto o multipunto, y canales conmutados o no conmutados. Una estación HDLC puede funcionar de una de estas tres formas:

- ☑ La estación principal controla el enlace de datos (canal). Esta estación envía tramas de comando a las estaciones secundarias del canal, de las cuales, a su vez, recibe tramas de respuesta. Si el enlace es multipunto, la estación principal es responsable además de mantener una sesión independiente con cada una de las estaciones conectadas al canal.
- ☑ La estación secundaria funciona como esclava de la principal, envía mensajes de respuesta a los comandos procedentes de la estación principal. Sólo mantiene la sesión en curso con la estación principal, y no interviene en el control del enlace.
- ☑ La estación combinada (primaria/secundaria) transmite comandos y respuestas, y también recibe comandos y respuestas de otras estaciones combinadas. Mantiene una sesión con otra estación combinada.

SDLC (Synchronous Data Link Control).

SDLC (Protocolo de Control Síncrono del Enlace de Datos) es un protocolo orientado a bit que establece los procedimientos de control del enlace de datos para el sistema de arquitectura de redes SNA de IBM.

Este protocolo presenta las siguientes características:

- ☑ Usa una "gramática" común.
- ☑ Incluye procedimientos de detección y recuperación de errores que pueden ser introducidos durante la transmisión por el enlace de comunicaciones.
- ☑ SDLC proporciona total transparencia e independencia de código. Esto es, se puede transmitir cualquier estructura de información de cualquier

longitud, pero siempre en múltiplos de 8 bits. La información es aislada completamente del control.

- ☑ Es un protocolo orientado a bits, donde no existen caracteres de control.
- ☑ Existen dos niveles de jerarquía constituidos por las estaciones primarias y secundarias.
- ☑ Cada bloque de transmisión de datos es denominada "trama" o marco (frame), la cual tiene un formato específico.
- ☑ Las tramas transmitidas por la estación primaria a la secundaria son llamadas comandos.
- ☑ Las tramas transmitidas en sentido inverso son llamadas respuestas.
- ☑ Los enlaces pueden ser punto a punto, multipunto o anillo.
- ☑ Maneja información en forma dúplex o semidúplex.

La mayor ventaja del SDLC, es que se puede usar en modo dúplex completo. Puesto que SDLC es un protocolo orientado a bit, se pueden mezclar diferentes dispositivos o diferentes formatos de código en la misma línea de comunicación, multipunto o de bucle. Gracias a las convenciones con respecto a la posición que se usan en la estructura de trama, también se puede lograr más fácilmente la transparencia. SDLC también opera el procedimiento de contención (contention) como el de exploración (polling) para controlar la actividad de la estación con enlaces dúplex completo. El hecho de que en SDLC el envío se limite únicamente a siete bloques o tramas a la vez, sin reconocimiento, puede ser un inconveniente, en particular la comunicación es CPU-CPU. Por otro lado, se permiten hasta 255 bloques sin reconocimiento, cada uno hasta de 16000 caracteres.

Protocolo X.25.

La recomendación X.25 fue desarrollada bajo los auspicios del CCITT. Emitida en 1976, ha sufrido revisiones en 1980, 1984 y 1985. Se compone de tres niveles de conexión

incorporados al modelo OSI: Capa Física (Physical), Capa de Enlace (Data Link) y Capa de Red (Network). El equivalente con el modelo OSI se ejemplifica en la Figura C12.

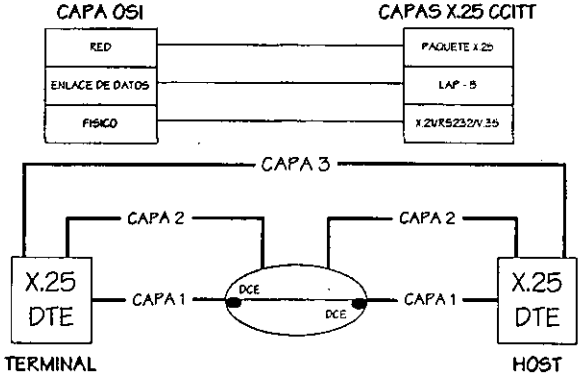


*Figura C12.. **X.25 y su equivalente con el modelo OSI.***

Se define a X.25 como un conjunto de protocolos que proveen un mecanismo de transporte de datos, independiente del protocolo de red. X.25 especifica las características de la interconexión entre el DTE (quien envía o recibe paquetes de datos) y el DCE (el nodo de la red que obra como entrada o salida de la misma).

Es importante señalar en este punto, que por el momento, el único protocolo que puede ser empaquetado siguiendo un estándar en X.25 es TCP/IP. Esto quiere decir que equipos de diferentes fabricantes que empaqueten TCP/IP en X.25, deben de ajustarse al estándar.

El éxito del protocolo X.25 para permanecer como estándar en la industria de comunicación de paquetes se debe a la garantía confiable de comunicación entre dispositivos.

Apéndice D.

La red de área amplia: Normatividad y Estándares.

La red de área amplia.

Con la rápida proliferación de las redes de área local (LAN) en los 80's, se hizo patente la necesidad de interconectarlas, y junto con ello la infraestructura propia de cada una de los diferentes tipos de redes. A este proceso se le conoce como interoperabilidad (*internetworking*). La interoperabilidad se efectúa a través de varios dispositivos como lo son: los puentes (bridges), ruteadores (routers) y compuertas (gateways), entre otros.

Estos dispositivos no se utilizan solamente para la interoperabilidad, pero sirven para crear una infraestructura que permite un nivel razonable de rendimiento en la red. Inicialmente, la interoperabilidad se usaba para enlazar a todos los usuarios de una organización, proveyendo un área común de trabajo. El correo electrónico sigue siendo una de las aplicaciones primarias para las redes corporativas. La tendencia según los observadores de la industria de la computación es la *computación distribuida*, un estilo de computación en la cual aplicaciones individuales pueden ser ejecutadas simultáneamente en más de una computadora al mismo tiempo.

No existe una fórmula para crear una organización de red para un edificio. Se inicia con una base ya instalada de aplicaciones, redes, sistemas operativos, protocolos, computadoras, y cableado, y lo que se espera es que esa misma base pueda ser utilizada durante muchos años. Diversos factores determinan el número de tipos de dispositivos de interoperabilidad que se usaran. El principal factor es el tráfico de la red: que protocolos controlan el tráfico, y hacia donde fluye el tráfico. Normalmente una red de área amplia, involucra la existencia de varios protocolos y tipos de computadoras; los protocolos TCP/IP, IBM SNA, por ejemplo, y los ambientes de LAN de las PC's tienen múltiples capas que pueden ser referenciadas al modelo OSI; de manera similar, los dispositivos corresponden a un nivel específico de la capa OSI.

Interoperando en el Nivel de Enlace de Datos.

La interoperabilidad comienza en el segundo nivel de la capa del modelo OSI, la capa de enlace de datos. Esta capa establece comunicación entre nodos adyacentes. Cada dirección de enlace de datos corresponde a la dirección de un nodo particular de la red.

En la capa de enlace de datos, el flujo de bits formado por los pulsos eléctricos en el nivel físico es organizado en paquetes. Los tres tipos mayores de LAN (Ethernet, Token-Ring, y FDDI) son definidos en la mayor parte por sus características en la capa física. la interoperabilidad esta confinada ampliamente al nivel de enlace de datos de estos tipos de LAN, aunque recientemente han aparecido productos que incluyen comunicación de FDDI a Ethernet y a Token-Ring.

Ethernet, utiliza CSMA/CD (Carrier Sensing Multiple Access/Collision Detection), es un técnica, en la cual, todos los nodos "escuchan" cada transmisión a través del medio. Un nodo listo para transmitir censa sino existe colisión, si el medio esta libre, empieza a enviar datos. Si uno o más nodos intentan transmitir al mismo tiempo, entonces ocurre una colisión. Los nodos emisores detectan la colisión y esperan un intervalo de tiempo y entonces reintentan la transmisión.

Interconeciando LANs

Uno de los papeles más importantes de las redes WAN de la actualidad es el de interconectar redes LAN que están geográficamente separadas. Las redes MAN también juegan un papel importante el la interconexión de LANs. La interconexión de LANs se refiere a la habilidad de interoperar LANs, MANs y WANs. También se refiere a la habilidad de interconectar dos LANs entre ellas. Todas las redes LAN, tienen un número máximo de estaciones práctico (por ejemplo, *token ring* esta limitado a aproximadamente 70

estaciones a través de una distancia de varios kilómetros y CSMA/CD esta prácticamente limitada a centenas de estaciones, el estándar 802.3 define hasta a 1024 estaciones, hasta una distancia de 2.8 km.). Que sucede, si se necesita o se quiere conectar más estaciones a la red; la única solución es interconectarlas.

Elementos que integran una WAN

Se emplean cuatro tipos de dispositivos genéricos para las interconexiones de redes LAN.

Repetidores (Repeaters).

La capa más baja del modelo OSI, el nivel físico, cubre el cableado y la señalización eléctrica. El dispositivo que opera en este nivel es el repetidor (*repeater*). Los repetidores, reciben una transmisión de un segmento de la LAN y regeneran la señal, de esta forma una transmisión de la red puede hacerse a una distancia mayor.

Actualmente, los repetidores no interconectan dispositivos ya que solamente se utilizan para extender los segmentos de la LAN.

Puentes (Bridges).

Un puente (bridge), se utiliza clásicamente para interconectar redes similares o homogéneas. Un puente(*bridge*) de *token ring*, por ejemplo, será utilizado para interconectar dos redes *token ring*. Los puentes pueden proveer un enlace punto a punto entre dos LANs.

Un puente es considerado como otra estación más de la red a la cual esta conectada, Figura D1.

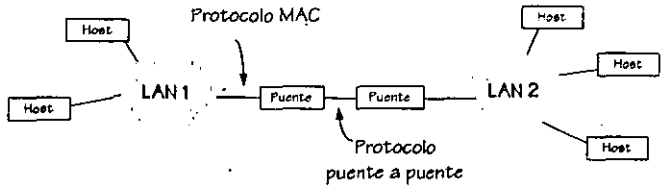


Figura D1. Puentes (bridges) en un ambiente de LAN

Ruteadores (*Routers*).

Un ruteador es similar a un puente, pero está diseñado para redes que utilizan diferente direccionamiento en la capa MAC (ver Figura D2). Donde un puente provee conexiones punto a punto entre LANs, un ruteador puede actuar como conmutador entre varias LANs.

Como un puente, un ruteador es considerado como otra estación en la red a la cual esta conectado. Si el ruteador observa una transmisión en la LAN-1 conteniendo una dirección de una estación de otra red, copiará el frame. Entonces ruteará el frame a la estación de destino correcta, si existe algún otro ruteador conectado.

En el ejemplo de la Figura D2, cualquiera de las tres LAN pueden intercambiar frames, de cualquier forma se presentará un ligero retardo para los frames a través de la red. Los ruteadores dan soporte a protocolos hasta la capa 3 de OSI (Capa de red). Por lo general, no realizan conversiones de protocolo terminal a terminal.

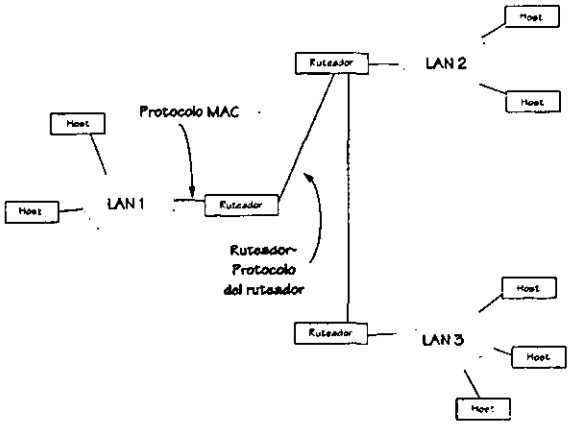


Figura D2. Ruteadores (routers) en un ambiente de LAN

Gateways (Compuertas).

Un *gateway* se usa para interconectar redes no similares, o heterógeneas. Como se indica en la Figura D3. Los *gateways* son por lo general, dispositivos muy inteligentes, dando soporte a protocolos a un nivel tan alto como la capa 7 del modelo OSI, tales como funciones de ruteo y conversión de protocolos. Los *gateways* son comúnmente utilizados para interconectar LANs a otros tipos de red, particularmente WANs. Debido a su habilidad para realizar conversión de protocolos, tiene gran relevancia en la interconexión de redes LAN con MANs.

La conversión de protocolos puede ser una tarea compleja, ya que las variables pueden diferir entre dos protocolos, incluyendo:

- ☑ El esquema de direccionamiento
- ☑ El tamaño máximo del *frame*
- ☑ El algoritmo de ruteo
- ☑ El esquema de MAC
- ☑ Los protocolos *peer-to-peer*.

La Figura D3 muestra un ejemplo de una hipotética configuración de *gateways*. El *gateway* de LAN-1 aparenta ser otra estación de la LAN, usando el protocolo MAC apropiado. Este *gateway* puede ser empleado para accesar a una red de conmutación de paquetes, utilizando la Recomendación de protocolo X.25 de la CCITT; por otra parte, para la red de conmutación de paquetes el *gateway* aparenta ser un *anfitrión* X.25. De manera similar, este *gateway* puede proveer acceso a ISDN usando los protocolos de ISDN de la CCITT. Para terminar, el *gateway* puede ser conectado a otro *gateway* como el de LAN-2, ya sea directamente o a través de otra red; la LAN-2, de hecho, quizá use algún otro protocolo de MAC. Así, los *gateways* pueden proveer conversión de protocolos de usuario final a usuario final, a través de la capa 7 del modelo OSI (Capa de aplicación).

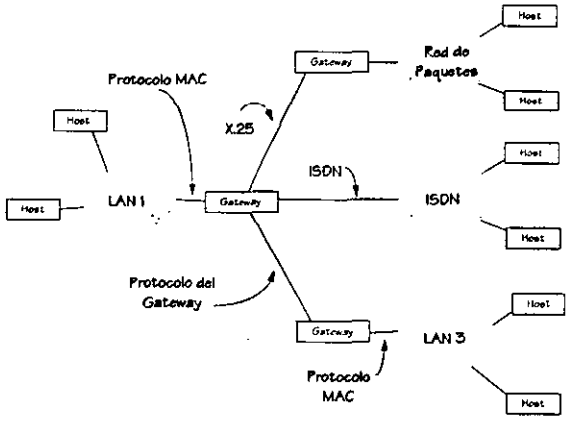


Figura D3. Gateways (Compuertas)

Tecnología Actual para la Transmisión de Datos

Frame *Relay*

Frame Relay es un protocolo de señalización y referencia de datos entre estaciones y nodos inteligentes dentro de las redes de área amplia, similar a los que existen para redes locales, cuya función es trasladar a aquellas la sencillez de éstas.

Para manejar el aumento de información en la carga de datos en las redes de área amplia y evitar retrasos, se ha propuesto utilizar esta tecnología a las redes futuras (como cell relay), Frame Relay pretende facilitar la interconexión de redes locales.

Precisamente, debido a lo beneficios de eficiencia que representa, mejores tiempos de respuesta, calidad adaptable del servicio transparencia y flexibilidad, las tecnologías de paquetes, como Frame y Cell Relay,- han comenzado a reemplazar a arquitecturas tradicionales tales como las de circuitos (IDM) y X.25.

Frame Relay opera sobre el supuesto de que las conexiones son confiables y transporta únicamente datos. Elimina gran parte del control y detección de errores de X.25, por lo que requiere menos procesamiento que éste. Cubre velocidades hasta las que contiene el estándar americano "T1" o el europeo "E1", aunque maneja el rango de 256 Kbps a 34 Mbps. La conmutación por células permite manejar de 34 Mbps hasta 155 Mbps en la interfaz del usuario y 600 Mbps entre los nodos conmutados.

Como X. 25, Frame Relay transporta datos dentro de frames y no maneja paquetes, tiene la capacidad de realizar funciones de enrutamiento a nivel de frame. En la realidad constituye una versión simplificada del nivel del frame , con alguna semejanza con el LAPD (Link Access Procedure, D Channel: procedimiento de acceso al enlace, canal D), el nivel de frame de RDI para el canal D. Este procedimiento de comunicación se ubica en la

capa 2 del modelo OSI. Funciona al transferir datos mediante un nivel rudimentario de frames que se denomina el núcleo, el cual consiste, básicamente, en paquetes de frame tipo HDLC.

Si bien Frame Relay no posee funciones para control de flujo de datos, si contiene un campo que actúa como un identificador lógico del canal a nivel del frame (el DLCI Data Link Connection Identifier: identificador de la conexión del enlace de datos). Este permite que los circuitos lógicos conmutados o permanentes se fijen en el nivel 2, lo que hace que las funciones de enrutamiento se lleven a cabo en este último.

Ventajas del *Frame* Relay

Permite al usuario aprovechar al máximo cualquier mejora cualitativa en la capa física. Los enlaces de fibra óptica han cambiado radicalmente la calidad del servicio en los medios de transmisión, además de las mejoras continuas en los enlaces bajo cables de cobre. Por lo tanto, se elimina la necesidad de realizar controles y correcciones de errores tan frecuentemente como con X.25.

La tecnología de *Frame Relay* ofrece casi cinco veces más velocidad en la conmutación, debido a la simplificación del proceso. Sus usuarios también pueden compartir canales muy costosos, tales como T1, E1, T3 y E3. Es importante señalar que considera el rápido aumento del poder de procesamiento de las estaciones de trabajo, que ahora pueden intercambiar grandes archivos y realizar funciones de telecomunicaciones, que antes se llevaban a cabo en los nodos de la red.

Frame Relay maneja con eficiencia un tráfico irregular e impredecible y suministra acceso de una sola línea a la red con conectividad lógica hacia cualquier otro destino. En consecuencia, se reducen los requerimientos de hardware, se simplifica el diseño de la red y se reducen los costos de operación.

Desventajas del Frame Relay

Para muchos resulta una desventaja que *Frame Relay* no corrija errores. Sin embargo, debido fundamentalmente a las recientes mejoras tecnológicas, tales como los adelantos en la electrónica de repetidores de línea, los errores que detecta pueden corregirse extremo a extremo por X.25 o TCP/IP, por ejemplo, de esta manera se aligera al software de conmutación del nodo, lo que permite una conmutación mucho más rápida.

Por otro lado, este protocolo no incluye un mecanismo de control de flujo que reduzca las ventanas de transmisión. En lugar de eso, señala los problemas de congestionamiento. Descarta los *frames* que provocaron aquél y deja que un protocolo de nivel más alto retransmita los mensajes correspondientes (X.25 o TCP/IP). Sin embargo, tanto los organismos reguladores como los fabricantes de productos para esta tecnología ya trabajan para solucionar esta situación.

ATM (Asynchronous Transfer Mode)

ATM (Modo de Transferencia Asíncrono, en inglés Asynchronous Transfer Mode), es una tecnología de transporte basada en conmutación de células (Cell-Switching), la cual es capaz de transportar voz, video y datos.

El modo asíncrono de transferencia tiene como característica la transportación y conmutación de la información a grandes velocidades, opera en la capa física y parte de la capa de enlace de datos del modelo OSI.

Transferencia de información a través de ATM

La Figura D4 ilustra el principio de ATM. En la terminal de origen, la información se divide en células. Cada célula es una especie de paquete fijo, o envolvente de unos 53 bytes (48 bytes de la célula transportan datos de usuario, 5 bytes son para el encabezado de la célula). Cada cabeza de célula, denominada etiqueta, contiene una dirección de destino. La red ATM transfiere cada célula de acuerdo con las instrucciones de su etiqueta. La conmutación de una célula se realiza mediante una lógica material conocida como circuito de autoenrutamiento. Esto permite transferir una célula a un nodo a velocidades de 155 y 622 Mbps, pero se espera que incrementen hasta 10 Gbps.

En la terminal de destino, a medida que llegan las células, unas tras otra, se rompe la envolvente al suprimir la etiqueta, y el contenido de las células se redistribuye en la forma original de la información. En cuanto a datos, ATM fue diseñado para dar soporte a transmisiones no orientados a grandes bloques de información a través del concepto de vías tributarías, la red garantiza que cada usuario tendrá un nivel de servicio para un rango de bits mínimo.

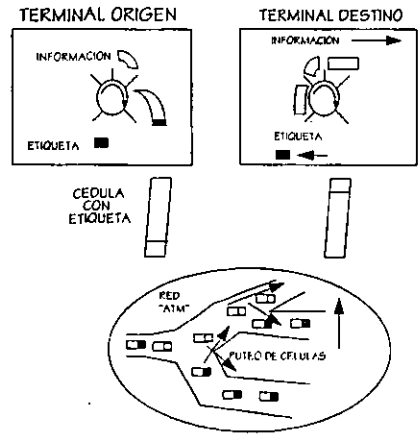


Figura D4. ATM, transferencia de información.

Una característica principal de ATM es su capacidad de proporcionar un gran ancho de banda, el cual resulta indispensable para muchas nuevas aplicaciones para redes tanto locales como de área amplia. Algunos ejemplos son las videoconferencias de escritorio a escritorio, la animación, el envío de mensajes y la comunicación multimedia, el trabajo cooperativo y el acceso a supercomputadoras.

Considerando que en la actualidad las redes de área local como Token Ring, Ethernet, FDDI, etcétera; no pueden proporcionar un ancho de banda en este modo de transferencia, el acceso a través de este servicio es posible mediante lo siguiente:

- ☑ A nivel local, cada usuario se enlaza con el concentrador ATM en una configuración de estrella. El concentrador da soporte a una UNI (*User-Network Interfaz*: Interfaz de usuario en la red de trabajo), en la cual el usuario opera en un ancho de banda dedicado de 155 o 622 Mbps. El *backplane* del concentrador, a donde la operación es en gigabits por segundo, constituye el único lugar donde los usuarios comparten el ancho de banda. Funciona en el modo TDM, con lo cual cubre la velocidad UNI para cada usuario activo.

Se añaden dos tipos de concentradores ATM. Uno de ellos utilizar buses con base en la computadora para conectar puertos, de la misma manera que los ruteadores *high end* utilizan buses de alta velocidad para enlazar redes multiprotocolo. El otro tipo de concentrador emplea algún conmutador de *Cell Relay* de no bloqueo. Este último que está orientado hacia la conexión, requerirá capacidades adicionales y *multicasts*.

- ☑ En cuanto al cableado, las especificaciones indican cables cortos de par trenzado sin blindar, aunque también se puede optar por fibra óptica, sobre todo para enlaces de largo alcance.

☑ ATM abre la posibilidad a la utilización de la misma tecnología a nivel local y a través de grandes distancias, con lo cual se reducirá la necesidad de puentes y ruteadores, sobre todo en lo que se refiere a conversión de velocidades y protocolos. Estos dispositivos de interconexión, ahora esenciales para el armado de redes en áreas amplias, se podrán convertir en facilitadores de la comunicación, en especial cuando el usuario desee tener la posibilidad de escoger, por ejemplo entre *Frame Relay* o ATM.

El modo asíncrono de transferencia trae también la ventaja añadida de una mejor administración. En primer lugar, simplifica la interconexión de redes locales. Los concentradores ATM permiten que las conexiones se realicen entre cualquiera de los dos puertos del concentrador, sin importar si los dispositivos que se han añadido se localizan en una red Ethernet, Token Ring o FDDI. Además, mapeará lógicamente la dirección física de un nodo terminal hacia los diversos puertos del concentrador.

El mecanismo de conmutación del concentrador podrá enlazar una estación de trabajo con cualquier red local de una instalación, a cualquier ancho de banda que se necesite, por ejemplo, con la red Ethernet, a 10 Mbps o con la FDDI a 100 Mbps.

Otro caso puede ser cuando un usuario se cambia de piso ya no hay necesidad de recablear y cambiar los direccionamientos lógicos del software de su estación de trabajo y del servidor correspondiente. Con un sencillo movimiento en la consola central de administración, ATM se encarga de restablecer todo el mapa de conectividad de la instalación y esto se aplica tanto para uno como para varios usuarios. Además, es más fácil modificar los derechos de acceso a los diversos recursos disponibles en cada segmento.

Otra ventaja para el administrador de la red es que ATM permite concentrar en una área central todos los servidores de una instalación de gran tamaño con lo que aumenta la seguridad y el control de los mismos sin que se sacrifique su desempeño.

A diferencia de otras alternativas tecnológicas con una configuración fija, ATM permite una gran flexibilidad en cuanto a la topología. Los concentradores ATM permitirán ordenar los nodos en estrella, anillo o en cualquier combinación que facilite el tráfico de señales en una instalación determinada. Los beneficios que se pueden derivar de esta característica son innumerables y de nuevo facilitan la labor del administrador de la red.

Se afirma que la tecnología ATM se instrumentará primero en las redes públicas, a las cuales se conectarán las redes de empresas e instituciones. Para empezar, se han elegido como fundamento para las redes públicas B-ISDN (Broadband Integrated Services Digital Network red digital de servicios integrados de banda ancha), que se han comenzado a instalar y que se multiplicarán en un futuro.

Cell Relay

Cell Relay es una arquitectura diseñada para redes públicas que requieren conmutación de paquetes a muy altas velocidades. A diferencia de *frame relay* en la cual son transmitidos paquetes de longitud variable, *cell relay* utiliza paquetes de tamaño fijo llamados células (*cells*). El utilizar células de un sólo tamaño permite que el procesamiento de paquetes sea más simple y rápido.

La implantación de *cell relay* está basada a través del uso de *hardware* especializado. En comparación, *frame relay* esta basado en el uso de *software*. Aunque las diferencias puedan parecer triviales, *cell relay* está diseñado para dar soporte a la transmisión de datos de mayor volumen, la cual se aproxima a los 150 Mbps. Uno de los primeros en ofrecer el uso de *cell relay* fue "*Switched Megabit Data Services*" (SMDS) el

cual provee acceso de 1.544 Mbps a 44.736 Mbps a una red conmutada basada en fibra óptica. *Cell Relay* ha sido diseñado para transportar voz, datos y video bajo el estándar IEEE 802.6. Se espera que en el futuro *cell relay* se emplee extensivamente en redes públicas para acarrear voz, datos y video a través de cables de fibra óptica comunes.

Glosario

Acceso múltiple

Técnica que permite que cierto número de terminales compartan la capacidad de transmisión de un enlace en una forma predeterminada o conforme a la demanda del tráfico. Es la posibilidad, proporcionada a varias estaciones terrenas, de transmitir simultáneamente sus portadoras respectivas al mismo transponder del satélite.

Acceso remoto.

Pertenece a la comunicación con una computadora a través de un terminal distante de la computadora.

Administrador de red (network administrator).

Persona responsable por la operación diaria y la administración de la red; también se conoce como administrador del sistema. Las labores de administración de la red incluyen: planear futuras expansiones; instalar nuevas estaciones de trabajo y dispositivos periféricos de la red; adicionar y remover usuarios autorizados; elaborar copias de respaldo del sistema y realizar labores de archivo de datos importantes; asignar y cambiar contraseñas; resolver problemas de la red; monitorear el comportamiento del sistema; evaluar nuevos productos; instalar actualizaciones de hardware y software; entrenar usuarios.

Ancho de banda.

Es el rango de frecuencias que un canal de comunicación es capaz de conducir sin una atenuación excesiva, manteniendo un rango continuo de frecuencias sobre el cual la ganancia no difiera de su valor máximo más que en una cantidad específica. Se define como la diferencia que existe entre la frecuencia. La capacidad de transmisión de datos de un enlace de transmisión, expresada en función de la frecuencia más alta y más baja que puede transmitir.

Ancho de banda sobre la demanda (bandwidth on demand).

Característica de una red de área amplia (WAN) que le permite al usuario conmutar un ancho de banda adicional cuando la aplicación lo exige. La mayor parte del tráfico de la red no fluye en corrientes estables y fácilmente predecibles, sino en ráfagas cortas, separadas por largos períodos de inactividad. Este patrón hace muy difícil predecir los picos de carga. El ancho de banda sobre demanda le permite al usuario pagar solamente por la cantidad de ancho de banda utilizada.

Anfitrión (Host).

Sistema informático que actúa como servidor de archivos, controlador de red o asume algún otro tipo de relación jerárquica, respecto a otras computadoras.

ANSI (American National Standards Institute).

Instituto Nacional Americano de Estandarización. Organismo no gubernamental que agrupa 300 comités de estandarización y que se encarga de emitir recomendaciones y normas para los sistemas de telecomunicaciones e informática en los EE.UU.

Arquitectura cliente / servidor (client/server architecture).

Arquitectura que distribuye el procesamiento entre clientes y servidores en la red. Los clientes piden información a los servidores. Los servidores almacenan datos y programas y proporcionan servicios a los clientes a través de toda la red. Esta disposición aprovecha la fuerza de computación disponible, dividiendo la aplicación en dos componentes distintos: un cliente frontal y un servidor en el fondo. La arquitectura cliente/servidor puede sostener varios niveles de complejidad organizacional, incluyendo los siguientes: aplicaciones standalone (sin conexión a la red), como procesadores de palabra locales; aplicaciones que corren en el cliente pero requieren datos del servidor, como hojas de cálculo; programas en los cuales la búsqueda física de los registros se hace en el servidor, mientras que un programa mucho más pequeño se ejecuta en el cliente, manejando todas las funciones de

interfaz de usuario, tales como las aplicaciones de bases de datos. La computación cliente/servidor disminuye la carga de procesamiento de los PC clientes, pero incrementa la carga en el servidor. Los computadores servidores tienden a tener unidades de disco más grandes y más veloces y mucha más memoria instalada que los servidores PC convencionales. El servidor también puede ser una minicomputadora o un mainframe.

Arquitectura de red (network architecture).

El diseño de la red, incluyendo el hardware, software, métodos de acceso y protocolos en uso. Varias arquitecturas de red bien aceptadas han sido definidas por comités de estándares y grandes fabricantes. Por ejemplo, la International Standards Organization (ISO) desarrolló el modelo ISO/OSI de 7 capas para comunicaciones computador a computador, e IBM diseñó SNA (Systems Network Architecture). Ambas arquitecturas organizan las funciones de red en capas de hardware y software, en donde cada capa construye las funciones suministradas por la capa anterior. El último objetivo es permitir que computadores diferentes intercambien información libremente de manera tan transparente como sea posible.

ASCII (American –National- Standard Code For Information Intercharge).

Es un código de paridad de 7 bits establecido por el American National Standars Institute para lograr compatibilidad entre servicios de datos y consta de 96 caracteres alfanuméricos y 32 caracteres de control no visibles.

Asíncrono.

Modalidad de transmisión de datos en que la velocidad de paso no guarda relación con ninguna frecuencia fija del sistema. Cada suceso se inicia al concluir el suceso anterior. La sincronización en un sistema asíncrono se obtiene añadiendo a cada palabra de datos un bit de comienzo -start bit-, y acabando con uno o con más bits de parada -stop bits-, y un opcional bit de paridad -parity byt- para detección de errores.

Atenuación.

Disminución de la amplitud de la señal, pérdida o reducción de amplitud de una señal al pasar a través de un circuito, debida a resistencias, fugas, etcétera. Puede definirse en términos de su efecto sobre su voltaje, intensidad o potencia. Se expresa usualmente en decibelios por unidad de longitud.

Automatización de oficinas.

Se refiere a esfuerzos realizados por generar automatización de tareas de oficina comunes, entre ellas procesamiento de palabras, archivo, contabilidad y otras tareas de oficina.

Balance de la carga (load balancing).

Técnica que distribuye el tráfico de la red a lo largo de rutas paralelas para hacer más eficiente el uso del ancho de banda, mientras al mismo tiempo se suministra redundancia. El balanceo de la carga moverá automáticamente un trabajo de un usuario, desde un recurso de red bien cargado, a otro menos cargado.

Banda base.

Característica de cualquier tecnología de red como Ethernet que utiliza una única frecuencia de portadora y requiere que todas las estaciones conectadas a la red participen en todas las transmisiones.

Baudio.

Número de veces por segundo que una señal puede cambiar en una línea de transmisión. Normalmente, una línea de transmisión usa sólo dos señales de estado, haciendo que la relación de baudios sea igual al número de bits por segundo que pueden ser transferidos.

Bit/seg.

Esta es una medida que describe exactamente la cantidad de bits que son transmitidos en un segundo. En la práctica este término se suele igualar término baudio, aún cuando técnicamente no son lo mismo.

Baudio.

Es una unidad binaria de transmisión de información por segundo. Mide la velocidad de traspaso de información por segundo que un canal es capaz de conducir. A este término, también se le conoce como baud.

Bridge.

Interconexión entre dos redes que utilizan los mismos protocolos, los mismos métodos de transmisión y la misma estructura de direccionamiento. Los bridges funcionan en el nivel de datos o enlace de datos del modelo OSI. Los bridges se diferencian de los repetidores en que los primeros almacenan la información de forma temporal, y la reenvían mientras que los segundos sólo amplifican o reenvían señales eléctricas.

Broadcast.

Una transmisión dirigida simultáneamente a más de una estación de la red. Un sistema de entrega de paquetes que entrega una copia dada de un paquete a todas las computadoras que están conectadas a él, está realizando un broadcasting –transmisión- del paquete.

Bus.

Ruta electrónica a lo largo de la cual se envían señales de una parte de una computadora a otra. Una PC contiene varios buses; cada uno se utiliza para un propósito diferente: El bus de direcciones, ubica direcciones de memoria; El bus de datos transporta datos entre

el procesador y la memoria; El bus de control transporta señales desde una unidad de control.

Canal dedicado.

A diferencia de un canal común, que puede ser utilizado por cualquier usuario del servicio telefónico, un canal dedicado está asignado a un usuario o a un servicio en especial en forma permanente. La vía de enlace puede ser física, por microondas o a través de satélite.

Capacidad del canal.

Número máximo de elementos de información (bits) que pueden ser transmitidos por un canal en la unidad de tiempo.

Carrier.

Infraestructura física por la cual se transportan los datos, voz e imagen; se le traduce como portador o portadora.

CCIR (Comitee Consultatif Internacional de Radiocommunication).

Comité Consultivo Internacional de Radiocomunicación. Organismo permanente de la Unión Internacional de Telecomunicaciones. Estudia y formula recomendaciones sobre cuestiones técnicas y de explotación relativas específicamente a radiocomunicaciones. Está divido en trece grupos de estudios y la comisión interina de vocabulario, que trata de unificar en lo posible, por medio de un vocabulario internacional, todos los medios de expresión (definiciones, terminología, símbolos, etcétera). Los resultados de los grupos de estudio se consideran antes de adoptarlos, como recomendaciones, reportes, opiniones, resoluciones o nuevas preguntas o programas de estudio. La asamblea plenaria debe estar de acuerdo con los documentos antes que sean válidos y publicados. Las asambleas plenarias se efectúan a intervalos de tres o cuatro años.

CCITT (Comitee Consultatif Internacional de Telegraphique et Telephonique).
Comité Consultivo Internacional Telegráfico y Telefónico. Organismo resultante de la reunión del Comité Consultivo Internacional Telefónico y del Comité Consultivo Internacional Telegráfico. Grupo de las Naciones Unidas especializado en normalizar y recomendar funciones en el ámbito de las telecomunicaciones internacionales; representando alfabetos, gráficos, información de control y otros intercambios fundamentales entre países.

CDMA (code division multiple access, acceso múltiple por diferenciación de código).
Es el método por el cual se pueden introducir o enviar señales de diferente información en un mismo período normado por valores binarios. Las señales se combinan a través de las técnicas de multiplexaje por división en tiempo y multiplexaje por división en frecuencias, por medio de una compleja elaboración de los datos multiplexados mediante su codificación, a fin de lograr una concentración de datos aún mayor, así como la detección o corrección de errores de tal manera que es posible recuperarlas (demultiplexarlas), mediante las correspondientes operaciones de decodificación. Sistema de acceso múltiple en la cual a las señales utilizan toda la banda del transponder simultáneamente, se utilizan técnicas de ensanchamiento de espectro. En este modo de transmisión, se asigna un código característico a cada señal transmitida al satélite. En la recepción, la estación reconoce por su código la señal que le está destinada, entre todas las señales que recibe y extrae la información correspondiente. Permite que los usuarios de satélite puedan transmitir simultáneamente y también compartir la frecuencia asignada. Es decir combina la transmisión simultánea por división de frecuencia y por división de tiempo. En este caso el código es del orden de un bit en tiempo.

Cliente-Servidor.
Modelo de interacción en un sistema distribuido en el cual un programa en una computadora envía una petición a un programa situado en otra computadora y espera su

respuesta. El programa que realiza la petición se le llama cliente; el programa que satisface a la petición se le denomina servidor.

Comunicación de datos.

Transferencia de información de un computador a otro a través de una línea de comunicaciones. La transmisión puede ser ocasional, continua o una combinación de ambas.

Concentrador.

Equipo de conmutación que permite dar servicio a cierto número de líneas de abonado, con un número de pares inferior al de estas líneas, y que en ella utiliza equipos individuales de línea de abonado.// Unidad funcional que permite la utilización de medios comunes de transmisión a un número de fuentes de datos, que puedan dar lugar a un caudal superior al permitido por la vía de salida del equipo.

Conectividad.

En una red de área local (LAN), la habilidad de cualquier dispositivo agregado al sistema de distribución, para establecer una sesión con cualquier otro dispositivo.

Conexión.

El camino establecido a lo largo de una red, que conecta a dos DTEs que cuentan con interfaces de transmisión de estándares como V.24.

Conmutación de circuitos.

La conexión eléctrica directa y temporal de dos o más canales, entre dos o más puntos, con la finalidad de proveer al usuario del uso exclusivo de un canal abierto, con el cual hace intercambio de información. También se le conoce como conmutación de líneas.

Conmutación de paquetes.

Técnica de enrutamiento de información desarrollada específicamente para las redes de transmisión de datos y en la cual los mensajes se dividen en unidades pequeñas llamadas paquetes, los cuales son manejados individualmente por las redes de transmisión.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Método de acceso a redes para manejar colisiones de paquetes de datos.

DB-25.

Conector de 25 pines que se utiliza comúnmente en Estados Unidos como dispositivo de elección del estándar de interfaz serial RS-232-C.

Circuito Virtual.

Es una definición propuesta por la CCITT, para los servicios de transmisión de datos. El usuario presenta un mensaje de datos para ser enviado, con un encabezado de un formado específico. El sistema envía dicho mensaje como si existiera un circuito directo hacia el destino especificado. Uno de varios diferentes caminos y técnicas puede ser utilizados para enviar dicho mensaje, sin embargo, no es necesario que el usuario conozca los procedimientos que se emplean. En forma virtual, al usuario le parece que existiera un circuito real.

Columna vertebral (backbone).

Porción de la red que administra el tráfico pesado. Puede ser el punto de conexión de varios edificios o localidades y también tener enlazadas pequeñas redes. Utiliza un protocolo de mayor velocidad que los segmentos individuales de las redes de área local (LAN).

Comunicaciones inalámbricas (wireless communications).

Método de conectar un nodo o grupo de nodos a una red principal mediante una tecnología diferente al cableado convencional. Se usan los siguiente métodos: Línea de señal infrarroja. Se usan para ondas de luz de alta frecuencia para transmitir datos entre nodos con distancias de hasta 24.4 metros, mediante una ruta sin obstrucciones; los rayos infrarrojos no pueden pasar a través de paredes de mampostería. La proporción de datos es relativamente alta en rangos de décimas de megabits por segundo; Radio de alta frecuencia. Señales de radio de alta frecuencia transmiten datos a nodos con distancias de 12.2 a 39.6 metros, dependiendo de la naturaleza de la obstrucción que los separe; la señal puede penetrar paredes delgadas, pero no admite mampostería. La proporción de datos generalmente es menor a 1 megabit por segundo; Radio Spread-spectrum. Pequeño conjunto de frecuencias disponibles para redes inalámbricas, sin aprobación FCC. La banda de 902 a 928 megahertz (Mhz) se conoce como banda industrial, científica, médica (ISM) y no está reglamentada. La banda de 2.4 a 2.483 gigaherts (Ghz) está reglamentada y requiere licencia FCC para su uso. Los nodos Spread-spectrum pueden estar distanciados hasta 243.8 metros en un ambiente abierto y estas ondas de radio pueden atravesar paredes de mampostería. Sin embargo, en un ambiente lleno de oficinas cerradas las distancias se limitan a 33.5 metros. Por lo general, la proporción de datos es menor a un megabit por segundo; Las LAN inalámbricas no siempre son completamente inalámbricas. Se pueden usar para reemplazar el cableado de ciertos segmentos de la red o para conectar grupos de redes que usan cableado convencional.

Conexión remota (remote connection).

Conexión de estación de trabajo a red, usando un módem y línea telefónica, que permite enviar o recibir datos a mayores distancias que aquellas logradas con cableados convencionales. También se conoce como acceso remoto.

CSMA (carrier sense multiple access)

Es un método utilizado en las redes de transmisión de datos que consiste en comenzar a emitir tras detectar un periodo más o menos largo de inactividad en el medio de transmisión.

CSMA/CA (carrier sense multiple access with collision avoidance)

Es un protocolo de acceso múltiple por detección de portadora que evita las colisiones en el medio de transmisión. Este protocolo ofrece prioridad a cada una de las estaciones de la red, de tal forma que la primera en acceder a la línea será la estación que tenga la prioridad más alta.

CSMA/CD (carrier sense multiple access/collission delection acceso múltiple del sentido de transporte/detección de colisiones)

Es una técnica de acceso a le red que permite el envío y recepción de información cuando el medio se encuentra libre de colisiones. Cuando dos a más nodos transmiten simultáneamente ocurren colisiones y entonces el proceso se repite hasta que la transmisión tiene éxito.

Datagrama (datagram)

Es un servicio de conmutación de paquetes en la que los paquetes son ruteados independientemente y pueden llegar fuera de orden. En cada datagrama está contenido tanto la dirección como la información de los paquetes.

DBMS (Data Base Manager System).

Sistema de manejo de base de datos. Es un conjunto de datos relacionados entre sí y un grupo de programas para tener acceso a esos datos. El conjunto de datos se conoce como base de datos. El objetivo del DBMS es crear un ambiente en el cual es posible guardar y recuperar información de la base de datos en forma conveniente y eficiente.

DCE (Data Communications Equipment).

En una interfaz RS-232-C, el módem o dispositivo de interfaz con la línea suele considerarse el DCE, mientras que la computadora actúa como equipo terminal de datos DTE.

Dirección (address).

Localización precisa en memoria o en disco del lugar donde se almacena la información. Cada byte en memoria y cada sector en el disco tiene una dirección única; identificador único para un nodo específico en una red. Una dirección puede ser física, especificada por interruptores o puentes en la tarjeta interfaz de red, o lógica, establecida por el sistema operativo de la red.

DTE (Data Terminal Equipment).

Equipo terminal de datos, un dispositivo terminal del usuario, como una terminal o una computadora, conectada a un DCE mediante una interfaz RS-232-C u otra interfaz serie cualquiera.

Enlace multipunto.

Línea de conexión compartida por más de dos nodos.

Enlace punto a punto.

Línea que conecta a dos nodos sin pasar a través de ningún nodo intermedio.

Enrutador (router).

Dispositivo inteligente de conexiones que puede enviar paquetes al segmento correcto de una red de área local (LAN) y así llevarlos a su destino. Los enrutadores enlazan los segmentos de LAN en la capa de red del modelo ISO/OSI para comunicaciones

computadora a computadora. Las redes conectadas por enrutadores pueden usar protocolos similares o diferentes. El enrutador puede ser de uno de los siguientes tipos: enrutador central. Actúa como espina dorsal de la red, conectando muchas LAN; enrutador periférico. Conecta LAN individuales a un enrutador central o otro enrutador periférico; enrutador local. Opera dentro de los límites del manejo de la longitud del cable de la LAN; enrutador remoto. Conecta más allá de las limitaciones del manejador del dispositivo, tal vez a través de un módem o conexión remota; enrutador interno. Parte del servidor de archivos de la red; enrutador externo. Está localizado en una estación de trabajo en la red.

Estación de trabajo (workstation)

Es una microcomputadora conteniendo un paquete integrado de software, diseñado para mejorar la productividad de la red.

Ethernet.

Protocolo popular de redes y esquema de cableado con un porcentaje de transferencia de 10 megabits por un segundo por segundo, desarrollado originalmente por Xerox en 1976. Ethernet usa una topología de bus y los nodos de la red están conectados por cable grueso o coaxial, fibra óptica o par trenzado. Ethernet utiliza CSMA/CD (Carrier Sense Multiple Access/Collision Detection) para prevenir fallas de la red o colisiones cuando dos dispositivos intentan acceder a la red exactamente al mismo tiempo. El estándar original DIX (Digital Equipment, Intel, Xerox) o Libro Azul, ha evolucionado hacia el estándar IEEE 802.3, ligeramente más complejo, y la especificación 8802.3 de ISO. Las siguientes son algunas ventajas de Ethernet: Fácil de instalar a un precio moderado; Tecnología disponible de varias fuentes y muy conocida; Ofrece variedad de opciones de cableado; Trabaja bastante bien en redes con tráfico pesado ocasional. Las desventajas son: El tráfico pesado vuelve lenta la red; Una rotura en el cable principal ocasiona caída en gran parte de la red y es posible que la depuración de errores en una topología de bus sea difícil.

Fast Ethernet (Ethernet rápida).

Término aplicado al IEEE 802.3. Grupo de estudio de la propuesta de Ethernet de mayor velocidad, que fue desarrollado originalmente por Grand Junction Networks, 3Com, SynOptics, Intel y otros. También se conoce como 100BaseT. Ethernet rápida modifica el estándar Ethernet existente para permitir velocidades de 10 ó 100 megabits por segundo, o ambas y utiliza el método de acceso CSMA/CD. El estándar oficial define tres especificaciones de capas físicas para diferentes tipos de cables: 100BaseTX, para dos pares, Categoría 5 par trenzado no protegido; 100BaseT4, para cuatro pares, Categoría 3, 4 ó 5 par trenzado no protegido; 100BaseFX, para cable de fibra óptica.

FDDI (Fiber Distribution Data Interfaz).

Un estándar, para una tecnología de red basada en fibra óptica, establecida por el ANSI. FDDI especifica una velocidad de datos de 100 Mbps utilizando una longitud de onda de luz de 1300 nanómetros y limita la red a aproximadamente 200 Km. de longitud, con repetidores alrededor de cada 2 Km. El mecanismo de control de acceso utilizado es la tecnología Token Ring.

FDM (Frecuency Division Multiplexing).

Multiplexaje por división de frecuencias. El método de pasar múltiples e independientes señales a través de un único medio asignando a cada uno, una única frecuencia de portadora. El hardware que combina las señales es un multiplexador; el hardware que las separa es un demultiplexador.

Fibras ópticas.

Tecnología para transmitir información vía ondas de luz a través de un fino filamento. Las señales se codifican variando alguna característica de las ondas de luz generadas por un

rayo láser de bajo nivel de energía, la salida se envía a través de una fibra conductora de luz a un dispositivo receptor que decodifica la señal.

Frame relay.

Estándar CCITT para protocolo de conmutación de paquetes, que corre a velocidades de hasta 2 megabits por segundo; también incluye el ancho de banda por demanda (bandwidth on demand). Frame relay es menos robusto que el X.25, pero suministra mejor eficiencia y mayor rendimiento. Frame relay está disponible en varias compañías, incluyendo AT&T, CompuServe, Sprint, WilTel y las compañías Bell.

Fuentes externas (outsourcing).

Subcontratar operaciones de procesamiento de datos de la compañía con contratistas externos en vez de mantener hardware, software y personal de la empresa. Las fuentes externas se emplean a menudo como un mecanismo de reducción de costo, aunque el ahorro en costos puede ser bastante difícil de cuantificar.

Full-dúplex.

Sistema de comunicación que permite la transmisión simultánea de datos en ambas direcciones.

Half-dúplex.

Sistema de comunicaciones que permite el intercambio de información en ambas direcciones, pero no de forma simultánea.

HDLC (High Level Data Link Control).

(High Level Data Link Control). Un protocolo estándar ISO al nivel de enlace de datos. CCITT más tarde lo adoptó para su protocolo de acceso de enlace -LAP- utilizado en redes X.25

Home page.

En World Wide Web de Internet, página inicial. Una Home Page puede ser elaborada por un individuo o una corporación y es un punto conveniente de salto a otras páginas Web o recursos de Internet.

HTML (HyperText Markup Languaje).

Lenguaje estándar de hipertexto que se utiliza para crear páginas World Wide Web y otros documentos hipertexto. Cuando se accede a un documento HTML se observa con una mezcla de texto, gráficos y encadenamientos a otros documentos. Si se selecciona un encadenamiento, el documento relacionado se abrirá automáticamente, sin importar su localización. Los documentos hipertexto tienen como extensión del nombre .html.

Hub.

El dispositivo central de una red en topología estrella o sistema de cableado; utilizado en ARCnet y Token Ring.

IEEE (Institute of Electric and Electronics Engineers)

Instituto de Ingenieros Eléctricos y Electrónicos. Organismo norteamericano, parte del ANSI, que mediante estudios propios promueve normas de estandarización. El IEEE es una organización profesional y una de sus principales actividades es el desarrollo de normas no obligatorias pero generalmente aceptadas, en el rea de comunicaciones y electrónica, con énfasis en técnicas de medición y definición de términos.

Interfaz.

Frontera compartida entre elementos del sistema; definida por interconexiones físicas comunes, señales y significado de señales intercambiadas.

Interoperabilidad (interoperability).

Capacidad de ejecutar programas de aplicación de diferentes vendedores a través de redes de área local, amplia y metropolitana, dándoles a los usuarios acceso, a datos y programas mediante redes heterogéneas. Un usuario de red no necesita conocer nada acerca del sistema operativo o la configuración de hardware de la red, para acceder a los datos del servidor de archivos. La interoperabilidad se amplía con el incremento de la disponibilidad de productos que se ajustan a estándares abiertos y no a protocolos patentados específicos. Los productos funcionan de acuerdo con estándares aceptados nacional e internacionalmente.

ISDN (Integrated Services Digital Network).

Red digital de servicios integrados. Combina servicios de voz y de red digital a través de un único medio, posibilitando a los usuarios servicios digitales de datos así como conexiones de voz.

ISO (International Standards Organization).

Se abrevia ISO. Organismo internacional emisor de estándares, radicado en Ginebra, que establece estándares globales para comunicaciones e intercambio de información. ANSI es el miembro de Estados Unidos en la ISO. El modelo ISO/OSI (International Organization for Standarization's Open Systems Interconnection) de siete capas para comunicaciones computador a computador, es uno de los modelos de recomendaciones ISO más ampliamente aceptado.

Línea dedicada.

Línea de comunicación que proporciona una comunicación permanente entre dos nodos y que se alquila a la compañía telefónica.

Línea conmutada.

Ruta establecida, entre el emisor y el destinatario, únicamente por el tiempo que dure la transmisión (al igual que ocurre con las comunicaciones telefónicas).

Macrocomputadora (Mainframe).

Sistema grande de cómputo capaz de manejar muchos dispositivos periféricos poderosos.

MIPS.

Millones de Instrucciones por segundo

Módem (MODulador/DEModulador).

Dispositivo que modula y demodula señales transmitidas a través de instalaciones de comunicación.

Modo de transferencia asíncrona (Asynchronous Transfer Mode, ATM).

Método utilizado para transmitir voz, video y datos en redes de área local (LAN) de alta velocidad, ATM usa estallidos continuos de paquetes de longitud fija, llamados celdas, para transmitir datos. El paquete básico consta de 53 bytes, 5 de los cuales se usan para funciones de control y 48 para datos. ATM es un protocolo orientado a la conexión, y tiene dos posibilidades: circuitos virtuales permanentes (PVC), en el cual las conexiones se crean manualmente y circuitos virtuales conmutados (SCV), en el cual las conexiones se hacen automáticamente. En las pruebas se han logrado velocidades de hasta 2488 gigabits por segundo. ATM encontrará una gran aceptación en las redes de área local y redes de área amplia (WAN) como solución a la integración de redes dispersas en grandes distancias geográficas. También se conoce como cell relay.

Nodo.

Cualquier ordenador que forme parte de una red de ordenadores. El término es equivalente a una estación de red.

OSI.

Abreviatura de International Standars Organization/Open System Interconnection model. Modelo de referencia de redes, definida por ISO, que divide las comunicaciones computador a computador en 7 capas conectadas. Tales capas se conocen como pila de protocolo: Capa de aplicación 7: es el nivel más alto del modelo. Define la manera como interactúa la aplicación con la red, incluyendo administración de la base de datos, correo electrónico y programas de emulación de terminal; Capa de presentación 6: define la manera como los datos se formatean, presentan, convierten y codifican; Capa de sesión 5: coordina las comunicaciones y mantiene la sesión tanto tiempo cuanto sea necesario, ejecutando funciones de seguridad, ingreso de usuarios y tareas administrativas; Capa de transporte 4: define protocolos para estructuración de mensajes y supervisa la validez de la transmisión, ejecutando algunos chequeos de errores; Capa de red 3: define protocolos de enrutamiento de datos para asegurar que la información llegue al nodo destino correcto; Capa de enlace de datos 2: valida la integridad del flujo de datos de un nodo a otro, sincronizando los bloques y controlando el flujo de datos; Capa física 1: define el mecanismo para comunicarse con el medio de transmisión y la interfaz de hardware.

Pared de fuego (Firewall).

Barrera establecida por un enrutador o por un programa especial que se ejecuta en un sistema de computador dedicado, que solamente permite tráfico en una vía hacia afuera, desde la red protegida. Un firewall es un dispositivo que se usa generalmente para proteger las redes de intrusos no bienvenidos.

Peer-to-peer.

Compartición de recursos de igual a igual. Cada nodo en la red puede compartir sus recursos con otros nodos. Este tipo de compartición de recursos no requiere un servidor de recursos dedicado, y por lo tanto es más barato de instalar. No obstante el método de compartición es apreciablemente más lento que el de las redes de servidor centralizado.

Plataforma.

Consiste en el equipamiento (hardware) y sistemas (software) que soportaran la transferencia de datos en una red.

Protocolo.

Una descripción formal de formatos de mensajes y las reglas que dos o más máquinas deben seguir para intercambiar esos mensajes. Los protocolos pueden describir detalles de bajo nivel de las interfaces de máquina a máquina, o intercambios de alto nivel entre programas de aplicación.

Protocolo de enrutamiento (routing protocol).

Protocolo que habilita el enrutamiento mediante el uso de algoritmos específicos de enrutamiento que determinan la ruta más apropiada entre los nodos destino y fuente.

Protocolo de ubicación de direcciones (Address Resolution Protocol).

Se abrevia ARP. Protocolo dentro de redes TCP/IP y Apple Talk que le permite al computador central encontrar la dirección física de un nodo en la misma red con sólo conocer la dirección lógica del objetivo. Bajo ARP, una tarjeta de interfaz de red contiene una tabla (conocida como address resolution cache –lista de direcciones acumuladas con gran definición) que relaciona direcciones lógicas con las direcciones físicas de los nodos. La próxima vez que el nodo necesite enviar un paquete, éste primero verifica la lista de direcciones acumuladas con gran definición para determinar si ya existe la dirección física.

Si es así, se usa esta dirección y se reduce el tráfico o, de lo contrario, se ejecuta un requerimiento ARP para determinar la dirección.

Puente (bridge).

Dispositivo que se utiliza para conectar redes de área local (LAN) para poder intercambiar datos. Los puentes pueden trabajar con redes que usan diferentes cableados o protocolos. Un puente opera con la capa de enlace de datos del modelo ISO/OSI para comunicaciones de computador a computador. Maneja el flujo del tráfico entre dos LAN leyendo la dirección de cada paquete de datos que recibe.

Puerta (Gateway).

Un dispositivo de comunicación de propósito especial, que conecta dos o más redes y dirige paquetes de una a otra. Los gateways encaminan paquetes a otros gateways hasta que puedan ser entregados a su destino final directamente a través de una red física.

Red (network).

Grupo de computadores y dispositivos periféricos asociados, conectados por un canal de comunicaciones capaz de compartir archivos y otros recursos entre varios usuarios. Una red puede ir desde una red par a par, que conecta un pequeño número de usuarios en una oficina o departamento, a una red de área local (LAN), que conecta muchos usuarios a través de cables instalados permanentemente y líneas de conmutadores, a red de área metropolitana (MAN) o de área ancha (WAN) que conecta usuarios de varias redes diferentes, esparcidas sobre un área geográfica amplia.

Red de área local (local area network, LAN).

Red de computadoras y comunicaciones que cubre una área geográfica limitada, que permite que todos los nodos se comuniquen con todos los otros nodos, y no requiere un nodo o procesador central.

Red de área amplia (wide area network, WAN).

Se abrevia WAN. Red que conecta usuarios a través de largas distancias, cruzando a menudo límites geográficos de ciudades o estados.

Repetidor.

Un dispositivo de hardware que copia las señales eléctricas de una red Ethernet a otra. Normalmente, los lugares que tienen repetidores los usan para conectar un cable físico Ethernet en cada planta de un edificio a un cable central. La principal desventaja de un repetidor comparado con un bridge es que el repetidor transfiere tanto paquetes como ruido eléctrico.

Respaldo (Backup).

Copia actualizada de todos los archivos. Existen varias razones para hacer una copia de respaldo: Como seguro en caso de una falla del disco duro o del servidor. En ocasiones, los discos duros fallan y se destruye toda la información. Si esto ocurre, se pueden copiar los datos y directorios desde el respaldo. Una copia de respaldo es el seguro contra fallas del disco que pueden afectar miles de archivos existentes en el servidor; Protección contra el borrado accidental de archivos o directorios. Si se borran por error archivos o directorios se pueden restaurar a partir de la copia de seguridad; Como archivo al finalizar de un proyecto; cuando una persona se retira de la compañía, o al concluir un período financiero como el cierre de un año fiscal. La decisión sobre cuándo o qué tan a menudo se debe de hacer una copia de respaldo depende de la frecuencia con que se cambie la información en el sistema. Si las aplicaciones dependen de ciertos archivos clave, es necesario hacer copias de respaldo de manera frecuente y consistente; Mantenga varias copias; la redundancia debe ser parte de su plan de copias de respaldo; Pruebe sus copias para asegurarse de que sean lo que usted cree que son y para que pueda volver a cargar la información que necesite; Guarde sus copias en sitio seguro, diferente al lugar de trabajo;

no las deje junto al computador (si por accidente se daña el computador, las copias pueden sufrir daños); Reemplace su medio de respaldo periódicamente; Piense en hacer más copias de la información más importante a intervalos más frecuentes.

RS232C.

Estándar de EIA que especifica las características eléctricas de las interconexiones de baja velocidad entre computadoras y terminales o entre dos ordenadores. La especificación limita la velocidad a 20 Kbps. y la distancia a 15 metros, aunque algunos fabricantes soportan velocidades de hasta 38.4 Kbps. y más largas distancias.

SDLC (Synchronous Data Link Control).

Un predecesor de HDLC definido por IBM y usado en sus productos para su red con protocolo SNA.

Servidor de acceso (access server).

Computador que permite el ingreso a usuarios remotos que llaman a través de líneas telefónicas y utilizan los recursos de la red como si estuvieran conectados directamente al sistema. Un servidor de acceso puede ser un computador designado para este propósito y que se vende como parte de la red, o puede tratarse de un computador en la red con tarjetas CPU multipuerto instaladas.

Servidor de comunicaciones asíncronas (asynchronous communications server).

Servidor de red de área local (LAN) que le permite a un usuario marcar un número de la red pública de teléfonos o utilizar líneas dedicadas a comunicaciones asíncronas. También se les puede llamar servidores de conmutadores de entrada/salida o servidores de módem.

SNA (System Network Arquitecture).

El nombre se aplica a una arquitectura y a una serie de productos ofrecidos por IBM.

Sistemas distribuidos.

Sistemas informáticos en los cuales la potencia informática se distribuye a través de toda la red entre cierto número de computadoras, en vez de encontrarse localizada en una unidad central de gran potencia. Las redes de área local son un método ideal de interconexión para los sistemas distribuidos.

Tamaño correcto (rightsizing).

Proceso de acomodar los objetivos de la corporación a las soluciones disponibles de computación y redes para maximizar la efectividad de los negocios en la búsqueda de estos objetivos.

TCP/IP (Transmission Control Protocol/Internet Protocol).

Protocolo desarrollado por el Departamento de Defensa Norteamericana para permitir que computadoras distintas puedan comunicarse a través de una red.

TDM (Time Division Multiplexing).

Multiplexaje por división del tiempo. Técnica usada para multiplexar varias señales en un único canal de transmisión permitiendo a cada señal usar el canal por un corto período de tiempo antes de proceder con el siguiente.

Terminador.

Conector que incorpora una resistencia y se conecta en cada extremo del cable de la red.

Trama (Frame).

Utilizado como sinónimo de paquete de datos. El flujo de datos se divide en pequeñas unidades de información conocidas como tramas.

Transmisión asíncrona (asynchronous transmission).

Método de transmisión de datos que utiliza bits de inicio y parada para coordinar el flujo de datos, de tal manera que el intervalo de tiempo entre caracteres individuales no tenga que ser igual. También se usa la paridad para verificar la exactitud de los datos recibidos.

Transmisión síncrona.

Modalidad de trabajo en que la velocidad de transmisión de datos entre dos elementos viene relacionada con los sucesos que tienen lugar en otros lugares del sistema al que están conectados estos elementos. En esta técnica de transmisión se envían bloques de datos sin interrupción a velocidad fija con los dispositivos receptor y transmisor sincronizados. Cada bloque va precedido de caracteres sync (sincronización), no necesitándose bits de start-stop, (inicio-paro) en cada carácter, como ocurría en la transmisión asíncrona.

Usuario remoto (remote user).

Usuario que ingresa a la red mediante un módem y una línea telefónica desde un sitio ubicado a cierta distancia de la red principal.

Bibliografía

Arquitectura cliente/servidor.

Publicación oficial.

Personal Computing México.

15 y 16 de marzo de 1994.

Cambios de paradigmas empresariales.

Don TapScott.

Art Caston.

Editorial. Mc Graw Hill.

1ª. Edición español.

Cellular radio handbook. Referance For Cellular System Operation.

Boucher, Neil J.

Computer Communication Networks.

Gill Waters.

Londres; en México: McGraw-Hill, 1991,

375p. (Essex series in Telecommunication and Information System).

Computer Networks.

Tanenbaum Andrew S.

Ed. Prentice Hall, New Jersey, USA, 1988, 658 pp.

Data Communications.

Kenneth Sherman;

Ed. Prentice-Hall

2da ed.; 1985.

Data Communications, Computer Networks and Open Systems.

Fred Halsall,

3ra ed.; Wokingham: Addison Wesley; 1992.

Data Communications, Networks and Systems.

Thomas C. Bartee, editor en jefe;

2da ed.; 1992.

Digital communications. Microwave Applications.

Feher, Kamilo.

Dvorak's guide to desktop Telecommunications.

John C. Dvorak; Berkeley;

México: Osborne/McGraw-Hill, 1990.

Enterprise Series Connectivity: Local Area Networks.

Drew Heywood; Carmel, Indiana.

New Riders; 1992.

IEEE: Standards for Local and Metropolitan Area Networks;

Technical Committee on Computer Communications of the IEEE Computer Society;

IEEE Addison;

1992.

Internet y seguridad en redes

Karanjit Siyan, Chris Hare

Editorial Prentice Hall Hispanoamérica,1995

Internetworking LAN's and WAN's: concepts, techniques and methods.
Held Gilbert; John Wiley & Sons
1993.

Introducción a la Tecnología y Diseño de Sistemas de Comunicación y Redes de Ordenadores,
Freer John,
Ed. Anaya-Multimedia, Madrid 1991,.

Ley de la Comisión Nacional Bancaria y de Valores
1995

Local Area Networks (The next generation),
Madron Thomas W.,
Ed. John Wiley And Sons, Inc. New York, USA, 1990, 256 pp.

Metropolitan Area Networks: Concepts, Standards and Services.
Gary C. Kessler, David A. Train.
McGraw-Hill; 1992.

Networks protocols.
Tanenbaum, Andrew.
Ed. Prentice-Hall.

Redes de computadoras. Protocolos, Normas e Interfaces.
Black, Uyless
Macrobit editores, 1990.

Redes de Telecomunicaciones.

Mischa Schawartz,

3ra ed., 1994.

Simplifying LAN-WAN Integration,

Burns Joseph,

Ed. Wellfleet Communications, USA, Febrero 1992, 66 pp.

Technical Aspects of Data Communications,

Mcnamara John E.,

Ed. Digital Press, USA, 1988, 330 pp.

Telecommunications and the computer.

Martin, James.

Ed. Prentice-Hall.

Telecomunicaciones vía Fibras ópticas,

Centro de información y documentación,

Ing. Bruno Mascanzoni, México, 1991, 365 pp.

Telecomunicaciones vía Microondas,

Centro de información y documentación,

Ing. Bruno Mascanzoni, México, 1991, 315 pp.

Telecomunicaciones vía Satélite,

Centro de información y documentación,

Ing. Bruno Mascanzoni, México, 1991, 285 pp.

Teleinformática: principios técnicos y mediciones físicas en comunicación,

Centro de información y documentación,

Ing. Bruno Mascanzoni, enero 1984, pag. 44 - 62 pp.

Telemática: técnicas informáticas de transmisión y proceso de datos,

Pujolle Guy,

Ed. Paraninfo , Madrid 1988,

Transmission System for Communications.

Bell Telephone Laboratories, Inc.;

5ta ed.; New Jersey,1992.