ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERIA ELECTRICA

PLANIFICACION DE LA RED DE COMPUTADORES DE AREA LOCAL DE LA COMPAÑIA PETROLERA OCCIDENTAL DE EXPLORACION Y PRODUCCION

TESIS PREVIA A LA OBTENCION DEL TITULO DE INGENIERO EN LA ESPECIALIDAD DE ELECTRONICA Y TELECOMUNICACIONES

LUIS FERNANDO GRANIZO CEDEÑO

QUITO, MARZO DE 1995

AGRADECIMIENTO

Agradezco a la Escuela Politécnica Nacional, a la Facultad de Ingeniería Eléctrica y a todos los profesores que, día a día, con su conocimiento y docencia, colaboraron con mi formación profesional.

Al Ing. Marco Coronel, al Ing. Luis Monge, al Ing. Alfredo Corral, al Sr. Carlos Ortega y al personal de MIS de OPEC, por su ayuda incondicional para la realización de este trabajo.

A todas las personas que de alguna manera colaboraron en el desarrollo de esta tesis.

Quiero dejar constancia de mi reconocimiento muy especial al Ing. Pablo Hidalgo por su acertada dirección y dedicación.

Dedicatoria:

A: Mis Padres
Miche, Mamina y Yoyita
Susy
Mis Hermanos
Padre Pepe Mendoza S.J.
Dr. José Rafael Estrada
Que supieron cultivar en mí el ideal superior de DIOS.

Certifico que la presente tesis ha sido elaborada en su totalidad por el Señor Luis Fernando Granizo Cedeño.

Ing. Pablo Hidalgo Lascano

INDICE GENERAL

INTRODUCCION

En la actualidad, las redes de datos, de manera particular las redes de área local, se constituyen como una herramienta fundamental dentro del desarrollo socio-económico de las empresas.

Estas redes que por su tamaño y versatilidad son las más utilizadas por la mayoría de empresas, permiten: compartir recursos, integrar a las personas, optimizar el costo de las aplicaciones, entre sus principales ventajas ventajas.

Pero como todo sistema productivo, las redes de datos necesitan planificarse y mantenerse de forma adecuada, ya que si no se las mantiene pueden provocar retardos dentro de los procesos; para ello, se necesita la documentación pertinente: manuales de los equipos, planos civiles y eléctricos, cableado de datos, etc.

Este trabajo de tesis responde a la necesidad de documentar de forma adecuada, las antiguas instalaciones de red (oficinas ubicadas en el edificio del Banco de los Andes) de Occidental Production and Exploration Company (OPEC), para planificar de mejor manera las prestaciones y mantenimiento de la red en las nuevas instalaciones.

Con la colaboración de esta empresa (OPEC), se pudo obtener una documentación confiable de los equipos, su distribución física, configuración y problemas que se venían suscitando. Esta información sirvió de base para establecer políticas de desarrollo y procedimientos técnicos funcionales en el área de Sistemas y Comunicaciones.

Luego, en base a dichas conclusiones se implementaron los cambios pertinentes dentro de la red, logrando mejorar notablemente el rendimiento en las nuevas instalaciones. Es decir, la planificación de la red se fue dando sobre el desarrollo de este estudio.

Adicionalmente, este trabajo tiene como objetivo mostrar el estado actual de las comunicaciones de datos, para que el estudiante de la Facultad disponga de un material bibliográfico acerca de los equipos y técnicas utilizadas en el procesamiento informático y comunicaciones en las redes de área local y área metropolitana.

En el desarrollo del trabajo se realiza una introducción general del funcionamiento de OPEC y un breve análisis de los conceptos generales sobre las redes de área local y redes de área metropolitana para el cabal entendimiento de los capítulos posteriores.

Luego, se muestra la configuración de la red de comunicaciones, poniendo especial énfasis en la red de datos; este estudio incluye una descripción de los equipos utilizados para dichos fines y su integración dentro del sistema. Este es el estado al que se llegó en base a la planificación de la red.

Así mismo, se estudian los aspectos principales que se deben tomar en cuenta para brindar las protecciones adecuadas al sistema (equipos e información).

En lo referente a la optimización de la red se hace incapié en los proyectos establecidos dentro de las áreas de servicios de la red, mantenimiento, operación e integración de plataformas de trabajo.

Finalmente el trabajo concluye enunciando las pautas para establecer las políticas de desarrollo y procedimientos técnicos, así como también sugiriendo recomendaciones de proyectos para dar solución a ciertos problemas puntuales de afinamiento de la red.

Se incluye una selección de Anexos para complementar y permitir al lector profundizar en algunas de las áreas de interés. Como por ejemplo en el Anexo 1 se presenta una descripción de los comandos del sistema operativo NetWare, en donde se detalla sus funciones y su sintaxis.

Entre los alcances de esta tesis no se muestra ningún análisis formal de tipo económico, ya que el estudio se orienta a una optimización de los recursos actuales del sistema, y a posibles alternativas de implementación de otros equipos de acuerdo a las proyecciones previstas.

1. GENERALIDADES Y USO DE LA RED EN OPEC

Occidental Oil and Gas Corporation (OPEC) es una compañía transnacional asentada legalmente en el país como concesionaria de PETROECUADOR en la exploración y extracción del petróleo ecuatoriano.

Occidental actualmente tiene centros de operación alrededor de todo el mundo. La matriz se encuentra en Tulsa, Oklahoma, Estados Unidos de Norte América.

Dentro de EEUU es una de las principales empresas que se dedica a la exploración, extracción, comercialización de petróleo, gas y carbón, teniendo varios centros operativos distribuidos a lo largo de su territorio.

Internacionalmente se encuentra establecida en Argentina, Bolivia, Colombia, Ecuador, Perú, China, Indonesia, Malasia, Omán, Pakistán, Siria, Yemen, Arabia Saudita, Reino Unido, y la Comunidad de Estados Independientes (Ex- Unión Soviética).

ORGANIZACION

Su administración está centralizada y su base de operaciones es Tulsa.

Occidental centra sus actividades en un departamento de ingeniería y operaciones, cuya finalidad es la de optimizar recursos y establecer procedimientos técnicos para la exploración y explotación de petróleo al más bajo costo y con el mayor rendimiento. Este departamento de ingeniería posee

una tecnología de punta con los más sofisticados medios electrónicos para el análisis de las estructuras y sedimentos de las capas geológicas de la tierra.

El departamento de sistemas y comunicaciones tiene que establecer un interfaz adecuado en la comunicación de voz y datos entre el campo de producción, el centro administrativo local y la matriz. Actualmente, la compañía está finalizando una etapa de exploración y muy próxima a comenzar la extracción del petróleo en nuestro país. Por tanto, la necesidad de establecer una comunicación de voz en primera instancia es imprescindible, la comunicación de datos toma mayor importancia a medida que se acerca la etapa de producción.

El campo de producción se encuentra localizado en la amazonía ecuatoriana, el centro administrativo local está en Quito y la matriz en Tulsa, EEUU.

El objetivo principal de la red es la de establecer un vínculo administrativo con los siguientes parámetros:

- Conocer en todo momento el estado económico-productivo de la empresa.

- Compartir la información dentro de los diferentes departamentos para facilitar las operaciones de control, supervisión y auditoría.

- Establecer una comunicación eficaz entre los diferentes niveles administrativos y los diferentes centros de operación.

DEPARTAMENTOS

Administrativamente OPEC se divide en departamentos, esto hace que la vinculación dentro del área correspondiente a cada uno de los departamentos sea ágil y eficaz. La vinculación de toda la empresa actualmente se basa en el sistema telefónico y en las radiocomunicaciones.

Los departamentos son:

Presidencia y Gerencia General
Gobierno y Control Ambiental
Legal
Finanzas
Operaciones
Exploración
Materiales
Sistemas
Recursos Humanos

2. VISION GENERAL DE LAS REDES DE AREA LOCAL (LAN) Y REDES DE AREA EXTENSA (WAN), TOPOLOGIAS Y TECNICAS MAS UTILIZADAS

Las redes de área local (LAN, Local Area Network)[1], son redes de computadores personales que están definidas por la cobertura física de ellas, es decir están concebidas para abarcar un área pequeña; todo lo contrario son las redes de área extensa (WAN, Wide Area Network)[1] que están concebidas para cubrir mayores extensiones.

Existen otro tipo de redes de datos que generalmente involucran grandes ordenadores o "mainframes"[1] y que se conectan a grandes distancias a través de enlaces de radio, cables submarinos e inclusive fibras ópticas.

[1] Ver glosario.

2.1 MOTIVOS PRINCIPALES PARA INSTALAR UNA RED DE AREA LOCAL

a. COMPARTIR RECURSOS

Histórica y técnicamente, el uso compartido de periféricos costosos es el motivo principal y el más conocido. Se puede compartir impresoras láser, impresoras en color, "Post-Scrip"[1] , "scanners"[1] de alta definición, "gateway"[1] o pasarela de comunicaciones síncronas con el mundo de los grandes sistemas IBM u otras marcas, pasarelas asíncronas (VT100), servidores, télex, fax, etc. Para esto se implementan colas de espera y el éxito depende de un buen ajuste de los recursos a las necesidades.

b. INTEGRAR A LA PERSONA

Este es un motivo inherente a la organización de las empresas. Las LAN permiten que cada puesto de trabajo disponga al mismo tiempo de una inteligencia local y autónoma y del acceso a puntos de convergencia, tanto a nivel departamental como general.

c. REFORZAR EL GRUPO

Las LAN constituyen estructuras ideales para realizar proyectos de trabajo y desarrollo en grupo. Dentro de una empresa es necesario establecer grupos de trabajo, tales como contabilidad, servicios de personal, publicidad, facturación, compra de materiales, etc. Estos modos de funcionamiento pueden coordinarse a través de las LAN, confiriendo una autonomía propia a cada área de trabajo, pero siendo parte de una misma estructura.

---

[1] Ver glosario.

d. ADMINISTRACION DE LA MICROINFORMATICA

Se puede crear estándares en el uso y control de aplicaciones y recursos, facilitando la labor del usuario final mediante un control del administrador de la red. Como consecuencia, se tiene una mejor gestión de los equipos y una mejor administración de los usuarios.

e. REFORZAR LA SEGURIDAD

A nivel de usuarios, se permite la entrada a la red solamente a personas autorizadas. A nivel de datos y aplicaciones, se restringe el acceso por jerarquía y por área.

f. REEMPLAZAR EL MODELO DE INFORMATICA CENTRALIZADA

La tendencia tecnológica es la de establecer un modelo de igual a igual, distribuido, en el cual cada computador es un nodo inteligente de una red.

g. REPARTIR EL COSTO DE LAS APLICACIONES

Se tiene la ventaja de una administración centralizada en un ambiente distribuido. El costo de las aplicaciones por usuarios disminuye y se puede implementar aplicaciones en un contexto cooperativo.

h. CONTROLAR LOS DATOS

Se lo realiza mediante la implementación de servidores de ficheros; además se puede permitir en ciertos casos el acceso a datos almacenados en puestos de trabajo individuales.

i. GENERALIZAR LOS SERVICIOS

Gracias a las LAN, el usuario puede al mismo tiempo beneficiarse de nuevos servicios, télex, tratamiento de imágenes, videotex, tan pronto como estén disponibles en la red, manteniendo al mismo tiempo la calidad individual de su trabajo en la estación.

En general, una LAN se utiliza para optimizar los recursos del sistema tanto de "hardware"[1] como de "software"[1] , es decir compartir periféricos e información. Además permite comunicaciones de datos más versátiles, ya sea dentro de la red o con otras redes u otros "mainframes".

La idea es que la LAN le permita al usuario acceder a datos y programas en cualquier parte de la red, compartir periféricos tales como impresoras láser o discos duros, además de establecer comunicaciones mediante correo electrónico con el resto de miembros de la red. Esto redunda en una relación interna más solvente y en un aumento de productividad para la empresa.

2.2 CONCEPTOS BASICOS

SERVIDOR

Un servidor es un computador que comparte sus periféricos con otros computadores.

Un servidor puede ser dedicado o no dedicado. Un servidor dedicado es aquel que, como su nombre lo indica, sólo está dedicado a ser servidor de la red, es decir no puede ser utilizado por ningún usuario, pero puede prestar opciones de monitoreo de la red[2] . Por otro lado, pueden existir servidores no dedicados, que además de servir a la red, permiten que un usuario pueda estar trabajando en él.

---

[1] Ver glosario.
[2] El servidor dedicado posee esta opción de monitoreo de la red y se denomina "consola".

SERVIDOR DE ARCHIVOS

Los usuarios de una LAN pueden hacer uso del disco duro de un servidor de archivos, pero cabe recalcar que el servidor de archivos restringe a un sólo usuario el acceso a un archivo o parte de él, es decir dos usuarios no podrían accesar al mismo tiempo el mismo archivo.

SERVIDOR DE IMPRESORAS

Permite a los usuarios de la red compartir las impresoras.

GATEWAY

Es un dispositivo que permite establecer una comunicación entre dos "plataformas" distintas. Entendiéndose por plataformas los distintos dispositivos de "hardware" y "software" no compatibles, que siguen diferentes estándares.
De manera general un "gateway" interconecta dos LAN que emplean protocolos de alto nivel diferentes, realizando una función determinada y específica. Por ejemplo un "gateway" de correo electrónico interconecta dos centrales postales de dos redes diferentes (tales como una Ethernet y otra "Token-Ring").

2.3 TOPOLOGIAS MAS UTILIZADAS

La topología de una red local está relacionada con el cableado de la misma. De manera general se dice que una LAN se puede cablear de las siguientes formas:
- Estrella,
- Bus,
- Anillo,
- Arbol,
- o sus combinaciones (una topología en malla sería la combinación de varias o todas las topologías anteriores).

ESTRELLA

Todos los computadores están conectados a un computador central. Su mayor inconveniente es la excesiva dependencia del computador central.

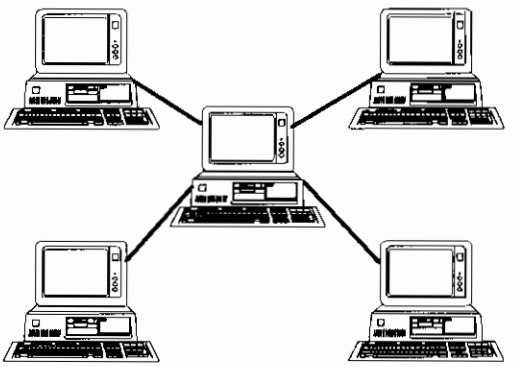


Figura I.1. Topología en estrella.

BUS

Todos los computadores acceden al bus, todos escuchan los mensajes existentes en el bus pero sólo acceden a los dirigidos a ellos.

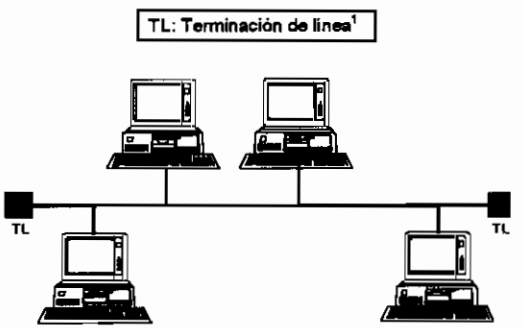


Figura I.2. Topología en bus.

ANILLO

Todos los computadores están dentro del anillo. Los datos pueden circular en cualquier dirección, un fallo en uno de los ordenadores no necesariamente implica la caída total de la red.

[1] Ver glosario.

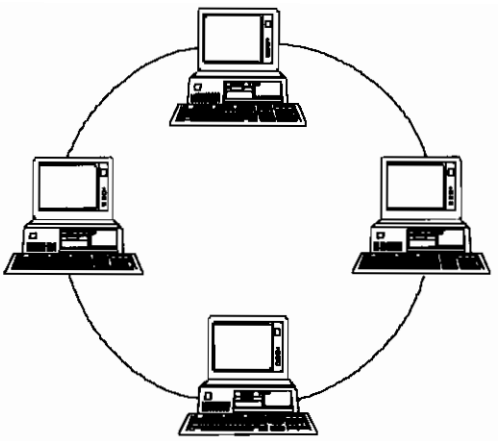


Figura I.3. Topología en anillo.

ARBOL

Esta topología utiliza buses interconectados a un bus principal, es decir es una aplicación más compleja de una red con topología en bus. Necesita un dispositivo especial en la raíz del árbol (TL), cualquier fallo puede interrumpir las comunicaciones con las ramas secundarias, mientras el resto de computadores pueden seguir operando en red normalmente.

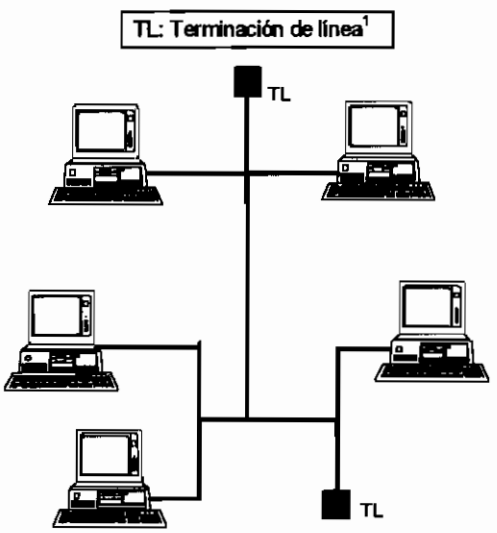


Figura I.4. Topología en árbol.

[1] Ver glosario.

Los diseños de los fabricantes de redes locales se basan en cuatro parámetros fundamentales:

- La velocidad y confiabilidad.
- El tamaño.
- Localización física y geográfica de la red y sus computadores.
- Costo y dificultad de cableado.

En la actualidad se le está dando mucha importancia a la dificultad del cableado. Una de las soluciones por ejemplo ha sido cableado en bus con cables de pares trenzados, a pesar de su menor ancho de banda y mayor susceptibilidad al ruido. Un ejemplo de esto es "EtherTwist".

2.4 NORMALIZACION

NORMAS OSI

Las normas OSI[1] (Interconexión de Sistemas Abiertos) se crearon para regular el intercambio de información entre computadores.

Aún hoy, en muchos aspectos de la informática, por ejemplo entre "mainframes", los computadores siguen siendo incompatibles y son necesarias soluciones propias de interconectividad de cada fabricante. Las ventajas de la normalización y estandarización son evidentes. La definición de un sistema abierto es difícil, pero se puede decir que es un sistema donde un usuario final se puede comunicar con otro sin preocuparse de ningún proceso intermedio ni del "hardware" del computador con el que se conecta. Entendiéndose aquí por usuario final tanto a la persona como a la aplicación residente en un computador.

[1] Open Systems Interconection, promulgadas por la ISO (International Standards Organization).

LOS SIETE NIVELES OSI

Los niveles OSI son una propuesta de la ISO[1] para que los diferentes fabricantes de la industria informática entreguen al mercado equipos compatibles que puedan ser interconectados entre sí.

Cada nivel representa un estado equivalente al cual debe llegar la información, de tal manera que cualquier equipo que soporte dicho nivel pueda identificar y procesar correctamente la información.

Con este propósito la ISO crea su modelo de 7 niveles o capas con sus respectivas normas. Estos niveles son los siguientes:

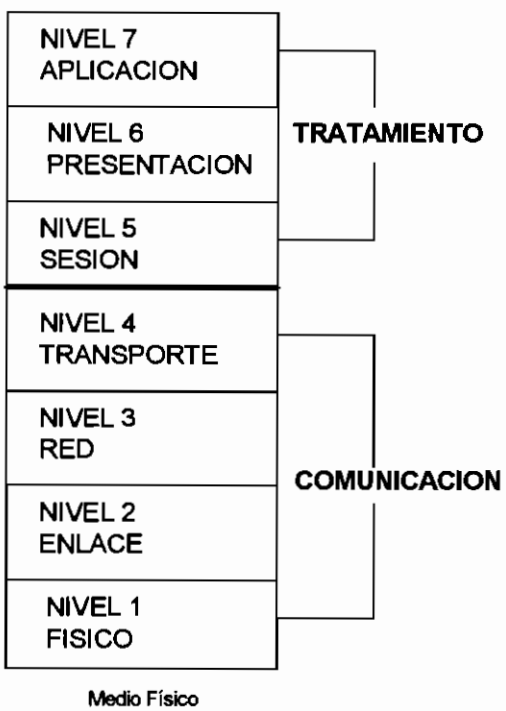


Figura I.5 Capas del modelo OSI.

Cada nivel se construye sobre el anterior. La función de cada nivel es brindar servicios a los niveles superiores.

[1] Organización de Estándares Internacionales.

Al pasar de un nivel a otro se necesita procesar la información para lograr el estado equivalente correspondiente a ese nivel; a dicho proceso se le denomina interfaz. Por tanto cada interfaz se constituye de elementos de "hardware" y de "software" que permiten la adecuación de la información para llegar al nivel requerido desde el nivel contiguo.

Por ejemplo, el nivel "n"[1] de un computador intercambia información con el nivel "n" de otro computador, las reglas y convenciones utilizadas en esta conversación se conocen como protocolo del nivel "n". En realidad no existe una transferencia directa de datos entre capa y capa de los dos computadores, sino cada capa pasa la información de datos y control a la capa inmediatamente inferior y así sucesivamente hasta alcanzar el medio físico a través del cual se realiza la comunicación real.

Al conjunto de niveles y protocolos se lo conoce como arquitectura de red. Por tanto, el modelo OSI en sí no es una arquitectura de red ya que no especifica en forma exacta los servicios y protocolos que se utilizaran en cada una de las capas. Aunque la ISO tiene normas para cada una de las capas, éstas no forman parte del modelo.

Los cuatro niveles inferiores (físico, enlace, red y transporte) aseguran la comunicación en sí, mientras que los tres superiores tratan la información enviada y la presentan en un formato adecuado para el usuario final.

El nivel físico asegura la transmisión de la información a través de un medio físico. El interfaz entre el nivel físico y el medio físico establece el medio de transmisión por donde se va a enviar la información, así como el procedimiento físico (eléctrico y mecánico) y lógico a seguir para la correcta transmisión de los datos. Asegura además que los bits enviados por un cable de determinadas características (coaxial, par trenzado, fibra óptica, etc.) van a llegar al otro

[1] "n" puede ser cualquier nivel del 1 al 7.

extremo. Este nivel determina si es una transmisión "full dúplex" [1] ó "half-dúplex" [1], si es transmisión sincrónica [1] ó asincrónica [1], niveles de voltaje, etc.

El nivel enlace establece un procedimiento por el cual los bits enviados de una estación (nodo) a otra, lleguen sin ninguna alteración. Es decir, garantiza una conexión entre dos nodos sin errores. Mediante este nivel, no se puede establecer una ruta de comunicación pero se puede enlazar nodo a nodo de forma continua y llegar desde el primero hasta el último de una serie de nodos que queramos comunicar. En este nivel los bits se agrupan para formar lo que se denominan tramas [1] , cada trama tiene una cabecera, los datos y un fin de trama. Según el protocolo [2] utilizado, se usará una convención u otra. Un ejemplo de protocolo en este nivel es el HDLC [1] (High Level Data Link Control), que usan las redes X25.

El nivel de red implementa procedimientos para establecer las rutas por donde la información va a transitar para ir desde el nodo que envía hasta el nodo destino. Para esto a la trama de enlace se le aumenta unos bits de cabecera, que indican a que punto de la red van dirigidos, así como algunos más de control y se habla entonces de paquetes de información. Un paquete puede contener varias tramas y tiene un número fijo de bits. Es importante aclarar que al hablar de comunicaciones síncronas, todos estos protocolos están orientados a bits, es decir tratan la información como un flujo de bits; al hablar de comunicaciones asíncronas se usan normalmente protocolos orientados a byte. Si se unen los paquetes, se forma un mensaje, siendo ese mensaje la información que el usuario que envía quiere hacer llegar a un destino. El nivel de red garantiza la transparencia de la ruta para el usuario final.

En cada nivel se presupone que los problemas que van por debajo han quedado solucionados. Además, cada nivel solo tiene como mucho dos interfaces; el

---

[1] Ver glosario.
[2] Protocolo es una serie de reglas para la conformación de la trama.

primero obtiene la información que le llega del nivel inferior, y el segundo, entrega esa información en el formato que necesita al nivel superior.

El cuarto nivel se encarga de darle a la información su forma inicial. Sólo se preocupa de que los mensajes enviados por un usuario lleguen a otro tal y como los envió. Este nivel asegura la comunicación "punto a punto" como se diría en terminología telemática. Por ejemplo en telefonía, este nivel sería el encargado de convertir de análogo a digital en un extremo, y luego en el otro extremo la conversión inversa, de digital a análogo.

Los tres niveles superiores garantizan el correcto entendimiento de la información transferida. Están orientados al tratamiento de dicha información, por lo tanto no se los encontrará definidos en las redes de comunicaciones, sino dentro del "software" de computadores.

A niveles superiores es todavía más difícil estandarizar. Uno de los intentos de normar el intercambio de información a este nivel es el EDI (Electronic Data Interchange). Pretende ser un estándar para que los computadores interpreten los datos siempre de igual manera, electrónicamente y sin posibilidad de error. En Europa existe un estándar, el EDIFACT que a pesar de ser el más difundido aún no es lo suficiente, existiendo un gran interés de ciertos sectores de la industria sobre todo de los sectores automovilístico y ferroviario para su completa aceptación.

Actualmente sólo se puede decir que están normalizados por completo los tres niveles inferiores (físico, enlace y red) quedando el resto con numerosas lagunas. El resto de normas no están definidas totalmente.

El hecho de haber dividido el problema en siete niveles distintos y aprobar normas distintas para cada nivel, permite cualquier avance técnico, que puede ir desde un nuevo medio físico hasta un algoritmo más rápido de

reencaminamiento de datos, de tal manera que se cambie sólo lo mejorado y se mantenga el resto igual.

Además de la ISO, se tiene entre los principales organismos de normalización al CCITT (Comité Consultivo Internacional para Telegrafía y Telefonía), la CEPT (Conferencia Europea de Correos y Telecomunicaciones) y el IEEE (Instituto de Ingenieros de Eléctrica y Electrónica).

NORMAS OSI MAS DIFUNDIDAS

La norma X25 del CCITT se definió a mediados de los años setenta, aunque se adaptó a las especificaciones OSI en 1984. Define los tres niveles inferiores y es una especificación para el intercambio de datos en redes de conmutación de paquetes. La mayoría de las comunicaciones empresariales mundiales dependen actualmente de esta norma.

Las redes X25 mundiales están conectadas internacionalmente, y al estar normalizadas se pueden conectar a través de ella computadores de cualquier país con un modem[1] X25.

El correo electrónico X400 se adapta totalmente a las especificaciones OSI. Se sitúa en los niveles más altos de los 7 niveles, incluyendo los de presentación y aplicación. Esta norma resulta compleja de implementar en los computadores precisamente por su afán de ser completamente compatible. Sin embargo, sus ventajas son evidentes, se puede enviar mensajes normalizados a cualquier usuario sin importar en que lugar se encuentre. Usa el sistema de directorios X500 del CCITT también normalizado por OSI. Actualmente, numerosos fabricantes de sistemas de correo electrónico han desarrollado "gateways" que siguen la norma X25.

[1] Ver glosario.

La tabla I.1 muestra las normas establecidas tanto por el CCITT como por la ISO para los distintos niveles OSI. Adicionalmente se describe el significado de las abreviaturas utilizadas.

	CCITT	ISO
	X200	ISO 7498
7	X400/X500	FTAM-IS 8571
6	X409	IS 8822/23
5	X215/X225	IS 8326/27
4	X214/X225	IS 8072/73
3	X25-3 I450/51	IP-IS 8473
2	X25-2 I440/41	MAC/LLC
1	X25-1 I430/31	CSMA/CD,TOKEN-RING/FDDI

	WAN	LAN

CSMA/CD	CARRIER SENSE MULTIPLE ACCESS/COLLISION DETECTION
FDDI	FIBER DISTRIBUTED DATA INTERFACE
FTAM	FILE TRANSFER AND ACCESS MANAGEMENT
IP	INTERNET PROTOCOL
IS	INTERNATIONAL STANDARD
LLC	LOGICAL LINK CONTROL
MAC	MEDIUM ACCESS CONTROL

Tabla I.1. Normas del CCITT y de la ISO para el modelo OSI.

Se puede decir que el CCITT se ha preocupado de una manera especial en dictar las normas para redes WAN, mientras que la ISO centra su atención en las LAN.

En lo referente a las LAN, la IEEE[1] ha venido realizando una ardua labor en lo que a estandarización se refiere. La IEEE tiene el comité 802, que define las pautas, directrices y estándares para las redes locales. Las normas IEEE 802 han sido adoptadas: por la ANSI[2] como una norma nacional norteamericana; por

[1] IEEE. Institute of Electrical and Electronics Engineers.
[2] American National Standards Institute.

la NBS[1] como una norma gubernamental en los Estados Unidos de Norteamérica; y por la ISO como una norma internacional conocida como ISO 8802 .

- La norma 802.1 es una introducción al conjunto de normas.
- La norma 802.2 describe el nivel de enlace[2], que utiliza el protocolo LLC[3].
- La norma 802.3 basada en Ethernet[4] .
- La norma 802.4 describe el "Paso de testigo en Bus" (Token-Bus).
- La norma 802.5 describe el "Paso de testigo en Anillo" ("Token-Ring").

Las normas 802.3 (CSMA/CD), 802.4 (TOKEN-BUS) y 802.5 (TOKEN-RING) difieren en la capa física (primer nivel OSI) y en la subcapa MAC pero resultan compatibles en el resto de la capa de enlace (segundo nivel OSI).

Actualmente las normas IEEE 802.5 para Token Ring y la IEEE 802.3 para Ethernet son las más utilizadas.

Estos métodos de acceso son los más comunes en todas las redes locales comercializadas actualmente. El más novedoso es FDDI, especial para redes distribuidas que utilizan fibra óptica. Lo anterior estaría encuadrado dentro del nivel físico. En los niveles superiores se encontrarían normalizados los protocolos LLC.

ETHERNET

Como ya se ha dicho, sigue el estándar IEEE 802.3. El denominador común a todas ellas es un esquema de acceso por contenciones[5] , cableado con topología en bus y cable coaxial como medio de transmisión.

---

[1] National Bureau Standards
[2] Segundo nivel del modelo OSI (Open Systems Interconection) de la ISO.
[3] Logic Link Control (Control Lógico de enlace).
[4] Ethernet es marca registrada de la compañía XEROX.
[5] Los computadores "contienden" por accesar al medio. El que logra ocupar primero el bus es el que transmite.

La norma 802.3 se refiere a CSMA/CD[1] . Cuando una estación desea transmitir escucha la información que fluye a través del cable, si el cable se encuentra ocupado, la estación espera hasta que esté en estado inactivo, en caso contrario transmite de inmediato. Si dos o más estaciones simultáneamente comienzan a transmitir a través de un cable inactivo generan una colisión. Las estaciones terminarán su transmisión y esperarán un tiempo aleatorio para repetir el proceso completo.

Entre las primeras redes comerciales de este tipo que aparecieron se tienen:

AT&T STARLAN,
CORVUS OMNINET,
Gateway Communications (G-NET),
Orchild PC Net,
3 COM EtherLink,
Ungermann-Bass Net/One Personal Connetion,
Allen-Bradley VistaLAN/PC,
Nestar Plan Series.

REDES CON PASO DE TESTIGO EN ANILLO (TOKEN-RING)

Se definen en el estándar IEEE 802.5. Utilizan el sistema de paso de testigo en anillo y cableado compatible al de la red "Token-Ring" de IBM.

El estándar IEEE 802.5 define dos niveles OSI: el físico y el de enlace. El primero se refiere a la forma de instalar la red, los tipos de cableado, las asignaciones y niveles de señales e inclusive los enchufes y conectores . El nivel de enlace define cómo un ordenador controla el acceso a la red y de qué forma se deben empaquetar los datos para su transmisión.

[1] Protocolo de detección de portadora de acceso múltiple al medio con detección de colisiones.

Los restantes niveles ISO/OSI se implementan en la tarjeta adaptadora de la red, en el programa PC LAN y en los programas de usuarios que comparten datos en la red.

En este punto, es importante definir el NETBIOS (NETwork Basic Input Output System). Es un estándar de IBM que garantiza virtualmente la compatibilidad de cualquier máquina conectada a la red. Físicamente se encuentra en la tarjeta adaptadora de la red. Para comprender la función del NETBIOS se relacionará con su homólogo en el computador personal, el BIOS, el cual hace posible que un mismo programa pueda funcionar en un PC, en un XT o en un AT. Similarmente, el NETBIOS controla los accesos a los recursos de una red, ordenando y distribuyendo las demandas de recursos de la red. Cuando un programa que funciona en un computador personal conectado a la red, necesita un recurso que no está conectado directamente a él, como por ejemplo una impresora remota, el NETBIOS toma el testigo y establece la conexión hacia el periférico solicitado a través del servidor de impresión, ayudándose de otros circuitos de la tarjeta adaptadora.

La misión del testigo ("token") es permitir el envío de datos solamente cuando se tiene el testigo libre ("free token"), de tal manera de evitar que dos estaciones diferentes envíen datos al mismo tiempo. Cuando una estación desea enviar datos tiene que esperar que le llegue el testigo libre; cuando éste llega, lo coge y lo marca como ocupado y transmite los datos al anillo. El testigo ocupado más los datos forman una trama de datos (dirección de la estación receptora, dirección de la estación fuente y las subtramas de control, de información, de "status" y de comprobación).

Es muy importante recalcar que el paso de testigos en anillo es ideal para redes medianas. En redes muy grandes, en cambio, se pierde mucho tiempo mientras

el testigo va de una estación a otra (ya que aunque las estaciones no necesiten transmitir la mayor parte del tiempo, siempre reciben un testigo).

Se pueden producir retardos innecesarios en la red por el simple hecho de pasar el testigo. Estos retardos se deben a que la estación que emite el mensaje es la encargada de liberar al testigo; es decir, la estación tiene que esperar que el mensaje sea recibido completo y sin errores en la estación receptora para poder liberar al testigo.

Estos retrasos se pueden obviar implementando anillos locales más pequeños entrelazados con puentes[1] , dividiendo de esta manera la red para que el tráfico originado en un anillo local se distribuya en él.

Entre las primeras que aparecieron se tiene la PROTEON ProNET, compatible con la "Token-Ring" de IBM.

REDES EN ESTRELLA

Entre sus ventajas se tiene que no necesita métodos de acceso al medio, pero sus desventajas pesan debido a que utilizan cables dedicados y excesiva dependencia del servidor central. Ejemplos de estas redes son la Novell S-NET y ARCNET.

[1] Ver glosario.

CAPITULO 1

1. SITUACION ACTUAL

La planificación de la red es un trabajo realizado por el autor de la tesis desde enero de 1993. Por tanto se presenta una descripción del sistema y como se ha logrado. Para su respectiva implementación se contó con la colaboración del personal del departamento de Sistemas y Comunicaciones de OPEC.

Existen algunos sistemas de telecomunicaciones en OPEC, entre los principales se pueden nombrar la central telefónica, el sistemas de comunicaciones vía satélite y la red de área local de computadores. Adicionalmente a ellos, las comunicaciones con el Oriente se realizan principalmente por un sistema de radio VHF, al que se añadirá un sistema que se está implementando en UHF.

1.1 SISTEMA DE TELECOMUNICACIONES

Los sistemas de telecomunicaciones en OPEC se enfocan hacia la transmisión de voz y datos de manera general.

Dentro de este esquema la Central telefónica y el sistema de comunicaciones vía satélite se constituyen como los sistemas principales a ser descritos. Además se podría incluir el sistema informático como un caso particular de los sistemas de telecomunicaciones, pero se ha preferido por motivos de enfoque y organización de este trabajo, el dedicar un acápite aparte para ello.

1.1.1 CENTRAL TELEFONICA

CENTRAL TELEFONICA DE QUITO

La central telefónica instalada en Quito es un sistema AD 3100 L de la ITT[1] . Es uno de los primeros sistemas que salió al mercado en el año de 1984. Es una central telefónica digital con conmutación temporal y control por programa almacenado. Presenta características muy limitadas principalmente en lo que a datos se refiere.

Las características generales de esta central son:

- Es completamente modular, permitiendo gran flexibilidad. Es digital de arquitectura de microprocesador distribuido.

- El sistema se conforma de tres módulos principales: fuente de poder, módulo de control y módulo de interfaces. Se utiliza una cinta multifilar para hacer las conexiones intermodulares.

- El tamaño mínimo del sistema es de 48 puertos, pudiendo ser expandido hasta 384 (8 módulos de 48 puertos cada uno).

- El módulo de control no requiere expansión ya que está diseñado para controlar los 384 puertos.

- El módulo de interfaces es de diseño universal permitiendo conectar a él líneas externas, líneas internas o de datos.

Este sistema está diseñado en base a un concepto de microprocesador, en un procesamiento jerarquizado de múltiples niveles. Un sistema de procesador central

[1] Ver glosario.

direcciona la operación de los procesadores de segundo y tercer nivel, que a su vez controlan una sección del "hardware". Para las comunicaciones internas entre los procesadores la arquitectura de bus es distribuida y modular.

El sistema utiliza "Pulse Code Modulation" (PCM) para transmisión interna en todos los módulos de interfaces. En cada módulo de interfaces existen dos etapas multiplexadas en el tiempo cuyo reloj maestro es de 1.544 MHz (2 x 24 canales = 48 canales).

La central telefónica es fácil de programar y de monitorear con un terminal conectado a un puerto.

El sistema permite tener múltiples servicios de voz, tales como: varias consolas de atención, espera de mensajes, conferencia, "sígame", parqueo de llamadas, numeración abreviada, entre muchas más.

En cuanto a los servicios de datos se limita sólo a transmisiones en modo asincrónico que sigan el estándar RS-232C y RS-422. Para este tipo de transmisiones puede prestar varios servicios como el tener un canal de voz asociado, establecimiento automático de la conexión, indicadores de estado de llamada, conexión de dos dispositivos de datos, enrutamiento y almacenamiento temporal de los recursos de datos, interfaz entre dispositivos seriales incompatibles, y otros más.

Sin embargo, actualmente no se utiliza la central para enviar datos y no se la tiene configurada con las tarjetas que se necesitarían para dichos propósitos.

CENTRAL TELEFONICA DEL ORIENTE

La central telefónica del Oriente es un sistema ALCATEL 100 modelo S2. Es una central telefónica digital (utiliza PCM) con conmutación temporal y control por programa almacenado.

Esta PBX permite la conexión de teléfonos análogos convencionales, estaciones multilíneas de dos pares (4 hilos) y transmisores digitales asincrónicos (ADT[1]).

Es de tipo modular. Se conforma de tarjetas insertadas en las ranuras de una tarjeta principal ("backplane")[2] .

Existen ranuras asignadas específicamente para la tarjeta CPU (Unidad Central de Proceso) y para una tarjeta de opción análoga[3] .

Existen ranuras para tarjetas de propósito general: para líneas troncales, extensiones, extensiones multilíneas (4 hilos), líneas de comunicación de datos, etc.

Los limites del sistema son:

- Máximo número de líneas troncales: 28
- Máximo número de extensiones: 120
- Máximo número de consolas de operadora: 2
- Máximo número de extensiones multilínea: 24

El modelo S2 posee:
- Una fuente de alimentación de 16 A (50V).
- Una tarjeta de control (CU, Control Unit).
- 10 ranuras para tarjetas de propósito general.
- Una ranura para una tarjeta análoga.
- 2 baterías de 24 voltios cada una.

---

[1] El terminal serial se conecta a través de su puerto RS-232 al ADT y éste a su vez a través de dos hilos telefónicos con la tarjeta para comunicación de datos.
[2] Esta tarjeta principal solamente interconecta las tarjetas.
[3] Se puede tener una tarjeta con opciones de música en espera, música de fondo, conferencia entre tres o más extensiones (o líneas troncales), etc.

La PBX está configurada con 8 líneas troncales y 64 extensiones, posee la opción de música en espera, el servicio de numeración abreviada, "sígame", entre otras.

1.1.2 SISTEMA DE COMUNICACION VIA SATELITE

El sistema de comunicaciones vía satélite de OPEC permite tener comunicación directa con Tulsa y con el Oriente.

El enlace con Tulsa se hace a través del satélite INTELSAT 307, encaminando la señal desde Quito a Detroit a una estación terrena de MCI[1]. Esta empresa se encarga de enrutar la señal de Detroit a Tulsa (figura 1.1).

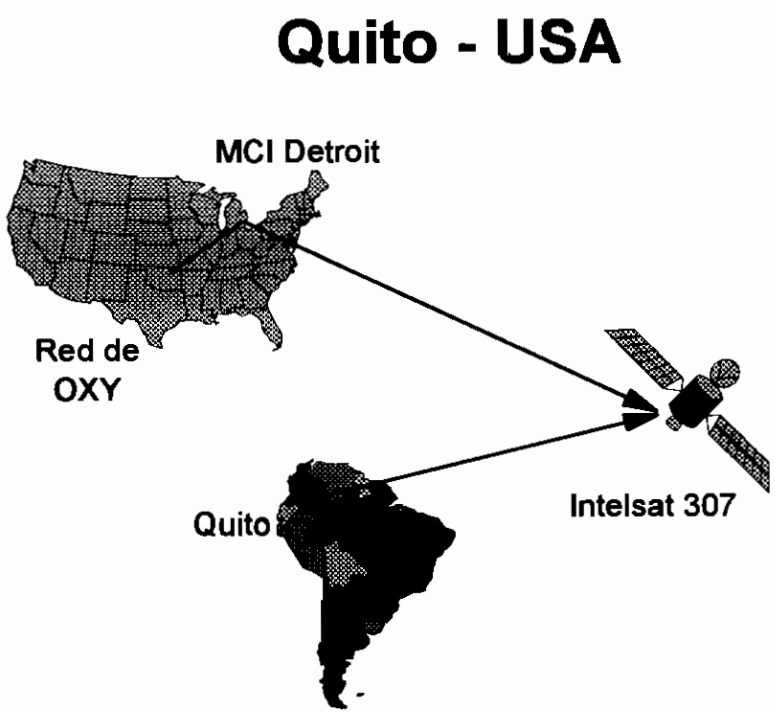


Figura 1.1. Enlace Quito-Tulsa

Con el Oriente el enlace se realiza directamente entre dos estaciones terrenas utilizando el INTELSAT 307. Este esquema se presenta en la figura 1.2.

[1] Compañia de telecomunicaciones que brinda servicios de telefonía y redes de datos en Estados Unidos de Norteamérica.

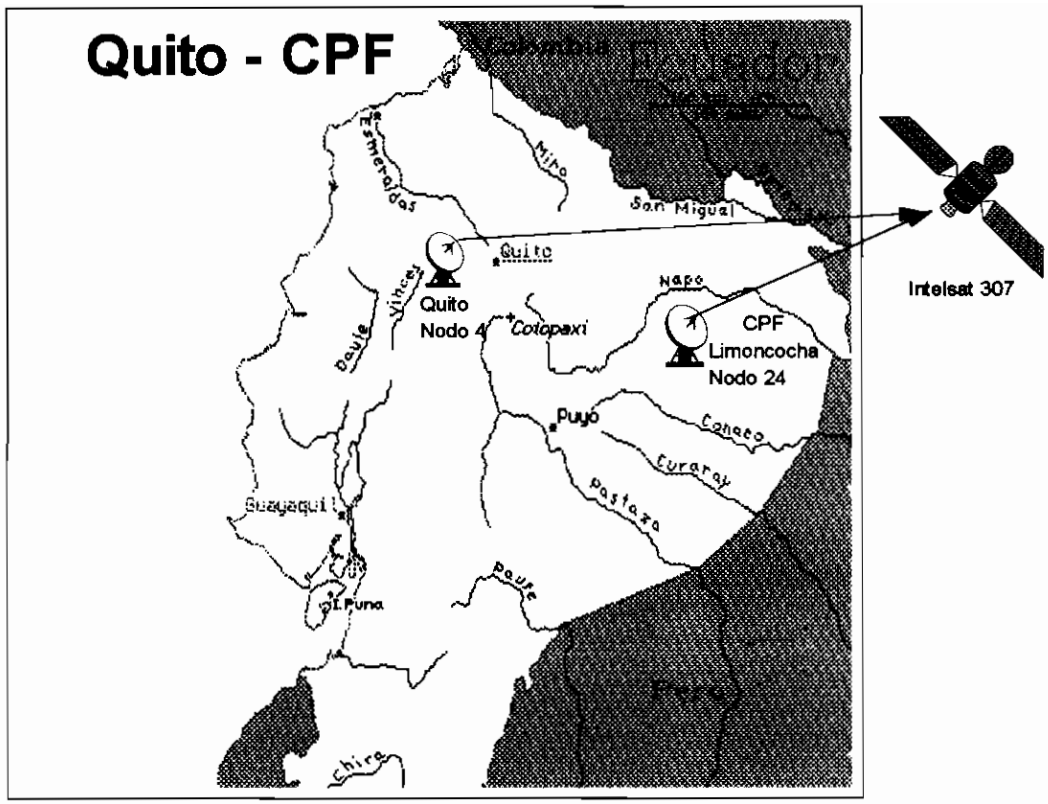


Figura 1.2. Enlace Quito-CPF.

Como se puede apreciar se tienen dos antenas instaladas, una en Quito y otra en el Oriente para enlazar Quito con Tulsa y Quito con el CPF[1] (Limoncocha) respectivamente.

Siendo SPACELINK la empresa ganadora de la licitación para instalar el sistema satelital, en el Anexo N.2 se presenta su propuesta. La importancia de este anexo radica en presentar un ejemplo real de una propuesta para una licitación internacional, la cual puede servir como material de consulta.

En la figura 1.3 se tiene un esquema de conexión desde el modem hasta la antena. La parte del multiplexaje (de los datos que recibe o envía el modem) se analizará más adelante.

[1] Central Production Facilities, Facilidades Centrales de Producción.

Sistema de Transmisión-Recepción

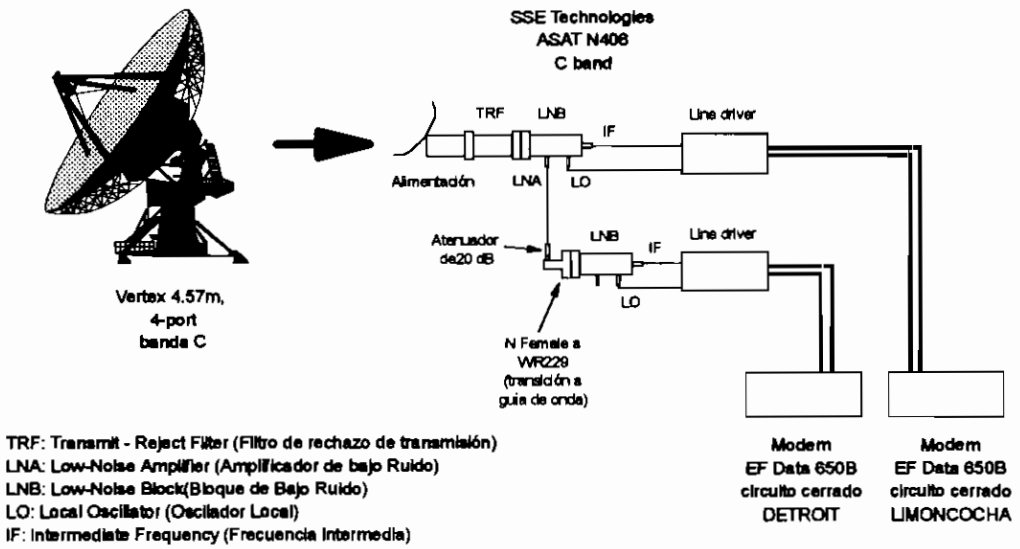


Figura 1.3. Sistema de transmisión/recepción.

Las antenas parabólicas instaladas tanto en Quito como en el Oriente, son marca VERTEX de 4.57 m. de diámetro, para transmisión en banda C (6 GHz). Estas antenas han pasado la aprobación de INTELSAT para la comunicación con sus satélites.

Junto a las antenas se tiene un amplificador de bajo ruido, el cual se conecta con cable coaxial a los equipos internos. Dicho amplificador de potencia que trabaja a la frecuencia de 6 GHz está instalado como equipo externo, y está conectado a la antena mediante una pequeña guía de onda.

El amplificador de potencia es un amplificador SSE 20W de estado sólido manejado por una última etapa de conversión a frecuencia de microondas para transmisión (Up-converter). Se tiene un oscilador local para dichos fines. Para recepción se tiene el conversor a frecuencias intermedias FI (Down-converter), el que se comunica con los equipos internos a través de cable coaxial. La FI está en el espectro de los 70 Mhz.

En el modem se utiliza un esquema QPSK[1] FEC[2] en conexión a la etapa de Radio-frecuencia (R). El modem tiene un interfaz con el multiplexor a un ritmo de 128 Kbps (pudiendo ser programados hasta un ritmo de 2048 Kbps). El equipo está diseñado para tener un BER[3] máximo de 10^{-7}, para asegurar una transmisión óptima punto a punto.

El multiplexaje y demultiplexaje de las señales que entran y salen del modem lo realiza un equipo marca TIMEPLEX. Este equipo realiza una multiplexación/demultiplexación en el tiempo y tiene un control por programa almacenado (Minilink/2+ para Quito y Microlink/2+ para el CPF).

El TIMEPLEX es un equipo modular que puede configurarse con las siguientes tarjetas:

- NCL (Network Control Logic) es la tarjeta principal de control y contiene el programa almacenado en memoria RAM.

- ILC (InterLink Control) es la tarjeta de Interfaz entre las tarjetas de voz y datos, es la que propiamente realiza el multiplexaje.

- EVM (Enhanced Voice Module) es la que realiza la digitalización de la voz, pudiendo manejar hasta cuatro canales de voz.

- QSC (Quad Synchronous) es la tarjeta de datos, la misma que puede soportar hasta cuatro canales de datos en modo serial asincrónico (RS-232).

Un dato interesante es que las tarjetas NCL poseen un puerto serial RS-232 que le permite al TIMEPLEX ser monitoreado desde cualquier sitio remoto y en caso de ser necesario alterar su programación.

---

[1] Quadrature Phase Shift Keying (Modulación de fase en cuadratura).
[2] Forward Error Correction (Corrección de error hacia adelante).
[3] Bit Error Rate (Tasa de Errores de Bits).

Una vez que se tiene una idea general acerca de los elementos, se puede entender la configuración del sistema.

Las figuras 1.4 y 1.5 muestran los equipos que constituyen la estación terrena en el CPF y Quito respectivamente. Se puede observar en dichas figuras el TIMEPLEX, el modem y el sistema de transmisión/recepción.

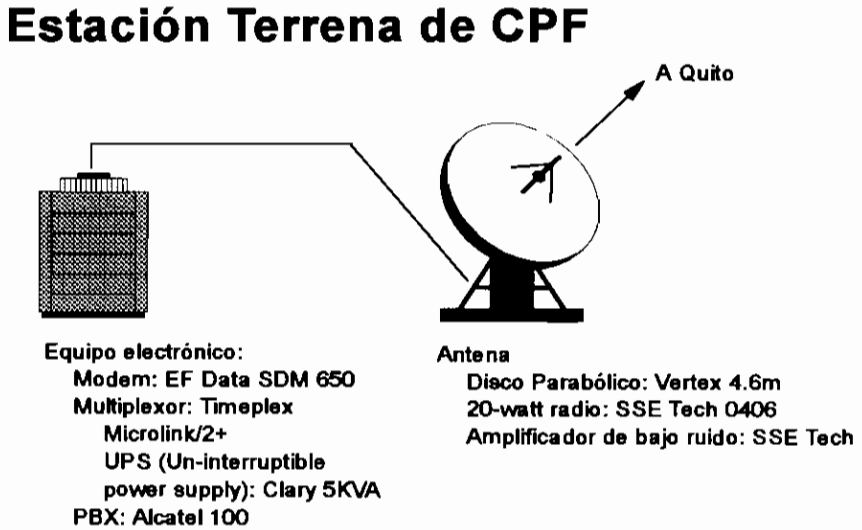


Figura 1.4. Componentes de la estación terrena del CPF.

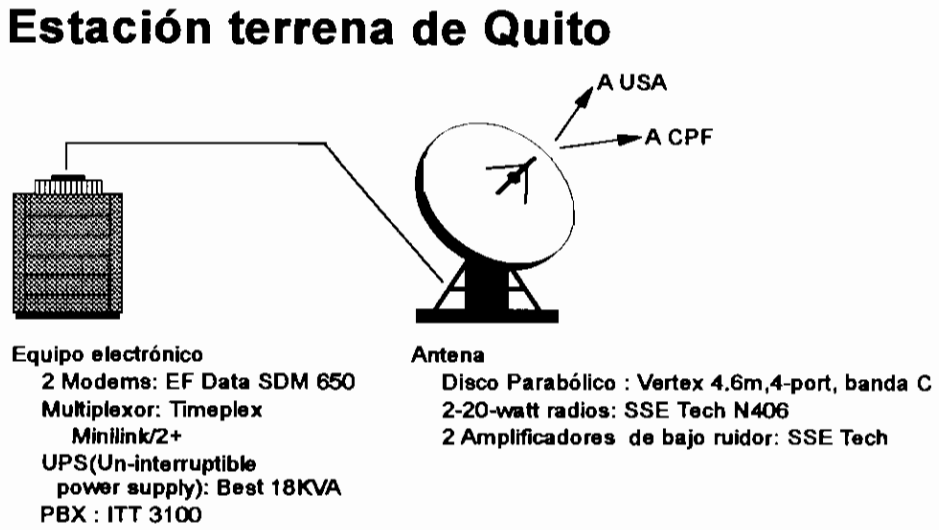


Figura 1.5. Componentes de la estación terrena de Quito.

En las figuras 1.6 y 1.7 se esquematizan las configuraciones de los multiplexores marca TIMEPLEX en el CPF (8 canales de voz y 4 de datos) y en Quito (16 canales de voz[1] y 4 de datos) respectivamente. En Quito se tiene una tarjeta de datos de repuesto, en caso que cualquiera de las tarjetas QSC falle.

Adicionalmente, dentro de cada módulo[2] debe estar activa sólo una tarjeta NCL, que es la que maneja la lógica central del TIMEPLEX, la segunda tarjeta NCL está como respaldo y entra en funcionamiento automáticamente en caso de falla de la primera. En la tarjeta NCL se encuentra el programa de control, y la definición (tipo y ubicación) de todas las tarjetas que conforman del módulo.

La tarjeta ICL es la de entrelazado, se encarga de entrelazar las señales provenientes de los canales de voz y datos, en una señal digital, de tal forma que ésta pasa a ser modulada a una frecuencia intermedia de 70 MHz, para luego ser transmitida sobre el enlace de microondas. En el TIMEPLEX de Quito existe una tarjeta ICL que se encarga de la información que viene y va a Tulsa, y otra para la información desde y hacia el CPF.

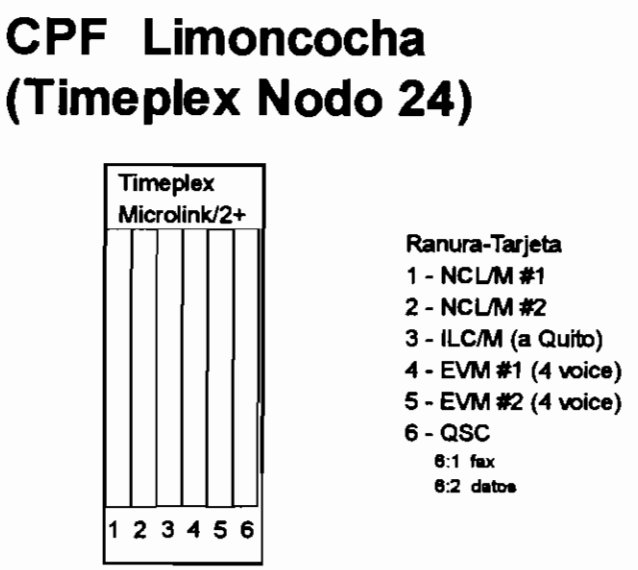


Figura 1.6. Configuración del multiplexor en el CPF.

[1] De los 16 canales de voz 14 están en servicio, 8 al CPF y 6 a Tulsa. Se tienen dos canales de voz de repuesto.
[2] Armario de conexión y conjunto de tarjetas que conforman el TIMEPLEX.

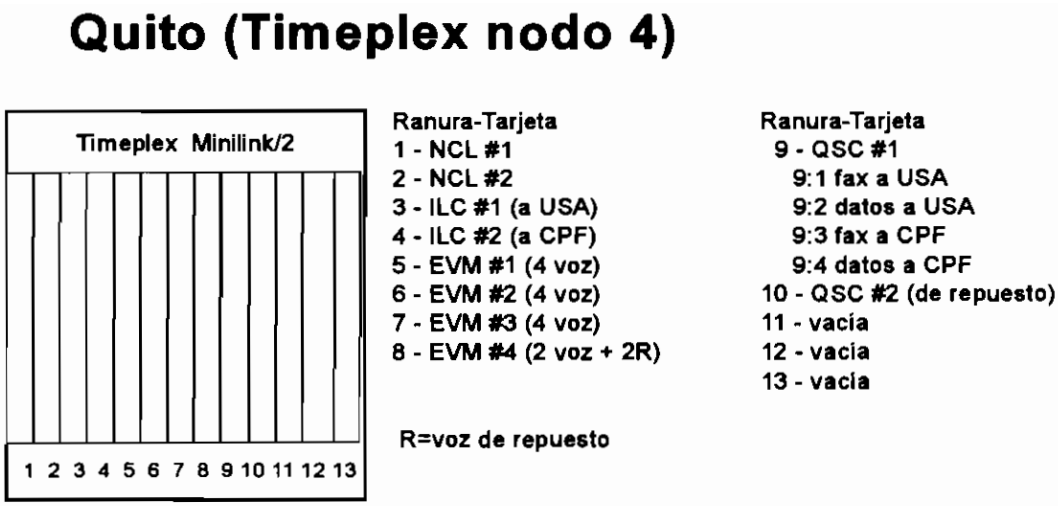


Figura 1.7. Configuración del multiplexor en Quito.

En el caso de las QSC, se tienen dos canales a Tulsa (uno de fax y el otro de datos) y otros dos al CPF, quedando una tarjeta (cuatro canales) de respaldo en caso de falla de la primera tarjeta.

En la figura 1.8 se puede apreciar la comunicación entre las tarjetas componentes de los multiplexores en Quito y el CPF (8 canales de voz y 2 de datos). Los restantes canales [8 de voz (2 de repuesto) y 2 de datos] son para las comunicaciones Quito-Tulsa.

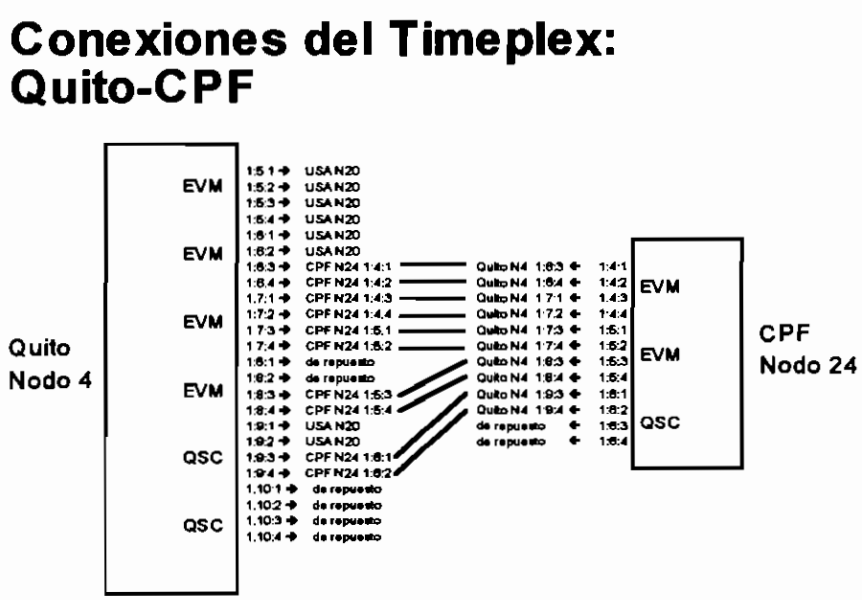


Figura 1.8. Conexiones de los multiplexores de Quito y CPF a través del enlace.

En la figura 1.9 se muestra como se realiza las comunicaciones de voz a través del enlace vía satélite.

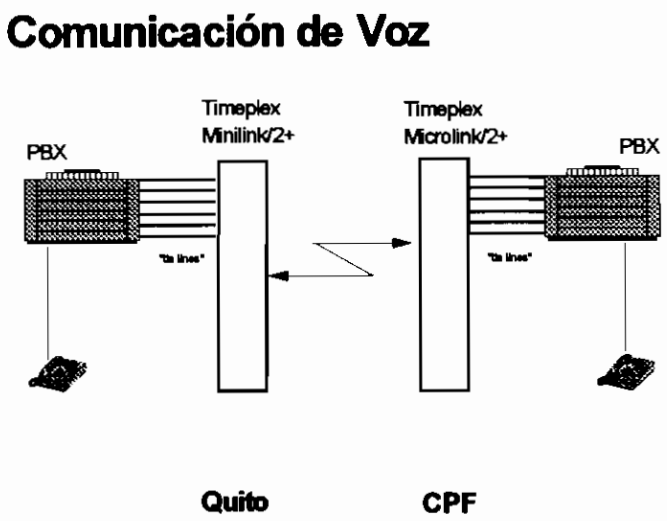


Figura 1.9. Comunicación de voz a través del enlace vía satélite.

Existen 8 "tie lines" (líneas dedicadas) conectadas permanentemente entre la PBX de Quito y la PBX del CPF a través del enlace. Para marcar un número de extensión de la central de CPF desde Quito, se debe marcar primero 85 y luego el número de extensión. El otro caso sería marcar un número de una extensión de Quito desde el CPF, esto se consigue marcando 88 y luego el número de extensión de Quito.

Los únicos elementos que faltarían por analizarse y que se sirven del enlace vía satélite son el "servidor de fax" y "el correo electrónico". Estos subsistemas se revisarán más adelante.

Una vez estudiadas las partes que conforman el sistema de comunicaciones vía satélite se puede realizar un diagrama general que integre dichos componentes (ver figura 1.10).

En Quito se tiene el sistema vía satélite que contempla 8 canales de voz al CPF y 6 canales de voz a Tulsa, 1 canal de datos al CPF y otro a Tulsa, un canal para fax al

CPF y otro para Tulsa. Se tiene la PBX conectada a este sistema para permitir desde cualquier extensión la utilización de los canales por el satélite, e inclusive se podría usar una línea externa para accesar a los canales del satélite.

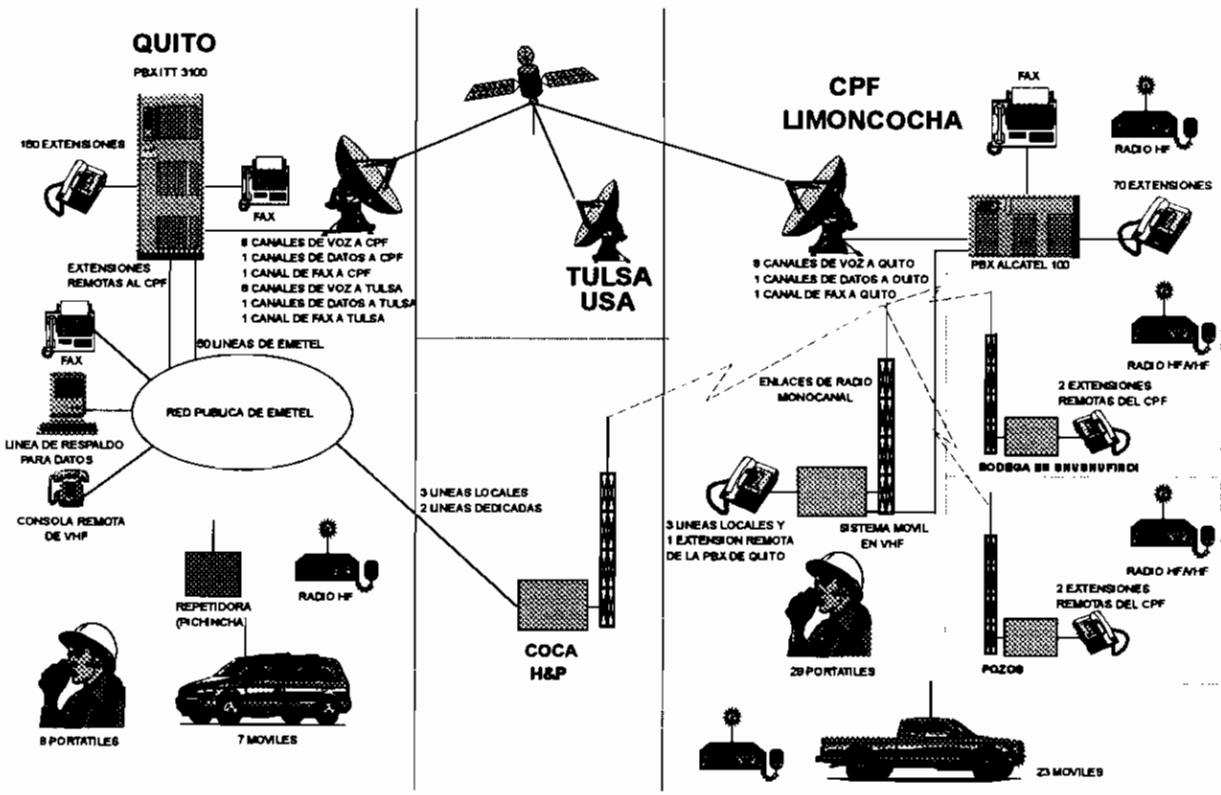


Figura 1.10 Red de telecomunicaciones de OPEC.

Adicionalmente, se tiene un servidor de fax[1] conectado al sistema de comunicaciones vía satélite.

En Quito se dispone de un sistema de radio UHF, que tiene una estación base, 7 radios móviles y 8 portátiles.

A manera de respaldo se utiliza la red de EMETEL, para voz y datos. Además, se tienen 3 líneas telefónicas normales y 2 líneas dedicadas a Coca, donde se encuentran

[1] Mayor información en el acápite 1.2.6.

las bodegas de H&P[1], y desde Coca se tienen los enlaces de radio monocanal hacia el CPF (mayor detalle encontrará en el Anexo 3).

El segundo centro de importancia es el CPF, donde se concentra la operación de OPEC. El sistema de comunicaciones vía satélite tiene 8 canales de voz, 1 canal de datos y un canal para fax con Quito, está conectado a una central telefónica ALCATEL 100 que enruta las extensiones y el fax ya sea a través del satélite o a través de los radioenlaces monocanal.

En el CPF se tienen 3 líneas normales (de abonado) y una extensión remota de la PBX de Quito.

Se tienen 2 extensiones remotas de la PBX del CPF en SHUSHUFINDI (Bodega) y en cada uno de los sitios de perforación.

Para comunicarse en el Oriente se utiliza un sistema de radio HF/VHF. Existen 29 radios portátiles y 23 móviles.

1.2 SISTEMAS INFORMATICOS

Luego de haber hecho una reseña general de los sistemas de comunicación de voz y datos, se verá el enfoque real de esta tesis, es decir el sistema informático de la red de datos de OPEC.

Para los fines operativos de la compañía, los datos deben fluir entre el CPF (ubicada en el Oriente cerca de Limoncocha) y Quito; y entre Quito y Tulsa, aunque por cambios administrativos dentro de la compañía en EEUU, la transmisión continúa de Tulsa (Oklahoma) a Bakersfield (California).

---

[1] Helmerich & Paine. Compañía contratista de trabajos de perforación.

De manera general el sistema informático está compuesto por una red de computadores en topología "Token-Ring", un minicomputador AS/400, un gateway de comunicaciones (correo electrónico[1]). Los sistemas de comunicación utilizados son: las centrales telefónicas privadas (PBX) descritas en el acápite anterior, las redes telefónicas públicas internacionales de EMETEL y de EEUU, y el sistema de comunicaciones de voz y datos utilizando enlace vía satélite.

Para una mejor comprensión se elabora un diagrama sencillo (Figura 1.11), que sin entrar en detalle globaliza la estructura de la red de datos de OPEC.

Este diagrama muestra las interconexiones de los equipos de procesamiento de datos, utilizando la red telefónica pública o el sistema de enlace vía satélite, entre Quito-CPF y entre Quito-Tulsa-Bakersfield.

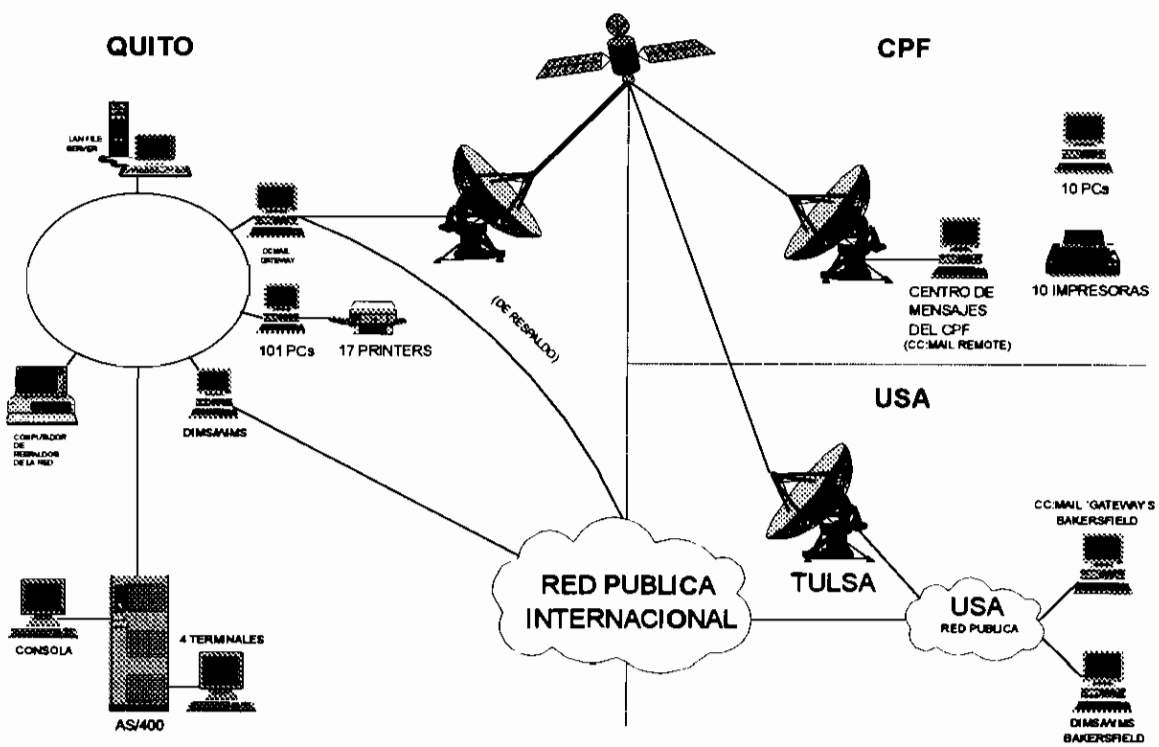


Figura 1.11. Red de datos de OPEC.

[1] El "software" utilizado es cc:Mail de Lotus.

Esta figura está dividida por localidades físicas, así en Quito, se tiene la red "Token-Ring" y el AS/400 conectado a ella, de manera que cualquier computador pueda accesar a los datos del AS/400. Además el AS/400 tiene sus terminales independientes para que en caso de problemas con la red, ellos pueden tener el acceso correspondiente a los datos almacenados en él.

Dentro de la red "Token-Ring" se tienen el servidor de la red, el computador que hace los respaldos de toda la información de la red, la pasarela de correo electrónico (cc:Mail gateway) y el computador que maneja la base de datos de perforación y producción de los pozos. A futuro se piensa implementar un RS/6000[1] y un servidor de base de datos para las aplicaciones de ingeniería. Luego, se tienen 101 computadores de usuarios, con 17 impresoras conectadas a 17 de los computadores de usuarios y distribuidas a través de todo el edificio.

El correo electrónico se realiza a través de la pasarela (cc:Mail gateway), utilizando un canal de datos del enlace vía satélite (Figura 1.12). Actualmente se utiliza un horario de transmisión que determina la comunicación con Tulsa-Bakersfield o con el CPF; en un futuro cercano se piensa implementar una segunda pasarela para que cubran ambas comunicaciones durante las 24 horas del día sin necesidad de estar conmutando. En caso de falla del enlace se tiene la ruta alternativa usando las redes telefónicas públicas. En el CPF se tiene un computador dedicado a las comunicaciones, dicho computador hace las veces de terminal remoto de la red que existe en Quito, de tal forma que puede accesar al correo electrónico, haciendo las veces de un centro de mensajes.

Finalmente, en la red en Quito se tiene un computador dedicado a mantener la base de datos de perforación y producción de los pozos, así como también para enviar reportes de dicha base de datos a las oficinas centrales en EEUU.

[1] Ver glosario.

Los computadores e impresoras que se encuentran en el Oriente están trabajando de forma independiente, no están conectadas en red, a futuro existe el proyecto de instalar una red de área local para integrar todo el CPF al sistema.

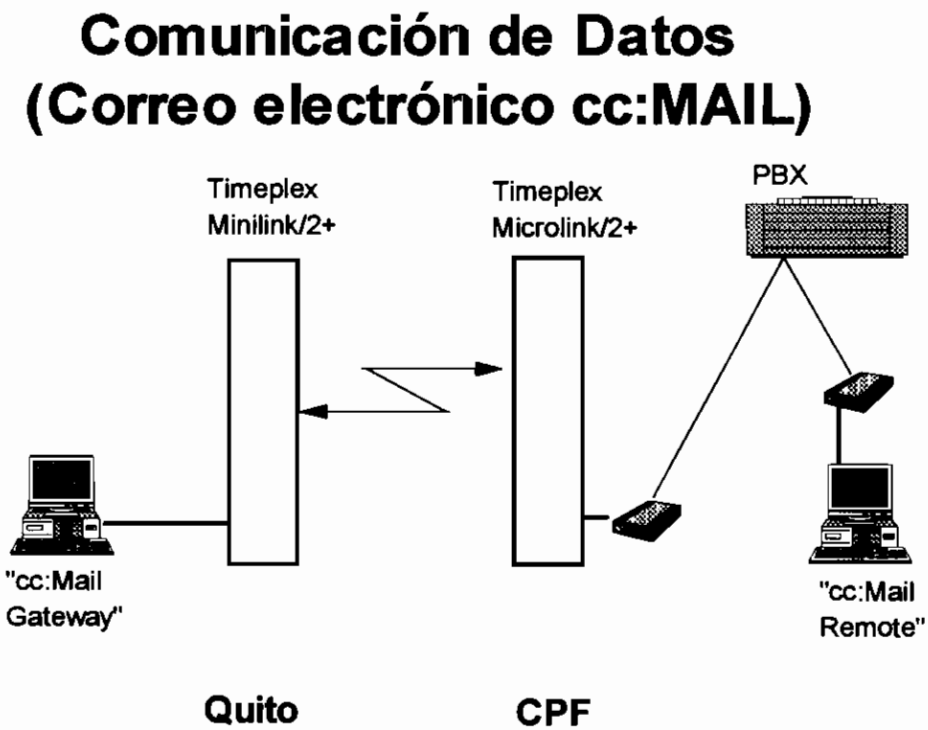


Figura 1.12. Conexión de correo electrónico remoto.

1.2.1 NECESIDADES DE PROCESAMIENTO DE DATOS DE OPEC

Se pueden visualizar estas necesidades mediante un pequeño análisis a nivel departamental. Como se mencionó en la introducción, se tienen 9 áreas de trabajo bien definidas que son: Presidencia y Gerencia General, Gobierno y Control Ambiental, Legal, Finanzas, Operaciones, Exploración, Materiales, Sistemas y Recursos Humanos.

Los departamentos que demandan los mayores recursos a nivel de usuarios de la red son el de Finanzas, Operaciones, Exploración, Materiales, Recursos Humanos y Legal. Los otros departamentos tienen menor incidencia en la demanda de la red.

Existe una aplicación en red tanto para el departamento financiero, que cubre las áreas de cuentas por pagar y contabilidad, así como para el departamento de materiales, en donde se procesan las órdenes de compra.

Por otro lado el departamento de exploración y perforación tiene un sistema de adquisición de datos y procesamiento en el área de ingeniería. Además, el procesamiento digital de señales y el procesamiento de gráficos son unas de las mayores demandas de esta sección de OPEC.

En Recursos Humanos y en el departamento legal tiene gran importancia el manejo de documentos.

Por lo demás, las necesidades básicas de los usuarios son el procesador de palabras, la hoja de cálculo electrónica, el correo electrónico y las opciones de impresión. En particular, cada departamento dispone de los programas de aplicación de su interés.

Adicionalmente, se deben receptar datos de producción y costos desde el CPF, y se deben generar reportes de los diferentes departamentos para enviar a las oficinas centrales en EEUU.

1.2.2 TOPOLOGIA DE LA RED

Antes de estudiar la topología de la red de OPEC se describirá el proceso de instalación de una red "Token-Ring" y las especificaciones de cables para redes IBM, conceptos que serán de mucha importancia para entender el funcionamiento de la red de OPEC.

1.2.2.1 Instalación de una red Token-Ring

Se enumera los dispositivos de "hardware" y "software" para instalar la red:

- Tarjeta adaptadora de red.
- Concentrador de cableado.
- Cables y conectores.
- Programas de manipulación de la tarjeta adaptadora ("drivers").

Los computadores tiene que cumplir ciertos requisitos básicos para formar parte de la red, como por ejemplo tener por lo menos 128 KB de memoria. Puede ser desde un PC, hasta cualquiera de los computadores modernos (AT, 386, 486, PENTIUM), y debe tener como mínimo una unidad de disco flexible de 360 KB. Actualmente, estos requisitos son cumplidos hasta por la computadora más modesta.

- Tarjeta adaptadora

Cada computador en la red debe tener instalada una tarjeta adaptadora de "Token-Ring Network" para poder comunicarse con la red. Esta tarjeta se debe instalar en uno de los "Slots" de expansión del computador y debe estar conectada por cable al concentrador de cableado.

- Concentrador de cableado

Más conocido como MAU (Multistation Access Unit). Este dispositivo (figura 1.13) interconecta las tarjetas adaptadoras y sirve como concentrador del cableado para ocho (8) computadores como máximo. Si se requiere conectar (cablear) más computadores se pueden conectar en cascada dichos MAUs (Daisy Chain).

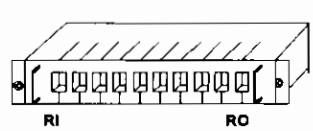


Figura 1.13. Concentrador de cableado (MAU).

El MAU lo que hace es interconectar internamente los computadores en un anillo. Existe un mecanismo dentro del MAU que obvia las entradas en las que no están conectados los computadores. Es decir si de las 8 entradas que tiene el MAU, sólo 3 de ellas están siendo utilizadas y las 5 restantes son de computadores que están fuera de la red o no existen computadores conectados, dicho mecanismo cerrará las 5 entradas que no están en red para permitir el flujo de información dentro del anillo. Esto se muestra en la figura 1.14.

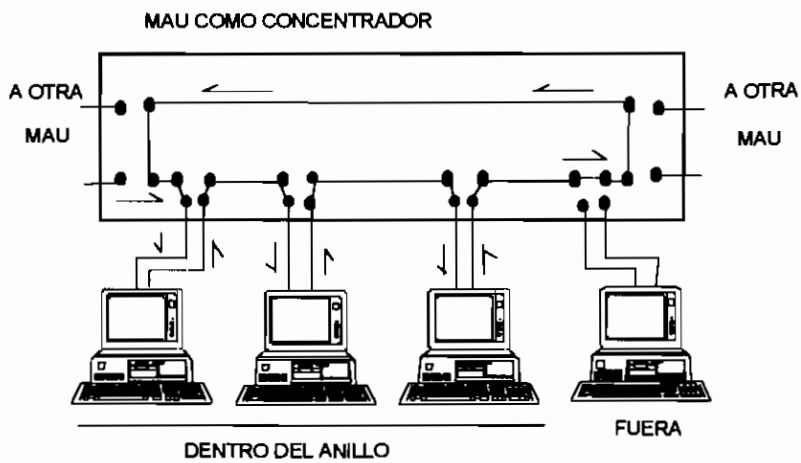


Figura 1.14. Conexión de los computadores al MAU.

"Se puede instalar la MAU en un "rack" estándar de 19 pulgadas o dentro de una caja especial que suministra IBM denominada "Component Housing"(algo así como kit de montaje). Al igual que la mayoría de equipos electrónicos (centrales telefónicas o cajas de conexión), las MAUs están diseñadas para instalarse en armarios especiales ("racks") de 19 pulgadas de ancho. La MAU se puede instalar en un "rack" que contenga otros aparatos y cableados. Las 19 pulgadas de ancho de los "racks" es otro estándar"[1] .

La interconexión de MAUs se conoce como racimo o CLUSTER. Las MAU de un racimo pueden estar en un mismo "rack" o en cualquier sitio donde estén juntas. La conexión de 2 MAU en un mismo racimo se consigue tendiendo un cable especial de IBM entre

[1] REDES LOCALES. Teoría y Práctica. Grupo WAITE.

el conector de salida de una MAU (RO, Ring Out) y el conector de entrada de la otra MAU (RI, Ring In) como se puede apreciar en la figura 1.15.

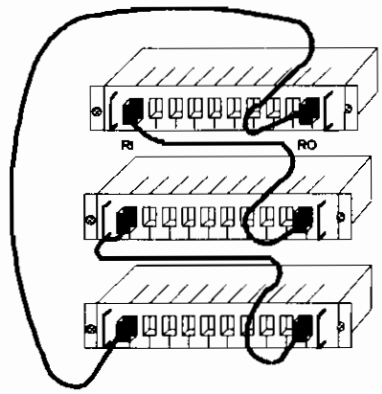


Figura 1.15. Conexión redundante entre MAU.

Para evitar que un computador dañado dentro de una red impida el paso del testigo es conveniente tener una ruta redundante, esto se logra conectando el RO del último MAU con el RI del primer MAU. De esta manera se establece un camino alternativo tal como se lo puede apreciar en las figura 1.15 y en la figura 1.16.

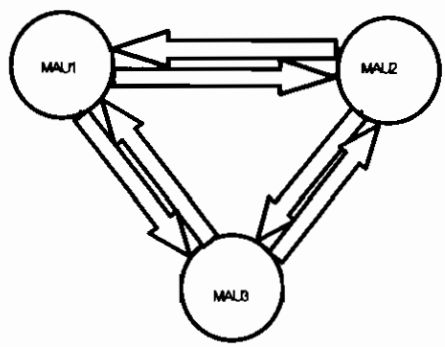


Figura 1.16. Rutas redundantes de la conexión de MAU de la figura 1.15.

Para unir los ordenadores a los MAU, se podría emplear cable de pares trenzado (telefónico) o cables con calidad para datos. La recomendación en general es usar un solo tipo de cables y conectores; los cables de datos están diseñados para soportar mayores distancias que los pares trenzados, por lo tanto, en una organización cuya red

está en continuo crecimiento debería utilizarse cables de datos. La experiencia demuestra que cuantos más adaptadores diferentes de cables y enchufes haya entre el computador personal y el MAU, mayor será la posibilidad de falla de comunicaciones debido a cables y conectores.

Los cables telefónicos están sujetos a interferencias de diverso tipo tales como motores eléctricos (aspiradoras, sacapuntas eléctricos, etc.), tubos fluorescentes, interferencias de radio, etc. Existe una guía editada por IBM para la instalación de cables trenzados que se llama "Token-Ring Network Telephone Twisted-Pair Media Guide, GA27-3714). En general la distancia máxima en una red con cable telefónico, entre un computador y el MAU, es de 110 m, se recomienda 50 m.

Los cables con calidad para datos (por ejemplo el tipo 1[1]), permiten que el tendido llegue a mucha más distancia que el cable telefónico, pudiéndose llegar hasta 350 m, aunque para este tipo de cable se recomienda 110 m.

Las especificaciones de los cables con calidad de datos se las puede encontrar en la "Guía de la Instalación de la Token-Ring Network" de IBM (GA27- 3678). Una comparación entre el cableado con cable trenzado y cable de datos tipo 1 se muestra a continuación en la tabla 1.1.

Descripción	Calidad telefónica (Tipo 3)	Calidad para datos (Tipo 1)
PC a MAU:		
Recomendado	50 m	110 m
Máximo	110 m	350 m
Grupos de MAU	2 "clusters"	12 "clusters"
"Cluster "a "Cluster"	135 m	215 m

Tabla 1.1. Comparación de cableado entre cable telefónico y cable con calidad de datos.

[1] Los tipos de cables se explicarán más adelante.

1.2.2.2 Especificaciones de cables para redes IBM

IBM define algunos tipos de cables en sus especificaciones para sus redes.

Tipo 1. Es un cable blindado de dos pares trenzados AWG #22. Se lo conoce como cable con calidad para datos (Data Grade). Sus hilos son rígidos y están blindados para evitar interferencias de ruidos externos.

Tipo 2. Igual que el anterior, pero lleva además 4 pares de hilos telefónicos (seis pares en total). Es ideal para instalar dentro de las paredes y combinar los datos y el teléfono en un solo cable.

Tipo 3. Es un cable de pares trenzados telefónico, sin blindaje. Es el que se emplea en el tendido telefónico normal.

Tipo 5. Es un cable de fibra óptica. que puede ser monomodo (se propaga un solo rayo de luz) ó multimodo (se propagan múltiples rayos de luz). Por costos se utiliza la fibra multimodo, aunque técnicamente la monomodo es la que permite alcanzar mejores rendimientos (mayores velocidades y distancias).

Tipo 6. Al igual que el tipo 1, está blindado pero lleva un cable de menor calibre AWG # 26. Se emplea para distancias cortas.

Tipo 8. Similar al tipo 1, pero es más plano. Ideal para instalar bajo alfombras, sobre el suelo y bajo las mamparas de separación entre distintos despachos.

Este estudio se centrará en el cableado usando el tipo 1. El cable para conectar un ordenador al MAU tiene un conector DB9[1] en un extremo y un conector de datos en el

[1] Es un conector que tiene 9 pines 5 en la primera fila y 4 en la segunda fila, tiene forma de "D", es muy utilizado en los puertos seriales de los PC.

otro. La conexión del cable tipo 1, cuyos hilos están codificados con cuatro colores que son: rojo, negro, verde y naranja; se realiza en el conector de datos, mientras en el DB-9, el pin 1 corresponde al rojo, el pin 5 al negro, el pin 6 al verde y el pin 9 al naranja.

Para interconectar los MAU se utilizan conectores para datos en ambos extremos del cable.

1.2.2.3 Topología de la red de OPEC

La topología de la red es en anillo, siguiendo el estándar IEEE 802.5, cuyas características generales son:

- Gestión de control: Paso de testigo con transmisión en banda base.
- Soporta al NETBIOS (Network Basic Input Output System) de IBM.
- Trabaja en base a un sistema operativo DOS 3.1 o mayor.
- Velocidad de transmisión de 4 Mbits/s. Pero podría ir hasta 100 Mbits/s utilizando fibra óptica.
- Medio de transmisión: Coaxial, cables trenzados, fibra óptica. En OPEC se utiliza el cable de calidad para datos Tipo 1.
- Máximo número de dispositivos: 72 con pares trenzados, 260 con cable coaxial, o ilimitado (90000) con anillos múltiples interconectados.
- Distancia máxima: virtualmente ilimitada.

Una de las principales características de este tipo de red es que se puede interconectar una gran variedad de productos IBM o compatibles: computadores personales, minicomputadores y "mainframes", así como controladores terminales de éstos.

La red "Token-Ring" está pensada para grandes compañías con más de 60 usuarios, pudiendo interconectar computadores alejados más de 350 m. Permite conectar con la misma red, computadores personales y terminales de grandes ordenadores, aceptando emular dichos terminales. Por su modularidad puede preveer un crecimiento de la red.

Actualmente a la red de OPEC se encuentran conectadas 101 computadoras (estaciones de trabajo). Adicionalmente se encuentra el servidor de archivos, que es un computador 486 de 50 Mhz de marca AST modelo Premium SE 486/50, 24 MB en memoria RAM, 4 GB en disco duro y una unidad de disco flexible de alta densidad de 3 1/2". Este es un servidor dedicado, posee 4 discos duros SCSI de 1 GB cada uno, utilizando la técnica de discos espejados (mirroring[1]), la capacidad es sólo de 2 GB y no de 4 GB.

Luego se tiene una pasarela ("gateway") de comunicaciones, que es un computador dedicado al correo electrónico, y otro computador que realiza automáticamente los respaldos ("backups") de toda la información de la red todas las noches. Los restantes computadores (101) en conjunto con el de la base de datos de perforación y producción de los pozos son estaciones de trabajo, en su mayoría computadores 486 de 33 MHz.

A 17 de los computadores de usuarios se encuentran conectadas 17 impresoras láser, configuradas como impresoras remotas para dar servicio a distintas áreas. Uno de los proyectos futuros es el de independizar las impresoras y conectarlas directamente al anillo sin necesidad de utilizar un computador para cada una de ellas.

[1] Esta técnica será explicada en el capítulo 2, acápite 2.5.2.

Los concentradores de cableado (MAU, Multiple Access Unit) son marca Star-Tek, tienen un puerto de supervisión que permite una conexión en cascada hasta un número de 32 MAUs, y mediante un programa que vende la misma empresa fabricante de este equipo, se pueden monitorear y determinar fallas en el cableado; en el futuro se implementará este sistema especialmente si se instala la red en el Oriente para poder hacer un monitoreo remoto. Este tipo de concentrador es activo (110V), posee diodos indicadores de las estaciones conectadas, facilitando de esta manera el localizar una falla de conexión entre el PC y el MAU visualmente. Además posee una característica importante, ésta es que en caso de falla de algún cable, permite aislarlo automáticamente hasta que se restablezca la comunicación a través de dicho cable.

Las tarjetas de red que se está utilizando es la "Token-Ring" de IBM de 8 bits (bus de datos), conmutable a 4 y a 16 Mbit/s. Cuando se "setea" las tarjetas través de los "dip switches" que hay en ellas, es necesario que se tome en cuenta la dirección de memoria que van a ocupar, porque en caso contrario cuando se utiliza los "drivers" manejadores de memoria expandida tales como el EMM386.EXE, puede producirse un conflicto de memoria con los programas de aplicación, especialmente con "LOTUS 123".

La Figura 1.17 es un esquema del cableado del anillo principal.

Existen dos cables de 12 m (A,C) entre Mezzanine y tercer piso y entre sexto piso y noveno; y los otros dos cables son de 18 m (B,D) que están entre el Mezzanine y el sexto piso, y entre el tercero y noveno piso.

Cabe mencionar que el ducto por donde se ha cableado el anillo principal (entre MAUs), es central, y la máxima distancia del ducto a un computador es de 60 m (incluyendo subidas y bajadas por el cielo falso). Por tanto no se tienen problemas debido a distancias muy grandes.

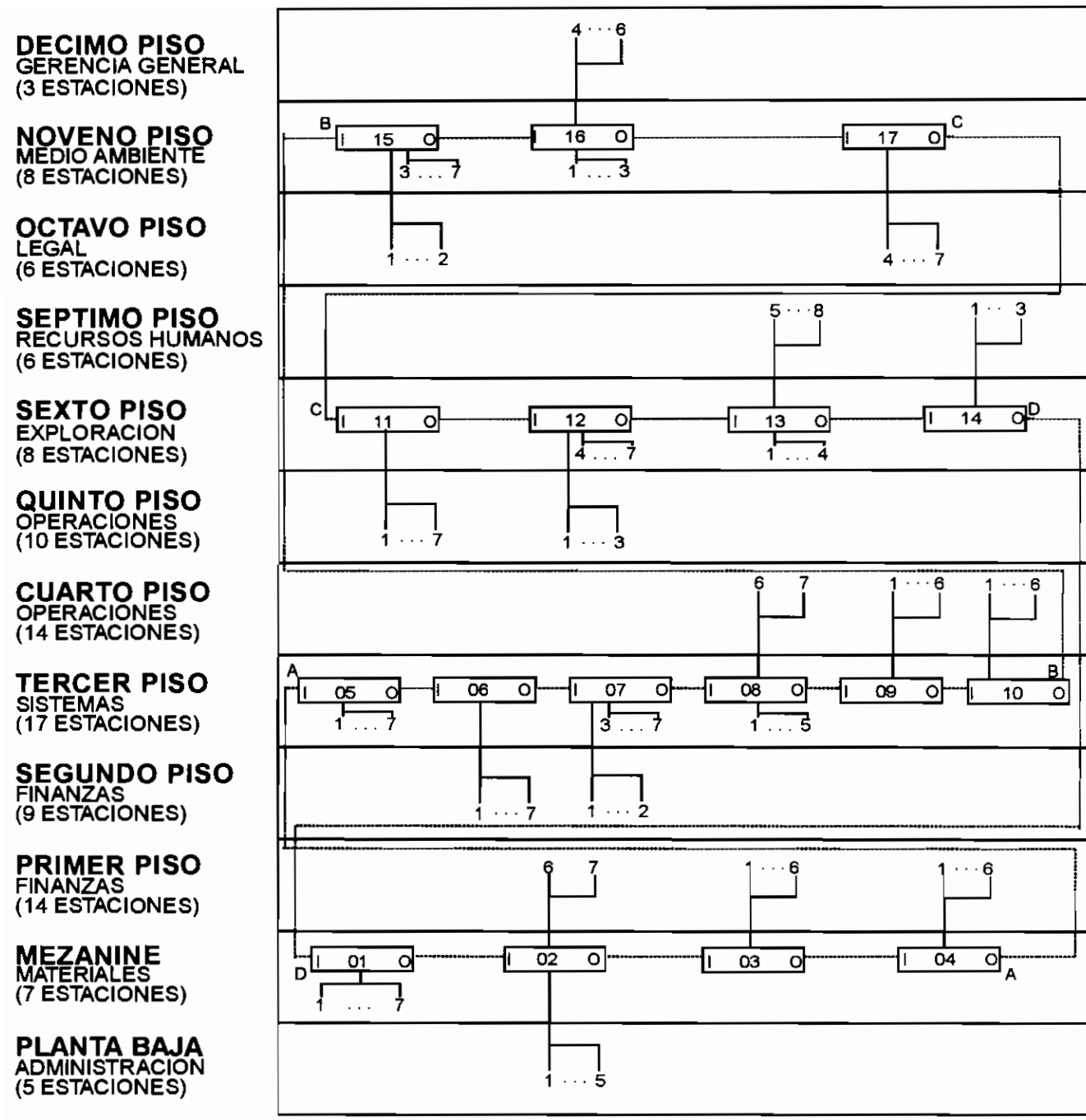


Figura 1.17. Distribuciòn y cableado de los MAUs.

Está diseñado para optimizar las distancias de los cables que interconectan los MAUs, así como las distancias desde el grupo de MAUs a los computadores conectados a él. El cable utilizado es el tipo 1; este cable puede llegar a cubrir una distancia de 350 m. entre el MAU y el computador (soportando un ritmo de transmisión de 4 Mbps).

Se tienen 4 grupos de concentradores de cableado, el primero en el Mezzanine con 4 MAUs, el segundo en el tercer piso con 6 MAUs, el tercero en el sexto piso con 4 MAUs, y el cuarto en el noveno piso con 3 MAUs.

1.2.3 SISTEMA OPERATIVO

Una vez configurada la red (en este caso particular en anillo), se tienen varias opciones para el sistema o entorno operativo. Existe mucha información de cada casa productora de sistemas operativos para red, pero no siendo este el objetivo de estudio, se dará una visión generalizada de lo que existe en el mercado. Cabe resaltar que, tanto la estructura como la instalación y uso son similares en todos ellos.

El siguiente análisis a realizarse se basa en un artículo de la revista Binary[1] .

Los sistemas operativos a analizarse son el Netware de Novell; 3+Open Lan Manager y 3+Share de 3 COM; PC Lan y OS/2 Lan Server de IBM.

PC Lan y 3+Share representan al entorno basado en MS-NET, Netware tiene su sistema operativo multitarea particular y 3+Open con OS/2 Lan Server son sistemas operativos basados en OS/2. Las versiones aquí revisadas no son las últimas existentes, pero si reflejan una tendencia en lo que a sistemas operativos de red se refieren, las actuales tienen algunas mejoras en sus prestaciones.

1.- PC LAN 1.3 de IBM

Sólo funciona con "hardware" PC Network o "Token-Ring" IBM, no soporta Ethernet. Una característica especial de este sistema es que permite compartir recursos entre estaciones iguales; cualquier estación en la red puede actuar como servidor, de modo que sus unidades de disco y demás recursos locales son accesibles desde todos los

[1] "Redes Locales: Batalla entre estrellas",Steve Apiki, Standford Diehl y Rick Greham.

nodos de la red. Netware, con su red basada en servidor sólo permite compartir recursos de un servidor central de archivos.

Las estaciones de trabajo de PC LAN trabajan bajo PC-DOS 3.3 o superiores. Cada una de ellas posee un subdirectorio especial, controladores para la tarjeta adaptadora "Token-Ring" y algunas líneas adicionales en el AUTOEXEC.BAT.

Todas las estaciones de trabajo utilizan un programa residente de 46 KBytes para redireccionar, ligado a la interrupción 21H. El redirector analiza las peticiones del sistema realizadas por los programas de aplicación y determina si las envía a la red o las maneja a nivel local.

Existen dos alternativas para manejar los comandos de PC LAN. La primera son los "Base Services", en donde se debe introducir los comandos desde el "prompt" del DOS. La segunda, son los "Extended Services", que utilizan un sistema de menúes para introducir los comandos. Los "Base Services" dejan la mayor parte del trabajo administrativo en manos de los usuarios, mientras que los "Extended Services" permiten que un administrador de la red asuma el control exclusivo de los recursos disponibles, además de proporcionar un mayor nivel de seguridad (el administrador puede asignar contraseñas a los discos, directorios e impresoras existentes en la red).

Los subdirectorios y archivos compartidos reciben el nombre de "fileset", y bajo los "Extended Services" el sistema les asigna automáticamente un nombre y una contraseña.

La experiencia indica que eliminar un usuario es más difícil que añadirlo, debido a que no sólo es necesario localizar todos los "filesets" a los que tiene acceso, sino que se debe localizar a los demás usuarios con acceso al directorio particular del primero y eliminar dichos enlaces.

Es fácil mediante el sistema de menúes de los "Extended Services" asignar los "filesets" a unidades lógicas, invocándolos en el momento de arranque.

El administrador del sistema restringe el acceso a los archivos usuario por usuario. Esto es adecuado para instalaciones reducidas, pero es problemático cuando se tiene un sistema multidepartamental, en el que grupos distintos de usuarios necesitan acceso a las diferentes bases de datos.

El PC LAN incluye un programa de correo electrónico bien rudimentario. Con los "Base Services", los mensajes pueden tener una longitud máxima de 100 caracteres, sin posibilidad de editarlos. Los "Extended Services" incorporan una pantalla de edición.

Con los "Extended Services" siempre se dispone de la tecla de ayuda F1.

2.- OS/2 LAN SERVER 1.00 de IBM

Es un sistema operativo compatible con PC LAN que disfruta de las ventajas de trabajar con OS/2. La compatibilidad es tal que el "software" de servidor en una red PC LAN puede ser sustituido por LAN SERVER sin tener que reinstalar ningún tipo de "software" de estación de trabajo; sólo se necesita informar al LAN SERVER que se tienen estaciones PC LAN basadas en DOS. Evidentemente, los servicios ofrecidos por LAN SERVER a estaciones basadas en DOS son limitadas y no aprovechan el potencial del OS/2. Ninguna estación de trabajo basada en DOS puede actuar como administrador.

Una opción interesante de LAN SERVER es el NETRUN, éste permite ejecutar programas desde localizaciones remotas; dichos programas así activados operan en la memoria del equipo servidor pudiendo ser redireccionada su salida hacia un archivo.
Este sistema operativo mantiene un registro de utilización, de tal forma que el administrador de la red puede visualizar de manera detallada los registros de error; además el sistema elabora estadísticas ininterrumpidas sobre las actividades del

servidor. Por último, el administrador puede realizar una auditoría, seleccionando los recursos para ver su utilización, guardando esta información en un archivo de auditoría.

Una de las deficiencias del LAN SERVER es que durante la creación de las configuraciones de usuario y de los "filesets", los menúes que ha de atravesar el administrador para definir los recursos compartidos y de usuario constituyen un laberinto, y sin un ratón ("mouse")el proceso resulta tedioso.

Una de las ventajas de LAN SERVER sobre PC LAN es que en el caso de PC LAN se permite modelar el perfil de un usuario a partir de otro ya creado; así cuando se incorpora un usuario puede conferírsele todos los privilegios de acceso de la base ya instalada, pero corresponde al administrador recordar a que grupo pertenece. LAN SERVER permite definir como grupo a un conjunto de usuarios y darle privilegios de acceso que son heredados instantáneamente por todos los miembros.

La documentación de LAN SERVER es abundante y la ayuda en línea tiene notables mejoras con respecto a la PC LAN.

3.- SFT[1] NETWARE 286/2.15 de NOVELL

Es un enfoque muy particular frente a las redes, al no basarse en DOS ha sido capaz de aventajar a sus rivales en cuanto a rendimiento.

Cuando se habla de redes, uno de los aspectos que puede producir desconfianza es la vulnerabilidad.

Una falla de un disco en un servidor puede paralizar toda una organización; Novell posee el mejor conjunto de funciones de protección de los datos. Netware comprueba automáticamente la existencia de bloques de datos incorrectos en el disco,

[1] Syetem Fault Tolerance, Tolerancia a Fallas del Sistema.

comparando cada bloque escrito en él con el mismo bloque almacenado en la memoria y lo guarda en un área especial del disco. También conserva la dirección del bloque defectuoso, para evitar ulteriores escrituras en esa área. Para mayor seguridad, Netware almacena en dos lugares distintos del disco copias duplicadas de la tabla de directorios y de la tabla de asignación de archivos (FAT, File Alocation Table).

La versión SFT (System Fault Tolerance) es capaz de mantener un duplicado de todo el disco del servidor (técnica de discos espejados). El usuario debe optar entre establecer dos discos en el mismo controlador, con el fin de eliminar los problemas causados exclusivamente por la contaminación de los datos y los errores de disco, o bien tratar el segundo disco a través de un canal independiente (controlador, cable, y fuente de alimentación) para lograr una mayor seguridad. Disponer de dos canales de disco acelera las tareas de "backup" al permitir la transferencia en paralelo. Las lecturas de disco también ganan en eficiencia, ya que es el disco más rápido el que atiende a una solicitud de lectura determinada, y los dos discos pueden atender a peticiones múltiples.

Aún con toda esa protección es posible que surjan contratiempos. El problema más grave se produce si el sistema falla cuando ya ha escrito los datos en el disco, pero antes de haber realizado la transacción en el índice subyacente de la aplicación. NetWare trata una secuencia global de escritura como una única transacción, sin conservar ninguno de los datos a menos de que aquella haya finalizado. Si NetWare no llega a detectar una transacción completa, "vuelve atrás", devolviendo los datos a su situación previa.

NetWare requiere un servidor exclusivo y utiliza un formato propio en el disco del servidor. Sigue siendo posible ejecutar DOS, pero en tal caso NetWare actúa como un sistema operativo huésped. Los sistemas operativos de red dedicados ofrecen mayor seguridad, ya que los usuarios no pueden arrancar directamente desde el disco del servidor, deben atravesar la red para acceder al mismo.

En las operaciones de red, Novell lleva a la práctica estrictamente el modelo servidor-cliente. Los recursos de la red se encuentran en un servidor centralizado, mientras que cada una de las estaciones cliente accede al mismo a través de la envoltura de NetWare. Esta interceptará todas las llamadas al DOS procesadas por la interrupción 21H; dirigirá la operaciones locales a DOS traduciendo las llamadas de red al NetWare Core Protocol (NCP) para que sean procesadas por el servidor.

El núcleo de NetWare es sorprendentemente compacto y sólo requiere entre 45 y 60 KBytes de RAM en cada estación de trabajo. Esta es una de las ventajas sobre otros productos de la competencia, ya que NetWare es el único que deja suficiente espacio en memoria del DOS a aplicaciones tan ávidas de RAM como dBASE IV.

La interfaz de usuario de NetWare consta de una serie de menúes y un conjunto de utilidades de línea de comando. El menú SYSCON rige las operaciones más habituales. A partir de él, el supervisor puede añadir o borrar usuarios, incorporarlos a un grupo, modificar los permisos de archivos, establecer restricciones de inicialización y otras medidas de seguridad, mantener el registro de errores, investigar el estado del grupo/usuario e incluso fijar cuotas por los servicios de la red.

Como supervisor o como dueño de un directorio se puede otorgar distintos permisos de archivos (leer, escribir, crear, borrar, abrir, modificar, buscar o controlar) a cada usuario.

Otra de las características de NetWare es la posibilidad de depurar cuentas inactivas, fijando una fecha de caducidad para las mismas; así mismo puede fijarse una fecha de caducidad para las contraseñas a fin de que los usuarios se vean en la necesidad de modificarlas a intervalos regulares. Además se puede limitar el número de sesiones simultáneas que un usuario puede tener abiertas. Otra opción es la de establecer restricciones de tiempo por usuario. También se puede inhabilitar una cuenta de usuario si se tiene un determinado número de intentos fallidos al digitar la contraseña.

Existen ciertas utilidades especiales que le ayudan al supervisor a crear un gran número de usuarios, sobre todo cuando se crea la red por vez primera.

Se pueden establecer cuotas de permanencia en la red o de capacidad de disco, esto es muy útil en la contabilidad y auditoría de los recursos de la red.

4.- 3+OPEN LAN MANAGER 1.0 de 3 COM

Aunque basado en OS/2, 3 COM fiel al DOS y al limitado estándar MS-NET optó por la compatibilidad. Al mantener la compatibilidad, puede soportar múltiples protocolos de capa red y transporte mediante la creación de un núcleo de selección de protocolo. Dicho núcleo permite la creación e instalación dinámica de un surtido de pilas de transporte compatibles.

3+OPEN carga inicialmente el NetBIOS Protocol (NBP) que es una versión recortada (25 KB) del Xerox Network Standard (XNS) con servicios limitados de archivos e impresión. Para otros servicios como el correo electrónico utiliza el XNS. Sin embargo, cuando una aplicación precisa un protocolo distinto, como TCP/IP o ISO TP/4, el gestor residente de protocolos lo intercambia automáticamente. Dado que 3+OPEN soporta varias pilas alternas de transporte no requerirá "gateways" ni "bridges" para las comunicaciones entre redes.

Por esta compatibilidad con LAN SERVER este producto se constituye en una opción adecuada para los servidores basados en OS/2.

La instalación es sencilla, regida totalmente por menúes y con una buena documentación.

3+OPEN utiliza la estructura de mandato de MS-NET. Los usuarios de las estaciones de trabajo acceden a los recursos del servidor mediante el mandato NET SHARE. La

introducción del mandato NET sin parámetros genera un sistema de menú en una estación de trabajo OS/2, las estaciones DOS sólo pueden emplear el interfaz de línea. La estructura de mandatos NET es fácil de dominar, además existe el NET HELP que proporciona ayuda en línea.

Sin embargo, 3 COM incluye una ampliación del DOS regida por menúes. Desde el menú "View", es posible compartir recursos o controlar las colas de los dispositivos de impresión y comunicaciones. El menú "Message" permite enviar y recibir mensajes. El menú "Config" permite establecer o cambiar opciones de configuración, incluídas las contraseñas. Además se tiene el menú "Status" que ofrece posibilidades de control estadístico. Existen otros menúes como el "Administration", "User", y "Account" con tareas específicas de administración, auditoría y contabilidad de los recursos de la red.

3+Open reconoce dos tipos de seguridad: a nivel compartido y a nivel de usuario. En el primero se asigna una contraseña a cada recurso concreto y todo usuario que tiene la contraseña del recurso obtiene autorización equivalente. En el segundo caso, el usuario posee una contraseña única.

Existen productos opcionales tales como 3+Open Secure y 3+Open Mail. El primero obliga a la modificación de la contraseña del usuario, ofrece un registro adicional de auditoría y analiza la información del mismo; mientras que 3+Open Mail es una opción de correo electrónico, con él también se incluye el 3+Open+Name Service, que hace posible que "hosts" remotos reconozcan nombres locales de la red, esta opción es muy importante si se piensa en las comunicaciones entre redes.

5.- 3+SHARE 1.3.1. de 3 COM

Es el precursor de 3+Open, basado en MS-NET. Es una alternativa más lenta y más barata para migrar a redes OS/2 de 3 COM.

Su instalación es un tanto complicada, depende del tipo de "hardware", si es de 3COM o no, carece de un material claro de soporte para "hardware" de otros fabricantes.

Se controla desde el interfaz de línea o 3+Menúes (la opción de menú es clara y abundante).

Reconoce tres tipos de usuarios: usuarios de red, administradores y usuarios del servidor.

CONCLUSION

Un criterio importante en la evaluación de los sistemas operativos son los tiempos de respuesta del sistema para que los usuarios sigan "manteniendo la idea" de que la unidad de disco duro de la red es simplemente otra unidad local.

En ese sentido, NetWare es muy rápido, tiene un sistema de caché en el disco del servidor compuesto de buffers de 4 KB, cuya única limitación en número viene dada por la cantidad de memoria disponible. Además, el formato de disco de NetWare presenta bloques lógicos mayores que los sectores de 512 Bytes del DOS y del OS/2, lo cual mejora el rendimiento en la transferencia de grandes archivos.

Aún con los "Extended Services" el PC LAN es sumamemte básico. No prevee la tolerancia a fallos, ni está dotado de capacidades de auditoría. Si la mayor parte de equipos dentro de la red son IBM PC o XT, vale la pena considerar PC LAN, aunque es probable que los usuarios en esta situación prefieran 3+SHARE.

LAN SERVER tiene mucho de lo que le falta a PC LAN. Al estar construido sobre el OS/2 tiene ventajas que van más allá de meras prestaciones; por ejemplo tiene una excelente compatibilidad gracias a una serie común de interfaces para los

programadores de aplicaciones y a una arquitectura de comunicaciones abierta y modular. Es fácil migrar de PC LAN a LAN SERVER.

Indudablemente NetWare sigue afincado en la cumbre, maneja con facilidad las tareas de red y sus funciones de gestión, contabilidad y seguridad superan enormemente a los demás. 3+OPEN sin embargo, se convierte en una alternativa para sistemas grandes con numerosos puentes inter-red y puertas de conexión con otros entornos.

A pesar de todo, según Stewart Alsop escritor en el semanario INFO WORLD, NetWare no es precisamente un sistema operativo para red, ya que un sistema operativo de red debe estar diseñado para permitir aplicaciones en ambiente distribuido con múltiples computadores "hosts" (minicomputadores y "mainframes"), y a decir verdad no existe ninguno hasta hoy. En los mini computadores y "mainframes" los sistemas operativos están diseñados para ser sistemas independientes y procesar grandes cantidades de datos, pudiendo ser accesados por muchos usuarios directamente conectados al procesador. En los computadores personales, en cambio los sistemas operativos están diseñados para administrar una o varias aplicaciones por un individuo. Pero en ninguno de los dos casos los sistemas operativos han sido diseñados específicamente para administrar el uso de una o más aplicaciones de forma cooperativa entre múltiples servidores de red.

Una nueva generación de sistemas operativos está siendo diseñada o rediseñada específicamente para trabajar en red. Por ejemplo Solaris de SunSoft, que se basa en Unix; Open DeskTop de SCO (Santa Cruz Operation); OS/2 de IBM, y NT de Microsoft.

Se dice que NetWare fue diseñado para proveer un servicio de archivo e impresión directamente a los computadores personales en un grupo de trabajo, y sólo últimamente está adquiriendo las características necesarias para ser usado en el desarrollo de aplicaciones. Novell adquirió los derechos de usar Unix y es muy posible

que cambie a Unix como su sistema operativo base para una futura versión de NetWare.

1.2.3.1 Descripción de los sistemas operativos NetWare y selección

Se realizará un enfoque general sobre las diferentes versiones de NetWare. Este enfoque tiene como material de referencia básico el libro "Domine Novell NetWare"[1], reforzado por los manuales del NetWare 386 y la experiencia propia.

NetWare puede funcionar en cualquiera de las redes físicas (o medios de acceso) más conocidas: Token Ring, Ethernet y ARCnet. El esquema de acceso proporciona el medio electrónico para el transporte de los datos; NetWare proporciona la inteligencia para controlar el proceso de los datos y los recursos del sistema.

Existen 4 tipos básicos de NetWare, el ELS (Entry-Level System), el Advanced NetWare 286, el Advanced NetWare 286 SFT y el NetWare 386.

Uno de los factores para elegir una de las versiones de NetWare es el tamaño y complejidad de la red. Una red pequeña podría elegir el ELS de NetWare, pero las funciones y oportunidades de crecimiento serían muy limitadas. Una red de tamaño medio debería elegir una de las versiones Advanced NetWare 286 (con o sin SFT); pudiendo funcionar bien en ordenadores con procesadores 80286 u 80386. En cambio, una red grande debería seleccionar el NetWare 386, éste tiene el sistema operativo más potente y contiene un gran número de funciones avanzadas no disponibles en las otras versiones. En general, la versión que se elija vendrá determinada por el número de estaciones de trabajo que se suponen van a conectarse en red.

[1] Cheryl C.Currid y Craig A. Gillet.

En el Advanced NetWare 286 y el ELS, las impresoras de red están conectadas directamente al servidor, por tanto se debe mantener a los usuarios de las impresoras cerca del servidor.

Las proyecciones de crecimiento de la red y las seguridades son dos de los factores a considerar también para la elección de la versión de NetWare.

A continuación se indica una pequeña tabla que resume algunas de las características de las distintas versiones de NetWare de acuerdo a dos criterios: el número de usuarios y la complejidad. La complejidad viene determinada por funciones especiales que se refieren a los puentes de red, servidores múltiples y respaldos, entre otras funciones.

VERSION	N.ESTACIONES	COMPLEJIDAD
ELS NetWare	3-6	Simple
Advanced NetWare 286	6-30	Simple
Advanced NetWare 286 SFT	6-30	Compleja
NetWare 386	30-250	Simple o Compleja

Tabla 1.2 Versiones de NetWare de acuerdo al número de estaciones y complejidad de red.

El ELS es relativamente barato. Puede configurarse para trabajar en modo no dedicado (servidor y estación de trabajo a un mismo tiempo). Tiene importantes limitaciones; entre ellas la que no puede tener discos espejados. En pocas palabras, es recomendado para redes muy simples y no críticas; no es recomendado para cualquier red con posibilidades de crecimiento, que contenga datos o procesos importantes para la compañía o que llegue a formar parte de una red más extensa.

Por otro lado como ya se indicó (en la tabla 1.2) para una red de tamaño medio, que incluya hasta 30 estaciones de trabajo, se recomienda utilizar el Advanced NetWare 286 o NetWare 286 SFT (System Fault Tolerant, sistema tolerante a fallos). Estas

versiones "corren" en servidores con procesadores 80286 y 80386. Es preferible un procesador 80386 por su velocidad extra y potencia.

El Advanced NetWare 286 (sin tolerancia a fallos) es una buena elección para redes de tamaño medio. Contiene un gran número de funciones operativas y de seguridad. La versión SFT tiene además el sistema de espejamiento de los discos del servidor. En caso de que falle el disco primario de la red se obtiene una copia instantánea de él; la transferencia se realiza en forma tan transparente que el usuario no sabe que está trabajando con el disco espejado.

Finalmente, para redes con más de 30 estaciones de trabajo o con gran potencial de aplicaciones complejas, lo más adecuado es el NetWare 386. Esta versión requiere que el servidor tenga un procesador 386 como mínimo, aunque no así las estaciones de trabajo que pueden ser hasta las más sencillas PC.

El NetWare 386 tiene una serie de características avanzadas que no están en otras versiones. Algunas de ellas son:

- Mayor seguridad.
- Capacidad de soportar un gran número de usuarios por servidor.
- Sistema de archivos perfeccionados.
- Capacidad para soportar grandes bases de datos.
- Opción de limpieza inmediata de archivos borrados.
- Mejores opciones de compartir impresoras.
- Configuración dinámica de los recursos.

Todas estas funciones extras son de gran utilidad en las redes grandes y complejas y vale la pena la inversión.

Una vez elegida la versión de NetWare se debe tomar en cuenta otra serie de decisiones antes del arranque. Se debe definir donde ubicar el servidor, el cableado y la(s) impresora(s) de red.

Dependiendo de cual versión de NetWare se ha elegido, la situación del servidor puede ser importante. Si se utiliza el ELS o el Advanced NetWare 286, deberá colocarse el servidor cerca de los usuarios. Tal situación es para facilitar el acceso de los usuarios a la impresora de la red. En caso de no ser posible esto, se puede colocar un cable de gran longitud y ubicar la impresora cerca de los usuarios, o comprar a terceras firmas un servidor de impresoras.

La situación de las impresoras deberá planificarse cuidadosamente con el objeto de ofrecer una máxima accesibilidad a los usuarios frecuentes. En el NetWare 386 el servidor de impresoras tiene la ventaja de poder distribuir las impresoras de red de forma remota, de tal forma que se pueda tener acceso a ellas sin necesidad de que éstas estén conectadas al servidor.

Algo que es importante decir respecto a los cables, es que éstos deben estar etiquetados para poder identificar alguna mala conección en caso de problema, o para dar mantenimiento. Por otro lado de ser posible deben ir todos juntos y por canaletas. Generalmente se pueden utilizar las canaletas utilizadas para proteger los hilos telefónicos. Localizar un problema cuando los cables están todos juntos es mucho más fácil.

1.2.3.2. Instalación del sistema operativo NetWare

El sistema operativo seleccionado para la red de OPEC es el NetWare 3.11.

De manera general para la instalación y configuración de la red NetWare se tienen que seguir los siguientes pasos:

- Preparación del local básico: se debe encontrar un local bien ventilado, libre de polvo y con una fuente de energía amplia. La instalación de los cables debe realizarla un contratista fiable para evitar futuros inconvenientes.

- Preparación del equipo físico: establece que la instalación se realice con una capacidad de memoria amplia y que la información clave sea registrada.

- Instalación de la gestión del NetWare: la instalación del NetWare está gestionada por un programa llamado NETGEN.

- Preparación del disco duro del servidor: se realiza con un programa utilitario del NetWare llamado COMPSURF. Este programa de análisis de la superficie comprueba los posibles defectos del disco del servidor y en caso de defecto los marca para no ser utilizados.

- Crear los programas de acceso de usuarios: estos se crean con el SHGEN.

- Instalar los iniciadores de comunicaciones ("login") especiales, para dirigir a las estaciones de trabajo en los llamados a ciertas funciones de la red.

- Instalar funciones de seguridad: limitar a los usuarios a las lecturas, escrituras, y aperturas de archivos y/o directorios.

- Instalar impresoras de la red.

- Instalar menúes de usuarios: estos se pueden crear con un utilitario de NetWare llamado MENU.

- Definir los procedimientos de administración de la red: deben planearse antes de la puesta en marcha y funcionamiento de la red.

Con esta secuencia a seguir se puede comenzar definiendo una lista de control, que no es más que definir con mayor precisión los pasos enumerados.

1. Preparar el equipo físico ("hardware")

a. Asegurarse que el NetWare puede soportar al servidor y a las estaciones de trabajo.
b. Repetir las rutinas de instalación cuantas veces sea necesario.
c. Grabar los protocolos de impresora si es necesario.

Se necesita verificar que tanto el servidor como las estaciones de trabajo puedan ser soportadas por el NetWare, además de que tengan una cantidad de memoria adecuada. Tomar todos los datos del SETUP de las computadoras; en el caso de impresoras tomar en cuenta si éstas son seriales, los datos de velocidad, protocolos, bits de paridad, etc.

Se debe proteger al servidor de la electricidad estática, del calor, de los ruidos eléctricos, de los altibajos de tensión y de los cortes de energía eléctrica.

De manera general se puede decir que se debe tener un piso antiestático conectado a tierra, y mantener la temperatura del lugar entre 18°C y 26°C, con una buena circulación de aire, asi como un buen UPS para estar dentro de los requerimientos y lograr que el servidor de la red opere normalmente.

Se debe documentar adecuadamente la ubicación de los cables. Debe realizarse un informe actualizado periódicamente, un mapa siempre a la vista y etiquetar los cables.

Como se indicó anteriormente uno de los problemas más frecuentes y más difíciles de diagnosticar proviene de las fallas en cables. Por tanto es necesario

dedicar tiempo en diseñar el cableado, tomando muy en cuenta las distancias de acuerdo al tipo de topología utilizada.

2. Configurar e instalar el NetWare

a. Configurar el sistema operativo.
b. Configurar y dar formato al disco duro.
c. Instalar las tarjetas de interfaz de la red.
d. Instalar el sistema operativo.

Todas estas actividades se gestionan mediante el NETGEN de NetWare.

Es importante crear una copia de trabajo de todos los "diskettes" del NetWare antes de comenzar a hacer la instalación. Se tiene que tomar en cuenta que el nombre de los volúmenes en cada diskette es muy importante, por lo que es preferible hacer un "DISKCOPY" de cada "diskette".

Es importante igualmente, para evitar complicaciones de instalación, que el equipo (computador y discos duros) que vaya a ser servidor de la red sea de buena calidad y de marca conocida, de tal forma que NetWare contenga en su lista de "drivers" los adecuados para ese equipo.

Configurar el sistema operativo implica seleccionar las opciones que van a incluirse en la red y definir el equipo ("hardware") que se va a instalar. De acuerdo a esto se genera un sistema operativo particular de cada red.

Para preparar el disco duro se "corre" el programa COMPSURF (COMPrehensive SURFace analysis). Este programa da formato y verifica el disco duro del servidor (Nota: Algunos discos duros modernos no necesitan que se "corra" el COMPSURF).

Luego se instala las tarjetas de red tanto en el servidor como en las estaciones de trabajo. Se pueden realizar algunas pruebas para verificar que estén trabajando adecuadamente y que las conexiones de los cables estén bien.

Finalmente se instala el sistema operativo de la red. El programa NETGEN controla este proceso. Cuando la instalación está completa, comienza a procesarse el NetWare con un programa llamado NET$OS. Ahora la red está activa, pero antes de poder realmente abrir el iniciador de comunicaciones ("login") hay que crear los programas de acceso de usuario.

3. Crear los programas de acceso de los usuarios

Antes de poder usar la red, debe generarse el "shell" de la estación de trabajo y crear un archivo "batch" que permita el fácil acceso de los usuarios.

El "shell" de la estación de trabajo se creará a través de la opción SHGEN. El SHGEN construye el "shell" de la estación de trabajo como un reflejo de la configuración de la red. Al finalizarse el proceso se obtienen dos archivos: el IPX.COM y el NET3 (NET4 o NETX, dependiendo de la versión de sistema operativo DOS que se está usando; se creará por ejemplo el NET3 si el DOS es el 3.1, 3.2, o 3.3, NET4 para DOS 4.x, el NETX es un genérico).

Una vez creado el IPX y el NETx, estos comandos pueden ejecutarse con otros del DOS para crear un interfaz de usuario particular de la estación de trabajo para la red. Luego la red pone un avisador ("prompt") con el "Login ID" (Identificación de entrada), donde el usuario debe poner su identificación que debe corresponder al asignado, luego pregunta por la contraseña de entrada ("password"), y si ambos datos son correctos permite el ingreso a la red.

4. Crear la estructura del directorio y cargar las aplicaciones

a. Poner en marcha la estructura del directorio básico tomando en cuenta la seguridad, la conveniencia y la lógica.
b. Asegurarse que las aplicaciones estén preparadas para ser utilizadas en la red.

Una vez en marcha la red se define la estructura de los directorios y los programas de aplicación que van a ser almacenados en el disco duro del servidor.

Por seguridad es conveniente clasificar los directorios de los usuarios con su identificación ("Login ID"). Además es conveniente agrupar para los respaldos ("Backup") los archivos que son modificados frecuentemente.

La instalación de las aplicaciones en el servidor generalmente se realizan como si se estuviera en un computador que no está en red. Sin embargo, hay que asegurarse que los programas estén preparados para trabajar en una red de área local (y que tengan licencia para hacerlo).

Las estructuras de los directorios del NetWare son similares a las estructuras del DOS.

Otro dato que es importante saber es que la instalación básica del NetWare crea cuatro directorios en el volumen del sistema, este volumen del sistema se crea generalmente como SYS. Estos directorios son el SYSTEM, PUBLIC, LOGIN y MAIL.

Existe un comando importante en NetWare para asignar alguna letra a un directorio o subdirectorio específico, éste es el comando MAP, además sirve para

establecer rutas de búsqueda, es similar al comando PATH del DOS. Los "drives MAP"[1] particulares de cada usuario pueden establecerse en el "login script"[2] .

Existen tres tipos de "drive maps":

1. Local drive maps (locales).
2. Network drive maps (de la red).
3. Search drive maps (de búsqueda).

Los "local drive maps" señalan a los directorios del disco instalado en la estación de trabajo local. El DOS siempre reserva un número de "drives" para uso local, si se quiere incrementar el número de "drives" de la red, se tiene que utilizar la opción LASTDRIVE del DOS para dicho efecto. Por ejemplo si se quiere utilizar "I:" como "drive" de la RED, se tiene que especificar en el config.sys LASTDRIVE=H (especifica que el último "drive" a ser asignado por el DOS será el "H:").

5. Poner en marcha el registro de los iniciadores de comunicación ("login") y los grupos de usuarios

a. Grabar los registros de los iniciadores de comunicación del sistema.
b. Grabar los iniciadores de comunicación de cada usuario individual.
c. Poner en marcha los grupos de usuario.

Los "Login Scripts" no son más que especificaciones de entrada a la red, es decir son instrucciones que guían a la estación de trabajo a la realización de una serie de funciones (algo así como los archivos batch del DOS). Una de las aplicaciones específicas es la asignación de "drives" o mensajes de bienvenida. NetWare

[1] Asignaciones de alguna letra a un directorio del servidor de archivos.
[2] Hace las veces del AUTOEXEC.BAT del DOS, establece la configuración inicial lógica de cada usuario.

permite que se creen dos tipos de "Login Scripts", los del sistema ("system login scripts") que se aplican a todos los que acceden a la red y los específicos de cada usuario.

La creación de grupos de trabajo facilita la concesión de derechos a un grupo de usuarios en vez de dárselos individualmente. Los grupos de usuario pueden crearse y modificarse con la opción SYSCON. Debe pensarse por motivos de seguridad y de lógica el agrupamiento más adecuado de los usuarios.

6. Añadir los recursos de seguridad

a. Añadir el iniciador de comunicaciones ("login") y la contraseña ("password") de seguridad.
b. Añadir la administración de los recursos de seguridad ("Trustee security").
c. Añadir los atributos de seguridad de los archivos y directorios.

El primer nivel se refiere a que el usuario para acceder a la red debe ingresar un nombre de usuario válido y la contraseña correcta. A este nivel es posible en NetWare limitar los intentos fallidos, limitar el acceso a ciertas estaciones de trabajo, y/o forzar a cambiar la contraseña después de cierto periodo de tiempo.

Una vez en la red, el mecanismo de seguridad es la "trustee security" que regula los derechos específicos de un usuario para utilizar un directorio en particular. Estos derechos son asignados a un usuario individual o a un grupo desde que son creados como usuarios de NetWare.

La seguridad a nivel de directorio regula los derechos de un usuario para utilizar un directorio independientemente de lo que diga sus "trustees security". Puede conceder o revocar derechos sobre un directorio. Este mismo concepto se aplica a los atributos que el usuario tiene sobre los archivos.

7. Configurar y verificar las impresoras de la red

Existen varias herramientas para definir y configurar las impresoras de la red. En OPEC se utiliza un servidor de impresión, que se ubica en el servidor de archivos. Este servidor de impresión puede tener hasta 16 impresoras. La versión de NetWare de OPEC permite tener hasta 16 servidores de impresión con 16 impresoras cada uno.

8. Crear los menúes

a. Utilizar la función MENU para dicha creación.

NetWare posee un utilitario que permite crear los menúes de usuarios de forma fácil, esta opción es MENU. En OPEC se utiliza el programa AUTOMENU que permite realizar menúes iterativos de varias páginas de acuerdo a las necesidades de "software" de los diversos departamentos de la empresa.

9. Planificar la administración de la red

Todas las LAN necesitan un grado de mantenimiento periódico. Respaldos de información, agregar nuevos usuarios, actualizar los usuarios, crear estándares en los menúes, nuevos programas de aplicación, etc.

Finalmente, NetWare permite expandir la red. La expansión de las comunicaciones en un mismo edificio puede completarse a través de puentes locales que operan dentro de las limitaciones impuestas por los cables de la red.

Las comunicaciones asíncronas pueden realizarse con varios tipos de modems. NetWare permite tener un servidor de comunicaciones asíncronas dedicado, de forma que permite compartir los modems.

Pueden construirse grandes redes dispersas geográficamente con la utilización del "hardware" y "software" de las redes de área extensa (WAN). Las WAN pueden construirse con las líneas telefónicas, las redes de datos públicas, las líneas alquiladas T-1[1], y las comunicaciones vía satélite.

Un puente asíncrono es barato pero utiliza comunicaciones relativamente lentas hasta 10.9 Kbits por segundo.

1.2.4 SISTEMA DE RESPALDOS DE LA RED

Los sistemas de respaldos ("backup") son unidades de almacenamiento masivo de información, que van desde discos duros (fijos y removibles) de alta capacidad hasta las conocidas unidades de cintas magnéticas.

En el mercado actual se puede ver un predominio de las cintas, aunque lentas frente a los discos duros pero resultan más económicas.

Existen formatos distintos de cintas, en tamaño cada vez más pequeños y en capacidades que varían desde las decenas de MB hasta los GB. Se debe tomar en cuenta el formato si es que de alguna manera se tiene que establecer compatibilidad con otras empresas o con otras divisiones de la propia empresa. Generalmente el controlador de las unidades de cinta es ESDI[1] o SCSI[1] . Cuando se trata de un controlador SCSI se debe tener mucho cuidado con las direcciones de los distintos dispositivos conectados al bus, porque un mal direccionamiento, por ejemplo varios dispositivos con la misma dirección pueden provocar fallos en el servidor. Existen dos tendencias de "backup", por imágen, o de fichero a fichero. La primera es sacar una copia exacta bit por bit del disco duro, es bastante rápido el proceso pero no permite recuperar archivos individuales, la segunda mantiene la estructura de un directorio de forma que se pueden volver a crear los archivos.

---

[1] ver glosario.

Otros dispositivos utilizados son los cassettes digitales, éstos son parecidos a los cassettes de audio. Son de poca capacidad (hasta 10 MB) con velocidades comparativas a las cintas de cartucho.

Actualmente también se pueden encontrar unidades de "backup" que trabajan con cintas DAT (Digital Audio Tape) que pueden llegar a almacenar hasta 1.4 GB. Es una tecnología nueva que está siendo a puesta prueba, pero todavía no existen resultados concretos respecto a su fiabilidad.

Además se disponen de los cartuchos de 8mm. La forma de codificar los datos es mediante una conversión digital/análoga del flujo de bits. Su capacidad de almacenamiento es bien alta (hasta los 5 GB) a una velocidad bien alta. La mayoría de unidades existentes en el mercado pueden utilizarse con un controlador SCSI o ESDI. Algunos fabricantes de otras tecnologías han criticado su posible baja fiabilidad y la posibilidad de pérdida catastrófica de datos, que pueden presentarse debido a la utilización de cabezas helicoidales, aunque no parece existir suficiente justificación técnica. El principal inconveniente es su alto costo.

También se utilizan los cassettes de VHS. Aunque se cuestionó mucho su fiabilidad y su mayor tamaño que las otras cintas. Actualmente casi han desaparecido del mercado.

En los sistemas grandes las cintas de media pulgada, de 9 pistas, (o de carrete abierto) se han constituído en un estándar. Su capacidad es relativamente pequeña y va hasta los 100 MB, pero son muy fiables, se han encontrado cintas de hasta 10 años que aún funcionan correctamente.

OPEC posee una unidad de cinta de 8mm de marca PALINDROME, con el "software" de la misma casa que es el "Network Archivist". Mayor detalle se verá en el acápite 2.5.3.

1.2.5 CORREO ELECTRONICO

El correo electrónico combina las mejores características de una red: edición fácil, enrutamiento automático y acceso instantáneo ya sea dentro del mismo edificio o a través de los distintos países.

El correo electrónico posee una base de datos en la cual registra los usuarios y sus direcciones; una segunda base de datos registra y hace un seguimiento de mensajes desde que son creados hasta que son enviados de usuario a usuario. Las redes de área local son el medio que las empresas han elegido para correo electrónico, sin embargo para mayores distancias se pueden utilizar modems sobre líneas telefónicas, enlaces X.25 o a través de puentes ("bridges").

El "software" del correo electrónico consiste básicamente de dos partes: una que es el programa en sí mismo y la otra que es el interfaz de usuario. El programa es el encargado de tomar el mensaje, descifrar la dirección y hacerlo llegar a su destino. Dependiendo de la dirección, el mensaje debe ser encaminado en la misma oficina vía LAN, entre servidores de datos o a través del país mediante "gateways" y "bridges". Este programa actúa de forma transparente hacia el usuario, siendo importante que éste sea confiable y que su interfaz con el usuario sea amigable y a la vez poderoso.

Para escoger un paquete de correo electrónico es necesario establecer los entornos (de las estaciones de trabajo dentro de la red) en que se trabaja, ya sea DOS, OS/2, MAC, etc. Así como, los entornos de red, NetWare, Netbios, MS-Net, etc. Luego, se debe ver lo concerniente al equipo, si es que necesita un servidor dedicado o no. Cada paquete posee un sinnúmero de características que de acuerdo al presupuesto y servicios que se desea que preste se pueden conseguir[1] .

[1] Un artículo que compara las características de los correos electrónicos más vendidos es "Please, Mister postman" de la revista Byte, de marzo de 1991. Se adjunta dicho artículo en el ANEXO 4.

El correo electrónico que tiene OPEC es el CCMAIL de LOTUS, este correo es privado y sus servicios cubren 15 naciones en el mundo entero.

El programa en sí, es decir el cc:Mail se basa en una plataforma que provee el "software" necesario para crear y administrar una oficina de correo, "post office", que normalmente corresponde a un servidor de archivos. Esta plataforma también incluye los programas que se necesitan para crear un usuario en cc:Mail, para un tipo de sistema operativo de las estaciones de trabajo. La plataforma incluye autorización para un usuario, que sería el administrador de la "post office". Para añadir más usuarios se compra los paquetes que incluyen las licencias para mayor número de usuarios. Existen plataformas de cc:Mail para DOS, windows, UNIX y Machintosh.

Existen otros programas como el "cc:Mail Remote", el "cc:Fax", y el "cc:Mail Automatic Directory exchange", que ayudan en la administración de grandes redes de correo electrónico.

Para la conexión física del "cc:Mail" se utiliza un canal de datos a Tulsa y uno al CPF, el segundo canal de datos se lo utiliza para el "fax server" (tanto a Tulsa como al CPF). En el caso que llegaran a fallar los canales de datos se tiene otra tarjeta QSC[2] de respaldo.

1.2.6 SISTEMA DE COMUNICACIONES

En este punto se analizará el sistema interno de comunicaciones de OPEC para documentos, ya que los sistemas de voz y datos han sido analizados anteriormente.

Para las comunicaciones entre departamentos, entre Quito y Tulsa, entre Quito y el CPF, o entre OPEC y otras empresas se utiliza mucho el "fax".

---

[2] Tarjetas de datos que configuran el TIMEPLEX.

El fax se lo utiliza para enviar órdenes de compras, proformas, órdenes de servicios, copia de documentos, para solicitar material técnico a empresas de servicios, etc. Un alto porcentaje de estos requerimientos deben venir del exterior o deben solicitarse al exterior.

En vista de esta necesidad, en OPEC se encuentra instalado un servidor de fax. El servidor de fax es un dispositivo que permite marcar el número de fax remoto (al otro lado del enlace vía satélite) como si se tratara de una extensión local. El servidor de fax se conecta a uno de los puertos de la tarjeta QSC (de datos) por un lado y por otro lado a una extensión interna de la PBX.

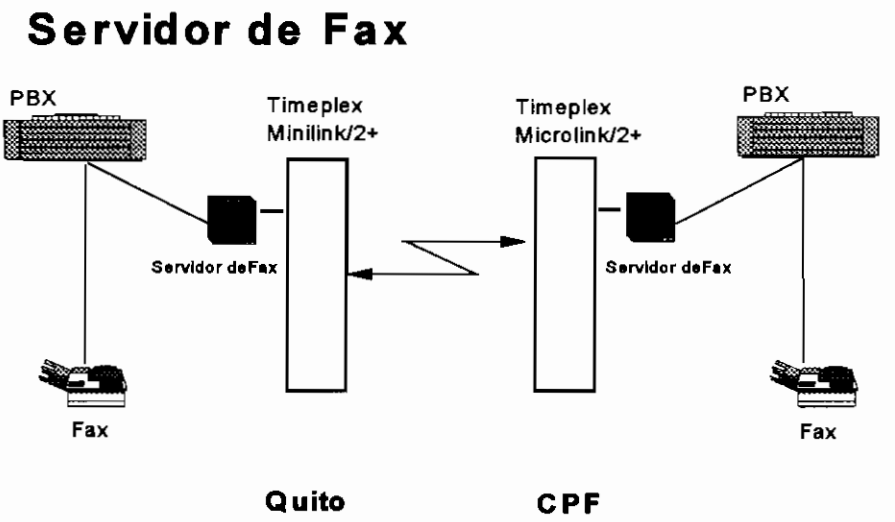


Figura 1.18. Servidor de fax conectado al enlace vía satélite.

Con esto se logra optimizar costos en las comunicaciones entre Quito y varias ciudades de Estados Unidos de Norteamérica, y de manera particular se permite una comunicación (envío de documentos y gráficos) óptima entre Quito y el CPF.

Por tanto, en OPEC se dispone de un Fax de alto volumen que está conectado a la PBX. La PBX enruta la llamada hacia la red telefónica pública para transmitir facsímiles a nivel local o hacia el sistema vía satélite (para el envío al CPF o a Estados Unidos).

1.2.7 PROTECCIONES DEL SISTEMA

Las protecciones del sistema se refieren al ambiente físico en el que están trabajando los equipos.

Se deben considerar sus tres grandes áreas: el centro de cómputo, las estaciones de trabajo y el cableado (incluyendo MAUs) desde las estaciones de trabajo al centro de cómputo.

En cuanto a las estaciones de trabajo, se puede decir por ejemplo que las instalaciones eléctricas del edificio del Banco de los Andes donde se encontraba laborando OPEC no fueron diseñadas para soportar la demanda de energía eléctrica que estuvo requiriendo. En algunas ocasiones tenía que estar funcionando el generador de emergencia para suplir cierto déficit del transformador. Los tableros de medidores no habían sido dimensionados para la demanda real. Existía una falta total de documentación en lo referente a las nuevas instalaciones eléctricas que se realizaron para suplir de energía a nuevos equipos y/o para solucionar problemas de sobrecarga en determinados circuitos.

Por otro lado, la temperatura dentro de las dependencias de OPEC era bastante elevada aún en los días fríos debido al efecto invernadero que tiene el edificio del Banco de los Andes.

Estos dos problemas son los que más afectaron el funcionamiento de la red en las antiguas instalaciones.

Para solucionar de alguna manera estos dos problemas OPEC optó por comprar un UPS Smart-UPS modelo 600 de APC por cada computador, y un UPS Smart-UPS modelo 900 por cada impresora láser.

Se puede decir que en lo referente a protecciones contra incendios, el centro de cómputo contaba solamente con 1 extintor de incendios instalado por las personas encargas de seguridad industrial en OPEC.

En la actualidad, no existe ningún sistema automático de detección de incendios. Pero en la noche, los guardias de seguridad tienen la consigna de revisar las condiciones ambientales del centro de cómputo, y si existe alguna anomalía se deben comunicar con el supervisor de la red o con el operador del sistema, ó en última instancia con el gerente del departamento de sistemas.

Finalmente, se debe mencionar que en las nuevas instalaciones del Edificio Vivaldi se realizó una planificación de las protecciones del centro de cómputo: Sistema de puesta a tierra, fuente ininterrumpible de poder, seguridades contra incendios, y acondicionamiento ambiental del centro de cómputo[1] .

Adicionalmente, de acuerdo a la experiencia que se tiene de las instalaciones del Edificio del Banco de los Andes, al diseñar las instalaciones eléctricas del Edificio Vivaldi se tomaron las debidas precauciones para evitar incurrir en los mismos problemas con las impresoras y estaciones de trabajo.

En cuanto al cableado (de datos) en sí, fue realizado por un profesional que conoce su oficio, y los concentradores no necesitan ningún mantenimiento especial. Solo se debe cerciorar que la alimentación eléctrica de cada uno de los MAUs no se vea interrumpida.

1.2.8 DISTRIBUCION FISICA Y TIPO DE EQUIPOS

Se considera dos tipos de equipos, las estaciones de trabajo y los equipos dedicados a prestar servicios.

[1] Esta planificación forma parte del estudio realizado en el capítulo 2.

1.2.8.1 Estaciones de trabajo

Las estaciones de trabajo en su mayoría son computadores AST 80486/33 MHz con 8 MB de memoria RAM y 210 MB en disco duro. Los restantes son computadores AST 80386SX/20 MHz con 2 MB de memoria RAM y 120 MB de disco duro.

Se tienen 101 estaciones de trabajo distribuidas de la siguiente manera:

5 en la planta baja (Depto. Administrativo).
7 en el Mezanine (Depto. de Materiales).
14 en el primer piso (Depto. de Finanzas).
9 en el segundo piso (Depto. de Finanzas).
11 en el tercer piso (Depto. de Sistemas).
14 en el cuarto piso (Depto. de Operaciones).
10 en el quinto piso (Depto. de Operaciones).
8 en el sexto piso (Depto. de Exploración).
6 en el séptimo piso (Depto. de Recursos Humanos).
6 en el octavo piso (Depto. Legal).
8 en el noveno piso (Depto. Gobierno y Medio Ambiente).
3 en el décimo piso (Gerencia General).

En la figura 1.17 se mostró como las estaciones están conectadas al anillo.

1.2.8.2 Equipos que prestan sus servicios

El Centro de cómputo se constituye en el cerebro de la empresa, en donde se procesa el 99% de la información vital. Estos equipos se encuentran ubicados en el centro de cómputo.

- Equipos existentes en el centro de cómputo:

1.- AS/400 IBM.

2.- UPS marca BEST, 18 KVA

3.- LAN Server AST, SCSI HDD

4.- LAN Backup Server IBM

5.- CCMAIL Gateway IBM

6.- Backup PC IBM AT 286

7.- Tape Backup Palindrome

8.- Timeplex y modem

-Equipos a adquirir en el futuro:

9.- Servidor de Base de Datos

10.-IBM RS/6000

11.-Segundo CCMAIL Gateway

12.-Misceláneos

Se numeran los sistemas implementados actualmente para la operatividad de las diferentes áreas técnicas y administrativas:

En el AS/400 se tiene:

-Sistema administrativo-contable.

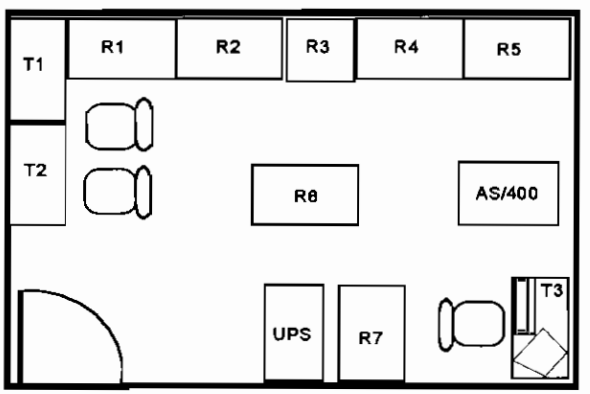
-Sistema del área de Recursos Humanos.

-A futuro se va ă implementar los sistemas para Materiales y para cuentas por pagar.

En la Red (LAN) se tiene:

- El sistema de cuentas por pagar y de materiales.
- Toda la información del departamento legal.
- Los sistemas de ingeniería.
- Toda la información de los programas de aplicación, principalmente de procesamiento de palabras y hojas electrónicas.

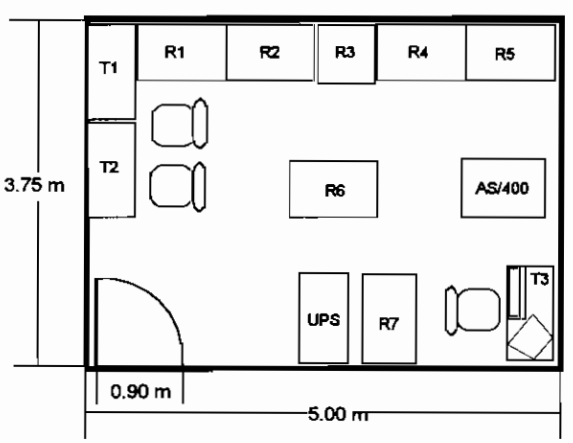
En cuanto a la ubicación de los equipos dentro del centro de cómputo es importante definir su distribución física de acuerdo a sus especificaciones: tamaño, requerimientos eléctricos, disipación térmica, accesibilidad, tipo de cableado, etc.



T1. MESA
T2. MESA
T3. MESA
R1. SERVIDOR + SERVIDOR (BACKUP)
R2. CC:MAIL + TNA
R3. EQUIPO DEL SATELITE
R4. RS/6000
R5. SERVIDOR "SYBASE"
R6. HERRAMIENTAS
R7. BATERIAS + HERRAMIENTAS
AS/400. IBM AS/400
UPS. BEST UPS 18 KVA

Figura 1.19. Distribución de equipos en el Centro de Cómputo del Edificio Vivaldi..

En la figura 1.19 se muestra la distribución física de los equipos dentro del centro de cómputo, mientras que la figura 1.20 da un estimativo de las medidas de cada uno de los elementos.

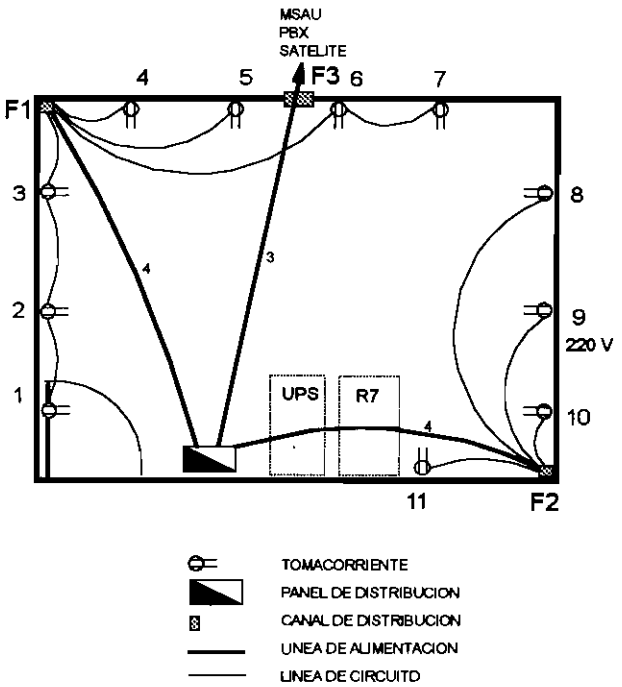


MEDIDAS DE LOS ELEMENTOS

T1,T2,T3 = 1.00X0.50 m
R1,R2,R4,R5,R6,R7 = 0.90X0.60 m
R3 = 0.60X0.65 m
AS/400 = 0.62X0.90 m
UPS = 0.46X0.92 m

Figura 1.20. Medida de los módulos que constituyen el Centro de Cómputo.

En la figura 1.21 se puede apreciar el diagrama eléctrico del cableado para suministrar energía (desde el UPS) a los equipos del centro de cómputo, a la PBX, a los MAUs y a los equipos en la base de la antena parabólica.



CANAL DISTRIB.	CIRCUIT #	TOMAS	ALIMENTAD. AWG #	TOMAS AWG#
F1	1	1,2,3	10x3	14x3
F1	2	4	14x3	14x3
F1	3	5	14x3	14x3
F1	4	6,7	14x3	14x3
F2	5	8	14x3	14x3
F2	6,7	9	10x3	10x3
F2	8	10,11	14x3	14x3
F3	9	MSAU		
F3	10	PBX		
F3	11	SATELITE.		
	12	FREE		

Figura 1.21. Suministro eléctrico desde el UPS a los diferentes equipos.

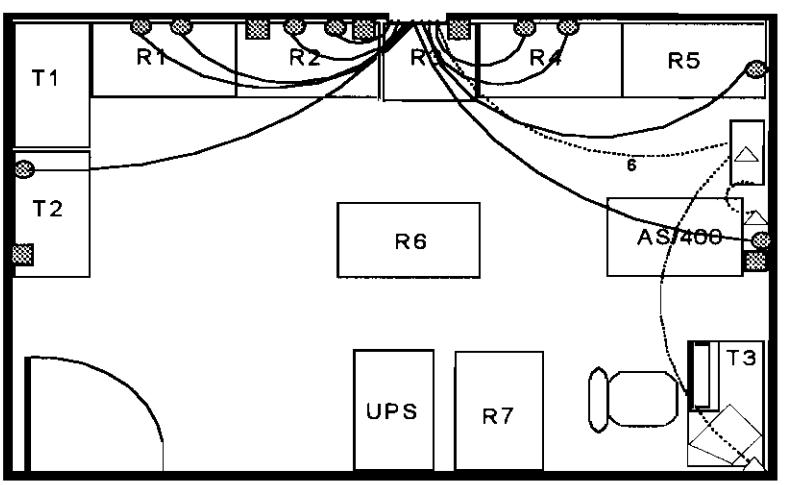


Figura 1.22. Esquema del cableado para datos.

La figura 1.22 es un esquema del cableado de datos para los diferentes equipos: Cableado "Token-Ring" para la LAN, Twin Axial para el AS/400 y telefónico para el sistema de comunicaciones vía satélite y la PBX.

Todos los cables de datos se distribuyen a través del ducto de conexiones eléctricas del edificio utilizando bandejas metálicas (para evitar ruidos electromagnéticos). Los cables telefónicos también son transportados en bandejas metálicas independientes a las que se utilizan para los cables de datos.

CAPITULO 2

2. PLANIFICACION DE LAS SEGURIDADES DEL SISTEMA

Para hacer una planificación adecuada de las seguridades se deben considerar los efectos que tendrían las contingencias sobre las operaciones de OPEC.

Los sistemas que se deben proteger principalmente son la LAN y el AS/400.

- **RED DE AREA LOCAL (LAN)**

  Existen varios niveles de desastre y de acuerdo a ello se va a exponer el efecto que tendrían esos niveles sobre las operaciones de OPEC.

  En caso de pérdida de "software" (datos o programas de aplicación), se tienen los respaldos ("backups") diarios de todos los volúmenes de la red. El procedimiento de recuperación de dicho "software" sería transferir dicha información de las cintas. Dichas cintas se mantienen en OPEC en la caja fuerte. La incidencia de este tipo de problema sobre las operaciones de OPEC, de manera general no son muy considerables ya que se puede recuperar la información de lo que se hizo el día anterior hasta las 10 pm.

  En caso de que fallen los discos del servidor de la red, existe el mecanismo de "mirroring", en donde están trabajando simultáneamente discos gemelos; en caso de que los originales fallen, pasan a trabajar los gemelos casi inmediatamente, de forma que esta transición es imperceptible para el usuario. La incidencia de este tipo de problema es nula sobre las operaciones de OPEC.

Si fallan el servidor de la red, los discos duros originales y sus gemelos espejados, existe un servidor de respaldo total[1]. Este servidor de respaldo se actualiza periódicamente, y luego se lo puede actualizar a partir de las cintas de "backup". Este tipo de falla se minimiza hasta el estado del día anterior a las 10 pm.

En caso de que el servidor de la red falle y no sus discos duros, se tiene un computador preparado para que en este caso pase a ser servidor (servidor parcial[1]) de la red utilizando los mismos discos duros. Este problema se minimiza al perder la red por un lapso corto en el orden de decenas de minutos, pero la red seguiría trabajando aunque un poco más lenta.

En caso de que el computador que realiza los respaldos de la red, o los "gateway" de comunicaciones fallen, ellos pueden ser reemplazados por otros computadores de los usuarios del sistema.

Las unidades que no tienen respaldo son: el UPS y la unidad de respaldos en cinta (Palindrome), cuya falla dejaría al sistema aunque trabajando, muy voluble a perder datos y sistemas en caso de fallas de los equipos servidores.

En caso de desastre total en el centro de cómputo, se pararían todas las operaciones de OPEC. No funcionaría ningún sistema. Se perdería el tiempo que demoren en comprar/arrendar nuevos equipos. No existe ninguna previsión en caso de desastre total.

AS/400

Se debe considerar que éste es un sistema relativamente nuevo. Recién se están haciendo los procedimientos a seguir en caso de desastre. Sin embargo se realizan respaldos en cinta de los datos de los sistemas instalados en él.

[1] Las características de este servidor serán analizadas en el acápite 2.5.1.

El tipo de respaldo que se hace son los respaldos diarios de los datos de todas las aplicaciones. Se tienen respaldos de las aplicaciones y del sistema. De tal manera que si se llegase a perder información se la puede recuperar desde cinta.

En caso de falla de "hardware" o en caso de desastre total se estaría dependiendo de la asistencia técnica de IBM.

Por tanto, resulta indispensable tomar medidas de seguridad para de esta manera evitar un desastre mayor que produzca una destrucción de los equipos. Cualquier otro tipo de falla se podría afrontar y recuperar el sistema en poco tiempo (minutos u horas).

Para planificar las seguridades de un sistema informático se tienen que considerar tres niveles:

- **SEGURIDAD FISICA DEL SISTEMA**

Corresponde a la seguridad de las instalaciones mismas del centro de cómputo y de los equipos en general. Se tiene que revisar todo lo concerniente con protecciones eléctricas, protecciones en caso de incendio, acondicionamiento ambiental y alarmas contra robo. Además se debe tener la información de respaldo almacenada en un lugar distinto, para que en caso de catástrofe física, no se pierda la información vital del sistema. Igualmente se debe asegurar los accesos al centro de cómputo, a los equipos (AS/400, consola del Server), a los computadores y terminales, y a las cintas que contienen los respaldos.

- **SEGURIDAD A NIVEL DE USUARIOS DEL SISTEMA**

Este tipo de seguridad es la que se implementa para restringir el acceso a personas no autorizadas a un sistema de información. Es decir, no todo el personal puede tener acceso a la red, sino solo las personas que por sus tareas

necesite tener dicho acceso. En este nivel de seguridad se implementan contraseñas, perfiles de grupo, perfiles de usuario, menúes y programas, además de restringir los días y las horas de trabajo del usuario de la red.

- SEGURIDAD A NIVEL DE RECURSOS DEL SISTEMA

Este nivel de seguridad involucra solamente a las personas que ya tienen el acceso a la red. Consiste en restringir la información de acuerdo a las tareas que desempeñe dentro de la organización; es decir este tipo de seguridades se da a nivel de archivos de datos, programas de aplicación y recursos, tales como espacio en disco, acceso a directorios y archivos e inclusive a dispositivos físicos, como por ejemplo impresoras. Se implementan grupos y/o lista de autorizaciones para manejo de archivos, directorios y dispositivos de impresión.

Los niveles segundo y tercero se detallaron a nivel del sistema operativo de la red. En el presente capítulo el análisis se centrará principalmente en la seguridad física del sistema.

La seguridad física en primera instancia debe considerar cuatro aspectos:

1.- Acceso al Centro de cómputo

Siendo el centro de cómputo el cerebro de la empresa donde se encuentra almacenada la información vital, es necesario restringir el acceso a dichas instalaciones. Sólo se le permitirá la entrada a personal autorizado. Dicho personal se refiere a quienes laboran en el departamento de Sistemas (MIS[1]), o personas autorizadas por los miembros del departamento para fines de servicio y/o mantenimiento bajo estricta supervisión del departamento de Sistemas.

[1] MIS, Management Information Systems. Sistema de Administración de la Información.

No se permite el ingreso de comida ni bebidas dentro de las instalaciones del centro de cómputo.

El centro de cómputo debe permanecer cerrado bajo llave durante las 24 horas del día, para evitar el ingreso de personas no autorizadas. Existen 2 copias de las llaves: la primera copia la tiene el supervisor del Departamento de Sistemas y la segunda copia la tiene la coordinadora de MIS.

El control de acceso al centro de cómputo actualmente no se encuentra restringido directamente. A mediano plazo se pretende establecer un acceso con clave y con registro de entrada/salida de las instalaciones del centro de cómputo.

2.- Protección contra fallas eléctricas

Una de las razones que motivaron a OPEC a proponer este análisis, es el tratar de planificar bien el ambiente eléctrico en el que deben trabajar los equipos para evitar cualquier problema de índole eléctrica (como los planteados en el capítulo 1).

Como primera medida se hizo un análisis de la demanda eléctrica por piso para las nuevas instalaciones, dicho análisis se realizó de acuerdo a la distribución de departamentos, personas y equipos eléctricos y electrónicos. De esta forma se quiere evitar cualquier tipo de problema debido a una sobrecarga de la red de suministro eléctrico.

3.- Control térmico del equipo

Se debe mantener la temperatura entre 20°C y 24°C . Se va a instalar un termómetro cuyo sensor se encuentra en el interior del centro de cómputo y su visualizador en el exterior, de manera que se pueda monitorear la temperatura del centro de cómputo sin necesidad de entrar en él. De esta manera el personal de seguridad durante las

noches puede establecer una alarma en caso de falla de la unidad de aire acondicionado.

En caso de falla del equipo de aire acondicionado (elevación de temperatura), el primer contacto a recurrir será el operador del sistema y luego el supervisor de la red.

4.- Protección de la información en caso de incendio

Se va a instalar un sistema de detección de humo por cámara de ionización para detectar posibles incendios, con alarma central en la planta baja del edificio que permita monitorear y determinar el lugar de la alarma.

En caso de incendio en el centro de cómputo se tiene un extintor de CO2. A futuro se va a implementar un sistema "sprinkler" de extinción de incendios.

Se están definiendo las políticas para establecer los "OFFSITE BACKUPS"[1] . Actualmente las cintas del "backup" de la red (TNA-Palindrome Unit) se mantienen en otro lugar al de OPEC. Se tiene información de todos los volúmenes de la red desde Noviembre de 1992 hasta la presente fecha. Para el AS/400 se está guardando la información mensual del sistema y de las bibliotecas de producción, mientras que los datos se mantienen durante un periodo máximo de 15 días, y dichas cintas se almacenan en la oficina del operador del sistema.

A continuación se exponen los mecanismos para proteger los equipos y la información contra cualquier contingencia.

[1] Son cintas de respaldo que se deben guardar fuera de las instalaciones de OPEC para que en caso de algún desastre (incendio, inundaciones, etc)esta información pueda estar a salvo.

2.1 SISTEMA DE PUESTA A TIERRA

"La función de la puesta a tierra de una instalación eléctrica es la de forzar la derivación, al terreno, de las intensidades de corriente, de cualquier naturaleza que se puedan originar, ya se trate de corrientes de defecto, bajo frecuencia industrial, ó debidas a descargas atmosféricas de caracter impulsivo"[1] .

Con ello desde el punto de vista técnico se logra:

- Limitar la diferencia de potencial, que en un momento dado, puede presentarse entre estructuras metálicas y tierra.

- Posibilitar la detección de defectos a tierra y asegurar la actuación y coordinación de las protecciones, eliminando o disminuyendo, así, el riesgo que supone una avería para el material utilizado y para las personas.

- Limitar las sobretensiones internas (de maniobra-transitorias y temporales) que puedan aparecer en la red eléctrica, en determinadas condiciones de explotación.

- Evitar que las tensiones de frente escarpado[2] , que originan las descargas de los rayos, provoquen "cebados inversos", en el caso de instalaciones de exteriores y particularmente en líneas aéreas.

Los objetivos básicos de la puesta a tierra de instalaciones son:

- Seguridad de las personas.
- Proteger las instalaciones.
- Mejorar la calidad del servicio.

---

[1] Rogelio Garcia Márquez, "La puesta a tierra de instalaciones eléctricas y el R.A.T."

[2] Son las tensiones que se inducen en las estructuras metálicas al producirse una descarga atmosférica.

- Establecimiento de un potencial de referencia.

En relación con la seguridad de las personas, se puede decir que están fuera de peligro siempre y cuando no lleguen a "puentear" con su cuerpo dos puntos con una diferencia de potencial determinada, y establezca la circulación de una corriente con intensidad y duración que determine efectos fisiológicos peligrosos.

El factor primordial a tomar en consideración en la puesta a tierra es la resistividad del terreno. Si bien los componentes más importantes del terreno son en (estado seco) aislantes: sílice, óxido de aluminio, etc., su resitividad disminuye en presencia de la humedad y sales solubles. La composición de la tierra varía mucho de un lugar a otro y por tanto su resistividad. Los factores del terreno que modifican la resitividad son:

-La composición.
-Sales solubles.
-Estado higrométrico[1] .
-Temperatura.
-Granulometría[2] .
-Compacticidad[3] .
-La estratigrafía[4] .

En general, el terreno es heterogéneo en cualquiera de las direcciones que se lo considere, por tanto el conocimiento de su resistividad y sus posibles variaciones es bien imperfecto, entonces no es posible realizar un cálculo preciso de la distribución de las corrientes que lo recorren y hay que realizar evaluaciones sencillas y aproximaciones de orden práctico.

---

[1] Humedad del suelo.
[2] El tamaño de los gránulos componentes de ese suelo.
[3] El suelo está compactado o no.
[4] La composición del suelo por capas o estratos.

Esta incertidumbre hace que muchas veces no se tome la instalación de tierra con la seriedad del caso. Muchas veces sencillamente se conecta la tierra a la tubería de agua potable, lo cual resulta una instalación poco técnica y no recomendada debido a que puede estar poniéndose la tubería a un potencial de riesgo ya que muchas veces puede estar aislada de la tierra y en determinadas circunstancias puede provocar accidentes de índole eléctrico, ya sean personales o al equipo que se trataba de proteger.

Se debe tener en cuenta un criterio bien importante, el que a menor resistividad del suelo, las líneas de potencial tienden a profundizarse en el suelo, y que a mayor frecuencia dichas líneas de potencial tienden a irse a la superficie.

Adicionalmente para una instalación de puesta a tierra para proteger las instalaciones eléctricas y electrónicas de un edificio, se debe tener en cuenta el siguiente aspecto: saber la capacidad total del transformador de servicio del edificio para poder establecer la magnitud de las corrientes y potenciales que se puedan presentar en determinadas circunstancias.

En la mayoría de los casos son transformadores de sub-distribución Alta tensión/Baja Tensión; en el caso particular de este estudio es un transformador trifásico cuyo lado de baja tensión tiene un voltaje por fase de 220 V y una potencia de 200 KVA.

Con este dato se puede ver que los voltajes y corrientes en caso de falla son bajos para que actúen las protecciones. Por tanto el diseño del sistema de protección a tierra es sencillo, e inclusive puede hacerse un análisis visual de las condiciones del terreno para determinar su resistividad, basado en la norma MIE RAT 13[1] , en su punto 4.1,

[1] Las Instrucciones Técnicas Complementarias (ITC) del Reglamento sobre Condiciones Técnicas y Garantías de Seguridad en Centrales Eléctricas, Subestaciones y Centros de Transformación- conocido abreviadamente como reglamento A.T.-, fueron aprobadas con la denominación MIE-RAT, en el número 20 por la orden ministerial del 6 de julio de 1984, en España.

acerca de la resistividad del terreno, para realizar el proyecto de una instalación de tierra:

> *"Sin embargo, en las instalaciones de tercera categoría, y de intensidad de cortocircuito a tierra inferior a 16 KA no será imprescindible realizar una investigación del perfil de resistividad del terreno bastando un examen visual del terreno, pudiéndose estimar la resistividad por medio de la Tabla 2.1, en la que se dan valores orientativos..."*

Para OPEC el caso más desfavorable sería 1 KA, que está muy debajo de los 16 KA.

Naturaleza del terreno	Resistividad (Ωm)
Terrenos pantanosos	Pocas unidades a 30
Limo	20 a 100
Humus	10 a 150
Turba húmeda	5 a 100
Arcilla plástica	Pocas unidades a 50
Margas y arcillas compactas	100 a 200
Margas del jurásico	30 a 40
Arena arcillosa	50 a 500
Arena silícea	200 a 3000
Suelo pedregoso con césped	300 a 500
Suelo pedregoso desnudo	1500 a 3000
Calizas blandas	100 a 300
Calizas compactas	1000 a 5000
Calizas agrietadas	500 a 1000
Pizarras	50 a 300
Rocas de mica y cuarzo	a 800
Granitos y gres procedentes de alteración	1500 a 10000
Granitos y Gres muy alterados	100 a 600
Hormigón	2000 a 3000
Balasto o Grava	3000 a 5000

TABLA 2.1. Resistividad del suelo según la naturaleza del terreno.

Otro factor que es interesante definir es la "agresividad" del terreno, dicha "agresividad" se refiere a la corrosión que el electrodo puede sufrir por agentes químicos del terreno. Esta es una de las razones por las que se recomienda electrodos de cobre en vez de cualquier otro material, ya que es más resistente a la corrosión por agentes químicos del suelo, mientras que el hierro por ejemplo se corroe y pone una capa de óxido resistiva entre el electrodo y la tierra. Los suelos humíferos y limosos son bastantes "agresivos", y no son muy recomendables a pesar de su baja resistividad. Mas los suelos cálcareos como la pizarra o carbonato de calcio si son recomendados por su baja "agresividad" y resistividad.

Otro criterio importante es el de evitar en lo posible las conexiones mecánicas con abrasaderas u otros dispositivos, es preferible el soldar dichas conexiones, para evitar que agentes dieléctricos se depositen en las conexiones mecánicas y realicen un mal contacto.

Se deben diferenciar dos tipos de puesta a tierra: de protección y de servicio. La puesta a tierra de protección según la norma RAT 01, se refiere a aquella conexión directa de las partes conductoras de los elementos de una instalación que normalmente no están sometidos a tensión alguna, pero que podrían ser puestos en tensión por averías o contactos accidentales, a fin de proteger a las personas y equipos contra contactos con tensiones peligrosas. Mientras que, la puesta a tierra de servicio se refiere a la conexión que tiene por objeto unir a tierra, temporalmente, parte de las instalaciones que están normalmente bajo tensión o permanentemente ciertos puntos de los circuitos eléctricos de servicio, por ejemplo los neutros de los transformadores que lo precisen para redes con neutro a tierra, así como también pararrayos para eliminar las sobretensiones o descargas atmosféricas.

Se puede decir que la interconexión de las diversas tomas de tierra tanto de servicio como de protección de una instalación, permite obtener con un mínimo costo la resistencia global más pequeña, así como la de reducir las diferencias de tensión

locales entre las partes de la instalación, a su mínima expresión. Es decir, de manera general es recomendable interconectar las tierras en el sistema, exceptuando los casos en los que es conveniente separar los neutros de los devanados de los transformadores, y en los limitadores de tensión de las líneas de corriente débil (tales como las telefónicas, telegráficas,etc.) que se extienden fuera de la instalación.

En el caso particular de OPEC se tienen 4 sistemas independientes de puesta a tierra:

- La del transformador, que pone el neutro a tierra.
- La del UPS que alimenta al centro de cómputo, y equipo de comunicaciones via satélite.
- La del PBX.
- La del sistema de radio UHF/Pararrayos.

De estas cuatro tierras ninguna de ellas está interconectada. La tierra del PBX por las razones antes mencionadas no debería estar interconectada, ya que ésta es una de las excepciones, puesto que son limitadores de tensión de corriente débil que se extienden fuera de la instalación. La tierra del pararrayos está siendo utilizada además para proteger el equipo de radio frecuencia en UHF, y se la mantiene separada del resto de tierras para evitar que se induzca ruido de radiofrecuencia en los otros equipos. La tierra del transformador principal del edificio y del UPS deberían estar interconectadas para bajar la resistividad total del sistema de tierra, pero aún no estando interconectadas debido a su proximidad, es como si lo estuvieran por que se inducirían corrientes entre ellas.

En casos como el de OPEC, donde el neutro del transformador está a tierra, basta con medir la diferencia de potencial entre el neutro y tierra en donde idealmente estos dos puntos serían uno, y se recomienda para casos prácticos que este voltaje no exceda en ninguna circunstancia los 4 voltios. Una buena puesta a tierra en esta situación sería

tener una lectura inferior a los 1.5 voltios. En las instalaciones de OPEC se tienen 0.5 voltios entre tierra y neutro.

Según la tabla 2.1 se podría establecer para las instalaciones de OPEC un suelo un tanto pedregoso con césped, poco arenoso, más humus, que en el peor de los casos estaría en los 500 Ωm.

En estas condiciones, generalmente se opta por enterrar una varilla de cobre en el terreno, siempre y cuando la resistividad del terreno sea media, y las tensiones y corrientes de fallas estén en el orden de una decena de kiloamperios como máximo. En OPEC se ha optado para mejorar la conductividad del terreno poniendo carbonato de calcio alrededor del electrodo para evitar además la corrosión, carbón molido alrededor del carbonato de calcio y tierra de jardín (humus) alrededor del carbón molido. La configuración de cada uno de los sistemas de tierra es de tres barras de cobre de 1.8 m. como electrodos distribuidos en forma de un triángulo equilátero. De esta forma se han obtenido muy buenos resultados.

Otra cosa que es importante recalcar es que el cable del pararrayos debe bajar de ser posible por el exterior del edificio, para que en caso de ocurrencia de una descarga atmosférica no induzca niguna corriente en estructuras metálicas y/o conductores aledaños.

En instalaciones que tienen los tomacorrientes con tierra, se hace necesario revisar que la fase y el neutro no estén invertidos, porque generalmente se protege los equipos respecto a la fase, y si están invertidos se estaría protegiendo respecto a problemas con el neutro, es decir no existiría protección. Existen equipos tales como los UPS[1] que dan una alerta cuando está reversa la posición del neutro y de la fase, entonces es menester cambiar la conexión a la forma adecuada.

[1] Uninterruptible Power Supply. Fuente de Poder Ininterrumpida.

2.2 FUENTE ININTERRUMPIBLE DE PODER (UPS)

Cuando se habla de UPS es necesario saber que tipos de UPS existen en el mercado.

Se puede decir que existen dos tipos de UPS según su principio de funcionamiento, el primero, llamado "STAND-BY" o "BY-PASS", y el segundo el denominado "ON-LINE".

El "STAND-BY" o "BY-PASS" es un UPS que simplemente deja pasar el voltaje de la red pública, carga las baterías (en caso de ser necesario) y cuando existe algún problema transfiere la carga al inversor[1]. Mientras no haya falla de suministro eléctrico de la línea, este UPS únicamente hace un filtrado de picos y de ruidos de radio frecuencia. Este tipo de UPS es el más económico porque requiere menor capacidad de respaldo (baterías), pero que por ese mismo hecho no es capaz de dar un mayor tiempo de soporte a las cargas (se puede estimar que soporta la carga nominal entre 5 y 10 minutos como máximo), siendo posible comprar bancos de baterías para incrementar el tiempo de soporte, lo que al mismo tiempo encarecería al equipo.

Respecto al "ON-LINE" se puede decir que es un UPS que siempre está tomando el suministro eléctrico de las baterías, es decir siempre está funcionando el cargador de las baterías y el inversor, en línea con la carga. Este tipo de UPS tiene una salida siempre regulada, con una frecuencia y forma de onda sumamente estables. El UPS "ON-LINE" necesita una capacidad bien grande de baterías, su tamaño y costos son superiores al "BY-PASS", y sus tiempos de soporte generalmente son mayores.

Actualmente existe en el mercado un tipo de UPS que son una mezcla de "BY-PASS" y "ON-LINE". Este tipo de UPS que tiene un transformador ferroresonante con núcleo de ferrita, tiene la ventaja de ser un excelente acondicionador de línea, brindando protección adicional al inversor propio del UPS y al equipo, debido a que el transformador ferroresonante hace de transformador de aislamiento entre la carga y la

[1] Circuitería que convierte el voltaje DC de las baterías en voltaje AC para alimentar las cargas.

línea pública. Además, como el inversor no está siempre funcionando se conserva la carga de las baterías hasta que realmente se la necesite.

Una ventaja importante de tener un UPS en un sistema es la de continuar con la operación de la red durante una interrupción de poca duración del suministro eléctrico. Con un UPS se puede preveer una baja del sistema sin que se pierdan cadenas de datos, así como restablecer el mismo de manera rápida, sin efectos graves, una vez recuperado el suministro de energía eléctrica.

El UPS además puede acondicionar la línea eliminando los transientes, y estabilizando el voltaje.

En ambientes hostiles de trabajo es recomendable utilizar un UPS ferroresonante por las ventajas citadas. En caso de usar un UPS "BY-PASS", se corre el riesgo de que el transiente de corriente sea muy rápido respecto al tiempo de respuesta del UPS y afecte a la carga; por otro lado el ON-LINE evitaría eso pero tendría tanto trabajo que las baterías y el inversor corren un alto riesgo de daño, mientras que el UPS ferroresonante se adapta a dichos ambientes hostiles brindando protección y no siendo suceptible a daño.

El UPS que se dispone en el centro de cómputo de OPEC es un UPS ferroresonante (FERRUPS), controlado por microprocesador:

Marca: BEST
Modelo: FD18KVA

Este FERRUPS proporciona hasta 18 KVA, a 60 Hz, con 240 V nominales de entrada y 208/120 V de salida.

Sus características principales son:

- Proteger el equipo alimentado por él contra picos de corriente, llegando a una atenuación de 2000 a 1.

- Regular el voltaje dentro del ±3% respecto del estándar de la "Computer and Business Equipment Manufacturers Association" (CBEMA), y ANSI C84.1.

- Alimentación continua, sin interrupción durante pérdida completa del suministro eléctrico o interrupciones momentáneas.

- Forma de onda de salida sinusoidal para óptimas condiciones de trabajo de los equipos electrónicos protegidos.

- Diseñado para cargas que utilizan fuentes de poder por conmutación[1] ("switching power supplies").

- Monitorea automáticamente las baterías bajo carga y advierte al operador cuando es necesario revisar o cambiar las baterías.

- Monitorea el inversor cada día (o con una frecuencia mayor si se desea), para determinar su funcionamiento en caso de falla del suministro eléctrico. Si el microprocesador advierte una falla se activa una alarma.

- FERRUPS puede producir un voltaje de salida limpio y de condiciones nominales de voltaje de salida, sin necesidad de que funcione el inversor aún cuando el voltaje de entrada sea tan bajo como el 70% del voltaje de entrada nominal. El microprocesador analiza el voltaje de entrada y decide mediante programación el nivel del voltaje de salida, evitando de esta manera que funcione el inversor y descargue las baterías innecesariamente.

---

[1] La gran mayoría de computadores utilizan este tipo de fuente de poder por sus tamaños que son pequeños y sus altas potencias de salida (200W en promedio).

- Cuando ocurre una interrupción del suministro eléctrico, el FERRUPS compara la capacidad de las baterías respecto a las cargas conectadas a él e indica de acuerdo a esto el tiempo que el UPS puede dar alimentación a los equipos protegidos.

- Posee un panel de control que permite leer alarmas, revisar los valores de los parámetros y hacer operaciones manuales de control.

- Adicionalmente tiene un puerto de comunicaciones RS-232 con velocidades seleccionables de 300, 1200, 4800 y 9600 Baudios.

- Las alarmas se pueden leer en el panel de control y adicionalmente el FERRUPS emite una alarma auditiva.

- Existe un registro de alarmas y un registro de las veces que ha funcionado el inversor. Estos registros ayudan a determinar cuando han existido las alarmas, de que tipo han sido y cuando y por qué el FURRUPS ha funcionado en modo de inversor.

- Existe una opción mediante la conexión del FERRUPS al equipo protegido para que en caso de agotamiento de las baterías por exceso de tiempo de soporte, se realice un apagado programado (SHUTDOWN) del equipo protegido.

- Se pueden programar ciertos valores de los parámetros de acuerdo a la necesidad del usuario, vía panel de control.

El FERRUPS opera en uno de cuatro modos disponibles: "Auto", "Inverter", "Line Condition", y "Off". Se puede cambiar de modo vía panel de control o vía enlace serial con un computador.

Modo "Auto": Es el modo normal de operación. En este modo el transformador ferroresonante acondiciona el voltaje hacia las cargas y está listo a pasar a modo de inversor en caso de falla del suministro eléctrico.

Modo "Inverter": Es el modo de inversor en donde las baterías proveen de energía al inversor que da el voltaje AC a las cargas a través del transformador ferroresonante.

Modo de "Line Condition": Este modo es un simple acondicionamiento de la línea de entrada a través del transformador ferroresonante, es decir el UPS sólo hace el papel de un regulador de línea. El FERRUPS pasa a este modo si el voltaje de las baterías está demasiado bajo. Si el suministro eléctrico falla, las cargas se quedan sin suministro.

Modo "Off": En este modo no se suministra electricidad a las cargas, pero el microprocesador sigue sensando los valores de los parámetros voltajes, corriente, frecuencia, etc., mientras exista voltaje DC de las baterías. El FERRUPS va automáticamente a este modo de apagado si no existe suministro eléctrico y las baterías están agotadas, o si ha existido una sobrecarga prolongada.

Algo que se debe considerar al adquirir un equipo de este tipo por su alto costo es el soporte técnico local e internacional que se puede obtener.

La opción de poder reprogramar los parámetros de acuerdo a las necesidades del usuario lo convierten en un UPS muy versátil. Generalmente viene con los parámetros pre-programados de fábrica para condiciones de trabajo en los Estados Unidos. Uno de los principales inconvenientes en nuestro medio es la variación de frecuencia de la red pública, principalmente cuando hay estiaje, o cuando existen apagones y los generadores varían la frecuencia de acuerdo a la carga conectada a ellos; esto produce que el FERRUPS de acuerdo a los parámetros de fábrica se vaya a modo de inversor, y estas variaciones prolongadas hacen que el inversor agote las baterías. Para evitar

este problema se procede a reprogramar las frecuencias de tolerancia del FERRUPS dando una mayor posibilidad de variación. Actualmente está programado entre 57 y 63 Hz, los parámetros de fábrica eran de 59.5 a 60.5 Hz.

Las principales desventajas de este UPS ferroresonante frente a los convencionales son el gran tamaño, la alta disipación de calor y el ruido. Todo esto se justifica para ambientes hostiles de trabajo, en que el ruido eléctrico, las variaciones de voltaje y de frecuencia, requieren de una adaptación de línea y una cobertura de falla en el suministro eléctrico.

Adicionalmente, es necesario poner un UPS secundario que puede ser "BY-PASS" a los equipos conectados a este UPS principal en caso de cortos mantenimientos del FERRUPS.

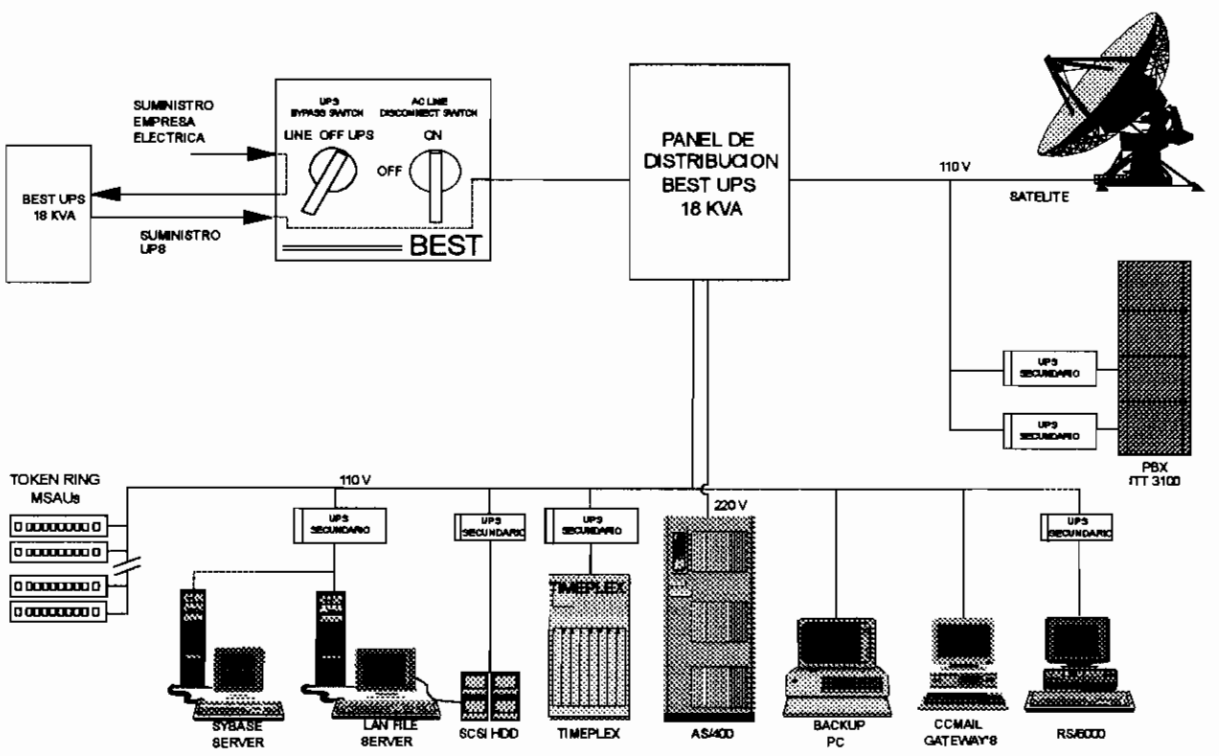


Figura 2.1. Diagrama de suministro del UPS a los equipos de la red de datos.

La figura 2.1 muestra como están conectadas las cargas al panel de distribución. Adicionalmente en esta figura se puede ver que existe un UPS secundario que brinda protección a los equipos en caso de falla del UPS principal.

El Centro de cómputo posee un tablero de alimentación al UPS que viene directamente del tablero general de medidores, en caso de cortocircuito en el UPS o antes del UPS este tablero prevee la protección contra sobrecargas y cortocircuitos.

El centro de cómputo posee un sistema de tierra independiente, dedicado exclusivamente a la protección de las instalaciones situadas dentro de él. De esta manera además se evita la inducción de otras cargas del edificio sobre nuestros equipos.

Antes de ingresar al UPS se tiene un conmutador de paso (by-pass switch), que conmuta la línea de alimentación hacia el UPS o hacia un segundo tablero que se tiene para distribuir la carga (tablero de distribución de carga). Este conmutador de paso sirve para que en caso de que las baterías del UPS estén completamente descargadas o el UPS esté averiado o en mantenimiento, se pueda provisionalmente aprovechar la energía eléctrica pública y seguir trabajando mientras se supera el problema.

A continuación se tiene el UPS, que es un UPS de 18 KVA, que suple la energía para todos los equipos del centro de cómputo, exceptuando el aire acondicionado[1] . Ha sido necesario el programar el UPS de tal manera de que tenga una buena tolerancia a las variaciones de frecuencia de la red de entrada. El UPS a plena carga puede soportar 10 minutos, y a mitad de carga 26 minutos; actualmente se está trabajando a un 10% de la carga, lo que da una alimentación de hasta 2.5 horas aproximadamente, el pedido del UPS se lo hizo pensando en un trabajo a media carga.

[1] La energía de respaldo del UPS es suficiente para mantener los equipos electrónicos funcionando durante poco tiempo (máximo 2 horas) y las variaciones de temperatura dentro de ese tiempo no van a ser tan grandes como para afectar el normal funcionamiento de los equipos. La energía debe aprovecharse al máximo para extender el tiempo de funcionamiento de la LAN.

El UPS (18 KVA) está configurado para suministrar tanto 120Vac como 208Vac.

Resumiendo, en caso de falla de suministro eléctrico la red y el AS/400 pueden mantenerse actualmente durante un tiempo aproximado de 2 horas y en el futuro cuando el UPS esté a plena carga el tiempo será de 20 a 30 minutos. Por su lado, las estaciones de trabajo soportarían 5 minutos sin suministro de la red pública.

2.3 SISTEMA DE SEGURIDAD CONTRA INCENDIOS

De manera general, se puede decir que una rápida detección del fuego es la base del éxito en la prevención de un desastre en un centro de cómputo. Es muy importante tener distribuidos los detectores de fuego en las zonas de mayor riesgo. Existen varios tipos de detectores: de calor, de humo, de ionización (de gases producidos por la combustión), infrarojos, etc.

Una vez detectado el fuego, pueden utilizarse tres tipos de extintores en el centro de cómputo:

- Extintores portátiles: Son manuales, y están diseñados para fuegos de origen eléctrico. El tamaño y cantidad de extintores de este tipo se puede determinar consultando los normativos para el caso. Generalmente son los más utilizados.

- Sistemas "Sprinkler": Estos sistemas para centros de cómputo deben ser del tipo de carga seca (para no dañar los equipos eléctricos). Tienen un sistema de compresión de aire que dispara la válvula, y éstas a su vez tienen un sistema automático de retardo de salida del líquido extintor, esto es debido a que si por casualidad se dispara la válvula, suena la alarma y ésta resulta ser falsa, existe un tiempo prudencial para desactivar el sistema "Sprinkler" evitando que se mojen los equipos.

- Sistemas de inundación total (Gas Halon): Estos sistemas son sólo efectivos en áreas completamente cerradas. Se extingue el fuego inundando el área con gas Halon (es un gas inerte) en un corto espacio de tiempo. Si se utiliza este tipo de sistemas, se debe reunir ciertos requisitos de seguridad del personal. Para dicho efecto es necesario editar procedimientos de alarma y evacuación basados en normas locales y nacionales. Se recomienda una alarma óptica y acústica que se active unos 30 segundos antes de empezar la inundación. Generalmente este tipo de sistemas se utiliza en zonas de alto riesgo y grandes volúmenes.

Un extintor manual a base de CO2 es recomendable para fuegos en el interior y alrededor de equipos electrónicos.

El sistema de protección contra incendios, y la planificación estuvo a cargo del departamento de seguridad industrial de OPEC basados en las normas y estándares de la NFPA[1]. El estándar NFPA 75[2] norma los procedimientos de cómo se debe proteger los computadores y equipos electrónicos de procesamiento de datos.

El sistema implementado es un sistema "sprinkler" de inundación de CO2. Este sistema es costoso, pero tomando en cuenta el capital invertido en los equipos, la importancia de los procesos que se realizan en el centro de cómputo, y la pérdida de tiempo que significaría un flagelo, se justifica una inversión de este tipo.

2.4 ACONDICIONAMIENTO AMBIENTAL DEL CENTRO DE COMPUTO

El aspecto térmico y el de humedad relativa son muy importantes para el normal funcionamiento de los equipos electrónicos. El acondicionamiento ambiental del centro de cómputo sigue las recomendaciones de los fabricantes para que los equipos trabajen en condiciones normales.

---

[1] "National Fire Protection Association" de los Estados Unidos de Norte América.
[2] Estas normas se incluyen en el Anexo 5. "Standard for the protection of Electronic Computer/Data Processing Equipment".

De manera general, se puede decir que la mayoría de especificaciones al respecto recomiendan que cuando se requieren acondicionadores de aire, por que se tienen temperaturas extremas y/o un exceso o falta de humedad, éstos deben estar diseñados para mantener la temperatura entre 21°C y 24°C y la humedad relativa entre 40% y 50%[1].

Según el estándar NFPA 75 los daños a equipos electrónicos pueden comenzar a partir de los 79.4°C (175°F), e irse incrementando a medida que aumenta la temperatura y/o tiempo de exposición.

Los daños a cintas magnéticas, discos flexibles pueden ocurrir a partir de los 37.8°C (100°F) y se puede considerar que hasta los 48.9°C (120°F) pueden ser daños recuperables; luego se vuelve más difícil la recuperación de los dispositivos a medida que aumenta la temperatura.

El exceso de humedad produce fallas en los sistemas de alto voltaje por ejemplo en monitores a color e impresoras láser. Mientras que el aire seco de humedad relativa bien baja produce acumulación de cargas electrostáticas, que en determinadas condiciones podrían alterar el funcionamiento de tarjetas diseñadas con elementos de tecnología CMOS.

Se debe tener mucho cuidado en ambientes altamente corrosivos o con excesos de partículas de carbón en el aire. Es necesario aislar el centro de cómputo del polvo, partículas de carbón y gases corrosivos; de ser así deben implementarse filtros en los ductos de entrada del aire acondicionado. Los filtros más utilizados son los de carbón activado. Los filtros usados, en lo posible, no deben ser combustibles.

[1] Valores tomados del "Manual de instalación eléctrica, térmica de IBM para el AS/400".

El equipo de aire acondicionado se selecciona primero de acuerdo a la disposición física del local, es decir si tiene o no acceso a alguna terraza, si existe la posibilidad o no de instalar ductos, para el ingreso y retorno del aire de una unidad externa. De acuerdo a la disposición física del centro de cómputo existen varias alternativas que van desde el simple aire acondicionado de ventana, hasta los sistemas complejos de aire acondicionado central, con ductos, circuladores externos y unidades externas de condensación del aire.

Lo primero que se debe definir es la disipación térmica de todos los equipos existentes en el área del centro de cómputo, así como el número de personas que van a trabajar dentro del local y calcular el volumen aproximado del centro de cómputo. Esto da una idea aproximada de la cantidad de calor por unidad de volumen que el equipo deberá disipar. Se debe tener en cuenta un factor de degradación y un margen de seguridad, además de preveer futuras demandas por expansión (adquisición de equipos y periféricos adicionales). El volumen se necesita para distribuir los circuladores a lo largo del centro de cómputo. La cantidad de calor para preveer la demanda de enfriamiento.

En las antiguas instalaciones de OPEC del edificio del Banco de los Andes, existía instalado provisionalmente un equipo de aire acondicionado de 14000 BTU en el centro de cómputo. La demanda calórica de todos los equipos era de 11000 BTUs[1] , tomando en cuenta un factor de degradación de 1.8 debido a los ductos, pérdidas por falta de aislamiento y efecto invernadero del edificio (todo cubierto de vitrales), se puede concluir que se necesitaba un aire acondicionado de por lo menos 18000 BTUs para mantener la temperatura en el límite inferior de 21°C. Con el aire acondicionado de 14000 BTU la temperatura promediaba en los 24°C.

[1] Debido principalmente al UPS (aproximadamente 5000 BTUs); luego a 3 computadores con monitores a color, cada uno de los cuales aporta con 1000 BTUs; adicionalmente se tiene el AS/400 y un equipo de comunicaciones que disipan cerca de los 3000 BTUs.

Según este análisis, la compra que realizó OPEC para las nuevas instalaciones del edificio Vivaldi estuvo bien concebida ya que el equipo ordenado es de 30.000 BTUs y con dicha capacidad puede abastecer necesidades futuras. Este sistema de aire acondicionado posee una unidad externa con ductos de ingreso y de retorno.

Este equipo fue utilizado temporalmente en el edificio del Banco de los Andes y luego reinstalado en el edificio Vivaldi.

2.5 SISTEMA DE SEGURIDAD FISICA DE LA INFORMACION

Es importante mantener copias de respaldo de la información, ya que de ésta información depende el funcionamiento de la empresa. Si no se dispone de un buen sistema de respaldos con políticas adecuadas para recuperar el sistema en el menor tiempo posible, esto podría significar una gran pérdida de tiempo y dinero.

Por tanto, el primer paso a dar es planificar y establecer políticas adecuadas de seguridad para los respaldos de la información.

El objetivo cuando ha existido un desastre es recuperar la información, de tal manera que el sistema pueda ser utilizado y que su estado esté lo más cercano posible al punto en que ocurrió el desastre. De esta manera, desde el punto de vista operativo, se puede minimizar los efectos del desastre.

En este estudio se establecerá los lineamientos de seguridad y respaldos más adecuados para la infraestructura disponible en OPEC.

Existen algunas técnicas que se pueden implementar para tener posibilidades de recuperar el sistema completo en caso de una catástrofe. Estas técnicas van de acuerdo al tipo de problema que se pueda presentar: falla del servidor de la red o de alguno de sus periféricos compartidos (Discos duros, o memoria RAM), corrupción de

datos o aplicaciones debido a virus, borrado involuntario de datos útiles para la red, entre otros.

Entre estas técnicas se tiene: servidor de respaldo, "mirroring" (discos espejados), respaldos en cintas, "checksum", jornalización, control de compromiso, auditoría, entre otras. La jornalización y el control de compromiso se utilizan generalmente en sistemas grandes tales como el AS/400 de IBM, y ellos consisten en un control en línea de las transacciones[1] .

A manera de referencia, paralelamente a la LAN se ha instalado un AS/400 en OPEC para toda el área financiera, y el departamento de materiales se ha decidido no utilizar ni el control de compromiso ni la jornalización debido a que las transacciones a realizarse son principalmente procesos BATCH[2] , no procesos en línea.

La jornalización y el control de compromiso son procesos de registro de cambios hechos a las bases de datos. Un ejemplo de esto son los sistemas de los bancos y financieras que tienen cajeros digitando información en línea, si un error ocurre, mediante el control de compromiso se puede deshacer la transacción mal digitada.

En el caso de OPEC se ha decidido realizar un control de transacciones a nivel de programa, es decir la aplicación en sí se encargará de realizar y confirmar cada transacción realizada, de esta forma se disminuye el trabajo del operador dejando este compromiso a un programa más inteligente.

Para un mejor entendimiento de las técnicas para evitar la pérdida total o parcial de la información se deben definir ciertos lineamientos generales:

---

[1] Transacción es un acceso de lectura/escritura a una base de datos, este concepto se utiliza generalmente en minicomputadores y "mainframes".
[2] Proceso diferido, utiliza colas de espera para ser atendido.

- Estar preparados para una restauración total.
- Las aplicaciones deben diseñarse para ser respaldadas y restauradas sin mayor inconveniente.
- Grabar el ambiente y configuración del Sistema.
- Respaldos rotativos.
- Grabar los cambios diarios.
- Probar y documentar los procedimientos.
- Guardar los respaldos fuera del lugar, para evitar daños por fuego, e inundaciones.

2.5.1 SERVIDOR DE RESPALDO DE LA RED

Este es un mecanismo sumamente útil para ahorrar tiempo en caso de que el servidor de la red falle totalmente o parcialmente.

Se definen dos tipos de servidores de respaldo. El primer tipo que se lo llamará total y el segundo parcial.

Un servidor de respaldo total será aquel que permite en determinado momento cuando se presenta una falla irrecuperable y total del servidor de la red, ser reemplazado inmediatamente por el de respaldo, y en un tiempo relativamente corto ser recuperado hasta por lo menos la situación del día anterior. Este servidor de respaldo total posee sus propias unidades de disco duro y controladores. Tener un servidor de este tipo involucra tener equipo e información duplicados, es decir es una inversión adicional bien alta que sólo se justificaría en donde el tiempo perdido signifique pérdidas en dinero mayores que la inversión.

Un servidor de respaldo parcial, será cualquier equipo con procesador y memoria RAM suficientes para abastecer como servidor de la red. Este tipo de servidor parcial no incluye los discos duros, es decir sólo serviría en caso de falla del servidor principal

más no de sus discos duros, tal que puedan estos discos duros trabajar con el servidor de respaldo parcial. Es una alternativa más económica, porque si se utiliza esta técnica combinada con la de los discos espejados (técnica de "mirroring", que se menciona en el siguiente acápite), se tiene una posibilidad de recuperar la información tal como con un servidor de respaldo total.

Como se menciona al inicio de este capítulo, existen varios niveles de desastre y de acuerdo a ello se expuso el efecto que tendrían esos niveles sobre las operaciones de OPEC:

Si llegaran a fallar el servidor de la red, los discos duros originales y sus gemelos espejados (mirroring), existe un servidor de respaldo total. Este servidor de respaldo se actualiza mensualmente, y luego se lo puede actualizar a partir de las cintas de "backup". Este tipo de falla se minimiza hasta el estado del día anterior a las 10 pm.

En caso de que el servidor de la red falle y no sus discos duros se tiene un computador preparado como servidor de respaldo parcial, para que en este caso pase a ser servidor de la red utilizando los mismos discos duros. Este problema se minimiza al perder la red por un lapso corto en el orden de decenas de minutos, pero la red seguiría trabajando aunque un poco más lenta, por la menor capacidad del procesador.

En OPEC se utilizan ambas técnicas para no descartar una falla de los discos duros que significaría, en caso de no tener el servidor de respaldo total, una pérdida significativa de tiempo, ya que la información tendría que ser recuperada totalmente de cintas y esto podría tomar varios días.

2.5.2 UTILIZACION DE LA TECNICA DE DISCOS ESPEJADOS

Esta técnica se utiliza para prevenir los efectos de falla de un disco duro de RED, y consiste en implementar dos discos duros gemelos, en los cuales el servidor escriba en

ambos al mismo tiempo y tome lecturas alternadas. En el caso de falla de un disco duro, automáticamente entra a funcionar el otro disco espejado.

Esta técnica está implementada en NetWare de Novell desde la versón 2.15 SFT en adelante, tal como se la describe en el capítulo anterior.

Una práctica recomendada para facilitar el control de la información, es la de establecer volúmenes (en lenguaje de DOS, particiones) en el disco de red para poder clasificar el flujo de información a determinadas partes del disco, y saber con un buen grado de precisión el tipo de información almacenado en él.

La principal desventaja de esta técnica es que el rendimiento del equipo es bajo, y el costo de un disco de red es alto (generalmente son discos SCSI de gran capacidad).

Otra técnica alternativa pero todavía poco utilizada a nivel de LANs es el CHECKSUM. Para implementarlo es necesario que la red tenga múltiples unidades de disco duro, y se establecen áreas dentro de cada disco duro para almacenar ciertos códigos de control de "checksum", en la cual se almacena la información de todo el conjunto de discos duros, y luego, si algún disco duro falla se puede restablecer completamente dicho disco en base a la información almacenada en los demás. Esta técnica tiene una mayor aplicación en los sistemas IBM, en toda la familia AS/400.

2.5.3 UTILIZACION DE EQUIPO PARA RESPALDO EN CINTAS MAGNETICAS

Es menester hacer un plan escrito de respaldos y recuperación para que en el momento que ocurra un desastre, exista un procedimiento de como recuperar el sistema. La planificación ahorra tiempo y dinero a la empresa.

Los ambientes a considerar para un buen respaldo son: el sistema y su configuración, los directorios de los utilitarios y compiladores, directorios de producción (Datos y

programas de aplicación), directorios de desarrollo, documentos y archivos del usuario final.

Entre los principales respaldos se tiene el "OFF-LINE BACKUP"[1] . Generalmente este "Backup" se lo realiza en cintas magnéticas de gran capacidad y de preferencia fuera de los horarios de oficina (si existiesen archivos abiertos no serían grabados).

No obstante, los requerimientos de OPEC se encaminan hacia cintas de alta capacidad y tiempos de almacenamiento bajos. Características que reunen las unidades de cintas de 8mm, a pesar de su alto costo se justifica por el menor tiempo requerido para realizar los respaldos y por su gran capacidad de almacenamiento.

Con una sola cinta se puede almacenar todos los cambios suscitados en el sistema durante un día, tal que los respaldos pueden hacerse sin interrupción y de forma automática, ya que no necesita de un operador para que esté realizando los cambios de cintas que otras unidades de menor capacidad requieren. Adicionalmente, como son unidades rápidas, hacen el respaldo en menor tiempo que otras unidades, característica indispensable porque para esta tarea se dispone solamente de 12:00 de la noche a 4:00 de la mañana[2] .

En OPEC se ha escogido como un estándar internacional las cintas de 8mm, con barrido helicoidal[3] , que permite almacenar en cada cinta 2.2 GB.

La marca de la unidad de cinta es PALINDROME, que utiliza un interfaz SCSI[4] y está conectada a un computador dedicado durante toda la noche a hacer respaldos de ciertos procesos y el respaldo total de la red.

---

[1] Respaldo fuera de línea.
[2] Los reportes diarios de producción desde el CPF se transmiten a partir de las 4 a.m.
[3] Técnica utilizada en cintas de video que consiste en una conversión digital / análoga.
[4] Small Computer System Interface.

El programa ("software") de respaldos también es de la compañía PALINDROME cuyas funciones principales se definen a continuación.

Este es un sistema de almacenamiento inteligente, que automatiza e integra las tareas más importantes de almacenamiento de datos:

RESPALDO
ARCHIVAR
RESTAURAR
ADMINISTRACION: HORARIO DE CINTAS ROTACION DE VOLUMENES DEPURAR EL DISCO DURO

El programa que maneja e integra todo es el "network Archivist" (El archivador de Red). Este programa también integra la información de la base de datos con las opciones de configuración seleccionadas por el usuario.

El NA ("Network Archivist") muchas veces es referido como un sistema experto debido a su inteligencia y funcionabilidad; toma sus decisiones en base a algoritmos que monitorean la base de datos y compara con lo que estaba antes, adicionalmente revisa las reglas que determinan cómo se debe tratar o qué se debe hacer con los archivos.

RESPALDOS ("backup"). Es el proceso de copiar los archivos a cinta para protegerlos de un desastre a corto plazo, o que sean borrados accidentalmente. El NA chequea la última versión del archivo y la respalda, es decir puede tener múltiples versiones del mismo archivo. Establece una secuencia de rotación de acuerdo a su configuración y nos dice la cinta que corresponde.

ARCHIVO (Archiving). Es el proceso de almacenar copias permanentes de los archivos a cinta con el fin de hacer una recuperación a largo plazo. Cuando un archivo no ha sido modificado en 6 semanas, el NA lo declara como ESTABLE. Luego, lo graba automáticamente a cinta, cuando un archivo estable ha sido grabado por lo menos a 3 cintas diferentes, se lo declara totalmente protegido.

RESTAURACION (Restoration). Este proceso le permite rápidamente copiar un archivo, una serie de archivos o un volumen completo de cinta, a la localización previa en disco (o puede ser una nueva localización). Para restaurar, el NA le da todas las versiones disponibles de ese archivo, con el tamaño y la fecha y automáticamente indica en que cintas se encuentra la copia de ese archivo. Puede presentar un catálogo en línea de los archivos almacenados en la cinta y hasta restaurar volúmenes completos.

ADMINISTRACION DE DATOS[1] . Automatiza la rotación de cintas, la rotación de volúmenes[2] y la migración de archivos.

Automatiza el proceso manual de rotación de archivos, determina la cinta a utilizarse para cada respaldo, cuando comenzar con nuevas cintas y cuando retirar las cintas viejas.

El modelo de rotación se basa en un algoritmo que garantiza una aproximación organizada y sistemática para la planificación de horarios de las cintas.

El NA pregunta por la cinta correcta, en el caso de no ser la correcta y es una operación automática, lo que hace es ajustarse de acuerdo a la cinta que está y mantiene la integridad de la biblioteca de la cinta.

---

[1] Para mayor detalle referirse al Anexo 7.
[2] Volúmen en este punto se define como un conjunto de cintas.

La rotación de volúmenes consiste en rotar las cintas y ponerlas en un lugar seguro para protección contra desastres. Cuando necesita dicha cinta el NA avisa con anterioridad.

Se puede migrar archivos, pero deben cumplir las siguientes condiciones:

- El archivo tiene que estar completamente protegido (grabado al menos 3 veces en cinta).

- El archivo debe tener un mínimo de 12 semanas sin ser accesado.

Se puede requerir una lista de archivos aptos para migración.

De esta manera el NA tiene un control inteligente de la información almacenada, y permite recuperar parcial o totalmente la información.

Por ejemplo, en caso de pérdida de "software" (datos o programas de aplicación), se tienen los respaldos ("backups") diarios de todos los volúmenes de la red. El procedimiento de recuperación de dicho "software" sería transferir su información de las cintas. La incidencia de este tipo de problema sobre las operaciones de OPEC de manera general no son muy considerables ya que se puede recuperar la información hasta lo que se hizo el día anterior hasta las 10 pm.

CAPITULO 3

3. OPTIMIZACION DE LA RED

Optimizar podría entenderse como lograr buenas condiciones de operación de un sistema al menor costo.

Una primera forma de optimización se logra mediante un análisis técnico-económico que permita definir las condiciones, procesos y equipos más adecuados de acuerdo a las necesidades de la empresa.

Otra forma de optimización sería, que una vez definidos todos los elementos que constituyen el sistema se proceda a "afinar" los procesos para poder obtener un mejor rendimiento.

En el caso de OPEC se dispone de un sistema ya establecido, es decir, se tienen que "afinar" los procesos para mejorar su rendimiento. Sin embargo, aunque no tan frecuente, cuando se necesite expandir el sistema se debe realizar un análisis técnico-económico de acuerdo a las necesidades de la empresa.

Para optimizar la LAN de OPEC, se debe trabajar tanto en la parte operativa como en el mantenimiento de la misma. Como dice una conocida frase en los medios industriales: "Sin mantenimiento no hay producción".

En otras palabras, se debe hacer una planificación de dos aspectos fundamentales de la LAN: sus prestaciones y su mantenimiento.

Dentro de las prestaciones de la red se tienen los servicios que dicha red brinda a los usuarios y el acceso que se puede lograr mediante ella a otras plataformas de trabajo.

El otro aspecto fundamental es el mantenimiento a realizar, como en cualquier sistema, sea este mecánico, eléctrico o informático.

En el caso de la red existen estos tres tipos de mantenimiento: mecánico en lo referente a la conexión física de los equipos, sus conectores y cableado del cual depende en gran parte el éxito en la administración de la red; eléctrico, el funcionamiento correcto de los equipos que conforman la red; y el informático, que se refiere al manejo y control de la información, de tal manera que la red mantenga un buen nivel de velocidad y la capacidad de almacenamiento de datos sea bien aprovechada.

3.1 SERVICIOS

Como ya se mencionó en los capítulos precedentes, la razón de ser de una red es la de dar servicios a sus usuarios, para optimizar sus recursos de espacio en disco y programas de aplicación, impresión y tiempo de trabajo.

3.1.1 COMPARTIR PROGRAMAS DE APLICACION Y DATOS

Es común oir en el lenguaje informático para algún programa de aplicación que puede ser denominado como "versión red" o "versión monousuario".

Se puede decir que existen estos dos tipos de versiones de los diferentes programas que existen en el mercado, y dependiendo de múltiples factores se hace necesario el establecer qué es lo más conveniente a instalar dentro de la red (si se obvia las razones legales). Para el caso de una LAN y dentro del marco legal no existe otra alternativa que comprar un programa en "versión de red" para ser instalado en el servidor, caso contrario debería comprarse versiones monousuarios para ser instaladas en cada una de las estaciones de trabajo, lo cual resultaría sumamente caro y se desperdiciaría mucho espacio en cada disco duro de las estaciones de trabajo.

En una red Netware existen servidores y estaciones de trabajo. En el servidor se podrían instalar tanto las versiones de red como las versiones monousuario, pero en las estaciones de trabajo se recomienda instalar sólo las versiones monousuario por obvias razones (la versión de red es mucho más cara, y sólo estaría usándose en una estación de trabajo).

Para continuar éste análisis, se necesita establecer un concepto adicional que es el de "licencias". Tener una licencia significa que ese programa puede ser utilizado simultáneamente sólo por una persona, es decir el número de licencias define el número de usuarios simultáneos que pueden existir en la red. En compañías transnacionales, la parte administrativa se cuida mucho de encuadrarse dentro de las leyes de derechos de autoría y licencias.

Dentro del marco legal, es estrictamente prohibido y penado por la ley el uso de versiones monousuarios en el servidor de la red sin contar con las restricciones del caso, porque permitiría que varios usuarios puedan trabajar simultáneamente con dicho programa sin contar con las licencias respectivas.

Con un programa en "versión red" se tiene la ventaja de poder establecer un control de las necesidades de los distintos programas de aplicación. Por tanto, es posible cuantificar las necesidades de los usuarios y de acuerdo a ello incrementar el número de licencias que se necesitan.

Actualmente se puede encontrar en el mercado programas utilitarios para red, que permiten hacer estadísticas del uso de los distintos programas de aplicación, e ir determinando el crecimiento y las necesidades de licencias según dichos análisis.

Existen otros tipos de utilitarios como por ejemplo el LANMETER de NOVELL que permite hacer un monitoreo total de la red: velocidad, estadísticas de funcionamiento y localización de fallas que se puedan presentar (en tarjetas de red, MAUs, conexiones, etc). Este tipo de utilitario es costoso, sólo se justificaría su adquisición para la administración de redes grandes y complejas.

Como ya se mencionó, existen varios tipos de redes de diferentes fabricantes, topologías, sistemas operativos, etc. Los diferentes programas de aplicación "versión red" ven de una forma transparente la topología de la red, más no el sistema operativo para el cual vienen definidos. NetWare es el sistema operativo de mayor difusión a nivel mundial, razón por la cual la mayoría de los programas de aplicación se pueden encontrar para este sistema operativo a precios razonables.

Para el caso de archivos de datos, el sistema operativo es el encargado de establecer los tipos de seguridades. Es decir, establece los derechos de los usuarios sobre el archivo.

Adicionalmente, NetWare realiza un control para que no se pueda modificar un archivo simultáneamente y de esa manera se evita que se pierda tiempo de trabajo de uno o varios usuarios. Por ejemplo si cinco usuarios tienen derechos de modificar un archivo (las cinco personas pueden verlo simultáneamente, pero no modificarlo), el único que podrá modificarlo es la primera persona que lo abrió, de tal manera que si alguien más requiere modificarlo, lo hace ya en base al primero que lo modificó, evitándose que todos modifiquen algo al mismo tiempo y la única modificación que quede sea la del último que grabó.

NetWare utiliza ciertos registros denominados banderas para establecer este tipo de control. El Supervisor de la red puede ir a la consola y ver el "status" de cada uno de los usuarios, ver que aplicación y qué archivo de datos está usando, y el tiempo que ha estado utilizando dicha aplicación.

Adicionalmente, se puede establecer accesos de grupos de usuarios a ciertos directorios comunes, los denominados "SHARE", para que puedan guardarse archivos de común interés. Por lo general, dentro de la estructura de la red cada usuario tiene asignado un directorio privado al que sólo él y el supervisor tienen acceso (dependiendo de las políticas de la empresa).

A cada usuario se le asigna un espacio en el disco del servidor de archivos de la red. De esta forma se tiene un control permanente del espacio con que se cuenta para cargar nuevas aplicaciones o para realizar labores de operación o para seguir aumentando el número de usuarios. Mediante este control se evita que se caiga la red por "overflow"[1] .

Los discos duros del servidor de archivo, generalmente son de gran capacidad (muchas veces en el orden de los GB, dependiendo de las necesidades de la red), con interfaces SCSI, y sus costos son muy altos (en el orden de los miles de dólares).

Es recomendable que el usuario, por razones de optimización de espacio en los discos de red, tenga los archivos estrictamente necesarios, y utilice el disco duro de la estación de trabajo para el resto de información secundaria.

Una deficiencia de NetWare 3.11 y versiones precedentes, es que no se tiene accesibilidad a los "discos duros" locales de las estaciones de trabajo. Al no tenerse acceso a dichos "discos duros" locales, no se puede hacer un "backup" centralizado y automático de ellos, dejándose esa tarea a cada usuario individualmente para que la realice en "diskettes".

Como una medida compensatoria se recomendaría adquirir una unidad de cinta de 250 MB con conexión al puerto paralelo para realizar "Backups" en cinta de los discos duros locales, según lo requieran los usuarios. De tal forma que el usuario pueda pedir cada cierto tiempo un "backup" de la información almacenada en la estación de trabajo y que la cinta de respaldo de dicha información quede con él.

3.1.2 COMPARTIR IMPRESORAS PARA LAS DIFERENTES APLICACIONES

NetWare permite el compartir impresoras, tal como se explicó en el capítulo 1 cuando se mencionó al sistema operativo NETWARE.

[1] Desbordamiento por falta de espacio en el disco duro de la red.

En el caso de OPEC se tiene un servidor de impresión que físicamente está localizado en el mismo servidor de archivos. Es decir, el servidor de archivos de la red es, adicionalmente, servidor de impresión. Esto se puede hacer cuando se tiene un servidor de archivos con un procesador y capacidad de memoria suficientes para mantener un buen nivel de funcionamiento de la red, en caso contrario se necesitaría definir servidores de impresión dedicados.

NetWare tiene la característica de poder cargar ciertos NLM[1], como por ejemplo la de funcionar como consola[2] remota desde cualquier estación de trabajo. Se debe considerar que todo módulo NLM requiere memoria adicional y no se recomienda tener muchos NLM en el servidor, ya que degradaría la velocidad y el funcionamiento mismo de la red.

Cuando se tiene una configuración como ésta, en donde el servidor de impresión está como un NLM funcionando en el servidor de archivos, se tiene un limitante de 16 impresoras como máximo, aún cuando sea un servidor dedicado. Cada servidor dedicado en esta versión de NetWare permite conectar hasta 16 impresoras. Según ciertos artículos, las versiones más recientes de NetWare van a permitir conectar un número indefinido de impresoras.

Por tanto, cuando se tiene un número de impresoras mayor a 16 es necesario implementar un servidor de impresión dedicado adicional.

En ambos casos, es necesario implementar impresoras remotas (que no están directamente conectadas al servidor de impresión), por tanto se necesita de estaciones de trabajo que enruten las impresiones a las distintas impresoras de red. Para esto, en la estación de trabajo que hará la función de enrutamiento de las impresiones, se carga un programa que se llama RPRINTER, en donde se define la impresora de red remota a ser conectada a este computador.

---

[1] NetWare Load Modules, son módulos de "drivers" que realizan funciones específicas complejas.
[2] La consola se encuentra en el servidor y permite monitorear el estado de la LAN.Una consola remota permite monitorear la red desde cualquier estación de trabajo en caso de emergencia cuando el supervisor se encuentra lejos del servidor.

Precisamente éste ha sido uno de los dolores de cabeza más grandes en la administración diaria de la red:

El RPRINTER es un programa que queda residente en la memoria de la computadora que tiene conectada la impresora remota. Dicho RPRINTER entra en conflicto algunas veces con otros programas residentes. Se tuvo el caso en que el RPRINTER entraba en conflicto con Windows, es decir cuando estaba "cargado" el RPRINTER, y luego se entraba y se "cargaba" Windows, automáticamente se "descargaba" el RPRINTER de memoria (debido a que Windows establece una administración de memoria distinta a la del DOS). Cuando se descarga de memoria el RPRINTER, la impresora deja de imprimir y se comienzan a acumular la impresiones en la cola de impresión correspondiente a dicha impresora en el servidor de impresión.

No existe solución sencilla a este problema, más adelante se revisa este asunto y la solución a la que se llegó.

Otro de los problemas que se presentan casi a diario como consecuencia directa del problema anterior con el RPRINTER es que, generalmente los operadores de las estaciones de trabajo que tienen las impresoras remotas tienen un conocimiento muy limitado de NetWare, tal que al descargarse el RPRINTER, ellos "corren" el RPRINTER y seleccionan otra impresora, o algunas veces están trabajando en otra computadora (que no tiene impresora remota) y cargan el RPRINTER, bloqueando el uso de esa impresora.

Para solucionar esto se decidió limitar el acceso al RPRINTER solamente a las computadoras que tienen impresora remota conectada. Mejoró mucho, la frecuencia con que se daban estos problemas bajó considerablememnte, pero no era como para estar satisfechos, ya que muchas veces se imprimía información que iba destinada a otra impresora con el agraviante que algunas impresiones eran confidenciales.

Se continuó en la búsqueda de una solución definitiva hasta que finalmente se encontró en el mercado estadounidense dos tipos de "hardware" adicional que facilitan la

administración de impresión en una red NetWare y evitan los dos problemas mencionados.

Estas alternativas de "hardware" permiten conectar las impresoras directamente al anillo (de un MAU a la impresora) y son: la tarjeta Token-Ring de la Hewlett Packard "JETDIRECT", y de INTEL el "INTEL-NETPORT".

La tarjeta HP JETDIRECT se introduce en las impresoras láser, en un "slot" de expansión, y están diseñadas para modelos LaserJet IV en adelante. Mientras, que los INTEL NetPort pueden utilizarse con las impresoras precedentes a la LaserJet IV (es decir con las láserJet III, y IIIP), y adicionalmente permite conectar dos impresoras al interfaz, en vez de una como en el caso de la tarjeta JetDirect. Pero como el costo de los Intel NetPort es mucho mayor, se optó por comprar los INTEL NetPorts estrictamente necesarios para conectar las impresoras más antiguas (LáserJet III, y IIIP).

Cada uno de estos dos dispositivos posee un "software" que interactúa con el sistema operativo NetWare, y para ser más precisos con el PCONSOLE, que es el programa de NetWare que permite administrar las impresoras, colas de impresión, usuarios, administradores de las colas de impresión, mensajes de problemas de impresión, etc.

Con estos dos dispositivos, al conectarse directamente al anillo, se evita el tener que usar computadoras para enrutar la impresión mediante el RPRINTER y se obvian los errores humanos de operación. Estos dispositivos tienen almacenado en memoria ROM el programa equivalente al RPRINTER. La confiabilidad de las impresiones aumentó casi a un 100 %.

Con esto se dió solución al problema del RPRINTER y adicionalmente se evitó el instalar un segundo servidor de impresión (ya que se tienen 20 impresoras de red que sobrepasa las 16 impresoras permisibles para un servidor de impresión), debido a que cada Intel-NetPort puede trabajar en modo de servidor de impresión y/o impresora remota, administrando cada uno de sus dos puertos de forma independiente.

3.1.3 CORREO ELECTRONICO

El estándar de OIEPC[1] desde 1982 es el CC:MAIL de LOTUS. Actualmente se tiene una red internacional privada de más de 1000 usuarios, distribuidos en 15 países alrededor del mundo en cuatro continentes. Este es un "software" muy versátil que permite una comunicación rápida y eficaz entre Quito-Tulsa y Quito-CPF.

La topología de esta red de correo electrónico, tal como ha sido estructurada es en estrella. La central internacional de comunicaciones se encuentra en Tulsa, es decir, todo mensaje que sale de un país pasa por Tulsa para ser enrutado al país destino. Por ejemplo, si se quiere mandar un mensaje a Bogotá, dicho mensaje va desde Quito a Tulsa y de Tulsa regresa a Bogotá. Este diseño involucra altos costos de transmisión, pero se evita el tener tareas administrativas muy complejas a nivel de los 14 países conectados con Tulsa (ya que la complejidad de la administración se centraliza en EEUU), lo que significa un ahorro de personal para ejercer específicamente dichas labores en cada uno de los países (nodos) conectados a la red.

Este programa permite transmitir mensajes, y archivos del DOS (documentos de procesador de palabras; hojas de cálculo, etc.), brindando además un interfaz muy sencillo en base a menúes para archivar, guardar mensajes temporalmente, direccionar un usuario o una lista de ellos, establecer prioridades, editar, responder a un mensaje, etc.
Es un programa muy seguro, para poder accesar a él se necesita estar creado como usuario, escribir el nombre del usuario (tal como está creado en la base de datos) y la respectiva contraseña de entrada.

Dentro de la misma red, en otras palabras, en la LAN los mensajes son transmitidos inmediatamente, pero cuando el mensaje tiene que salir al exterior, según su prioridad tienen intervalos de salida. Los mensajes más urgentes salen con mayor frecuencia, luego los de prioridad normal, y por último los de baja prioridad.

---

[1] Occidental International Exploration and Production Company.

La transmisión de los mensajes fuera de la LAN se la realiza a través de un "gateway"[1] de comunicaciones, dicho "gateway" es un computador dedicado que tiene un programa de comunicaciones funcionando permanentemente.

Este programa es el "cc:Mail Gateway", que se utiliza tanto para recibir como para transmitir los mensajes. Dentro de su configuración se establecen los horarios, direcciones (números telefónicos), frecuencias de envío y tamaños máximos de los mensajes.

En la conexión física más sencilla, el "gateway", se conecta a un modem (V.32o V.42)[2] a través de uno de sus puertos seriales asincrónicos con interfaz RS-232, y éste a su vez a la línea telefónica. Es decir, en este caso la transmisión se la realiza vía red telefónica (Red pública de EMETEL). Esta configuración fue la primera en utilizarse en OPEC, actualmente se la tiene como un sistema de respaldo en caso haya problemas con el equipo de comunicaciones vía satélite.

Cuando se tiene un sistema privado de comunicaciones (PBX y líneas internas entre PBXs), se pueden realizar configuraciones más óptimas que aprovechan estas líneas internas (tie lines)[3] .

A continuación se presenta un gráfico en detalle de la configuración del sistema de comunicaciones vía satélite (figura 3.1), que muestra como están interconectados los distintos componentes del sistema de comunicaciones vía satélite, los PBX, los "fax servers" , los "cc:Mail gateways" y el "cc:Mail Remote" .

Se usa para el correo electrónico un canal de datos a Tulsa y un canal al CPF, el segundo canal de datos se lo utiliza para el "fax server" (tanto a Tulsa como al CPF).

---

[1] Ver glosario.
[2] Normas establecidas por el CCITT para comunicaciones seriales asíncronas.
[3] Líneas dedicadas a enlazar dos PBX. A través de ellas pasa todo el tráfico telefónico entre las dos PBX.

En el caso de que fallen los canales de datos se tienen tarjetas de datos QSC[1] de respaldo, o se podría usar uno de los canales de voz ("tie lines") ya sea a Tulsa ó al CPF con la configuración de modem descrita anteriormente.

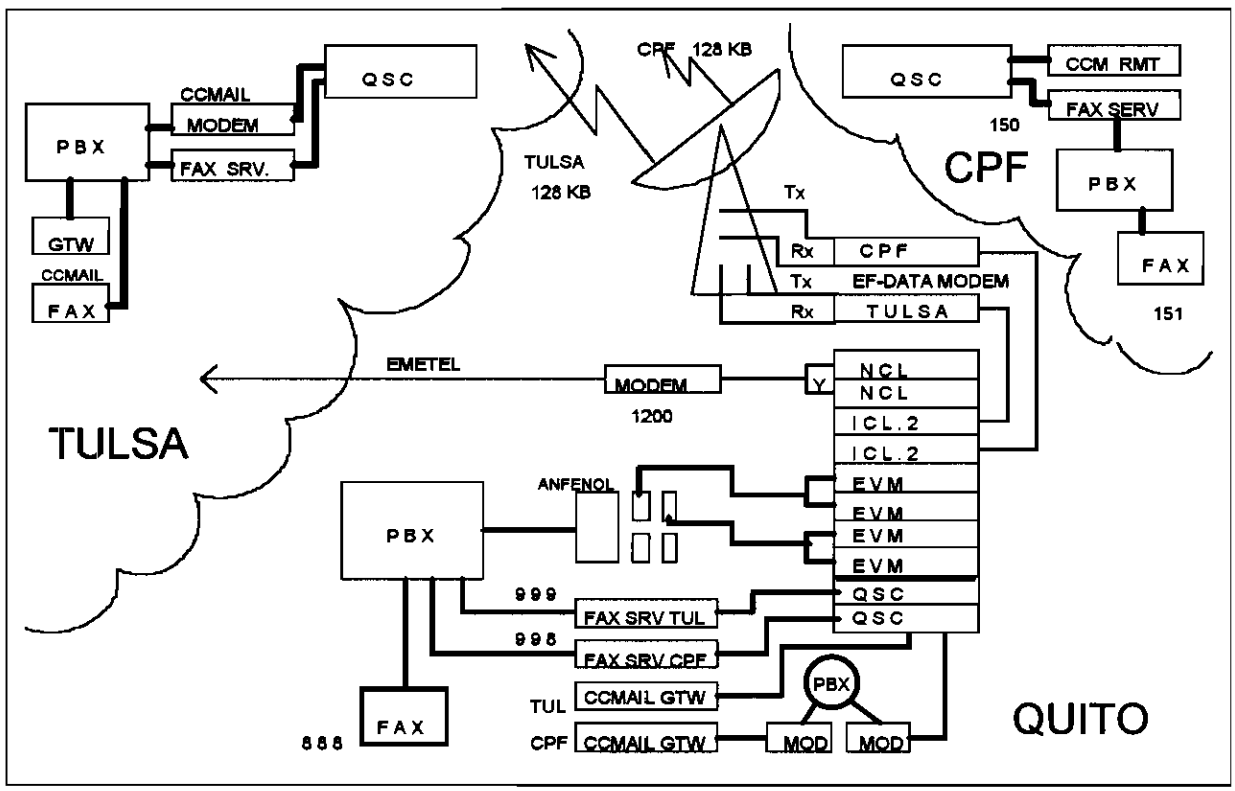


Figura 3.1. Componentes del sistema de comunicaciones vía satélite.

Desde el punto de vista operativo, para la conexión física del "cc:Mail Gateway" a través del enlace vía satélite se tienen que considerar dos casos distintos, el primero para el enlace con Tulsa y el segundo con el CPF.

En el primer caso, éste está conectado directamente, es decir la conexión se la realiza mediante un cable desde un puerto RS-232 del "gateway" a un puerto de la tarjeta QSC. Se lo realiza de esta manera porque en Tulsa existe un "gateway" (con un modem interno) dentro de la red. El proceso funciona de la siguiente manera: los datos llegan a la QSC de Tulsa provenientes de Quito, éstos pasan a través del modem que corresponde a Ecuador, marcando una extensión telefónica (desde el "cc:Mail gateway"

[1] Tarjetas de datos que configuran el TIMEPLEX. Ver capitulo 1.

de Quito) se comunica con el modem interno del "cc:Mail gateway" de Tulsa, y se establece la comunicación y transmisión de los mensajes. En otras palabras el modem correspondiente a Quito está en Tulsa en vez de estar en Quito al lado del "gateway". Por tanto en Tulsa existe un modem que corresponde a cada uno de los "gateway" alrededor del mundo en donde tiene oficinas OIEPC. El número de "cc:Mail gateways" en Tulsa depende del tráfico de los diferentes países que pueda manejar cada uno de ellos. Actualmente existen dos "gateway" en Tulsa que atienden y enrutan todo el tráfico del correo electrónico de todas las filiales.

Para el CPF se tiene el caso contrario, acá en Quito se tienen los dos modems, el correspondiente al CPF, que marca a través de la PBX de Quito a una extensión correspondiente al modem del "cc:Mail gateway" de la red de área local de Quito, es decir existe un sólo computador en el CPF que se conoce como el "CPF Message Center", al cual los usuarios deben acudir para hacer uso del servicio de correo electrónico (en el gráfico está representado como CCM RMT que quiere decir "cc:Mail Remote"). En el Oriente no existe una LAN, por tanto no se puede instalar un "gateway", porque éste solo tiene sentido en caso de una LAN, por tanto se utiliza un programa que permite a un computador remoto comunicarse con un "gateway"; este programa se llama "cc:Mail Remote".

La experiencia ha demostrado que tener este sólo computador ocasiona muchas molestias a los usuarios en el campo, porque las distancias son grandes y las necesidades de correo electrónico han ido creciendo, igual que el número de computadores allá, a tal punto que se ha decidido cambiar la configuración e invertir los papeles, y poner ambos modems en el CPF. La conexión funciona de la siguiente manera: el usuario que tiene un computador y un modem puede marcar a una extensión de la PBX que corresponde al modem de Quito, que está conectado a la tarjeta QSC del TIMEPLEX del CPF y se enlaza directamente a la QSC de Quito y al "cc:Mail gateway" de Quito (tal como funciona en el diagrama la conexión Quito-Tulsa). De esta manera se optimiza el uso de los computadores que se encuentran en el CPF y en los pozos, agilitándose la transmisión de los datos de producción, ajustándose de mejor manera a las necesidades de la gente que labora en el campo.

Adicionalmente, se puede decir que los puertos Asincrónicos/Sincrónicos de las tarjetas QSC del TIMEPLEX tienen un mayor rendimiento en cuanto a velocidad de transmisión cuando trabajan en modo sincrónico (por obvias razones), por tanto se ha instalado conversores asincrónicos/sincrónicos a las salidas de los puertos RS-232 de los "cc:Mail gateway", para que la entrada a las tarjetas QSC sea sincrónica.

Como un dato adicional, se debe analizar la probabilidad de instalar un multiplexor adaptivo para el TIMEPLEX para aprovechar de mejor forma el ancho de banda del enlace, según la información que se está transmitiendo en el momento.

Como un consejo práctico se puede decir que es necesario que se tenga muy en cuenta el tipo de modem y la marca que se utiliza. Muchas veces por ahorrar un poco de dinero se compra modems baratos, que a corto plazo representan muchos dolores de cabeza. OIEPC a nivel internacional ha adoptado MULTITECH como un estándar, cierto es que en el mercado se pueden encontrar modems a mitad de precio, pero la experiencia en Quito y en el Oriente ha demostrado que muchos de esos modems baratos presentan mucha vulnerabilidad al ruido y otros problemas que los convierten en verdaderos pasatiempos. Por tanto, es recomendable trabajar con productos conocidos si es que se quiere ahorrar tiempo en la instalación y tener un enlace de mejor calidad.

BASE DE DATOS DE CC:MAIL

Para finalizar esta reseña acerca del correo electrónico es necesario establecer un procedimiento para mantener la base de datos de la "oficina postal" que se encuentra en el servidor de la red. Para estos fines cc:Mail dispone de una serie de utilitarios que sólo pueden ser utilizados por el administrador del correo electrónico, que en el caso de OPEC corresponde al mismo supervisor o al operador de la LAN.

Deben establecerse políticas de limpieza de los mensajes obsoletos, es decir, mensajes que tengan más de 30 días y que ya hayan sido leídos deben ser removidos

de la oficina postal. Después de eliminar dichos mensajes es necesario optimizar la base de datos para compactarla y eliminar ciertas cadenas perdidas que se pueden generar a partir de la limpieza.

3.2 MANTENIMIENTO Y OPERACION DE LA RED

Es muy importante definir criterios de mantenimiento del sistema, ya que de un buen mantenimiento depende el éxito de éste.

Dar mantenimiento es "mantener" el equipo en perfectas condiciones de operación. En este sentido se debe diferenciar dos tipos de mantenimiento, el uno "preventivo" y el otro "correctivo".

El mantenimiento preventivo consiste en tomar todas las consideraciones del caso para mantener el equipo en perfectas condiciones de operación y "prevenir" sus fallas.

Mientras que, el matenimiento correctivo se hace para corregir un daño inminente del equipo; es de índole aleatorio (siempre y cuando las fallas no sean debidas a una falta de mantenimiento preventivo), por tanto es impredecible y fuera de control (accidentes, fallas de fábrica, etc).

Un criterio importante cuando se tiene que hacer una compra de equipos, aparte del análisis técnico-económico, es que se debe tomar muy en cuenta el soporte técnico local de la empresa proveedora de dichos equipos. Este soporte debe incluir tanto partes y piezas disponibles en existencia, como la disponibilidad del personal técnico a nivel local (muchas veces debe valorarse la disponibilidad de tiempo de dichos técnicos). De esta manera se puede asegurar que en caso de cualquier falla de los equipos exista un respaldo para la pronta reparación y/o sustitución de los equipos.

Una vez cubierto el detalle de probable falla de los equipos por causas fuera de control, se debe dedicar un poco de tiempo para planificar el mantenimiento preventivo

que garantice la operación eficaz del sistema. Por tanto, de aquí en adelante, se entenderá como "mantenimiento" al mantenimiento preventivo, ya que de éste dependerá que los equipos y el sistema funcionen correctamente.

El sistema de OPEC (la LAN) está constituido de dos grandes componentes: "hardware" y "software".

El "hardware" corresponde a los equipos y conexiones (computadores, cableado, concentradores, fuentes y reguladores de energía, etc). Mientras que, el "software" agrupa al sistema operativo y a todos los programas de aplicación que funcionan sobre él.

Un mantenimiento del "hardware" se planifica desde su instalación, siguiendo las recomendaciones de los fabricantes y representantes de los equipos, que por lo general se enmarcan dentro de las condiciones físicas de operación (ambiente eléctrico, térmico, libre de polvo, sistema de puesta a tierra, etc) y que ya se ha hecho referencia en capítulos anteriores.

Luego, una vez que han sido instalados los equipos y en operación, es menester mantener las condiciones de trabajo estables.

Es necesario establecer normas como pedir al personal el "no comer, no beber y no fumar" cerca de los equipos, y establecer un cronograma de limpieza para eliminar las partículas de polvo y de carbón que se acumulan dentro de los equipos.

Dichas limpiezas deben realizarse periódicamente, por lo menos una vez al año en ambientes relativamente limpios. En ambientes con mayor porcentaje de partículas de polvo y carbón deben realizarse con mayor frecuencia.

Se habla particularmente de partículas de polvo y carbón porque son las más comunes, y éstas además de envejecer los materiales con rapidez pueden ionizarse y causar problemas. Esta limpieza es muy importante en los monitores (principalmente en los de

color), ya que los voltajes son elevados e ionizan las partículas más fácilmente (con mayor razón si el clima es muy seco[1]).

Algo que vale la pena mencionar para tomar las precauciones del caso, es que Quito, en época de verano tiene un clima muy seco, propenso a que se acumulen cargas electrostáticas en las prendas de vestir y en alfombras. Este tipo de situaciones puede provocar que se dañen ciertas tarjetas de tecnología CMOS (las tarjetas Token-Ring por ejemplo) cuando se las manipula sin las precauciones del caso. Es muy conveniente tener en los lugares de mantenimiento pulseras antiestáticas para eliminar dichas cargas indeseables a tierra. Es recomendable que en las oficinas donde existan equipos de computación y electrónicos, si son alfombradas, de ser posible estas alfombras sean antiestáticas, esto ayuda mucho a minimizar este problema.

Cuando de "software" se trata, no solo es cuestión de instalar el sistema operativo (configurar la red para las necesidades de la empresa y de los usuarios: distribuir los recursos del sistema, dar derechos y espacios en discos, etc), y los programas de aplicación, si no el mantener y optimizar los recursos.

Una red de computadores es muy dinámica, se necesita estar dedicado a tiempo completo a su mantenimiento y operación. Las tareas más frecuentes son: crear nuevos usuarios, borrar información no deseada, evitar la infección de virus informáticos, establecer respaldos, dar soporte a los usuarios, entre otras.

Las redes a medida que crecen en servicios y en usuarios se vuelven más complejas, por tanto se hace indispensable el documentarlas de una manera adecuada, de tal forma que existan normas y procedimientos para permitir un crecimiento ordenado y facilitar las tareas y resolución de problemas.

Otro asunto que es importante, es el tener algunas personas capacitadas para dar soporte en caso de problemas con el sistema, es decir no sólo el administrador o

[1] Es común ver en Quito monitores con problemas después de sólo unos meses de trabajo que en otras partes del mundo no dan problemas sino hasta después de varios años.

supervisor de la red, sino otras personas que puedan dar solución siguiendo la documentación y los procedimientos para caso de contingencia.

Una vez confirmada la validez[1] de dichos procedimientos, se puede pasar a conformar el manual de operación de la LAN para que sean de fácil acceso.

Como ejemplo de la documentación que se debe elaborar, se añaden los anexos 6, 7, 8 y 9, que tratan de la administración de la red, desastre y recuperación (backups),"help desk" (escritorio de ayuda), y plan de contingencia para redes locales.

3.3 INTEGRACION DE VARIAS PLATAFORMAS DE TRABAJO

Para este análisis se deben introducir algunos conceptos básicos en lo que a IBM se refiere y luego a las redes en general.

En tiempos no muy remotos podían clasificarse los ordenadores como microcomputadores, minicomputadores y "mainframes" por la cantidad de usuarios que a ellos podían accesar, en actualidad esa conceptualización está alejada de la realidad debido al desarrollo de los microcomputadores.

Para este enfoque se va a definir un "mainframe" como un ordenador multiusuario que "corre" un sistema operativo propiedad de IBM.

Existen muchas razones para comunicarse con un "mainframe" a través de una red, siendo la principal la de disponer de la gran cantidad de datos que pueden ser almacenados en uno de ellos, por otro lado la potencia de realizar cálculos, transacciones y operaciones, además de un enorme potencial de ampliar las comunicaciones a través de otros "mainframes" o una red de ellos.

---

[1] Estos procedimientos deben elaborarse y probarse hasta el punto que una persona sin mayores conocimientos de la estructura de la red pueda ser guiada a través de ellos sin riesgo de equivocarse.

Al principio se utilizaba el "mainframe" y los terminales, éste era un esquema maestro-esclavo. Con el desarrollo de los microcomputadores, se podía aprovechar el poder de cálculo de los microcomputadores para obtener ciertos resultados y luego ser ingresados en el "mainframe", pero el problema radicaba en la comunicación de esos datos al "mainframe". Para ello había 2 opciones: la primera era imprimir esos datos y luego ingresarlos en el "mainframe", o en su defecto realizar un programa para transferir los datos desde el microcomputador al "mainframe", pero era un programa diferente que había que realizar para cada aplicación.

A nivel de "mainframes", IBM había desarrollado su arquitectura SNA (System Network Architecture), estructurando los protocolos para los dispositivos existentes, y como máximo soportaba la emulación de los microcomputadores como terminales "no inteligentes".

Debido a las necesidades cada vez mayores de transferir información en ambos sentidos, desde el "mainframe" a los microcomputadores y viceversa, IBM decidió desarrollar un juego de protocolos para comunicar 2 dispositivos cualquiera (microcomputadores y mainframes), a diferencia de los anteriores que estaban dedicados a dispositivos específicos, con una filosofía diferente, denominada peer-to-peer (de igual a igual) que consiste en darle iguales derechos de arrancar, parar y controlar las transmisiones.

Este juego de protocolos se conoce con las siglas APPC (Advanced Program-to-Program Communications). APPC consta de un protocolo de unidad física, el PU 2.1, y un protocolo de unidad lógica, el LU 6.2. Pero cabe mencionar que la simple definición de protocolos no resuelve el problema de las comunicaciones, es necesario que se desarrollen programas que los utilicen[1] .

La red "Token-Ring" soporta los dos interfaces de programación tanto el APPC como el NETBIOS. El NETBIOS no soportaba el protocolo LU 6.2, hasta hace poco que se

[1] Para mayor información sobre el tema se puede consultar en el "SNA Transaction Programmer's Reference Manual for LU Type 6.2, GC30-3084-1".

hicieron modificaciones tanto de "software" como de "hardware" y se ha conseguido a través de los "drivers" LANSUP[1] superar este problema; consecuentemente se pueden integrar permitiendo elegir entre uno de los dos entornos de trabajo (esto es hablando de los sistemas propietarios de IBM, como son Token-Ring, y SNA). IBM tiene SNA como una arquitectura cerrada[2] , y difiere de los estándares de la ISO, mientras que "Token-Ring" si se encuentra estandarizado, por tanto se lo considera como de arquitectura abierta.

A continuación se hablará de los sistemas de red, éstos son los que comprenderían redes estandarizadas a nivel de la industria.

Sistema de red. El estado actual de la tecnología, si bien es cierto permite integrar varias plataformas de trabajo (redes Ethernet, Token-Ring, servidores de terminales, emuladores, concentradores, puentes, ruteadores, "gateways", etc) para satisfacer las necesidades básicas de los usuarios, son redes que resuelven el problema de interconectividad pero presentan de inconvenientes de gran importancia.

Entre los inconvenientes principales se tienen la complejidad de la gestión física de la red y la estructura del cableado. Es decir, haría falta un servidor y un cableado distinto de red para cada plataforma de trabajo. Además de no prestar ninguna garantía para que la red pueda evolucionar en tecnología o tamaño manteniendo la compatibilidad entre los componentes (nadie garantiza que un nuevo componente es compatible con los demás existentes en la red). Todo esto hace que en muchos casos estas redes tengan que ser totalmente reemplazadas al cabo de algún tiempo.

Ante este tipo de inconvenientes, algunos fabricantes han respondido con una solución de sistema de red.

---

[1] Son un conjunto de "drivers" que permiten las comunicaciones "peer to peer" entre el AS/400 y los computadores personales.

[2] Arquitectura propia que no sigue los estándares de la industria.

Las características principales que una red de este tipo debería tener son las siguientes:

- Estar basada en estándares.
- Soporte de todos los tipos de cableado y en particular del par trenzado.
- Soporte multiprotocolo (TCP/IP, OSI, SNA, DEC-NET, XNS, IPX)[1] .
- Gestión centralizada.
- Integración de tecnologías estandarizadas tales como Ethernet, Token-Ring y FDDI.
- Integración LAN/WAN; libre elección de la estación de trabajo y del "Host".
- Configuración y evolución modular.

CONCENTRADORES INTELIGENTES (SMART HUBS)

Este tipo de redes basan sus soluciones en los concentradores inteligentes (smart hubs). Estos son cabinas dotadas de buses internos y una serie de ranuras en las que se pueden insertar módulos electrónicos que reciben energía de la cabina y se comunican entre ellos a través de los buses.

Cada tipo de módulo sirve para un tipo de conectividad. Los hay de Ethernet 10 Base T[1]; Token-Ring; Thin Wire Ethernet[1]; Ethernet de fibra óptica; puentes locales y remotos; puentes FDDI[1] ; puentes Token-Ring-Ethernet, etc.

---

[1] ver glosario.

Se instalan una o más de estas cabinas por cada planta del edificio. Las cabinas se cablean a un repartidor de par trenzado, cuyo papel es el de conectar el computador de la planta al módulo que le corresponde. De esta forma modular, si un usuario cambia de lugar de trabajo, un simple cambio en el repartidor restaurará la conectividad a dicho usuario.

La conexión entre plantas o cableado vertical (troncal) se realiza mediante par trenzado, cable coaxial o fibra óptica, atendiendo a consideraciones de distancia, costo, ancho de banda y topología requerida.

Las conexiones externas al edificio se hacen a través de puentes remotos, FDDI o ruteadores X25, que no son más que módulos adicionales que se alojan en una de las cabinas.

En OPEC actualmente se está en plena expansión de las soluciones del tipo descrito. La evolución futura apunta a un fuerte asentamiento del estándar 10 base T, una expansión de Token-Ring y FDDI, y una fuerte mejora en las prestaciones de los ruteadores mediante la introducción de tecnología RISC[1] .

Los esfuerzos de mejora en los sistemas de gestión se centran hoy en día en dos frentes: la estandarización de agentes para control físico, tales como SNMP[2] ; y su integración en niveles superiores tales como NETVIEW, EMA[3] , etc.

La cada vez mayor potencia de las estaciones de trabajo favorece la evolución del modelo informático basado en la arquitectura cliente/servidor. El definitivo asentamiento requerirá la existencia de sistemas de red fiables y gestionables.

---

[1] Ver glosario.
[2] Simple Network Management Protocol.
[3] Programas de administración de las WAN.

En el caso particular de OPEC se ha optado a nivel internacional por el estándar Token-Ring para la LAN, y el AS/400 como el minicomputador para el desarrollo de aplicaciones financieras, de contabilidad, materiales y recursos humanos.

Estas dos plataformas por ser de IBM no tienen ningún problema en integrarse tanto físicamente como a nivel de "software". Es decir, no se tiene implementado ningún sistema de red, solo es una interconexión de plataformas IBM.

El AS/400 a pesar de ser un buen equipo, no es la mejor elección, quizá un equipo de arquitectura abierta tales como los de arquitectura RISC , que "corren" bajo el sistema operativo UNIX como el RS/6000[1] podría ser una alternativa más económica y con mayores perspectivas a futuro (desde el punto de vista de compatibilidad) para desarrollar todas las aplicaciones que se están "corriendo" con el AS/400.

Se eligió el AS/400 porque anteriormente se había estado trabajando con sistemas IBM ("mainframes") a nivel mundial, y se había invertido mucho en desarrollar las aplicaciones mencionadas en este sistema, tal que, tratar de migrar a nuevos sistemas no compatibles con ellos hubiera significado una mayor inversión en tiempo y dinero hasta llegar al mismo punto de desarrollo en las aplicaciones; adicionalmente, por razones de compatibilidad se hubiera tenido que realizar un cambio de todos los equipos a nivel mundial.

Por tanto, el AS/400 resultó la mejor alternativa para OPEC.

Antes de adquirir el AS/400, las aplicaciones financieras, de contabilidad y materiales se realizaban en un sistema denominado "Baby 36", que corre sobre NetWare y que emula las condiciones de trabajo y programación del S/36 de IBM. Es decir migrar del "Baby 36" a la red fue sencillo. Pero era indispensable dejar el "Baby 36" porque ya daba muchos problemas "corriendo" sobre NetWare, y los volúmenes de datos

[1] Sistema de arquitectura abierta de IBM que utiliza el sistema operativo UNIX.

procesados ya lo requerían; se volvió lento, se perdían datos, no era totalmente multiusuarios, se "colgaba"[1] , y así por el estilo.

El AS/400 para conectarse con la red Token-Ring necesita de una tarjeta adaptadora de red y del programa PC SUPPORT/400. El programa se instala de forma modular, parte en el AS/400 y parte en el computador que va a comunicarse con él.

PC Support le permite desde cualquier computador que esté instalado en la red accesar al AS/400, disponer del espacio en disco duro del AS/400 como si fuera otro disco en DOS del computador, enrutar cualquier impresora de la red y/o conectada independientemente como impresora del AS/400, subir y bajar archivos desde el computador al AS/400, tener hasta cinco sesiones de trabajo, entre otros servicios.

También se puede introducir Windows como plataforma de trabajo e interfaz visual entre el AS/400 y la red.

A futuro se va a instalar un equipo IBM RS/6000 para desarrollar las aplicaciones de ingeniería, y un servidor de base de datos "SYBASE Server". Esto es posible debido a que Novell se ha afincado como el vendedor No 1 en el mundo, y todas las empresas están desarrollando aplicaciones para NetWare. Estos equipos descongestionarían el servidor de archivos de la LAN, que actualmente está prestando estos servicios, y descentralizaría los procesos para lograr un rendimiento más óptimo.

También se piensa implementar una red en el CPF, de iguales características. Se está a la espera de que se construya el campamento definitivo para comenzar su instalación. El medio de comunicaciones entre ambas redes sería un "gateway" de correo electrónico, y los usuarios podrían accesar remotamente a su LAN mediante modem y el programa "OnLan"[2] ; y se utilizaría el enlace vía satélite para estos fines.

---

[1] El equipo no logra seguir la secuencia del proceso y se queda detenido de forma indefinida.

[2] Programa que permite un acceso remoto a través de un modem a una LAN con sistema operativo NetWare.

CAPITULO 4

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Como se ha indicado al inicio de este trabajo, OPEC es una empresa transnacional afincada legalmente en nuestro país que tiene convenios con PETROECUADOR en el área de exploración, extracción y comercialización del petróleo ecuatoriano, la cual comenzó la etapa de explotación en el mes de mayo de 1993.

Sus necesidades en el área de procesamiento de datos han ido incrementándose a medida que se acerca al cupo de producción de crudo impuesto en el contrato de servicios con PETROECUADOR. Dicho crecimiento fue de cierta manera desordenado, hasta que en base al trabajo desarrollado por los técnicos del departamento de sistemas (al cual pertenece el autor de este trabajo) se logró establecer una planificación adecuada y hoy los frutos están a la vista.

En el mes de septiembre de 1993, se realizó un cambio de oficinas a un edificio que actualmente soporta las necesidades físicas de OPEC. Se deseaba obviar los problemas que se habían estado suscitando en las instalaciones anteriores en el Edificio del Banco de los Andes. Cabe mencionar que en ningún momento se paralizaron los trabajos por no tener lista la red "Token-Ring", ya que se hizo el traslado de los computadores (estaciones de trabajo), servidores, "gateways", "UPS", en dos días (durante el fin de semana), de tal manera que los usuarios de la red no tuvieron ningún inconveniente en continuar con el procesamiento de datos requerido por ellos.

Se tuvo que afrontar la planificación de todas las variables físicas que podrían afectar a la red de computadores, desde su inicio, como por ejemplo: alimentación de energía eléctrica, ambiente térmico, ventilación, cableado de la red y ubicación de los concentradores de cableado, etc. Este es un punto a favor, porque a pesar de que se requirió de un esfuerzo bien grande de planificación y coordinación con los contratistas encargados de las instalaciones, se documentó todos los detalles de dichas instalaciones y de esta manera se aseguró el poder dar mantenimiento eficaz a la red de computadores.

Este trabajo ha cubierto en gran medida el requerimiento de la empresa de documentar en forma adecuada todo lo referente al ambiente eléctrico, térmico, de conectividad y comunicaciones de su sistema de transmisión y procesamiento de datos, y ciertos procedimientos operacionales de la red. De tal forma que a futuro, cualquier persona con suficientes bases técnicas pueda con una simple revisión de este trabajo tener una idea bastante clara de como está configurado el sistema.

En base a la documentación obtenida, se ha hecho un análisis de ciertos problemas y se los ha ido solucionado de acuerdo como se han presentando.

El enfoque principal de este trabajo de investigación fue el de establecer ciertas políticas técnicas en el área de Sistemas y Comunicaciones. Es decir tener una planificación adecuada de los cambios que se van a realizar a futuro, en base a la documentación actual y experiencia operacional de la red.

De manera general, las pautas y aspectos a considerar para la puesta en marcha de una red de área local son:

1. Definir las necesidades. Una LAN no rendirá servicios eficientes y fiables a menos que éstos hayan sido analizados con el mayor cuidado. El diseño del sistema se debe hacer en base a una buena idea de los tráficos de datos que deberá soportar

la red y las perspectivas de nuevos servicios. El administrador de la red debe tener un conocimiento en el área de microcomputadores, telecomunicaciones, sistemas centrales y el correspondiente "software". Además, una buena cultura de empresa y cierta capacidad de diálogo con los usuarios.

2. Definir el tipo de cable. La elección del cable adecuado de acuerdo al tráfico de datos y la distancia. Es recomendable hacer un pre-cableado de todas las oficinas, pero esto resulta poco económico, la otra alternativa es hacer una planificación que prevea el crecimiento de servicio hacia nuevas oficinas.

   Definir un local para las cajas de reparto, especialmente para las redes "Token-Ring", las arquitecturas en estrella (tipo Starlan) y para redes Ethernet con cableado en estrella y funcionamiento lógico en bus.

   Si se utilizan HUBS[1] , es necesario definir el tipo ya que de ello dependerá la calidad de la administración de la red. En estos HUBS se podrán conectar pasarelas, puentes o derivaciones que servirán a la red para comunicarse con otras redes locales.

3. No escatimar en potencia para los servidores ("Servers") de la red. Debido al gran avance tecnlógico de "software" y de "hardware", se necesita preveer los recursos suficientes de procesador, memoria RAM y capacidad de almacenamiento, para estar a la par con dichos avances. Un ejemplo de esto es que el computador más accesible al público hace dos años era un 286 de 12 Mhz con una memoria RAM promedio de 1MB y capacidad de disco duro de 40 MB, actualmente se puede hablar de valores como procesador 486 de 66 Mhz con 4 MB en RAM y más de 200 MB en disco duro, y los programas que se desarrollan actualmente necesitan de esos recursos.

[1] Son dispositivos modulares tipo armarios que permiten conectar pasarelas, puentes, ruteadores, para dar solución integrada a las comunicaciones.

4. Definir las demandas de comunicaciones para implementar los servidores de comunicaciones.

5. El administrador de la red es quien generalmente instala el sistema operativo de la red. El procede a la implantación del sistema en cada "server", y después en cada estación. Se trata de un trabajo largo y laborioso, que debe ser realizado de forma metódica. Además, debe definir los usuarios de la red.

6. Una vez instalada físicamente la red, el administrador deberá preocuparse de las aplicaciones, es decir, de los programas a ser utilizados por los usuarios. Su instalación depende de numerosos parámetros: el número máximo de usuarios simultáneos, las protecciones específicas, una administración particular para las bases de datos, etc.

7. Definir la frecuencia de los respaldos. Se debe establecer una política adecuada de respaldos del sistema. Por lo general se realizan los respaldos en cintas magnéticas.

8. El administrador debe establecer políticas de seguridad respecto a la seguridad de los datos. Por ejemplo utilizar "discos espejados"[1] . Aunque esto repercute en una degradación de la red. Este aspecto debe ser tomado en cuenta, para que se pueda tener un servidor más potente.

9. Finalmente, debe hacerse un análisis de funcionamiento y "afinamiento" de la red a fin de optimizar los rendimientos globales. Para esto es necesario implementar archivos que se denominan "LOG" (son archivos que van guardando los registros sobre incidentes de la red y ciertas operaciones de seguridad).

[1] Técnica de respaldo simultáneo de disco duro que se estudió en el capítulo 2.

10. Se deben preparar procedimientos de a quien recurrir en caso de avería o falla de la red.

11. A veces es necesario el tener un servidor de respaldo en caso de falla de uno de los servidores de la red.

Como ejemplo de las políticas desarrolladas se pueden mencionar los procedimientos de administración de la red, de desastre y recuperación, de ayuda de escritorio, y el plan de contingencia para redes de área local[1] .

Adicionalmente, se recolectó todos los datos de los equipos (computadores, monitores, UPS) para alimentar una base de datos de mantenimiento que contiene los mantenimientos correctivos y preventivos realizados en cada uno de los equipos, si tienen o no tienen garantía, direcciones físicas de dichos equipos en la red, el usuario a cargo de quien están los equipos, departamento, área, número de activo fijo, etc.

También se dedicó mucho tiempo en definir la disposición física del cableado y los equipos, para de esta manera tener la mayor confiabilidad en las comunicaciones de datos a través de la red. Actualmente, la red está trabajando a 4 MB/s, pero se podría subir la velocidad de transmisión a 16 MB/s en un futuro muy cercano sin tener problemas, ya que la planificación se hizo tomando en cuenta este parámetro.

Cabe mencionar que actualmente la red consta de casi 110 computadores, y cerca de 130 usuarios, es decir está catalogada entre las redes de área local más grandes del país. Cuando se comenzó este proyecto se tenían cerca de 70 computadores.

El material bibliográfico referente a la conectividad y políticas técnicas en el área de redes locales y redes de área metropolitana es mínimo y en caso que existiera es de difícil acceso para el estudiante de nuestra especialización. Por tanto, se espera que

[1] Anexos 6,7,8 y 9 respectivamente.

esta tesis sirva no como un manual técnico, sino como una guía de lo que se tiene en nuestro país, en lo que a redes LAN se refiere, y sirva como un ejemplo del cual pueden obtener algunos criterios. Los manuales sirven para dar solución a problemas específicos y se puede decir con certeza, que cuando se tiene una visión general del problema y se sabe como plantear sus soluciones, sólo queda recurrir a los manuales para implementar las soluciones puntuales.

Por tanto, se ha cubierto en gran parte y de buena forma los objetivos planteados al inicio del proyecto:

- Obtener una documentación confiable, acerca de los equipos, su distribución física, y su configuración. Así como también una documentación de los problemas que se han estado suscitando mediante el procedimiento de HELP DESK (Anexo 8).

- Se establecieron políticas de desarrollo (tal como la estandarización de la nomenclatura utilizada por los usuarios tanto de la LAN como del AS/400), y procedimientos técnicos operacionales. Adicionalmente, se ha hecho una planificación de las proyecciones a futuro de la red, tal es el caso que para inicios de 1995 ya se aprobó el presupuesto para la instalación de la LAN en el CPF.

- Que el estudiante de la Facultad disponga de material bibliográfico acerca de los equipos y técnicas utilizadas en el procesamiento y comunicación de datos para redes locales y de área metropolitana.

De acuerdo a los alcances presentados en el correspondiente temario de tesis, se puede concluir que los mismos se han mantenido dentro de sus límites para cumplir con los objetivos planteados.

4.2 RECOMENDACIONES

- Es necesario seguir desarrollando una buena documentación acerca de los estándares que se llevan a nivel nacional e internacional (referente a las estructuras informáticas, tipo de usuarios, etc) de tal forma de que a futuro se pueda integrar fácilmente todas las LAN existentes en los distintos países para conformar una red WAN de OIEPC.

- Adicionalmente, deben establecerse normativos de uso de la LAN para permitir una operación confiable de la red tales como las normas de seguridad en todos sus niveles. Existen planteamientos acerca de este tópico, pero falta elaborar el documento correspondiente.

- Se deben elaborar los procedimientos operacionales destinados a contrarrestar los efectos de cualquier contingencia a nivel de operación y supervisión de la red, y a la optimización de los recursos a nivel de usuarios de la red. Existe un documento que se ha ido elaborando en base a la experiencia de este proyecto (Anexo 9), pero quedan algunos aspectos por concretarse.

A continuación se presentan a manera de recomendación algunos proyectos que podrían complementar el presente trabajo.

- Un proyecto que es bastante interesante es el de establecer estadísticas de uso de los distintos programas de aplicación, para saber a ciencia cierta el número de licencias requeridas por los usuarios. Existen programas que realizan este tipo de estadísticas y hacen un análisis de los intentos infructuosos de los usuarios por acceder a determinada aplicación.

- Adicionalmente, como OPEC es una compañía transnacional, existen muchas rotaciones temporales de personal. Esto implica el crear nuevos usuarios en la red, y

luego borrarlos de ella, si el número es grande y la frecuencia se incrementa, se puede perder control sobre esos usuarios temporales, por tanto es mucho mejor si se tienen creados "usuarios invitados" para que dicho personal los utilice mientras permanecen en el Ecuador.

- Otro proyecto sería el conectar la señal de emergencia que sale del UPS principal al AS/400, permitiendo hacer un apagado normal y programado del AS/400 en caso de ausencia de energía. Caso contrario, se podría perder datos y tiempo en reconstruirlos en el caso de un apagón prolongado que agote las baterías del UPS.

- Sería importante establecer un monitoreo local (y a futuro remoto para el CPF) del anillo de la LAN, lo cual facilitaría la solución de cualquier problema, mediante la determinación exacta del lugar del problema. Para este proyecto se necesita conectar en "daysy-chain" los puertos de supervisión de los concentradores de cableado, y comprar el software para supervisión, con el dispositivo de interfaz al puerto serial de cualquier computador (que podría ser el del supervisor o el del operador de la red). Esto podría ser sumamente útil cuando se instale la red en el Oriente.

- Se puede optimizar el "backup" de la red utilizando un módulo NLM (NetWare Load Module) que se carga en el servidor de la red y que se ocupa de realizar los respaldos automáticamente desde el mismo servidor a la unidad de cinta. De esta manera se evita dedicar un computador adicional a dicha tarea y se obvia la posibilidad de que exista cualquier problema de comunicaciones entre el servidor y el computador dedicado a los respaldos. Adicionalmente, cuando se trata de recuperar información desde cinta al disco duro no se aumentaría el tráfico de información dentro del anillo, dando como resultado un mejor aprovechamiento del canal de comunicaciones.

- Restringir el acceso de personas no autorizadas al centro de cómputo. Esto se podría lograr instalando un control de acceso electrónico mediante una contraseña. Establecer este control se vuelve prioritario ya que al no existir se corre el riesgo de que personas no autorizadas ingresen al centro de cómputo y de forma accidental ó intencional causen algún problema que repercutiría en la operación del sistema.

- En lo referente a la detección y control de incendios, sería necesario que el departamento de seguridad industrial capacite a las personas que laboran con los equipos de computación sobre los agentes extintores de incendio y su uso.

Tomando en cuenta la relación técnico-administrativa se ha estado desarrollando una planificación de proyectos en las distintas áreas y departamentos de la empresa, entre los cuales se pueden mencionar los siguientes:

Finanzas:

Implementar sistema de gráficos para presentaciones.
Sistema de base de datos de activos fijos.
Migrar el sistema de cuentas por pagar de la LAN al AS/400.

Recursos Humanos:

Base de datos del personal en el AS/400.

Ingeniería de producción/Perforación:

Sistema de Reportes diarios de producción.
Sistema de seguimiento de inventarios para completaciones de pozos.
Entrenamiento a los usuarios en el TMS (Total Maintenance System).

Exploración:

Reportes diarios de perforación.

Instalar estación de trabajo de exploración.

Sistema de mapeo-interpretación geológica.

Materiales:

Seguimiento de pedidos de compra.

Usuarios adicionales para el sistema administrativo.

Migrar el sistema desde la LAN al AS/400.

Asuntos de Gobierno y Medio Ambiente:

Base de datos de asuntos de comunidades.

Base de datos de proyectos de medio ambiente.

Legal:

Sistema de seguimiento de contratos.

Sistema de seguimiento de litigios.

Para concluir este trabajo, se espera haber cubierto de forma clara una gran gama de aspectos que se deben tomar en cuenta en una red de datos LAN. Cabe mencionar que cada uno de estos aspectos podría haber sido tema de un trabajo de tesis, por la complejidad de análisis a la que se puede llegar, sin embargo, se ha tratado de hacer una síntesis de estos aspectos y presentarlos como un todo para generar una comprensión general de los sistemas y permitir en base a esto que se pueda profundizar en cada aspecto pero entendiéndolo como parte de ese todo.

GLOSARIO

ANSI	American National Standard Institute, Instituto de estándares nacionales americanos.
ASCII	American Standard Code for Information Interchange, Código estándar americano para intercambio de información.
Asincrónica	En comunicación de datos, es una transmisión que no está relacionada con una frecuencia específica o temporización; es una transmisión de comienzo/parada caracterizada por bytes que tienen bits de comienzo (START) y parada (STOP).
Bridge o Puente	Es un dispositivo que interconecta LANs usando los dos primeros niveles OSI (físico y enlace).
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía.
Conmutación de paquetes	Una técnica de transmisión de datos donde los recursos físicos de la red se utilizan para transmitir y conmutar en base de paquetes de información.
CPF	Central Production Facilities, facilidades centrales de producción, ubicadas cerca de Limoncocha, provincia de Sucumbios.
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection (Detección de portadora de acceso múltiple con detección de colisiones), es un método de acceso utilizado en redes de área local.
DEC-NET	Arquitectura de red propiedad de "Digital Equipment Corp."
ESDI	Enhanced Small Device Interface. Tecnología diseñada para controlar dispositivos periféricos tales como discos duros, unidades de cintas, etc.
Estación	Es un punto de entrada y/o salida de un sistema de comunicaciones.
Ethernet	Nombre que se le da a una tecnología de conmutación de

	paquetes para redes de área local. Esta fue inventada por XEROX. La norma que la identifica es la IEEE 802.3. Se pueden usar tres tipos diferentes de cable: cable coaxial de 1/2" de diámetro ("Thick Ethernet"), cable coaxial más fino ("Thin Ethernet") y cable de par trenzado ("10 Base T Ethernet").
Fax	Dispositivo que permite el envío/recepción de documentos o gráficos a través de la red telefónica.
Fibra óptica	Filamento o fibra hecha de materiales dieléctricos que consisten de un núcleo (para propagar señales de luz, generadas por ejemplo por un láser) y de una envoltura que refleja la señal hacia el núcleo. Generalmente se utilizan fibras de vidrio, aunque a veces se prefieren fibras plásticas por su mayor flexibilidad.
Full dúplex	Modo de comunicación de datos que permite transmitir los datos simultáneamente en ambas direcciones (transmisión y recepción) del enlace.
Gateway	Dispositivo que interconecta dos o más redes que utilizan diferentes protocolos de alto nivel (realizando las conversiones de protocolos necesarias).
Half dúplex	Modo de comunicaciones que permite transmitir an ambas direcciones del enlace pero de forma alternada, no de forma simultánea.
Hardware	En el contexto de esta tesis se define como todos los componentes físicos que conforman el computador: tarjetas, fuentes de energía, disco duro, etc.
HDLC	High-Level Data Link Control, Control de Enlace de datos de Alto-Nivel. Este es un protocolo (orientado a bit) de capa de Enlace especificado por el CCITT.
IEEE	Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos.
Internet	Red de redes (interconecta varias redes) que utiliza el protocolo TCP/IP. Esta red se extiende a nivel mundial incluyendo las

	redes de numerosas universidades, laboratorios de investigación, oficinas gubernamentales, negocios y usuarios particulares.
IPX	Internetwork Packet Exchange, Intercambio de Paquetes inter-red. Protocolo de nivel de red utilizado por NetWare de Novell.
ISDN	Integrated-Services Digital Network, Red Digital de Servicios Integrados. Red digital definida por el CCITT.
ISO	International Standards Organization, Organización Internacional de Estándares.
Isocrónico	Igualmente temporizado. En comunicación de datos, la información de temporización se transmite conjuntamente con los datos por el mismo canal -enviando datos asincrónicos por un medio sincrónico. Este método involucra el enviar sincrónicamente los caracteres asincrónicos entre cada par de "bits" de comienzo/parada.
ITT	International Telephone and Telegraph, Teléfonos y Telégrafos Internacionales.
LAN	Local Area Network, Red de Area Local. Es una red de alta velocidad (en el rango de los Mbit/s) para cubrir cortas distancias.
LLC	Logical Link Control, Control Lógico de Enlace. Es el protocolo definido por las normas IEEE 802 para el tercer nivel del modelo referencial de la LAN.
Mainframes	Computadores diseñados para realizar complejos cálculos matemáticos, almacenar y transmitir grandes cantidades de datos y que generalmente son de arquitectura y sistema operativo exclusivo de la casa fabricante (sistema cerrado). Generalmente permiten el procesamiento múltiple de grandes cantidades de datos. Estos computadores son utilizados por instituciones bancarias, agencias gubernamentales, universidades grandes, etc.
MAN	Metropolitan Area Network, Red de Area Metropolitana, es una red que se define para áreas más extensas que las LAN, para

	unas distancias en el orden de los 50 Km. La IEEE tiene el estándar IEEE 802.6 para MAN.
Modem	Dispositivo que modula/demodula una señal para adaptarla al medio de transmisión.
Nodo	Punto terminal de los enlaces de comunicaciones.
OPEC	Occidental Production and Exploration Company, Compañía Occidental de Producción y Exploración.
OSI	Open Systems Interconection, Interconexión de Sistemas Abiertos.
Paquete	Unidad de datos consistente de dígitos binarios (datos y "bits" de control) que son conmutados y transmitidos como un todo dentro de la red.
PBX	Private Branch Exchange, central telefónica privada.
Post Script	Lenguaje para generación y edición (formas y tamaños) de gráficos, e impresión en alta resolución.
Protocolo	Serie de reglas que se establecen para establecer, mantener y controlar una comunicación.
RISC	Reduced Instruction Set Computer. Es una arquitectura de microprocesadores que tienen un set reducido de instrucciones con la finalidad de que al tener menos instrucciones se necesite menor número de ciclos de máquina por cada instrucción y se gane en velocidad de procesamiento.
Router	Dispositivo que emplea los primeros tres niveles OSI (físico, enlace y red) para interconectar redes distintas.
RS/6000	Computador con arquitectura RISC de IBM.
Scanner	Dispositivo que sirve para digitalizar imágenes mediante un proceso de exploración óptica.
SCSI	Small Computer System Interface. Tecnología diseñada para controlar dispositivos periféricos tales como discos duros,

	unidades de cintas, etc.
Sincrónico	Transmisión de datos en la cual ambas estaciones (transmisión y recepción) están sincronizadas, y los datos son enviados en forma continua. Los intervalos de tiempo son constantes y no se utiliza información redundante como bits de comienzo y parada.
SNA	Systems Network Arquitecture, Arquitectura de Sistemas de Red, modelo referencial de IBM para sus redes.
Software	En el contexto de esta tesis se define como los programas que necesitan los computadores para realizar sus funciones y tareas.
Terminación de línea	Elementos que se instalan en las terminaciones de las líneas de comunicaciones para evitar reflexiones indeseadas de las ondas que se propagan en la línea.
TCP/IP	Transmision Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Internet. Desarrollado por el departamento de Defensa de EEUU.
Télex	Dispositivo que permite el envío/recepción de caracteres a través de su red propia.
Trama	Bloque de datos que se definen para transmisión cuando se utilizan ciertos protocolos. Este término deriva de los protocolos orientados a caracter que añaden caracteres especiales de comienzo y fin de trama cuando transmiten un mensaje o un paquete de datos.
T1	1,544 Mb/s.
Unix	Sistema operativo originado en AT&T.
Videotape	Cinta de Video.
WAN	Wide Area Network, Red de Area Extensa. Es una red que por su definición puede enlazar nodos distantes. Generalmente se utiliza en estándar X.25 del CCITT.
XNS	Xerox Network Standard. Es una especificación estándar de

Xerox para un interfaz de red.

X.25 Recomendación del CCITT que especifica cómo deben establecerse, mantenerse y controlarse las comunicaciones en una red de conmutación de paquetes. Esta recomendación contempla los tres primeros niveles OSI (físico,enlace y red).

ANEXO 1

COMANDOS DE NETWARE

ANEXO 1

COMANDOS DE NETWARE

En las tres primeras páginas se hace un resumen de los comandos mas utilizados clasificados de acuerdo a su tipo: de supervisor, consola y usuario.

Luego, se presenta una lista de comandos mas utilizados que aparecen en el capítulo 22 de "Domine Novell NetWare" de Cheryl C. Currid-Craig A. Gillet. Esta lista corresponde a los comandos de consola y de usuario.

COMANDOS DEL SUPERVISOR.

CPMOFF	Evita que se habra un archivo cerrado.
CPMON	Permite abrir un archivo cerrado.
EOJOFF	Mantiene un fichero abierto. Necesario para bloquear ficheros de algunas aplicaciones de usuario.
EOJON	Desactiva EOJOFF.
HIDEFILE	Oculta un fichero para las búsquedas en directorios.
SHOWFILE	Desactiva HIDEFILE.
SYSCON	Llama al directorio y utilidades de usuario.

COMANDOS DE CONSOLA.

BROADCAST	Envia un mensaje a toda la red.
CHANGE QUEUE	Modifica la prioridad de la cola de la impresora.
CLEAR STATION	Le quita la autorización a una estación de trabajo de tener los recursos de la red.
CONFIG	Visualiza una relación de las tarjetas adaptadoras de red instaladas.
DISABLE LOGIN	Evita la entrada de una estación de trabajo.
DOWN	Limpia la red y la prepara para apagar.
ENABLE LOGIN	Permita la entrada a una estación de trabajo.
FORM CHECK	Comprueba la alineación de una impresora.
FORM SET	Avanza una página en la impresora.
KILL PRINTER	Detiene una impresora y elimina la cola de la misma.
KILL QUEUE	Elimina una cola de impresora.
MONITOR	Se utiliza para monitoreo.
NAME	Visualiza el nombre del servidor de archivos.

OFF	Borra la pantalla de la consola.
QUEUE	Lista la cola de la impresora.
REROUTE PRINTER	Redirecciona una impresora a otra.
REWIND PRINTER	Detiene, hace una copia de backup y comienza de nuevo la impresión de un fichero.
SEND	Envia un mensaje a un computador determinado.
SET TIME	Establece la fecha y la hora para un servidor.
START PRINTER	Rearranca una impresora después de una orden STOP, KILL, o REROUTE.
TIME	Visualiza la hora del sistema.

COMANDOS DE USUARIO

ATTACH	Introduce un usuario en un servidor.
CASTOFF	Evita los mensajes.
CASTON	Desactiva CASTOFF.
CHKVOL	Visualiza los datos de información de un disco.
ENDSPOOL	Envía archivos en spool a la impresora.
FLAG	Modifica o visualiza los atributos de un archivo.
HELP	Ayuda.
LARCHIVE	Guarda archivos en un disco local.
LISTDIR	visualiza los directorios y sus condiciones de acceso.
LOGIN	Identifica a un usuario y establece su entorno de trabajo.
LOGOUT	Hace que un usuario salga del servidor de archivos.
LRESTORE	Recupera los archivos guardados con LARCHIVE.
MAP	Asigna un nombre de dispositivo local del DOS a un directorio.
NARCHIVE	Guarda archivos en el disco del

	servidor.
NCOPY	Copia archivos del directorio de la red.
NPRINT	Envía archivos a la cola de impresión de la red.
NRESTORE	Recupera los archivos guardados con NARCHIVE.
PURGE	Borra completamente los archivos que han sido borrados, sin opción a ser recuperados.
QUEUE	Visualiza el estado de la cola de impresora y permite modificarla.
RIGHTS	Visualiza las condiciones de acceso del directorio actual.
SALVAGE	Recupera archivos borrados.
SEND	Envía mensajes a otros usuarios.
SET LOGIN	Adapta el entorno de un usuario de la red.
SETPASS	Cambia la contraseña de entrada del sistema.
SLIST	Visualiza de servidores de archivos.
SPOOL	Envía los requisitos de impresora a una impresora de red.
SYSTIME	Visualiza la fecha y la hora del sistema.
TARCHIVE	Guarda archivos en un dispositivo de almacenamiento en cinta.
TRESTORE	Recupera los archivos guardados por TARCHIVE.
USERLIST	Visualiza una lista de los usuarios actuales.
VOLINFO	Visualiza el contenido de un disco.
WHOAMI	Visualiza información de quien es el usuario que está usando la red en esa estación de trabajo.

CAPITULO 22

Este capítulo proporciona una referencia rápida de los comandos del NetWare.

LA NOTACION EMPLEADA EN ESTE CAPITULO

Esta capítulo describe los comandos del NetWare utilizando los mismos formatos que en la documentación del NetWare. Por ejemplo, el formato presentado para el comando NDIR es el siguiente:

NDIR *(path | filespec option)*[...]

La parte del comando en mayúsculas es constante y debe incluirse cuando se ejecute el comando. Aunque las constantes aparecen siempre en mayúsculas, en este sentido los comandos del NetWare no son restrictivos, esto es, puede entrarse el comando con cualquier combinación de letras mayúsculas y minúsculas.

Los elementos del comando mostrados en letra cursiva son parámetros variables. En el comando NDIR, *path, filespec* y *option* son las variables del comando. Cuando se introduce el comando, puede reemplazarse path con el path del directorio adecuado, *filespec* con el path del directorio y nombre del fichero (file name) apropiado y option con la opción deseada.

Los corchetes ([ ]) indican un parámetro opcional del comando. Cualquier dato contenido dentro de un juego de corchetes no es requerido obligatoriamente para ejecutar el comando, pero puede utilizarse para cualificar las instrucciones del comando.

Algunos comandos tienen juegos de corchetes anidados: por ejemplo ([ ]). El anidamiento indica que el comando tiene niveles de datos opcionales. Sin embargo, la opción dentro de los corchetes más interiores puede utilizarse sólo en conjunción con los datos de los corchetes más externos.

La barra vertical (|) entre dos parámetros del comando indica que pueden utilizarse uno de los dos, pero no ambos. En el comando NDIR, puede introducirse path o filespec. Los paréntesis se utilizan para facilitar la lectura de un grupo de opciones.

La elipsis (...) significa que la variable inmediatamente precedida de la elipsis puede utilizarse más de una vez. En el comando NDIR, pueden especificarse varios parámetros de option.

LOS COMANDOS DEL NETWARE

La siguiente sección presenta los comandos del NetWare en orden alfabético.

ATTACH

Descripción

ATTACH permite conectar a otro servidor en una inter-red, cuando la estación de trabajo ya está conectada (logged) a un servidor.

Sintaxis

ATTACH [server[|user]]

Opciones

La opción *server* permite especificar el servidor deseado, cuando se introduce el comando ATTACH. Si no se especifica el servidor, el avisador de NetWare requerirá el nombre del servidor. La opción *user* actúa de un

modo similar. Si no se especifica un usuario cuando se introduce el comando, el avisador del NetWare requerirá el nombre del usuario.

Ejemplo

El usuario TORRES puede conectarse al servidor FS2 con uno de los dos comandos:

ATTACH

o

ATTACH FS1/TORRES

BROADCAST

Descripción

El comando BROADCAST es un comando de consola o de estación de trabajo. Este comando permite enviar un mensaje, de hasta 60 caracteres, a todas las estaciones de trabajo de la red. Visualiza un mensaje en la línea 25 de la pantalla y detiene toda la actividad de la estación de trabajo, hasta que el usuario borra el mensaje al presionar simultáncamente las teclas Ctrl y [↵].

El comando BROADCAST es muy parecido al comando SEND, que también puede introducirse tanto por consola como por estación de trabajo. Sin embargo, hay dos diferencias importantes: primera, el BROADCAST no incluye el nombre del login del usuario a quien va dirigido el mensaje, lo que permite que se envíe un mensaje más extenso que en el comando SEND. Segunda, BROADCAST no permite especificar el destinatario (usuario, grupo o estación de trabajo) del mensaje; envía el mensaje a todos los usuarios de la red.

Sintaxis

BROADCAST *message*

Opciones

El mensaje no necesita estar encerrado entre comillas.

Observar que BROADCAST no interrumpe a ninguna estación de trabajo. Generalmente, el logical de gráficos (GUI, graphical user interface) de ventanas, ciertos tipos de software de emulación (como el de emulación del 3270) y el software ACS no reciben el mensaje hasta haber salido de la aplicación.

Ejemplo

Para enviar a todas las estaciones un mensaje relativo a la reunión semanal del equipo de seguimiento, introducir:

BROADCAST La reunión semanal del equipo de seguimiento se ha cambiado al 21 de mayo.

CAPTURE

Descripción

El comando CAPTURE redirecciona los trabajos de impresión en la impresora paralela de la estación de trabajos, a una impresora de la red.

Sintaxis

CAPTURE *[option ...]*

Opciones

Pueden utilizarse veinte opciones con el comando CAPTURE. Algunas de las más usadas son:

OPCION	SIGNIFICADO
SH	Muestra (SHows) el estado de los puertos paralelos (parallel ports) de la estación de trabajo; esto es, si son capturados y encaminados a un fichero o a una impresora de la red. (Esta opción no puede combinarse con ninguna otra opción).
TI=*n*	Opción de tiempo de duración *(TImeout)*; especifica el número de segundos entre la hora en que se presiona la tecla *print* y la hora en que el trabajo

OPCION	SIGNIFICADO
	de impresión se encola para imprimir. Reemplazar n por el número de segundos (especificar un número entero entre el 1 y 1.000).
L=*n*	Especifica el puerto local LPT (parallel) de captura. Reemplazar n por el número del puerto LPT.
S=*server*	Direcciona el trabajo de impresión a una impresora o a un servidor *(Server)* distinto que el servidor por defecto. Reemplazar *server* por el nombre del servidor.
P=*printer*	Direcciona el trabajo de impresión a una impresora específica de la red. Reemplazar *printer* por el número de la impresora.
C=*n*	Indica el número de copias *(Copies)* a imprimir. Pueden especificarse hasta 256 copias. Reemplazar n por el número de copias a imprimir.
A	Opción de autocaptura; deja el puerto LPT a la impresora de la red. Para anular esta opción, introducir un comando ENDCAP o CAPTURE NA, que restaura el puerto LPT a al puerto local de la impresora.
NA	Opción de *No Autocaptura;* inhibe los datos que se envian a la impresora cuando se entra o se sale de una aplicación.
J	Opción de trabajo (Job) de impresión; permite especificar una definición particular de trabajo de impresión (si los trabajos de impresión arrancan con la utilidad PRINTCON).
Q=	Opción *Queue* (cola); permite que la salida de impresión se envíe a una cola determinada. Reemplazar *n* por el nombre de la cola *(queue name).*
F=*n*	Opción de formato *(Form);* permite que la salida por impresión sea en un formato especifico. (Los formatos se definen con la utilidad PRINTDEF.) Reemplazar n por el número o el nombre del formato.
T=*n*	Opción de tabulado *(Tabs),* busca en el documento de impresión los caracteres de tabulado e inserta el número n de espacios en blanco.
NT	Opción de no tabulado *(No Tabs).*
NAM=*name*	Reemplaza el nombre *(NAMe)* del usuario en la página de portada *(banner page).* Reemplazar name por el nombre que se desea que aparezca. El nombre por defecto es el nombre de *login.*
Banner =*banner*	Opción de portada *(banner)* particularizada; permite introducir hasta 12 caracteres como portada particularizada, en la parte baja de la portada. Reemplazar *banner* por el contenido de la portada. (Nota: Utilice el carácter de subrayado cuando se necesite insertar un espacio en blanco entre palabras, por ejemplo (PRUEBA_MENSAJE).
NB	Opción de quitar la portada *(No Banner),* evita que salga una portada impresa entre dos trabajos de impresión.
FF	Opción de alimentación de formato *(Form-Feed);* inserta una página extra entre dos trabajos de impresión.
NFF	Opción sin alimentación de formato *(No Form-Feed);* impide que salga una página extra entre dos trabajos de impresión.
CR =*filespec*	Opción de crear *(CReate)* las especificaciones de fichero; captura en un fichero todo lo que pudiera haber sido enviado a la impresora de la red. Reemplazar *filespec* por el nombre del fichero que se va usar.

Ejemplos

El siguiente comando visualiza el estado actual de los puertos LPT de la estación de trabajo:

```
CAPTURE SH
```

El siguiente comando redirige el trabajo de impresión enviado a LPT 2 a la impresora 1 y con cinco copias:

```
CAPTURE L=2 P=1 C=5
```

CASTOFF

Descripción

CASTOFF bloquea los mensajes provenientes de otras estaciones de trabajo.

Sintaxis

```
CASTOF[A]
```

Opciones

Al especificar A bloquea todos *(All)* los mensajes, incluyendo los mensajes BROADCAST de consola, e impide que se reciban en la estación de trabajo.

Ejemplo

Para evitar todos los mensajes e impedir que se reciban en la estación de trabajo, introducir el comando siguiente:

```
CASTOFF A
```

CASTON

Descripción

Permite que se reciban los mensajes que llegan a la estación de trabajo. (La especificación por defecto activa el CASTON).

Sintaxis

```
CASTON
```

Opciones

No tiene opciones.

Ejemplo

El comando siguiente permite que los mensajes se reciban en la estación de trabajo:

```
CASTON
```

CHKVOL

Descripción

El comando CHKVOL visualiza información sobre cualquier volumen de la red. Los datos visualizados incluyen el nombre del servidor *(file server name)*, el nombre del volumen *(volume name)*, la capacidad total de almacenamiento *(total storage capacity)* y el espacio disponible *(remaining storage space)*.

Sintaxis

```
CHKVOL[path...]
```

Opciones

Introduciendo CHKVOL sin designar el encaminamiento *(path)*, la información presentada se refiere al volumen en curso. También pueden entrarse uno o más encaminamientos *(paths)* designando la letra del *drive* como el nombre del volumen.

Ejemplo

Para ver la información sobre el volumen en el *drive X*, introducir

```
CHKVOL X:
```

Para comprobar los datos de varios volúmenes (SYS, VOL1 y VOL2) del servidor FS1, introducir el siguiente comando:

```
CHKVOL FS1/SYS:FS1/VOL1:FS1/VOL2:
```

A continuación, un ejemplo de la salida del comando CHKVOL:

```
Statistics for fixed volume FS1/SYS:
     41254912 bytes total volume space,
     7614464 bytes in 454 files,
     33640448 bytes remaining on volume,
     33640448 bytes available to user SUPERVISOR,
     2618 directory entries available.
```

CLEAR STATION

Descripción

CLEAR STATION es un comando de consola. Rompe la conexión entre el servidor y la estación de trabajo. CLEAR STATION es útil cuando ocurre un problema en la estación de trabajo, que impide que pueda hacerse una desconexión (log out) apropiada. Si falla la estación de trabajo, los ficheros abiertos pueden dejarse en el servidor. El comando CLEAR STATION cierra todos los ficheros abiertos y los quita de las tablas internas que el servidor estaba utilizando para guardar la pista de la estación de trabajo.

Sintaxis

```
CLEAR STATION xx
```

Opciones

Reemplazar *xx* por el número de conexión de la estación de trabajo que se va a desconectar.

Utilizar este comando con precaución; podría desconectarse inadvertidamente un número equivocado. Muchos administradores de redes prefieren emplear la utilidad FCONSOLE, en lugar del comando de consola CLEAR STATION, para quitar la conexión a la red. El comando FCONSOLE es más amigable, ya que visualiza el nombre login *(login name)* del usuario y el número de conexión.

Observe que, al igual que en otros comandos de consola, puede teclear el comando incorrectamente y no aparece ningún mensaje de error. Por ejemplo, si se introduce el comando **CLEAR STATION 7** y no hay nadie conectado a la estación 7, no pasa nada. En la pantalla no se visualizará ningún mensaje de error, ni en ninguna estación de trabajo se cortará la conexión con la red.

Ejemplos

Para cortar la conexión entre la estación de trabajo 3 y el servidor, introducir

```
CLEAR STATION 3
```

CONFIG

Descripción

CONFIG es un comando de consola. Proporciona una información práctica acerca de la red soportada por el servidor. Si se tienen varias tarjetas en el servidor, CONFIG proporciona información sobre todas ellas.

El comando CONFIG sólo puede emitirse desde la consola del servidor y proporciona la siguiente información:

- Número de *service processes*
- Configuración de la red de área local LAN A:

  Dirección de posicionamiento *(address setting)* de la red

  Tipo de hardware *(hardware type)*

  Ajustes de hardware *(hardware settings)*

Sintaxis

CONFIG

Opciones

Este comando no tiene opciones.

Ejemplos

La salida del comando CONFIG depende de cómo esté activado el servidor. Será algo parecido a lo siguiente:

```
Hardware Configuration Information for Server FS1

Number of Service Processes: 05
LAN A Configuration Information:
Network Address:[1986BEEF][AAAAAAAA]
Hardware Type:NetWare RX-Net
Hardware Settings:IRQ=2,I/O Base=2E0h, RAM Buffer at
    D000:0
```

DISABLE LOGIN

Descripción

El comando de consola DISABLE LOGIN evita que los usuarios puedan abrir el iniciador de comunicaciones (login). Se emplea mucho cuando el supervisor necesita parar el servidor, por ejemplo para mantenimiento. El comando evita que puedan entrar usuarios en el sistema, pero no afecta a los usuarios que ya están trabajando.

Una vez introducido DISABLE LOGIN, nadie puede hacer *log* hasta que se introduzca el comando ENABLE LOGIN.

Sintaxis

DISABLE LOGIN

Opciones

Este comando no tiene opciones.

Ejemplos

Para evitar que los usuarios puedan conectarse al servidor introducir

DISABLE LOGIN

Ahora si un usuario intenta el *log* en el servidor, la pantalla visualizará el mensaje:

Access denied. The Supervisor has disabled logins

que viene a decir: "Acceso denegado. El Supervisor ha dejado inactivo el login".

DISK

Descripción

DISK es un comando de consola. Sólo está disponible en las versiones avanzadas de NetWare. Ofrece un informe rápido acerca del estado del disco donde está instalado el servidor. Los datos que obtiene el informe, entre otros, son: el canal utilizado, el número del drive físico del drive del disco, el número de errores de I/O (entrada/salida) ocurridos, el número de bloques libres en el disco y el número de bloques utilizados.

Sintaxis

DISK *
DISK *volumename*

Hay dos variaciones en el comando DISK disponibles en la versión SFT de NetWare. Introduciendo **DISK** * ofrece la información de cada uno de los volúmenes, del *drive* físico y del *drive* espejo (si lo hay).

Introduciendo **DISK** *volumename*, donde volumename indica un volumen específico; visualiza información sobre tal volumen.

Ejemplos

Para visualizar información sobre SYS, introducir:

DISK SYS

la pantalla visualizará la siguiente información sobre SYS:

Physical drive number
Physical drive type
IO errors on the drive
Redirection blocks available
Redirection blocks used

DOS

El comando de consola DOS se utiliza solamente con las versiones no dedicadas del NetWare tal como la ELS. No funciona en las otras versiones del NetWare.

El comando, ejecutado desde la consola, conmuta desde el modo de consola al DOS local.

Sintaxis

DOS

Opciones

Este comando no tiene opciones. Para volver desde el DOS al modo de consola, teclear **CONSOLE.**

Ejemplos

Para pasar desde el modo de servidor al modo DOS local, introducir

DOS

DOWN

Descripción

DOWN es un comando de consola, que sirve para tirar abajo el sistema. Debe utilizarse DOWN antes de haber apagado el servidor a fin de cerrar el sistema de una forma ordenada. El comando cierra todos los ficheros abiertos, graba en disco todas las memorias cache y actualiza lo

Para asegurarse de que todos los ficheros están cerrados apropiadamente, todos los usuarios deben haber cortado sus comunicaciones *(logout)* antes de emitir el comando DOWN. Si alguna estación de trabajo permanece sin haberse desconectado del servidor, recibirá un mensaje de aviso cuando se ejecute el comando DOWN.

Sintaxis

DOWN

Opciones

Este comando no tiene opciones.

Ejemplos

Para tirar abajo el sistema entero, teclear

DOWN

ENABLE LOGIN

ENABLE LOGIN es un comando de consola. Se utiliza después del comando DISABLE LOGIN, para permitir a los usuarios conectar (login) al servidor. Debe usarse este comando para devolver a los usuarios la posibilidad de establecer la conexión *(login)* con el servidor.

Sintaxis

ENABLE LOGIN

Opciones

Este comando no tiene opciones.

Ejemplos

Para permitir a los usuarios conectarse *(login)* al servidor después de haber sido dejado fuera de servicio, teclear

ENDCAP

Descripción

END CAP termina la captura de uno o más puertos *(ports)* de la impresora paralela de la estación de trabajo.

Sintaxis

ENDCAP [option ...]

Opciones

Pueden emplearse las siguientes opciones con el comando ENDCAP:

OPCION	SIGNIFICADO
L= *n*	Termina la captura de un puerto paralelo específico. Reemplazar n por el número del puerto LPT.
ALL	Termina la captura de todos *(ALL)* los puertos paralelos.
C	Termina la captura de LPT1 y elimina todos los trabajos de impresión, sin imprimirlos.
CL= *n*	Termina la captura de un puerto paralelo específico y elimina todos los trabajos de impresión, sin imprimirlos. Reemplazar n por el número del puerto LPT.
C ALL	Termina la captura de todos *(ALL)* los puertos paralelos y elimina todos los trabajos de impresión, sin imprimirlos.

Ejemplos

Para acabar la captura del LPT2, introducir el comando:

FLAG

Descripción

Se emplea el comando FLAG para visualizar o modificar los atri
tos de un fichero.

Sintaxis

FLAG [[path | filespec] [option ...]]

Opciones

Al introducir FLAG sin ningún parámetro opcional se visualiza
lista de los ficheros —y sus correspondientes atributos— existentes e
subdirectorio en curso. En el caso de introducir el encaminamiento *(p*
o la especificación *(filespec),* podrán verse los ficheros (y sus atributos)
sidentes en otras localizaciones de los discos duros de la red.

Si sus derechos efectivos en un directorio incluyen la búsqueda
modificación, puede cambiar los atributos de ficheros, incluyendo un
varias de las siguientes opciones:

OPCION	SIGNIFICADO
S	Sharable (compartible)
NS	Nonsharable (no compartible)
RO	Read Only (sólo lectura)
RW	Read-Write (lectura-escritura)
N	Normal (nonsharable y read-write)
T	Transacional (usado con SFT NetWare)
I	Indexed (indexado)
SUB	Incluya todas las subdirectorias del fich

Ejemplos

Introducir lo siguiente, para ver los atributos de todos los ficheros del directorio FS1/SYS:PROGRAMS:

FLAG FS1/SYS:PROGRAMS

Para cambiar los atributos de todos los ficheros del subdirectorio en curso, a no compartidos *(nonsharable)* y lectura-escritura *(read-write)*, introducir:

FLAG N

Para cambiar los atributos de todos los ficheros que tengan la extensión .BAT en el *drive* P a compartibles y sólo lectura *(sharable y read only)*, introducir

FLAG P:*.BAT S RO

FLAGDIR

El comando FLAGDIR permite cambiar los siguientes atributos del subdirectorio: Normal, Hidden (oculto), System y Private. Este comando también permite ver dichos atributos. Para usar FLAGDIR deben tenerse derechos de supervisor o derechos *parental* o de *modificar* el directorio padre, y debe conectarse a la red a través del servidor.

Sintaxis

FLAGDIR *[path [option...]]*

Opciones

Puede introducirse FLAGDIR desde cualquier subdirectorio, haciendo referencia a la letra del *drive map* del subdirectorio. Por ejemplo, si el *drive M* tiene el encaminamiento a FS1/SYS:PRIVATE, la orden **FLAGDIR M:** retorna los atributos del directorio.

También se pueden ver los subdirectorios subordinados al directorio en curso, introduciendo **FLAGDIR ***. Este comando visualiza el estado de todos los subdirectorios situados bajo el directorio en curso. También se

puede calificar completamente el subdirectorio en la búsqueda FLAGDIR. Por ejemplo, se puede introducir **FLAGDIR FS1/SYS:PRIVATE/CURRID/*** para visualizar el estado de los subdirectorios subordinados al subdirectorio SYS:PRIVATE/CURRID.

Con FLAGDIR pueden cambiarse los atributos de los directorios, utilizando alguno de los atributos siguientes:

OPCION	SIGNIFICADO
Hidden [oculto]	Oculta al directorio o subdirectorio del directorio de búsqueda utilizado en los comandos DIR y LISTDIR. NOTA: Los usuarios pueden cambiar a un directorio oculto y acceder a sus ficheros si saben que existe el directorio y tienen los derechos de acceso al directorio y a los ficheros.
Normal	El atributo por defecto. Puede también urilizarse esta opción para restaurar o cancelar los otros atributos.
Private	Impide que los usuarios vean el contenido de un subdirectorio. Sin embargo, si los usuarios tienen el derecho de búsqueda al directorio padre, pueden ver los ficheros. Como con el atributo Hidden, los usuarios pueden cambiar al subdirectorio, si conocen su nombre.
System	Especifica un subdirectorio necesario para el funcionamiento del sistema. Como con los otros atributos, la búsqueda de un directorio visualiza el subdirectorio.

Pueden cambiarse dos o más atributos al mismo tiempo. Los cambios en directorios se introducen especificando los atributos después de la *path*.

Ejemplos

Si el *drive* P se direcciona como FS1/SYS, introducir

FLAGDIR P:

lo que visualiza la siguiente información:

```
FS1/SYS
    PRIVATE        Normal
```

Introduciendo

```
FLAGDIR FS1/SYS:PRIVATE/CURRID/* PH
```

se aplican los atributos Private y Hidden a los subdirectorios situados directamente bajo SYS:PRIVATE/CURRID.

Observe que FLAGDIR no aplica automáticamente los atributos a los subdirectorios subordinados a los que se especifican. Por tanto, el comando precedente oculta SYS:PRIVATE/CURRID/WORDS pero no oculta al SYS:PRIVATE/CURRID/WORDS/TEMP. Los directorios subordinados a aquellos que están ocultos pueden buscarse con los comandos DIR y LISTDIR.

GRANT

Descripción

GRANT asigna derechos trustee *(trustee rights)* a los usuarios y a los grupos. Puede emplearse este comando en lugar de asignar derechos trustee a través de SYSCON.

El usuario que ejecute el comando GRANT debe tener derechos parental en el directorio al cual van a asignarse los derechos.

Sintaxis

```
GRANT option ...[FOR path] TO {[USER] user | [GROUP] group}
```

Opciones

Para poder utilizar el comando GRANT, deben existir los usuarios y los grupos especificados.

Las opciones de GRANT corresponden a los ocho derechos trustee del NetWare:

OPCION	SIGNIFICADO
R	Read /Lectura
W	Write / Grabación
O	Open / Abrir
C	Create / Crear
D	Delete / Borrar
P	Parental / Padres
S	Search / Búsqueda
M	Modify / Modificar
NO RIGHTS	Revoca todos los derechos trustee
ALL	Asigna los ocho derechos trustee

Ejemplos

Para asignar los derechos de leer, grabar y abrir ficheros al usuario Herrera en el directorio en curso, introducir

```
GRANT R W O TO USER HERRERA
```

Para asignar los mismos derechos al grupo (ACCTNG) en el directorio TEST del servidor FS1, volumen SYS, introducir el siguiente comando:

```
GRANT R W O FOR FS1/SYS:PROGRAMS TO GROUP ACCTNG
```

HOLDOFF

Descripción

El comando HOLDOFF cancela los efectos del comando HOLDON (que impide que otros usuarios tengan acceso a un fichero que esta siendo utilizado en la estación de trabajo).

Sintaxis

HOLDOFF

Opciones

Este comando no tiene opciones.

Ejemplos

Para ejecutar el comando HOLDOFF, introducir

HOLDOFF

HOLDON

Descripción

El comando HOLDON impide que otros usuarios tengan acceso a un fichero que esta siendo utilizado en la estación de trabajo. (La mayoría de las aplicaciones de software realiza esta función automáticamente).

Sintaxis

HOLDON

Opciones

Este comando no tiene opciones.

Ejemplos

Para dejar en estado "hold' todos los ficheros a los que se accede desde la estación de trabajo, introducir el siguiente comando:

HOLDON

LARCHIVE

Descripción

El comando LARCHIVE archiva los ficheros y atributos de la red, en un dispositivo de disco local (disquete o disco duro). Como se discutió en el Capítulo 19, la utilidad LARCHIVE puede utilizarse tanto para salvar como para archivar ciertos ficheros.

Para emplear la utilidad LARCHIVE, se debe estar conectado al servidor al menos con los derechos de lectura, búsqueda, apertura y modificación a los directorios y ficheros que se van a salvar (back up).

Sintaxis

LARCHIVE [path | SYSTEM]

Opciones

Se pueden especificar los directorios o subdirectorios que se desean salvar, especificando la *path* con la cualificación completa del nombre o bien con la letra del *drive*. Para salvar el sistema entero, especificar SYSTEM.

Una vez activado el programa, LARCHIVE visualiza una serie de avisadores para determinar el disco de destino de lo volcado, si se va a imprimir un informe y si se van a salvar los derechos del directorio y los derechos trustee. Después, LARCHIVE pregunta si se desea volcar (back up) todos los ficheros cualificados en el directorio o solamente los que han sido modificados desde el último volcado.

Ejemplos

Para salvar el directorio SYS:COMMON, direccionado al drive I, entrar

LARCHIVE SYS:COPMMON

o

LARCHIVE I:

LISTDIR

Descripción

LISTDIR visualiza una lista con todos los subdirectorios pertenecientes a un directorio, además de otra información especificada en las opciones.

Sintaxis

LISTDIR [path][option ...]

Opciones

LISTDIR puede ejecutarse para ver los subdirectorios del directorio por defecto o, especificando la opción *path*, para ver los subdirectorios de otro directorio.

En *option* pueden especificarse las siguientes opciones:

OPCION	SIGNIFICADO
/S	Además de los subdirectorios en curso, también visualiza todos lós subdirectorios subordinados.
/R	Visualiza la máscara de derechos máximos de los subdirectorios.
/D	Visualiza la fecha de creación de los subdirectorios.
/T	Visualiza la hora de creación de los subdirectorios.
/A	Hace efectivas todas las opciones: esto es, lista los subdirectorios subsecuentes y visualiza la máscara de derechos máximos de los subdirectorios y la fecha y hora de creación de los subdirectorios.

Ejemplos

El siguiente comando lista los subdirectorios situados en el directorio por defecto:

```
LISTDIR
```

Para ver los subdirectorios situados en el directorio PROGRAMS del volumen SYS1 en el servidor FS1, y visualizar la máscara de derechos máximos de los subdirectorios y la fecha y hora de creación de los subdirectorios, teclear el siguiente comando:

```
LISTDIR FS1/SYS:PROGRAMS/R/D
```

LOGIN

Descripción

Una vez que se ha cargado el shell de NetWare, el comando LOGIN permite a un usuario de la red acceder al servidor e invocar al sistema y al *login script* del usuario.

Sintaxis

```
LOGIN [server/[user]]
```

Opciones

Cuando se introduce LOGIN sin los parámetros opcionales, accede al servidor por defecto. El avisador del sistema inquiere el nombre del usuario (user name). Para acceder a un servidor distinto del que está lógicamente más cerca en la red y para especificar el nombre del usuario sin esperar al avisador, utilizar las variables del servidor y del usuario.

Ejemplos

Para acceder al servidor por defecto, introducir el comando siguiente:

```
LOGIN
```

El usuario Alonso puede acceder al servidor FS2, introduciendo el comando:

LOGIN FS2/ALONSO

LOGOUT

Descripción

LOGOUT termina todo acceso a uno o más servidores.

Sintaxis

LOGOUT [server]

Opciones

LOGOUT desconecta (log out) todos los servidores, si no se especifica la variable opcional del servidor.

Ejemplos

Para desconectarse (log out) de todos los servidores, introducir

LOGOUT

Para desconectarse (log out) del servidor FS1, introducir

LOGOUT FS1

LRESTORE

La utilidad LRESTORE recupera los ficheros y directorios volcados (back up) con la utilidad LARCHIVE. Se deben tener los derechos apropiados a los directorios y subdirectorios, antes de poder recuperar los ficheros. Deben tenerse, por lo menos, los derechos de crear, borrar, abrir, grabar y buscar ficheros.

Sintaxis

LRESTORE

Opciones

Aunque el comando LRESTORE no tiene parámetros, LRESTORE visualiza una serie de avisadores. El primero, pide para seleccionar el *drive* del cual van a recuperase los ficheros. Seguidamente pregunta si se desea recuperar la *security information* (información de seguridad; se debe haber conectado como supervisor para recuperar la información de seguridad). A continuación, solicita que se seleccione el directorio especifico a recuperar.

Durante el proceso de recuperación, el LRESTORE va parando en todos los ficheros que ya están en el subdirectorio de la red y envía el mensaje *"File already exists. Recreate? (Y/N)"* que significa *"El fichero ya existe. ¿Se graba encima? (Sí/no)"*. Puede elegirse entre grabar encima (se borra lo anterior) o abandonar y dejar el fichero antiguo como está.

Ejemplos

Para restaurar o recuperar un fichero volcado (back up) con LARCHIVE, ir al directorio que contiene el fichero y teclear

LRESTORE

Después ir respondiendo a los avisadores en la pantalla, hasta recuperar el fichero.

MAP

Descripción

Se utiliza el comando MAP para visualizar y modificar los *drive maps*.

Sintaxis

MAP *[drive]*	Visualiza los *drive maps* en curso.
MAP *path*	Hace un map o un remap del *drive* por defecto.
MAP *drive:=[drive: | path]*	Hace un map o un *remap* de cualquier *drive* de la red.

MAP *[INS]drive:=[drive:path]* Hace un map de un *drive* de búsqueda.

MAP DEL *drive* Borra un *drive map.*

Opciones

Cuando se hace o rehace un map de los *drives* con el comando MAP, se puede reemplazar la variable *drive* por la letra del drive de la red (por ejemplo, F: o T:) o por un número del *search drive* (por ejemplo, S1 o S4). La variable *path* deberá incluir el volumen, el nombre del directorio y el nombre del subdirectorio.

Ejemplos

Para listar el *current drive maps* (en curso), introducir el siguiente comando:

MAP

Para visualizar el *drive map* asignado al *drive T,* introducir

MAP T:

Para cambiar el *map* del *drive* por defecto a FS1/SYS:PROGRAMS, introducir el siguiente comando:

MAP FS1/SYS:PROGRAMS

Para hacer el *map* (o cambiar el *map*) del *drive* T a FS1/SYS:PROGRAMS, introducir el siguiente comando:

MAP T:= FS1/SYS:PROGRAMS

Si el servidor FS1 es el servidor por defecto, el comando precedente puede acortarse así:

MAP T:= SYS:PROGRAMS

Para añadir un *search drive* (S3) al subdirectorio FS1/SYS:PROGRAMS/LOTUS, introducir el siguiente comando:

MAP S3:=FS1/SYS:PROGRAMS/LOTUS

o

MAP INS S3:=FS1/SYS:PROGRAMS/LOTUS

La diferencia entre los dos comandos anteriores es la forma en qu el NetWare maneja el *search drive* S3 si este *search drive* ya existe. El pri mer comando cambia el *search drive* existente, a un *drive* regular de la re —designado drive X— y añade el nuevo *search drive* (S3) como *drive* W El segundo comando inserta el nuevo *search drive*, entre el *search drive* S2 y el previo *search drive* S3, que se convierte en *search drive* S4.

El siguiente comando borra (deletes) el *drive* R del *drive maps:*

MAP DEL R:

Monitor

Descripción

MONITOR es un comando de consola. Visualiza una de las pantallas más familiares del NetWare. Visualiza la actividad de seis estaciones de trabajo así como el rendimiento del sistema operativo. Puede controlarse cualquier estación de trabajo de la red especificando su número de conexión *(connection number).*

Sintaxis

MONITOR xx

Opciones

Puede controlarse cualquier estación, reemplazando el xx por el número de la estación. Tecleando solamente **MONITOR**, se visualiza información acerca de las estaciones de trabajo con los números de conexión del 1 al 6.

Además de la información sobre la conexión, se visualizan otras informaciones desde la pantalla MONITOR, tales como:

. Número de la versión del NetWare y fecha de la revisión.

. Tasa de empleo del servidor en curso (actualizada a cada segundo).

. Cantidad de entrada/salida (I/O) pendiente en disco (basada en el espacio en la memoria caché de la memoria del servidor que ha sido cambiada pero no grabada en disco).

. Número de la estación y hasta 44 mensajes de petición.

. Lista de los ficheros abiertos e información del estado de cada fichero.

Los mensajes visualizados en el área de petición (request area) muestran lo que se está haciendo en ese momento en cada estación de trabajo especificada. Pueden visualizarse cuarenta y cuatro mensajes que se muestran en la Tabla 22.1.

Tabla 22.1. Mensajes de la utilidad MONITOR

Aloc Resource	Get File Size	Release File
Begin Trans	Lock File	Release File Set
Clear File	Lock Phy Rec Set	Release Record
Clear File Set	Lock Record	Rename File
Clear Record Set	Log Out	Search Next
Close File	Log Pers File	Semaphore
Clr Phy Rec	Log Phy Rec	Set File Atts
Clr Phy Rec Set	Log Record	Start Search
Copy file	Open File	Sys Log
Create File	Pass File	Unlock Record
Dir Search	Read File	Win Format
End of Job	Rel Phy Rec	Win Read
End Trans	Rel Phy Rec Set	Win Write
Erase File	Rel Record Set	Write File
Floppy Config	Rel Resource	

La pantalla de MONITOR también proporciona otras clases de información: ficheros en uso y mensajes de estado de los ficheros. La parte de cabecera de la pantalla visualiza *File* y *Stat* (fichero y estado). Se muestran los nombres de los cinco ficheros más recientemente abiertos con un código que indica el estado de tales ficheros; los códigos de los estados son los siguientes:

CODIGO	SIGNIFICADO
n	Número de la tarea DOS.
P	El fichero esta protegido contra la lectura por parte de otras estaciones de trabajo.
R	El fichero esta abierto para la lectura.
P	El fichero esta protegido contra la lectura por parte de otras estaciones de trabajo.
W	El fichero esta abierto a la escritura por otras estaciones de trabajo.

Los códigos se listan en el formato **nPRPW**.

Pueden visualizarse otros dos identificadores: *Pers* y *Lock*. *Pers* indica que el fichero ha sido conectado pero no cerrado. *Lock* indica que el fichero ha sido cerrado. Si el servidor está funcionando con la versión SFT de NetWare, con TTS activado, pueden visualizarse dos letras más: T y H. Cuando se visualiza T en la primera columna, el fichero transaccional está abierto. Cuando se visualiza H en la segunda columna, el fichero transaccional está en estado hold (no activo).

Ejemplos

Para visualizar información de la estación de trabajo 12, teclear:

```
MONITOR 12
```

NAME

Descripción

NAME es un comando de consola. Simplemente identifica el nombre del servidor.

Sintaxis

NAME

Opciones

Este comando no tiene opciones.

Ejemplos

Para visualizar el nombre del servidor al cual se ha conectado, introducir

NAME

NARCHIVE

Descripción

La utilidad NARCHIVE vuelca (back up) los ficheros y atributos en otro *drive* de la red. Como se discutió en el Capítulo 19, la utilidad NARCHIVE puede utilizarse tanto para volcar (back up) como para archivar ciertos ficheros.

Para usar la utilidad NARCHIVE, debe haberse conectado (logged) al servidor al menos con los derechos de leer, abrir, buscar y modificar los directorios y ficheros que se desean volcar.

Sintaxis

NARCHIVE [path | SYSTEM]

Opciones

...ificarse los directorios y subdirectorios que se desean vol-

ficado o la letra del *driver*. Para volcar el sistema entero, especi
SYSTEM.

Una vez activado, el programa NARCHIVE visualiza una serie d
sadores, para determinar el disco de destino del volcado, si se impri
informe y si se desean salvar los derechos del directorio y los derechos tr
de los ficheros y directorios a salvar. Después NARCHIVE pregunta
desea volcar todos los ficheros contenidos en el directorio o solamente a
llos que han sido modificados desde la última operación de volcad

Ejemplos

Para salvar el directorio SYS:COMMON, con map al *drive* I, intro

NARCHIVE SYS:COMMON

o

NARCHIVE I

NCOPY

Descripción

NCOPY copia los fichero de un directorio de la red a otro. Pued
lizarse el comando NCOPY para copiar ficheros a y desde dispositiv
cales.

Sintaxis

NCOPY filespec [TO][path][filename][/V]

Opciones

Utilizar la opción /V para verificar que el fichero original y el fi
recién creado son idénticos. Los caracteres comodines de DOS (* y ?)
bién pueden utilizarse con el comando NCOPY.

Ejemplos

Para copiar un fichero llamado MEMO.TXT desde el disposit

```
NCOPY G;MEMO.TXT TO
FS1/SYS:/PRIVATE/MORENO/WORDS
```

o

```
NCOPY G;MEMO.TXT FS1/SYS:/PRIVATE/MORENO/WORDS
```

El siguiente comando copia todos los ficheros que tienen extensión .DOC en el subdirectorio FS1/SYS:COMMON al dispositivo T de la red y cambia la extensión a .TXT. Este comando también verifica que los ficheros copiados son idénticos a los originales:

```
NCOPY FS1/SYS:COMMON/*.DOC t:*.TXT/V
```

NDIR

Descripción

NDIR visualiza información acerca de los subdirectorios y de los ficheros dentro de los subdirectorios. La información que se lista sobre los subdirectorios incluye el nombre del directorio, la fecha de creación, máscara de derechos máximos, el usuario creador y los derechos efectivos del usuario. La información acerca de los ficheros incluye el nombre del fichero, el tamaño (en bytes), la fecha y la hora en que el fichero fue actualizado y se tuvo acceso a él, la fecha de creación, los atributos y el usuario creador del fichero.

Sintaxis

NDIR [path] | [filename]	Para utilizar sin opciones.
NDIR [path | filespec) option [...]	Para utilizar con opciones.

Opciones

Las siguientes opciones pueden utilizarse en conjunción con el comando NDIR:

OPCION	SIGNIFICADO
Selectoras de ficheros:	
FILENAME [NOT]=*file*	Visualiza ficheros que contienen el nombre del fichero (file name) especificado (los comodines están permitidos). Utilizar el NOT opcional para excluir los nombres de ficheros especificados. Reemplazar file por el nombre del fichero deseado.
OWNER [NOT]=*name*	Visualiza los ficheros creados (o no creados) por el mismo usuario.
CREATE [NOT] (BEF| = |AFT) *mm-dd-yy*	Visualiza ficheros creados (o no creados) antes (bef), en, o después (aft) de la fecha especificada (mes-día-año).
SIZE[NOT](GR| = |LE) than *nnn*	Visualiza ficheros con un tamaño en bytes (o sin un tamaño en bytes) mayor (gr), igual o menor (le) que el tamaño especificado en *nnn*.
ACCESS [NOT] =BEF | =| AFT *mm-dd-yy*	Lista los ficheros cuyo último acceso ha sido antes (bef), en o después (aft) de la fecha especificada en *mm-dd-yy* (mes-día-año).
UPDATE[NOT]= BEF| = |AFT *mm-dd-yy*	Visualiza los ficheros cuya última actualización ha sido (no ha sido) antes (bef), en o después (aft) de la fecha especificada en *mm-dd-yy* (mes-día-año).
Clasificación de los ficheros	
[REVERSE] SORT FILENAME	Clasifica los ficheros por el nombre de fichero (file name) en orden ascendente o descendente (inverso, reverse).
[REVERSE] SORT OWNER	Clasifica los ficheros por el usuario creador en orden ascendente o descendente (inverso, reverse).

OPCION	SIGNIFICADO
[REVERSE] SORT ACCESS	Clasifica los ficheros por la fecha del último acceso, de la más antigua a la más moderna o en el orden inverso.
[REVERSE] SORT UPDATE	Clasifica los ficheros por la fecha de la última actualización, de la más antigua a la más moderna o en el orden inverso.
[REVERSE] SORT CREATE	Clasifica los ficheros por la fecha de creación, de la más antigua a la más moderna o en el orden inverso.
[REVERSE] SORT SIZE	Clasifica los ficheros por el tamaño, del más pequeño al más grande o en el orden inverso.
Filtros de selección	
DO	Visualiza solamente los subdirectorios en un directorio especificado.
SUB	Visualiza los subdirectorios (y todos los subsecuentes subdirectorios) en un directorio especificado.
FO	Opción Files-Only. Visualiza solamente los ficheros en el directorio o el subdirectorio.
BR	Opción de BReve descripción. Lista solamente parte de la información. Muestra solamente el tamaño y la fecha de la última actualización de los ficheros.
Selección de archivado	
BACKUP	Lista los ficheros y muestra la fecha en que fueron modificados y salvados por última vez. Esta opción utiliza un formato ligeramente diferente que otras selecciones de NDIR.

OPCION	SIGNIFICADO
WIDE	Visualiza la información en el formato ancho (wide) por defecto de NDIR.
[NOT] ARCHIVED	Visualiza los ficheros que han sido (o no han sido) salvados y en qué fecha.
A D BEF | = | AFT *mm-dd-yy*	Lista los ficheros que tienen una fecha de archivado antes (bef) o después (aft) de la fecha especificada en *mm-dd-yy* (mes-día- año).
CHANGED	Visualiza los ficheros que han sido modificados desde la última operación de volcado.
[NOT] A B	Lista los ficheros en los cuales se ha (o no se ha) colocado el *archive bit* de DOS.
TOUCHED	Lista los ficheros modificados desde la última operación de archivado. La opción comprueba tanto el *archive bit* de DOS y la fecha y hora del último proceso de archivado.
HELP	Visualiza un mensaje de ayuda (help) mostrando el formato y las opciones del comando NDIR.

Ejemplos

Para visualizar un mensaje de ayuda para el comando NDIR, introducir

```
NDIR HELP
```

Para listar todos los subdirectorios y ficheros en el directorio en curso introducir el siguiente comando:

```
NDIR
```

El siguiente comando visualiza todos los ficheros almacenados en el drive T de la red, que tengan la extensión .TXT, que hayan sido creados

por el propietario (owner) Moreno y que sean mayores de 100.000 bytes. El comando visualizará estos ficheros clasificándolos por el nombre del fichero (file name).

```
NDIR T:FILENAME=*.TXT OWNER=MORENO SIZE GR 100000
SORT FILENAME
```

NPRINT

Descripción

El comando NPRINT imprime los ficheros en una impresora de la red.

Sintaxis

```
NPRINT filespec [option ...]
```

Opciones

Con el comando NPRINT pueden utilizarse catorce opciones. Entre las más utilizadas están las siguientes:

OPCION	SIGNIFICADO
S=*server*	Designa el servidor al cual debe ser encaminado el trabajo de impresión. Reemplazar *server* (servidor) con el nombre del servidor.
J=*job*	Especifica el nombre de la configuración del trabajo de impresión que se va a usar cuando se imprima. Reemplazar *job* por el nombre del trabajo de impresión.
P=*printer*	Indica la impresora que se va a utilizar cuando se imprima la corriente del sistema. Reemplazar *printer* por el número de la impresora.
C=*copies*	Designa el número de copias a imprimir. Reemplazar *copies* por el número de co-

OPCION	SIGNIFICADO
D	Automáticamente borra (delete) un fich ro, después de imprimirlo.

Ejemplos

Para imprimir el fichero llamado DOCUMENT.TXT en el director por defecto, en la impresora por defecto, del servidor por defecto, introd cir el siguiente comando:

```
NPRINT DOCUMENT.TXT
.. ..
```

Para imprimir tres copias de un fichero llamado WORDS.TXT almacen do en el directorio FS1/SYS:COMMON, por la impresora 2, introducir siguiente comando:

```
NPRINT FS1/SYS:COMMON/WORDS.TXT P=2 C=3
```

NRESTORE

Descripción

La utilidad NRESTORE restaura los ficheros y directorios salvad con la utilidad NARCHIVE. Se deben tener los derechos apropiados sobr los directorios y subdirectorios antes de poder restaurar los ficheros. Se debe tener al menos los derechos de crear, borrar, abrir, escribir y buscar.

Sintaxis

```
NRESTORE
```

Opciones

Aunque el comando NRESTORE no tiene parámetros, NRESTOR visualiza una serie de avisadores. El primero pide seleccionar el *drive* d cual van a recuperase los ficheros. Seguidamente pregunta si se desea recu perar la *security information* (información de seguridad; se debe haber co nectado como supervisor para recuperar la información de seguridad). A

Durante el proceso de recuperación, el NRESTORE va parando en todos los ficheros que ya están en el subdirectorio de la red y envía el mensaje *"File already exists. Recreate? (Y/N)"* que significa *"El fichero ya existe. ¿Se graba encima? (Si/no)"* Puede elegirse entre grabar encima (se borra lo anterior) o abandonar y dejar el fichero antiguo tal como está.

Ejemplos

Para restaurar o recuperar un fichero volcado (back up) con NARCHIVE, ir al directorio que contiene el fichero y teclear

NRESTORE

Después ir respondiendo a los avisadores, en la pantalla, hasta recuperar el fichero.

NSNIPES

Descripción

NSNIPES ejecuta un juego interactivo para uno o más usuarios de la red.

Sintaxis

NSNIPES [option]	Para utilizar en un monitor monocromo.
NCSNIPES [option]	Para utilizar en un monitor de color.

Opciones

Especificar en option el nivel de dificultad del juego SNIPES. Introducir un valor entre 4 y 10. El valor por defecto es 4.

Ejemplos

Para jugar al SNIPES con un moderado grado de dificultad en un monitor de color, introducir el siguiente comando:

NVER

Descripción

El comando visualiza los números de las versiones de varios servidores y del software de las estaciones de trabajo. Visualiza el número de versión del NetBios (si está cargado), IPX, SPX, el *driver* de LAN, el sh y la estación de trabajo.

Sintaxis

NVER

Opciones

Este comando no tiene opciones.

Ejemplos

Para visualizar información acerca del servidor y del *software* de l estación de trabajo, introducir

NVER

en el avisador de DOS. Saldrá algo similar a:

```
NetBIOS:A NetBIOS error has occurred,
unable to obtain the NetBios version information.

IPX Version:2.12
SPX Version:2.12

LAN Driver:IBM Token Ring Network V1.00
Self Configurable

Shell:V2.12 Rev.B
DOS:MSDOS V3.31 on COMPAQ

FileServer:FS1
Novell SFT NetWare 286 TTS V2.15Rev.A 12/11/88
```

Como muestra este ejemplo, si NetBi

OFF

Descripción

OFF es un comando de consola. Borra la pantalla de la consola. Por eficiencia y para impedir que las imágenes lleguen al monitor, conviene tener el monitor de la consola inactivo (OFF) si no se necesita.

Sintaxis

OFF

Opciones

Este comando no tiene opciones.

Ejemplos

Para quitar la visualización en la consola, introducir

OFF

PRINTER XX FORM

El comando PRINTER xx FORM informa al servidor del número de papel (form) que debe montarse en la impresora. Si la impresora recibe desde una estación de trabajo un trabajo que requiere otro tipo de papel, el servidor envía un mensaje requiriendo que se cambie el papel. El servidor detiene el trabajo de impresión hasta que se teclee el comando PRINTER xx FORM en la consola.

Sintaxis

COMANDO	FORMA ABREVIADA
PRINTER xx FORM MOUNT yy	*P xx FORM yy*
PRINTER xx MOUNT FORM yy	P xx MOUNT yy
PRINTER xx FORM yy MOUNTED	P xx FORM yy

Opciones

Las tres formas del comando PRINTER xx FORM funcionan idénticamente. Reemplazar xx por el número de la impresora y reemplazar yy por el nombre del papel.

Ejemplos

Si se identifica el papel con membrete como número 5 y un trabajo de impresión llega al servidor solicitando papel con membrete, la consola visualiza el siguiente mensaje:

Mount form 5 (UNKNOWN) in printer 0. Then use PRINTER 0 MOUNT FORM 5

La impresión no se realizará hasta haber introducido el siguiente comando en la consola del servidor:

P 0 FORM 5

Después, se imprimirá el trabajo en la impresora de la red. Todos los demás trabajos (si los hay) dirigidos a la impresora y con formato de papel número 5, también se imprimirán. Con el siguiente trabajo de impresión que llegue y necesite un tipo de papel distinto, el servidor enviará un mensaje para cambiar el tipo de papel.

PRINTER XX REWIND YY PAGES

Descripción

PRINTER xx REWIND yy PAGES es un comando de consola. Permite reimprimir hasta las últimas 10 páginas de un trabajo de impresión. Este comando es muy útil cuando se necesita reimprimir la última parte de un documento.

Sintaxis

PRINTER xx REWIND yy PAGES

Opciones

Reemplazar xx por el nombre de la impresora. Reemplazar yy por el número de páginas a reimprimir.

Ejemplos

Para reimprimir las últimas dos páginas por la impresora 0, introducir

PRINTER 0 REWIND 2 PAGES

Este comando puede abreviarse como:

P 0 REWIND 2 PAGES

PRINTER XX START

Descripción

PRINTER XX START es un comando de consola. Reactiva una impresora que ha sido detenida con el comando PRINTER xx STOP.

Sintaxis

PRINTER xx START

Opciones

Reemplazar xx por el nombre de la impresora.

Ejemplos

Para rearrancar la impresora llamada *impresora 0*, parada con el comando PRINTER xx STOP, introducir

PRINTER 0 START

Este comando puede abreviarse como

PRINTER XX STOP

Descripción

PRINTER es un comando de consola. Detiene todo envío del ser dor hacia la impresora. El comando es muy útil cuando se necesita pa la impresora, en los casos de tener que cambiar la cinta o arreglar la a neación del papel.

Sintaxis

PRINTER xx STOP

Opciones

Reemplazar xx por el número de la impresora. Debe conocerse el n mero de la impresora para poder utilizar este comando.

PRINTER xx STOP detiene la impresora hasta que se emita el coman PRINTER xx START.

Ejemplos

Para detener la impresora denominada *impresora 0,* introducir

PRINTER 0 STOP

Este comando puede abreviarse como

P 0 STOP

PSTAT

Descripción

Se ejecuta PSTAT para ver la información sobre las impresoras de red. En esta información se incluye el número de impresora, el estado impresión y el tipo de papel que se está utilizando.

Sintaxis

Opciones

Pueden utilizarse dos opciones en conjunción con el comando PSTAT:

OPCION	SIGNIFICADO
S= *server*	Emplear esta opción para ver la información sobre las impresoras de un servidor distinto al servidor por defecto.
P = *printer*	Utilizar esta opción para ver información relativa a una impresora especifica.

Ejemplos

Para ver información acerca de todas las impresoras de la red del servidor por defecto, introducir

```
PSTAT
```

Para visualizar la misma información sobre la impresora 1 en el servidor FS2, introducir el siguiente comando:

```
PSTAT S=FS2 P=1
```

Un ejemplo de la salida del PSTAT podría ser:

```
Server FS2:Network Printer Information
Printer   Ready    Status   Form: number, name
1         On-Line  Active   0,Etiquetas
```

PURGE

Descripción

El comando PURGE borra totalmente de la estación de trabajo los ficheros que fueron borrados (erased) del disco duro del servidor con los comandos DEL o ERASE de DOS o por la utilidad FILER del NetWare. A menos que se especifique PURGE, estos ficheros pueden recuperarse con el comando SALVAGE.

Sintaxis

```
PURGE
```

Opciones

Este comando no tiene opciones.

Ejemplos

Para dejar los ficheros borrados totalmente irrecuperables, introducir el siguiente comando:

```
PURGE
```

REMIRROR

Descripción

El comando de consola REMIRROR se utiliza solamente con las versiones SFT del NetWare. Restaura tanto los discos espejo *(mirroring)* como duplicados *(duplexing)* que hayan tenido algún fallo o se hayan apagado.

REMIRROR realiza primero un ciclo a través de todos los dispositivos, para asegurarse de que todos los datos han sido copiados en el dispositivo espejo *(mirrored drive)*. Según va realizándose el proceso de la copia, va apareciendo un mensaje informativo.

Sintaxis

```
REMIRROR xx
```

Opciones

Reemplazar xx por el número del drive al cual se va a copiar todo.

Ejemplos

Para copiar el contenido del disco físico drive 0 al disco físico *drive 1*, introducir

```
REMIRROR 01
```

REVOKE

Descripción

REVOKE rescinde los derechos trustee asignados previamente a los usuarios y a los grupos. Puede emplearse este comando, en lugar de SYSCON, para anular los derechos trustee.

El usuario que ejecute este comando debe tener derechos parental sobre el directorio al cual se van a rescindir los derechos.

Sintaxis

REVOKE *option* ... [FOR *path*] TO [[USER]*user* | [GROUP] *group*]

Opciones

Para que el comando REVOKE sea efectivo, debe existir la especificación de usuario o de grupo.

Cualquiera de estos ocho derechos trustee de NetWare pueden especificarse en option:

OPCION	SIGNIFICADO	
R	Read	Lectura
W	Write	Escritura
O	Open	Apertura
C	Create	Creación
D	Delete	Borrado
P	Parental	"Parentesco"
S	Search	Búsqueda
M	Modify	Modificación

Asignados los ocho derechos trustee

Ejemplos

Para revocar los derechos de *read, write y open* del usuario Herrera en el directorio en curso, introducir el siguiente comando:

```
REVOKE R W O TO USER HERRERA
```

Para revocar los mismos derechos al grupo ACCTNG en el directorio TEST del servidor FS1, volumen SYS, introducir el siguiente comando:

```
REVOKE R W O FOR FS1/SYS:TEST TO GROUP ACCTNG
```

RIGHTS

Descripción

El comando RIGHTS visualiza los derechos efectivos de un usuario en un directorio.

Sintaxis

RIGHTS [path]

Opciones

Especificar el *path* para visualizar los derechos efectivos de un usuario en un directorio distinto al directorio en curso. Si no se especifica el *path*, se visualizan los derechos efectivos del directorio en curso.

Ejemplos

Para visualizar los derechos efectivos del directorio en curso, introducir el siguiente comando:

```
RIGHTS
```

Para visualizar los derechos efectivos del usuario en el directorio FS1/SYS:PROGRAMS, introducir el siguiente comando:

```
RIGHTS FS1/SYS:PROGRAMS
```

Ejemplos

Para cambiar la *password* en el servidor por defecto, teclear

```
SETPASS
```

Para cambiar la password del usuario en el servidor FS2, introducir

```
SETPASS FS2
```

SET TIME

Descripción

SET TIME es un comando de consola que permite establecer la fecha y hora en el servidor.

Sintaxis

SET TIME *[mm/dd/yy][hh:mm:ss]*

Opciones

Reemplace *mm/dd/yy* por el mes, el dia y las dos últimas cifras d año. Reemplazar *hh:mm:ss* por la hora, minutos y segundos. Si se omite las entradas de la fecha y de la hora, el comando simplemente visualiz la fecha y la hora en el servidor.

Ejemplos

Para establecer la fecha del 23 de septiembre de 1990 y la hora a l 5 40 de la tarde, en el servidor, introducir el siguiente comando:

```
SET TIME 09/23/90 17:40:00
```


SETTTS

Descripción

El comando SETTTS sólo puede utilizarse con las versiones S (system fault tolerant, sistema tolerante de fallos) del NetWare. Reempl el nivel lógico de los registros bloqueados que el TTS (transaction track system) dejó pasar antes de que el TTS empezase el rastreo.

Utilizar SETTTS únicamente si en el servidor hay *software* instala que específicamente llame a la función TTS. Puede emitirse el coman desde DOS o colocarlo en un programa *batch* para ejecutarlo en cier ocasiones.

Sintaxis

SETTTS *[logical level [physical level]]*

Opciones

Especificar los *logical level y physical level* (nivel lógico y nivel físic utilizando números del 1 al 255.

Ejemplos

Para ver el TTS en curso, simplemente introducir desde el avisador DOS

```
SETTTS
```

Generalmente el nivel lógico se coloca para un bloqueo y el nivel fí co para dos bloqueos. Para cambiar esta especificación, introducir

```
SETTTS 2 2
```

Este comando cambia a la vez los niveles fisico y lógico, antes de q el sistema comience el rastreo de la transacción.

SYSTIME

Descripción

SYSTIME visualiza el día, la fecha y la hora en cualquiera de los servidores de una inter-red.

Sintaxis

SYSTIME [*server*]

Opciones

La opción *server* visualiza la hora del sistema de los servidores distintos al servidor por defecto.

Ejemplos

Para visualizar la hora del sistema en el servidor FS2, introducir

SYSTIME FS2

TLIST

Descripción

El comando TLIST visualiza una lista con las asignaciones trustee de un directorio especificado.

Para utilizar el comando TLIST, el usuario debe tener los derechos parental del directorio.

Sintaxis

TLIST [*path*[USERS | GROUPS]]

Opciones

Puede ejecutarse TLIST desde el directorio en curso o puede especificarse otro directorio con el encaminamiento de la opción *path*. Al especificar USERS o GROUP, se limita la visualización de las asignaciones trus-

Ejemplos

Para visualizar las asignaciones trustee tanto a un usuario como a u grupo, introducir el siguiente comando:

TLIST

Para visualizar sólo las asignaciones trustee del usuario en el directo rio en curso, introducir el siguiente comando:

TLIST.USERS

El punto (.) indica que el directorio que se va a visualizar es el direct rio en curso.

Para visualizar las asignaciones trustee para el directorio PROGRAM del volumen SYS en el servidor FS1, introducir el siguiente comando:

TLIST FS1/SYS:PROGRAMS GROUPS

UNMIRROR

Descripción

El comando de consola UNMIRROR se utiliza solamente en las v siones con SFT de NetWare. Desactiva la aplicación del espejo *(mirrori* en disco.

Sintaxis

UNMIRROR xx

Opciones

Reemplazar xx por el número del drive que estaba siendo utilizado cc receptor.

Ejemplos

Si se ejecuta el comando

entonces el contenido del disco físico de drive 0 ya no se copiará más en el disco físico de drive 1. En la pantalla se visualiza el mensaje *Mirroring turned off on volume SYS* cuando el comando ha acabado.

USERLIST

Descripción

El comando USERLIST visualiza una lista con los usuarios conectados al servidor en ese momento.

Sintaxis

USERLIST [*server*/][*user*][/A]

Opciones

Utilizar la opción *server/* para visualizar los usuarios conectados a un servidor distinto del servidor por defecto. Utilizar la opción *user* para visualizar la información de un usuario específico. Utilizar la opción /A para ampliar la información visualizada incluyendo el *network numbers* y el *node addresses.*

Ejemplos

Para listar los usuarios del servidor por defecto, introducir el siguiente comando:

USERLIST

Para visualizar la información ampliada de los usuarios en el servidor FS2, introducir

USERLIST FS2/A

VERSION

Descripción

El comando VERSION visualiza el número de la versión de cualquier [illegible] si el programa utiliza *overlays* (solapa-

Sintaxis

VERSION [*path* / *filespec*]

Opciones

Especificar el *path* solamente cuando el fichero ejecutable no está el *search directory.* En *filespec,* especificar el nombre del fichero.

Ejemplos

Para ver qué versión del NetWare está siendo utilizada por el comando USERLIST, teclear

VERSION USERLIST

WHOAMI

Descripción

El comando WHOAMI permite a los usuarios ver información acer de quienes están en la red. Con la selección de la opción adecuada, pue visualizarse la siguiente información del propio usuario: el servidor al cu se está conectado, el nombre de usuario en cada servidor, fecha y hora su login, el grupo al que se pertenece, las equivalencias de seguridad, l derechos efectivos en cada directorio de la inter-red.

Sintaxis

WHOAMI [*server*][*option ...*]

Opciones

Además de especificar el servidor para la información del usuario, pu den seleccionarse las siguientes opciones:

OPCION	SIGNIFICADO
/G	Visualiza el grupo al que se pertenece

OPCION	SIGNIFICADO
/R	Visualiza los derechos efectivos en cada directorio.
/A	Visualiza toda la información disponible.

Ejemplos

Para visualizar los servidores a los que se está conectado, los nombres de usuario, los números de conexión y la hora login, introducir el siguiente comando:

```
WHOAMI
```

El siguiente comando proporciona al usuario información acerca del grupo al que pertenece y equivalencias de seguridad, en el servidor FS1:

```
WHOAMI FS1 /G /S
```

ANEXO 2

PROPUESTA DE SPACELINK

ANEXO 2

ECUADOR SATELLITE SYSTEM

September 1, 1992

Prepared for:

OCCIDENTAL INTERNATIONAL EXPLORATION
AND PRODUCTION COMPANY
110 W. 7th Street
P. O. Box 300
Tulsa, Oklahoma 74102-0300
Oxy Ref/PO Number: BEQ-50101-QR

Prepared by:

Spacelink SYSTEMS INC.

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Scope

Spacelink Systems, Inc. (SSI), will design, fabricate, test, deliver and supervise the installation of a "C" band satellite based network for operation in Ecuador. Spacelink Systems assumes full responsibility for the integration of the earth station into a fully functional, totally integrated system. The system will be fully compatible with Intelsat satellite space segment requirements.

Spacelink Systems' extensive experience in supplying satellite telecommunications systems for international and domestic drilling projects will ensure that the proposed system will meet all of OXY's requirements. This unique combination of oil field experience coupled with exceptional telecommunications expertise will provide OXY with a confidence level not available from any other source.

1.2 Proposed System Summary

The Spacelink Systems system design places emphasis on system reliability, transportability, and ease of assembly/use. Cost containment, although a major design consideration, was not the primary consideration. Based on the experience of Spacelink Systems personnel, the proposed design will provide OXY with the most cost effective system for this project.

The antenna and the outdoor electronic assemblies proposed are rugged and light weight. The mount is a simple kingpost structure with azimuth and elevation adjustments for easy alignment. The kingpost can be used with a concrete foundation or skid load frame.

The proposed antennas are crucial to providing a system design which meets all OXY's requirements. Spacelink Systems personnel are very familiar with the proposed antenna having used it in similar applications in which high performance was required.

The Quito site will consist of a 4.5 meter antenna system with two (2) 20 Watt C-Band outdoor RF Terminals that are power combined. The indoor equipment will be contained within a standard 19 inch cabinet to be placed within the OXY building in Quito. It will be the responsibility of OXY to provide conduits (if necessary) to connect the outdoor equipment to the indoor equipment cabinet. This interfacility link (IFL) routing is assumed not to exceed 500 feet in cable length.

The IFL will consist of one transmit and one receive 70 MHz IF coaxial cable and an AC prime power cable run from the uninterruptable power supply (UPS) that will be mounted within the rack cabinet along with the QPSK data modems, multiplexer, and any other customer supplied equipment.

1.3 Program Schedule

The milestone schedule is illustrated in Figure 1.3.1. A preliminary design review (PDR) will be held two (2) weeks after receipt of order (ARO) and all equipment will be placed on order within the following week. A critical design review will be held within four (4) weeks after the PDR. System integration will be complete 3 months ARO and the system will be ready to ship. Should OXY wish to ship the system at an earlier date the program can be accelerated. Spacelink Systems is fully capable of expediting the project, however, additional cost would be incurred.

1.4 Program Manager

A dedicated Program Manager will be assigned to the project and will be responsible for the entire project including design, fabrication, test, and installation. The Program Manager will also interface closely with the OXY Project Engineer and will conduct two (2) design reviews during the course of the project.

A section of the Spacelink Systems facility will be dedicated to this project for equipment receiving, integration and testing. A project management software program shall be used to track project status and insure that the project schedule is met. Monthly progress reports will be submitted to keep OXY informed as to adherence to project schedule and design plan.

A full trial assembly will be performed on the antenna systems in Houston to ensure that all parts have been supplied by the manufacturer and to ensure all parts have been properly machined. Additionally, all mechanical fabrications and modifications necessary to mount the RF terminals to the antennas will be done in Houston during the trial assembly. This activity will burden the project with the cost to build the system, state side, as well as in country, however, this cost is justified by the savings most certainly to be realized during the in country installation activity. By finding discrepant or missing material here, we will save large amounts of cost associated with expediting materials from the states as well as save the costs of non productive labor who are waiting for material to arrive at the installation site.

The entire system shall be fully tested, end-to-end in Houston, utilizing a test loop translator. This will insure proper operation of each component as well as functionally demonstrating the entire system.

The system shall be packaged (crated) for export and shipped by air to Quito. Extra care shall be taken to insure safe arrival of the equipment in Quito. Spacelink Systems will furnish the export license. OXY will be responsible for import into Ecuador.

Training shall be provided to OXY personnel during the time the equipment is being installed in Quito. Installation supervision will be provided on a time and materials basis, however, estimated costs are included.

System documentation will consists of equipment suppliers' operation/maintenance manuals and Spacelink Systems generated drawings. Five (5) copies of the system documentation package, including a drawing tree, shall be provided. Spacelink Systems is committed to continued support after the system is installed. OXY can rely on Spacelink Systems for technical assistance, qualified maintenance personnel, and system up-grades.

1.5 Management and Technical Capability

Spacelink Systems, Inc., and its sister companies, as providers of telecommunications components and systems, have aggregate annual sales of over $8,000,000. This strong financial backing provides a high level of stability to the Spacelink Systems organization.

Mr. Gregory P. Varisco is President of Spacelink Systems, Incorporated. With an extensive experience in the telecommunications industry, Mr. Varisco has been instrumental in the design and implementation of numerous communications systems in North America, South America, Africa, and Southeast Asia for several major energy companies.

Mr. Peter Zilliox will also be a major contributor to this project. Mr. Zilliox was co-founder of Dalsat, Inc. a major supplier of satellite telecommunications systems for the past eleven years. He is officed in Dallas.

Spacelink Systems technicians are experienced and highly qualified to integrate, and install complete satellite communications earth stations for the petroleum industry.

1.6 Proposal Outline

This proposal includes sections on System Design, System Description, Program Management, In-Plant Integration & Test, Acceptance Test, Documentation, Product Assurance, Training, Tools/Spares/Test Equipment, and Options.

2.0 SYSTEM DESCRIPTION

2.1 Introduction

The following sections provide a technical overview of the proposed earth station network and the design of the individual earth stations. The technical overview includes a detailed bill of materials for each earth station configuration, a functional description, a system performance analysis, a physical configuration summary, and a description of the system/equipment features.

The proposed equipment configurations were selected based upon requirement and adherence to operational specifications for the space segment. All equipment proposed are off-the-shelf products with a reliable field history. No new product development tasks are proposed.

2.2 Reference Standards

Our proposed system design was established in accordance with industry recognized standards and specifications. Where conflicts between this proposal and the following reference standards exist, this proposal shall dictate. The standards applicable to the proposed system designs are:

1. Intelsat IESS 309, 402, 601

2. EIA Standard RS-411, Electrical and Mechanical Characteristics of Antennas for Satellite Communications.

3. MIL-HDBK-217B, Reliability Prediction of Electronic Equipment.

4. Department of Labor, Occupational Safety and Health Administration (OSHA) Industry Construction Safety and Health Regulations/Standards.

5. CCITT V.35 Data Interface Specification

6. ANSI/NFPA 70, 1987, National Electric Code (NEC)

7. FCC Rules and Regulations, Part 25, Satellite Communications

2.3 General

The proposed system consists of one hub earth station facility in Quito and the a U.S. Hub Earth Station in Florida.

2.4 Functional Description of the Systems

Vertex 4.5 meter antennas are proposed. The Vertex antenna was selected because of their superior mechanical and electrical performance. Intelsat has previously qualified this antenna for access to their spacecraft. In addition, the

robust mechanical design will withstand multiple assembly and disassembly activities. Spacelink Systems proposes 65° K low-noise amplifiers be placed on the antennas and a high quality 1/4 inch coax cable will connect the LNA to the outdoor equipment package. The 6 GHz transmit power amplifiers are proposed to be part of the outdoor equipment. The power amplifiers will be connected to the antenna via a short waveguide.

The SSE 20W Amplifier is a solid state power amplifier is driven by a final conversion stage up-converter located within the same antenna mount package. RF conversion at the antenna is proposed for its simplicity and inherent reliability as well as it's cost effectiveness. Transponder selection is controlled by a low-phase noise, reliable, high stability synthesized oscillator controlled internally within the outdoor unit. The down-converter proposed is similarly double conversion located within the outdoor box. It's output interface is a 70 MHz IF spectrum that is routed indoors via a coaxial cable IFL.

A QPSK FEC rate 1/2 digital modem interfaces to the RF Terminal. The FEC rate and QPSK phase state selection are consistent with the sample link budget criteria presented. The modem channel frequency is selectible in 25 kHz steps over any 36 MHz segment of the operational transponder. The modem interfaces with the station multiplexer at an aggregate I/O rate of 128 Kbps, but can be field programmed for rates up to 2.048 Mbps.

The remote station will be equipped with a 5 KVA uninterruptible power supply with 10 minutes of battery back-up. The UPS system is equipped with RF filtering, isolation, and transient surge protection.

2.5 System Performance

2.5.1 General

The system components selected will yield excellent end-to-end voice and data channel performance. The design is governed by the Intelsat's technical parameters using adequate design margins to yield consistent bit-error-rate (BER) performance in excess of 1×10^{-7} throughout the life of the satellite and ground system hardware. The G/T and EIRP margins proposed to maintain the low BER design criteria are presented in detail in the following sections.

2.5.2 System G/T

The receive G/T is an important parameter because it is a measure of the receive system sensitivity and hence the downlink carrier-to-noise ratio (CNR) for a given level of satellite downlink EIRP. The CNR determines the system's bit error-rate (BER) performance and ultimately the quality of the voice and data channels.

The earth station G/T is determined by the effective antenna gain and the receiver system noise temperature, both referenced to the low-noise amplifier (LNA) input. The system noise temperature includes the contributions of the equipment and the

noise coupled into the antenna from the local environment.

The G/T analysis for the remote drill site station follows:

The analysis is based on the following conditions:
1. Clear sky
2. Antenna mid-band gain
3. Operational elevation angle of
4. Outside ambient temperature 290.0°K

The downlink elements are as follows:

Element	Gain (Loss)	Temp(K)
ANT	44.1 dBi	25
Feed	(.1) dB	inc.
TRF	(.1) dB	6°K
LNB	65 dB	65°K
D/C	0-60 dB	NF=15

T_s (System Noise Temperature) =

$$\frac{T_{ant}}{L_1 L_2} + \frac{(L_1 - 1)\, T_{amb}}{L_1 L_2} + \frac{(L_2 - 1)\, T_{amb}}{L_2} +$$

$$T_{MISM} + T_{LNA} + \frac{10^{(N_F'/10)} - 1}{G_{LNA}} \times 290$$

Where:

L_1 = Feed Loss = 0.1 dB (1.023)
L_2 = TRF loss = 0.1 dB (1.023)
T_{amb} = 290°K
G_{LNA} = 65 dB
T_{MISM} = Ant VSWR 1.25:1 = Mismatch Loss 0.06 dB = 4°K
NF' = The effective noise figure of the system after the LNA=15 dB
$G_{Net} = G_{ANT} - (L_1 + L_2) - L_{MISM}$
$G/T = G_{Net} - 10 \log Ts$

2.5.3 System Available EIRP

The available Effective Isotropic Radiated Power (EIRP) is determined by the high power amplifier (Solid State P.A.'s), transmission line loss, and effective antenna gain. The EIRP available figure-of-merit calculation is based on the following:

1. HPA Saturated Power Output
2. Antenna midband transmit gain
3. Waveguide run is 1' (Loss 0.25)
4. One twist flex section mates to the transmit feed (Loss = 0.25 dB)

The EIRP for the Quito site is as follows:

	4.5m
Solid State Amplifier Output	+48.95 dBM
Total Transmission Line Losses	.25 dB
Antenna Midband Gain	47.7 dBi
Available EIRP	66.2 dBW

2.5.4 Link Design and System Trade-offs

The EIRP and G/T, determined in the last sections, can now be utilized to perform the earth station to satellite link analysis and demonstrate the end-to-end performance of the network.

The link budget is an analysis of the system parameters including uplinks between earth stations and the satellite; and downlinks between the satellite and earth stations. The link budget considers one earth station to be located in Quito and the other in the Limoncocha and a U.S. hub.

Given the above parameters Spacelink Systems' link budgets indicate the proposed system will satisfy Intelsat's space segment allocation with an adequate power margin.

2.5.5 Availability

The availability refers to the signal path availability which is a measure of the percentage of time that the signal path is available for its intended purpose of carrying and processing the applied communication signals. Availability is directly related to the skill levels of the operating personnel, spares complement levels, test equipment complements, and proximity of all of the above to the earth station (i.e. travel time, shipping times, etc.). The equipment reliability (mean time, between failures) also plays an important role in the system availability. The signal path availability must consider the complete communications channel which includes the uplink equipment (baseband to RF) at the transmitting earth station and the downlink equipment (RF to baseband) at the receiving earth station. Accordingly, the availability analysis for single thread station is expected to be at least .998. For the purposes of the analysis, the satellite availability is assured to be 1.0 over the life of the system.

2.5.6 Intermodulation Analysis

USA Uplink EIRP = 55.1 dBw
Remote Uplink EIRP = 47.0 dBw

If total uplink EIRP is equal to 56.0 dB and the total EIRP capability is 62.14 dB, then the uplink margin is

Quito 61.5 dB back off

As seen in the uplink block and level diagrams, the uplink margin at end of life is as follows:

Quito 6.37 dB back off

The SSE Technologies solid state PA has the following intermodulation performance: with -3 dB total output back off yields third order intermodulation products at a level of -24 dBc. Therefore, the IM products are expected to be as follows:

Quito -30.7 dBc
Remote -27.6 dBc

The resulting IM densities are as follows:

Quito EIRP - 30.3 - 10LOG[128/4] = 55.1 - 30.3 - 15.0 = 9.57 dBw/4 KHZ

The Intelsat IESS 401 Intermodulation specification is 21 dBW/4 KHZ. Therefore, this SLS design meets the specification with adequate margin.

For example: 21 - 2.5 = 1.85 dBW/4 KHZ

2.5.7 Antenna Foundation Design

The Quito antenna will be mounted on a loadframe. Drawings will be supplied at the PDR.

2.5.8 Physical Layout and Design

The physical layout and design of the equipment is packaged to meet the reliability requirement. It should be noted while reducing the size of the overall containers, only the most reliable equipment has been chosen.

The Quito rack will be isolated from the surroundings since vented doors will serve to protect the equipment. Cabinet layout will be supplied at the PDR.

2.5.9 Electrical Power System

The electrical power system design is critical to the overall operation of each station. It has been Spacelink Systems' experience that microprocessor based

3.0 EQUIPMENT DESCRIPTION (Major Components)

3.1 Antenna

The Vertex 4.5 meter C-band Antenna with circular-polarized feed and kingpost pedestal are proposed. They feature high performance coupled with ease of disassembly for shipment. This antenna offer proven performance while operating in severe environmental conditions.

3.2 LNA

SSE 65° K LNA/LNB with 65 dB gain and remote power supply. These units are designed for unsheltered outdoor operation and have built-in protection against voltage transients.

3.3 HPA

SSE 20 Watt solid state HPA with external mount power supply and a waveguide power combiner for the Quito Station will be mounted at the dish.

3.4 Frequency Converters

SSE double conversion, synthesized control RF up-converters and down-converters. Features low intermodulation distortion and low phase noise.

3.5 Modem

EF Data Variable rate, QPSK synthesized satellite modem with 1/2 rate forward error correction. Extensive monitoring and control are supported via a flexible and powerful control interface.

3.6 Uninterruptible Power Supply (UPS)

Clary 5 KVA on-line UPS's. Features transient free AC power and static transfer switch for reverting to line power in the unlikely event of a UPS failure.
The Quito site will be equipped with Best Technologies 18KVA UPS for greater backup capacity.

A Program Management system will be utilized so that work in progress will be continually compared with established schedules. In the event of technical problems, corrective action(s) will be proposed. Design reviews will be conducted by the Program Manager and supported by the personnel working on the project.

4.5 Design Reviews

Two design reviews are proposed, as shown on the project schedule. A design package will be generated for each review and will be made available to OXY at the design review. The first or Preliminary Design Review (PDR) will present as a minimum:

1. Design philosophy and basic implementation approach.

2. Functional block diagrams.

3. Preliminary outdoor and indoor equipment configurations.

4. Preliminary rack and equipment layouts

5. Characteristics of vendor equipment.

6. Preliminary test plan outline.

The second or "critical" design review will be held no later than four (4) weeks after the PDR. Spacelink Systems will present as a minimum:

1. Detailed design data.

2. Finalized block diagrams.

3. Finalized indoor and outdoor equipment configurations.

4. Finalized rack and equipment layouts

5. Description of equipment, characteristics and detailed specifications.

6. Preliminary test plan.

5.0 IN-PLANT INTEGRATION AND TEST

System integration will take place in a dedicated, secure section of the Spacelink Systems facility. All equipment received will undergo a thorough inspection to insure that it was not damaged during shipment. Strict controls will be implemented on the handling and storage of all project materials and components.

Adequate space will be provided so that the equipment can be assembled and tested (end-to-end) as a completely functioning system. It is anticipated that all tests will be witnessed by a OXY representative. Test procedures, previously approved by OXY, will be strictly adhered to. All test data will be documented on data sheets within the test procedure. Any abnormality that may occur during a test will be fully described. Testing will not be considered complete until the OXY representative has signed-off on all test data.

6.2.2. Test Reports

The test report will be submitted within the (10) working days after the completion of the acceptance testing. The test report will include a performance verification tabulation with a side- by-side comparison of measured performance versus expected results. If any test yields unsatisfactory result, then only that test will have to be reperformed after corrective action is taken. This will allow Spacelink Systems to waive an entire retest of the system unless of course the corrective action taken may affect the results of other test data previously taken. In that event, only those tests whose results may have been altered by a corrective action will have to be reperformed.

6.2.3 Vendor Test Results

The vendor in-plant acceptance test results will be submitted via the monthly program progress reports.

6.3 Equipment Configuration for Testing

The acceptance testing will be conducted on the equipment and the system in an operational configuration using the actual cable, coax, waveguide and connectors intended for installation. In addition, all test equipment utilized for acceptance testing will be calibrated prior to the start of formal testing.

6.4 Test Verification

OXY is invited to witness any in-plant test including OEM vendor acceptance testing. Spacelink Systems will prove a two-week notice in writing prior to the start of in-plant testing.

7.2 Drawing List and Family Tree

The drawing list will present, in a table-of-contents format, all drawings comprising the station equipment. The family tree will present the same information in the block diagram format. Both the list and the family tree will include assembly drawings, block diagrams, schematics and cabling diagrams.

7.3 Equipment Drawings and Data

Spacelink Systems will provide complete documentation required for defining the installation, maintenance and repair of earth station equipment. The following data identifies those requirements and lists the types of drawings to be provided to the customer.

1. Block and Level Diagrams - These will clearly and accurately depict the station equipment and interconnections, from the overall block diagram to the printed circuit board level or equivalent. Operation ranges, frequencies and nominal levels will be shown at appropriate points, from the antenna to the channel equipment interfaces.

2. Cabling Diagrams - These will show the location, type, size, number of conductors, etc., of the cabling interconnecting the various equipment throughout the station. The plug, jack, and terminal identification markings will correspond to that found on the equipment.

3. Wiring Lists - These will list the terminals of all wiring and cabling that interconnect separate chassis outside a given bay or rack.

7.4 Interface Document

Spacelink Systems will provide OXY with an interface document which will include but not be limited to the following items.

1. Detailed drawings with associated documentation to readily identify and define all interfaces with other station systems and/or facilities.
2. A complete delineation of input and output levels, frequencies and impedances.
3. Description of connectors used for signal interface and prime power connections.
4. Cabling proposed for equipment/control panel interconnections.

5. Space provided for all non-contractor provided equipment.

7.6 Earth Station System Manual - Content and Layout

Information in the Earth Station System manual will be placed in the following sequence:

Index

System Description

Theory of Operation

Routine Maintenance

Warranties

Appendices

7.6.1 Index

The index will be arranged and presented in such a manner to provide the user with a means to locate any and all data in all manuals.

7.6.2 System Description

The content of this section will be such that the users having a general interest in the system can easily and rapidly determine the purpose, physical and functional characteristics, and the operational capabilities of the system. The information will include but is not limited to the following:

1. Purpose and use of system
2. Physical arrangement of system
3. Equipment description
4. Performance specification
5. Reference data

7.6.3 Theory of Operation

This section will include a detailed analysis of the principles of operation and the overall subsystem and its major functions. The discussion will be presented in three levels. The first level will be on the complete subsystems and will be keyed to an overall functional block diagram. The second level will discuss each of the major functions and will be keyed to detailed block diagrams that will illustrate the development of each major function from its origin to its output. The third level will provide a detailed analysis of those circuits and components that are unique or unusual. This analysis will be keyed to simplified schematics or logic diagrams, as applicable.

3. Master Provisioning List

This list will be a tabular listing of all repairable and replaceable parts comprising each equipment item, assembly, or subassembly. The list will be prepared in sections, corresponding to the various separately identifiable systems of the station. It will conform as closely as possible to the systems breakdown used for other documentation.

4. Spare Parts List

The list will be a compilation of those items recommended to be purchased from the list of spares submitted at the OXY's request.

5. Tools and Test Equipment List

The tools and test equipment list will specify all tools, appliances, accessories, and test equipment required for the efficient operation and maintenance of the station. The list will identify each item by name, manufacturer, part number of model number, any required options or modifications, and major use.

6. Master Maintenance Schedule

A master maintenance schedule will be provided listing and recommending a schedule of all periodically-required maintenance activities, such as adjustments, cleaning and lubrication for the entire station. Detailed procedures will not be included if they are found in the system handbooks or other documentation and are clearly referenced in the master maintenance schedule.

7.7 Equipment Manuals - Content and Layout

Equipment manuals will be furnished to provide an integrated explanation for the operation and maintenance of each of the following subsystems in the following sequence:

Antenna structure
Antenna electronics
Uplink
Downlink
All power
Miscellaneous equipment

The manual will include all text, block and level diagrams, parts lists and schematic diagrams, as required for technicians to install, operate, troubleshoot, and maintain the equipment.

7.8 Training Manual

The training manual offered in the optional training package, if purchased, will duplicate much of the system manual information as well as provide general information not contained in the above deliverable documentation complement.

8.0 PRODUCT ASSURANCE

8.1 Spacelink Systems Quality Assurance Program

The Spacelink Systems Quality Assurance Program is based upon the considerations of the technical, production and fabrication requirements for Spacelink Systems products and services. The Spacelink Systems quality program provides adequate assurance of quality throughout all phases of performance, reliability, design, development, fabrication, inspection, integration, tests, delivery and site installation.

The Spacelink Systems Quality Assurance Program shall provide:

1. Objective evidence of quality conformance to include records of inspection sand tests.

2. Control of purchased and fabricated materials, services and related contracts.

3. Vendor qualifications and control.

4. Quality assurance considerations of engineering design changes.

5. Materials handling, storage and packaging controls.

6. Fabrication process controls.

7. Effective execution of responsibilities relating to customer furnished equipment.

8. In process and final product inspection and test.

9. Reliability considerations

10. Maintenance and maintainability considerations

The Spacelink Systems Quality Assurance Program shall assure the following services:

1. Inspection and Test: Receiving and shipping inspection and test to ensure that all supplies, products, materials and service conform to contract and or specification requirements. In-process inspection and test to substantiate conformance to drawings, specifications and contract requirements.

   Subsystem final inspection and test of completed products, systems and services to assure their conformance to performance specifications and contractual requirements. In the event modifications, repairs or replacements are required subsequent to final Inspection or test, reinspection or retest of the affected characteristics shall be performed. Inspection and test records for review of specified tests and inspections.

8.3.1 Quality Policy and Procedures

Process instructions and checklists are the responsibility of the operating element responsible for the work. Quality assurance audits the operations for adherence to their published instructions and checklists.

8.3.2 Production and Operations Work Orders

Production work orders and operations work orders are originated and controlled by the Program Manager. The work order system provides the visibility required to effectively control program execution and schedules.

8.3.3 Inspection

Inspection is performed utilizing drawings, operations sheets, job travelers, and inspection checklists/procedures. Tests are performed in accordance with the specified test procedure. All inspections and tests shall be recorded for traceability of subsystem and system quality conformance.

8.3.4 Corrective Actions

Corrective actions are originated by the Program Manager, as required, as the result of inspections, tests or audits. Copies of the corrective actions are forwarded to the responsible individual for corrective action. A built in suspense system and follow-up procedure for corrective actions assures the resolution of the discrepant condition or process. The corrective action system provides the basis for analysis and feedback of information for quality improvements. Reliability considerations requiring failure analysis techniques will be instituted as required on a closed-loop reporting system to ensure actions to rectify unsatisfactory performance.

8.3.5 Material Handling, Storage and Movement

Material handling, storage and movement shall be accomplished in a manner that will preserve the item in terms of quality and functional requirements. Material handling is the responsibility of the functional managers supporting the program.

8.3.6 Engineering Design

Engineering design adequacy is the responsibility of the engineering department. Quality implications and characteristics shall be considered in the applications of design review.

8.3.7 Procurement Cycle

Incoming shipments of material and services will be inspected in accordance with the purchase order for compliance to specifications and/or purchased material inspection instructions. Supplier performance will be measured through an analysis of incoming inspection records and vendor evaluation techniques.

9.0 TRAINING

9.1 Introduction

Spacelink Systems, Inc., is proposing an operations and maintenance training program in accordance with the requirements of the specification. The proposed personnel training includes formal classroom training and practical hands-on training.

The following sections provide a description of the proposed training course.

9.2 Scope of Training

The operations and maintenance (O&M) training proposed for the program will consist of the following:

Maintenance and Operations Training Course

The training course will be conducted in two sessions including the classroom phase and the hands-on phase. The classroom phase will include formal training for up to five (5) individuals. The classroom training will be conducted at Spacelink Systems Headquarters in Friendswood, Texas over a period of five (5) days.

The hands-on phase will be conducted after the classroom phase and will be held concurrently with the final in-plant acceptance test.

The above training courses will utilize the furnished earth stations and the supplied documentation to familiarize the company employees with the operations and maintenance of the earth stations.

9.3 Training Course Objectives

The purpose of the O&M training course is to familiarize the company employees with the day-to-day operations and maintenance of the satellite earth stations and equipments, and the use of the supporting O&M manuals, drawings and documentation.

3. Classroom Training Aids

The classroom training aids will include a chalkboard, overhead projector/screen, student handouts and examination materials.

4. Equipment to be Supplied

The actual equipment to be supplied will be used for the familiarization operations and maintenance training.
In general, the system related subjects will use the system-level documentation as training material. Typical subjects in this category include the system/network familiarization, overall system operation and maintenance, performance verification and testing.

On the other hand, the equipment related subjects will utilize the vendor O&M manuals and the actual equipment for the training materials. The training aids will supplement the above training materials, where required.

The above training material accomplishes the training objective by familiarizing the students with the earth station system, the various subsystems and equipments comprising the system, the system level documentation and the equipment level operations and maintenance manuals.

9.6 Training Course Details

Spacelink Systems will develop and submit for OXY approval a training plan course outline by the Critical Design Review. The outline will indicate the subject to be covered as well as the emphasis on each subject. In addition, the outline will indicate the formal, hands-on and OJT sessions for each course.

A typical equipment training session agenda, shown in Table 9.6- 1, will cover overall equipment operation, detailed discussion of equipment functions, operating procedures, preventative (scheduled) maintenance, fault isolation and troubleshooting, module replacement procedures, and the equipment repair and alignment procedures.

The training course will be conducted on an eight hour per day basis with time allocated for subject review, group discussions and examination purposes. The course instructor will be an engineer with an overall understanding of the entire earth station. For the hands-on and OJT sessions, the course instructor will be assisted by a Spacelink Systems technician.

9.7 Training Program Evaluation

The training course will be evaluated to ensure student comprehension and the achievement of the course objectives. The evaluation will be as follows:

1. The formal classroom training will be evaluated through the administration of the final examination. The examination will be followed up with a discussion/review session to resolve problems, unanswered questions and any area of misunderstanding.

2. The "hands-on" maintenance and operations training will be evaluated by the instructor. The instructor will "hands-off" supervise the students while they perform the maintenance and operations procedures.

The students will also be asked to critique the training program at graduation. In addition, each student will be issued a training certificate at the completion of the training course.

ITEM	QTY	DESCRIPTION	EXTENDED COST
.	1	Hub Related Equipment for Link from Quito to the U.S. including: a) SSE 20W Satellite Radio b) Variable Power Combiner c) EF Data Variable Rate Modem d) IF Splitter/Combiner Panel e) Miscellaneous Cable, Connectors, and Hardware	$ 41,000

ayment

Progress payments as follows:

Contract Award	: 40%
System inspected and sealed for delivery to freight forwarder	: 40%
Installation Acceptance	: 20%

Warranty

Spacelink Systems, Inc. warrants that the equipment will be free from defects in material and workmanship for a period of one (1) year from the date of equipment delivery.

At any time within the one (1) year period from delivery, Spacelink Systems, Inc. at its facilities in Houston, Texas, and at its own expense, will correct or replace, within thirty (30) days (if materials are available within a reasonable time), any equipment which is defective in design, materials, or workmanship, provided the Customer gives Spacelink Systems, Inc. prompt written notice of such defect and pays all costs of shipment to the Spacelink Systems designated repair facility. Shipments of repaired or replaced equipment to the Customer will be FOB Houston, Texas.

Should the defective equipment be a fixed part of the earth station, field warranty service may be necessary. In this case, unless otherwise agreed upon, Spacelink Systems, Inc. will begin on-site repairs within five (5) days of receipt of notice of defective equipment and make every effort to begin repairs within twenty four (24) hours of arrival. The Customer shall reimburse Spacelink Systems, Inc. for all per diem and travel expenses. Spacelink Systems will bear the costs of materials and labor associated with the on-site repairs.

Spacelink Systems, Inc. makes no warranties, express or implied, except as stated above, and Spacelink Systems, Inc. shall have no responsibility or liability for any special, incidental or consequential damages, including loss of profits, incurred or suffered by the Customer or others, even if Spacelink Systems, Inc. has been advised of the possibility of such damages.

11.0 REFERENCES

EXPERTISE AND REFERENCES

SPACELINK SYSTEMS TEAM have established themselves as industry leaders in providing th services and skills required to successfully complete all the requirements of the project proposed.

The **SPACELINK SYSTEMS TEAM** has successfully completed complex international and domest projects. Examples of previously completed projects include:

ECUADOR

Designed, engineered, installed and maintain a private digital satellite network providing voice electronic mail and facsimile transmissions for a major oil and gas company.

EGYPT, MALAYSIA AND TUNISIA

Engineered and installed a VHF/UHF radio based voice and data network supporting operations fo an offshore major international oil company.

GABON

Engineered and installed VHF/UHF radio based voice and data network supporting operations for an offshore major international oil company. This includes international connectivity to the United States.

NDONESIA

Microwave network engineering.

IEXICO

arth Station engineering and installation services.

ERU

esigned, engineered, installed and maintain a private digital satellite network for a major oil company.

RINIDAD

signed, engineered. installed and maintain a private digital satellite network for a major oil company.

U.K.

Provided secure phone lines for voice, fax and data transfer.

U.S.A.

Designed satellite based digital voice network for helicopter flight tracking from centralized cor center, covering Gulf of Mexico.

Provide satellite communications services supporting domestic drilling and production operations Spacelink's 7.2 Meter C-Band earth station.

Designed, engineered and installed a stabilized Ku-Band Satellite System providing Voice/D communications in offshore deep-water Gulf of Mexico.

Installed various radio microwave communication systems in Alaska for the Valdez clean-up.

Engineered, designed and installed a Ku-Band hub facility and transportable earth stations for a ma exploration & production company to be used throughout the Midwest U.S.

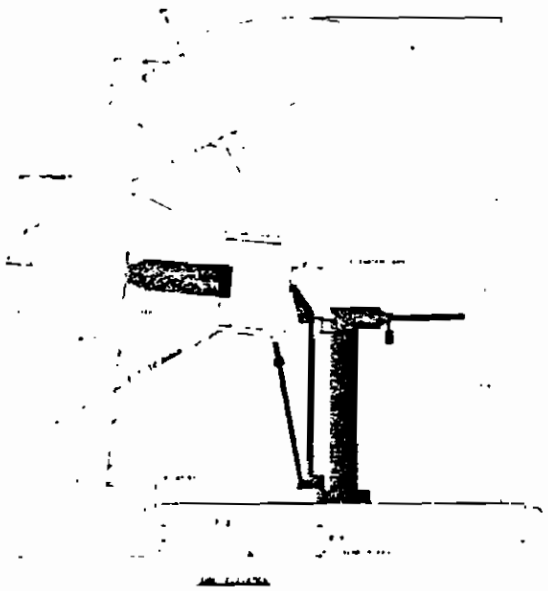
Company	Contact	Telephone
Mobil	Bill Hebert	(214) 951-4701
Mobil	John Marchand	(214) 951-4701
Unocal	Willie Frost (now working w/Arco Int'l)	011-5932500919
Conoco	Jim Jeffries	(318) 236-5252

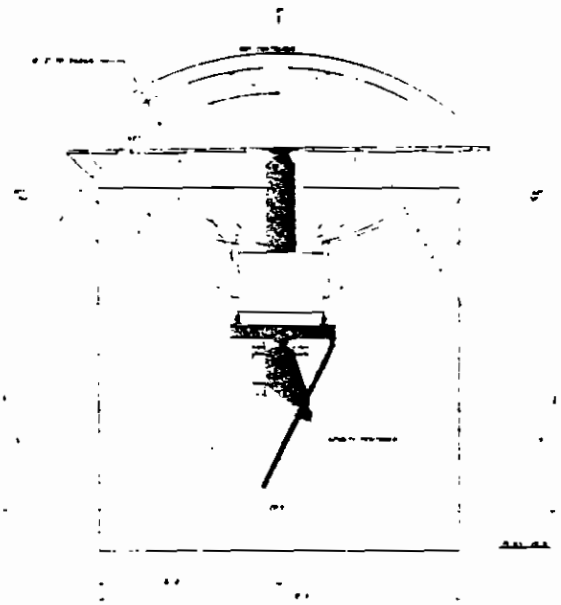
PERFORMANCE SPECIFICATIONS

ency*	3 7-4 2 GHz	5 925-6 425 GHz	3 7 4 2 GHz	5 925-6 425 GHz	11 7 12 2 GHz	
al Gain at Midband	43 6 dB	47 2 dBi	43 6 dB	47 2 dBi	53 0 dBi	
h	1 25 1	1 25 1	1 25 1	1 25 1	1 25 1	
width – 3 dB	1 14°	0 70°	1 16°	0 75°	0 37°	
– 15 dB	2 40°	1 47°	2 35°	1 54°	0 76°	
ma Noise Temperature at Midband					2 Port Feed	
E Elevation	47°K		52°K		72°K	
E Elevation	36°K		41°K		56°K	
E Elevation	30°K		35°K		47°K	
E Elevation	25°K		30°K		43°K	
al G/T at 20° Elevation Clear Horizon 4 GHz						
th 40°K LNA dB/°K	24 8		24 5			
th 65°K LNA dB/°K	23 6		23 3			
al G/T at 20° Elevation Clear Horizon 12 GHz						
th 90°K LNA dB/°K					31 3	
th 150°K LNA dB/°K					29 8	
er Handling Capability		10 kW**		10 kW**		
Interface	CPR-229G	CPR 159G	CPR 229G	CPR-159G	WR-75 Choke	
Insertion Loss	0 10 dB	0 15 dB	0 15 dB	0 20 dB	0 3 dB	
to-Port Isolation Tx to Rx	30 dB	30 dB	30 dB	30 dB	30 dB	
Rx to Rx, Tx to Rx Linear (4 Port Feed)			30 dB	30 dB		
Rx to Rx, Tx to Rx Circular (4 Port Feed)			21 dB	21 dB		
s Polarization Isolation On Axis	35 dB	35 dB	30 7 dB	30 7 dB	35 dB	
Within 1 dB Beamwidth	35 dB	35 dB	30 7 dB	30 7 dB	35 dB	
Ratio (Circular Polarization) 2 Port Tx/Rx	1 8 dB***	1 8 dB***				
4 Port Frequency Reuse			0 5 dB	0 5 dB		
obe Pattern Performance						
st Sidelobe	– 14 dB		– 14 dB		– 14 dB	
or A beyond 1st Sidelobe to 48°	32 25 Log A dBi		32-25 Log A dBi		32 25 Log A	
or A from 48° to 180°	– 10 dBi		– 10 dBi		– 10 dBi	
ther frequencies available	Meets IESS (Intelsat		Meets IESS (Intelsat			
higher power optional	Standard F)		Standard F)			
Other ax al ratio feeds available	specifications)		specifications)			

Operational Winds	45 mi/h (72 km/h) gusts to 60 mi/h (97 km/h)
Survival Winds (Any Position)	125 mi/h (200 km/h) @ 58°F (15°C)
Ambient Temperature (Survival)	– 29° to 60°C (– 20° to 140°F)
Rain (Operational and Survival)	Up to 4 in/h (10 cm/h)
Relative Humidity (Operational and Survival)	0% to 100% with condensation
Solar Radiation	360 BTU/h/ft² (1000 Kcal/h/m²)
Radial Ice (Survival)	1 inch (2 5 cm) on all surfaces or 1/2 inch (1 3 cm) on all surfaces with 80 mi/h (130 km/h) wind gusts
Shock and Vibration	As encountered during shipment by commercial air rail or truck
Corrosive Atmosphere	As encountered in coastal regions and/or heavily industrialized areas
Seismic (Survival)	Mercalli X

Specifications and product availability subject to change without notice





Azimuth Travel	120° continuous	Finishes	
Azimuth Trave Rate	1 8°/second variable	Reflector Surface	Aluminum panels with heat-diffusing white paint
Elevation Travel	5° to 85° continuous	Pedesta	Red oxide primer and two coats of enamel
Elevation Trave Rate	1 0° second variable	Surface Accuracy	0 020 inch (5 mm) Static
Polarization Trave	± 90°	Foundation Sizes	12 5 ft x 12 5 ft x 1 25 ft (3 81 m x 3 81 m x 0 38 m)
Polarization Travel Rate	1 5°/second		
Weight – Reflector	650 pounds (295 kg)	Concrete Volume	7 25 cubic yards (5 5 m³)
Weight – Pedesta	800 pounds (363 kg)	Reinforcing Steel	500 pounds (227 kg)
Shipping Weight (Typical)	3 150 pounds (1429 kg)	Soil Bearing Pressure	2,000 PSF (10 000 kg/m²)
Shipping Volume	485 cubic feet (13 7 m³)		

VERTEX

2600 LONGVIEW STREET • P.O. BOX 1272 • KILGORE, TEXAS 75662 • 214-984-0555

ANEXO 3

COMUNICACIONES DE OPEC

ANEXO 3

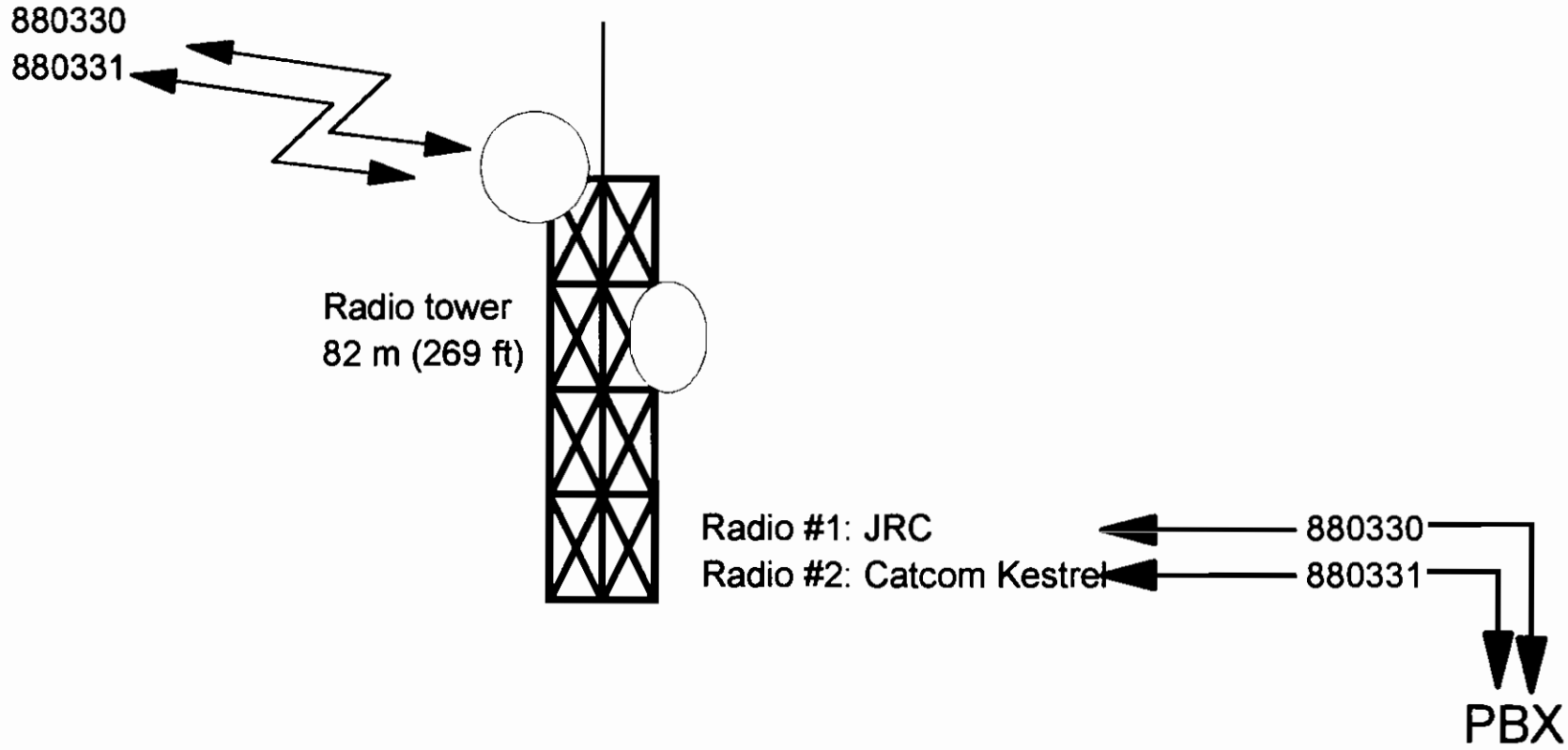
Los gráficos que se encuentran en este Anexo son: "Radio Telephone line stretchers (Coca-CPF, CPF)", "Dedicated line remote radio telephone", "VHF remote radio".

La importancia de estos sistemas radica en que antes de ser instalado el sistema de comunicaciones vía satélite las radiocomunicaciones a través de Emetel eran el único enlace que se tenía desde el CPF. Las comunicaciones se limitaban a transmisiones de voz ya que para datos la calidad de los canales no era buena.

Adicionalmente, este tipo de documentación facilita la comprensión general de los sistemas, de tal manera que una persona que no tenga conocimiento de ellos, puede en el menor tiempo posible tener una comprensión de la lógica de trabajo de éstos.

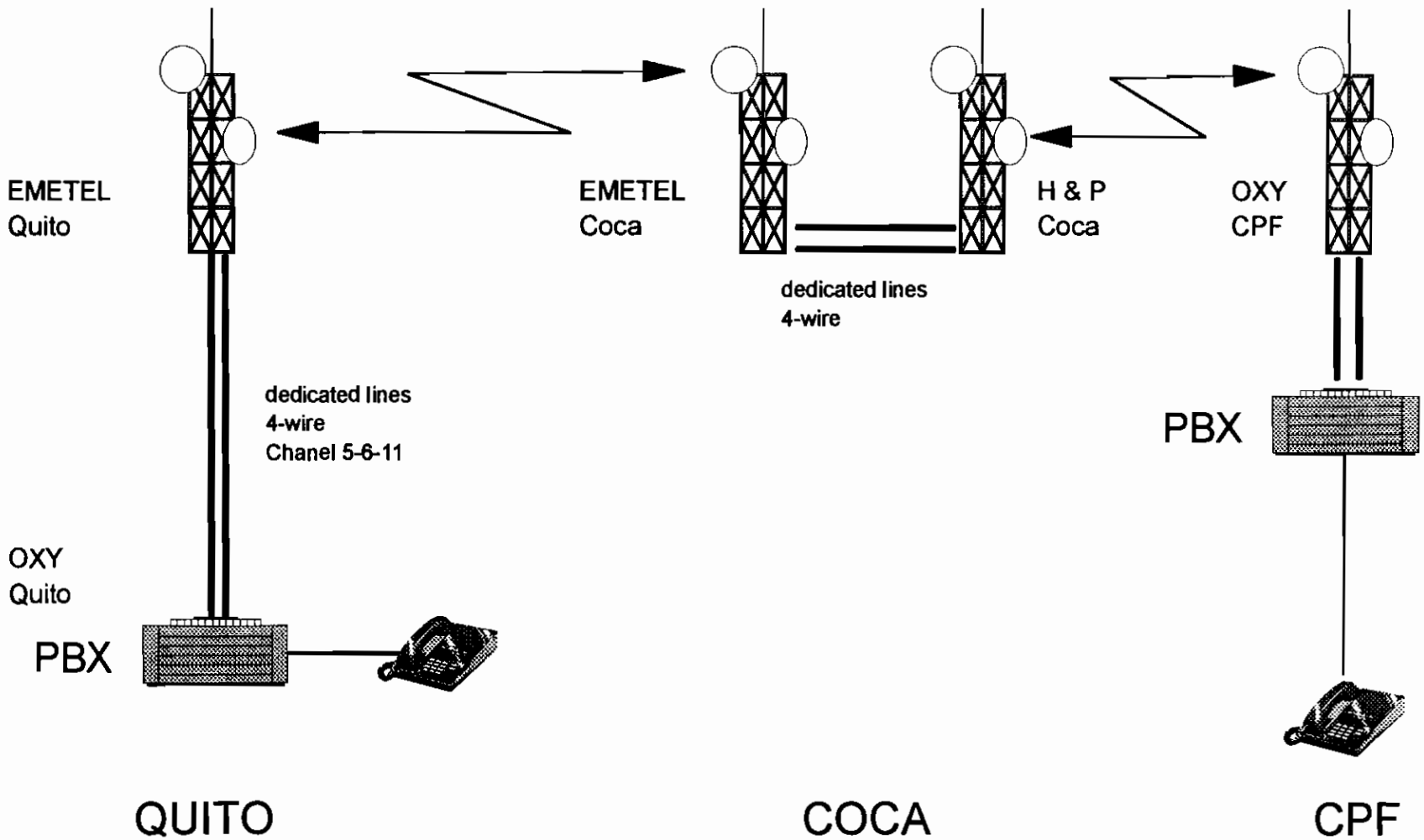
Este folleto fue elaborado en conjunto con una serie de folletos de comunicaciones por el Ing. Luis Monge, el Ing. Alfredo Corral y Fernando Granizo con el afán de documentar esquemáticamente el estado actual de las comunicaciones.

Line stretchers: CPF



CPF

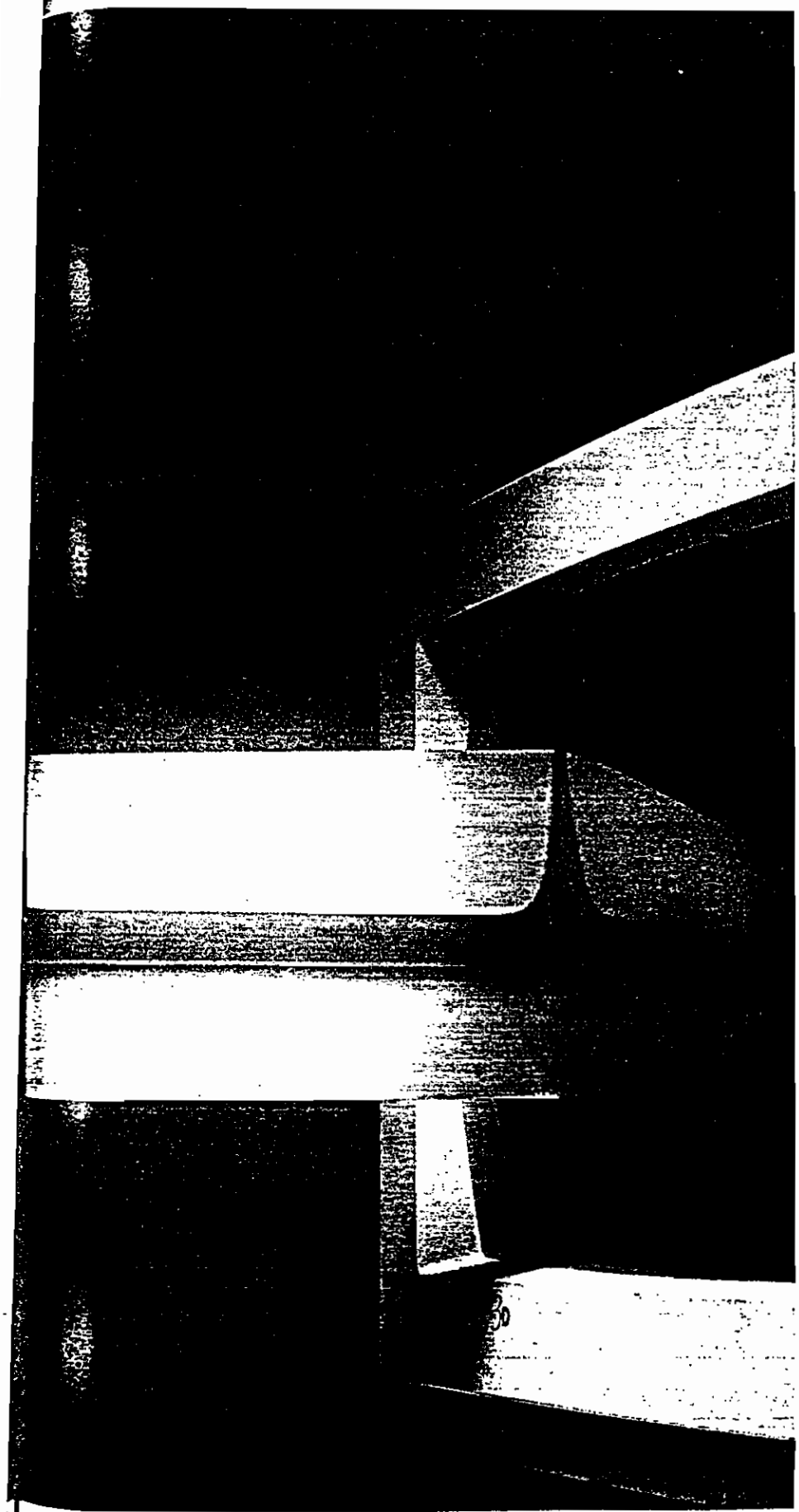
Dedicated Line
Remote Radio Telephone



ANEXO 3-4

ANEXO 4

ARTICULO "PLEASE MISTER POSTMAN"



PHOTOGRAPHY: PAUL AVIS © 1991

BYTE ACTION SUMMARY

- **E-MAIL SOFTWARE**
- **WHAT IT DOES**
  E-mail packages let you compose, edit, and send messages and attach files to them for delivery to other users. Many packages also offer optional gateways that let you exchange messages with users at remote sites or who are using a different E-mail system.
- **SHOULD YOU BUY?**
  E-mail software makes the most sense in LANs where users are geographically dispersed. In workgroups where users sit in proximity, the extra headaches of administering the E-mail system probably aren't worthwhile. For users who need to correspond with people across the building or across the country, E-mail systems can eliminate "phone tag" and improve productivity.
- **WHAT WE RECOMMEND**
  QuickMail's superb user interface, gateway options, and voice-mail capability make it our choice for AppleShare users. For mixed PC and Mac LANs (non-AppleShare), cc:Mail has the best user interface; it also includes a graphics editor and an array of gateway options. The Coordinator supports PC LANs only, but we found its ability to organize messages as ongoing communications threads particularly useful.

UUCP (Unix-to-Unix copy) or SMTP gateway (for the Unix perspective on E-mail, see the text box "E-Mail Under Unix" on page 226).

Some packages support a few specific LANs; others will work with any LAN that supports DOS 3.1 file locking. All packages offer at least a rudimentary text editor, and some offer a graphics editor as well. Some products restrict the number and type of files you can attach. And not all E-mail programs encrypt files—an important consideration if you don't want your mail read by others.

Other extras include voice-mail capability, on-line conferencing, and the ability to set up BBSes where people can post public messages. Many packages also let you call in and download your mail messages when you're out of the office. The E-mail features table on page 224 will

E-MAIL SYSTEMS: FEATURES SUMMARY

Finding the right E-mail system starts with the computer systems and network environments you need supported. Some vendors offer and support their own gateways to E-mail services and other LAN- and host-based E-mail systems. Other vendors rely on companies like Soft•Switch to fill in the gaps. Support and licensing policies also vary considerably. (N/A = not applicable; ● = yes; ○ = no.)

Product name and version	cc:Mail 3.15	The Coordinator 2.1	eMail 1.07	Higgins Mail 2.3	Microsoft Mail 2.0	InBox Plus 3.0	The Network Courier 2.1	QuickMail 2.2.3	Network Mail for Vines 4.0
Company name	cc:Mail, Inc.	Action Technologies	Da Vinci Systems	Enable Software	Microsoft Corp.	Sitka Corp.	Consumers Software	CE Software	Banyan Systems
CONFIGURATION									
Workstation environments supported	DOS, OS/2, Mac	DOS	DOS, OS/2, Windows, NewWave	DOS, OS/2	DOS, Mac	DOS, Mac	DOS, OS/2, Windows, Mac	DOS, Mac	DOS, Windows
Network environments supported	Any DOS 3.1+ compatible or AppleTalk Filing Protocol–compliant network	NetWare 286/386, NetBIOS, MS-Net	Any DOS 3.1+ compatible network	Any DOS 3.1+ compatible network	AppleTalk or compatible	NetWare 286/386, LAN Manager, Vines, AppleShare, TOPS, NFS	NetWare 286/386, LAN Manager, Vines, NetBIOS, MS-Net	AppleShare	Vines
Requires dedicated mail server?	○	○	○	○	○	○	●	○	○
Mail location	Server	Server or local disk	Server or local disk	Server	Server	Server or local disk	Server or local disk	Server or local disk	Server
BBS support	●	○	○	○	○	●	●	●	○
Conferencing	○	○	○	○	○	○	○	●	With Vines
Remote user access	●	●	●	●	○	●	Option (DOS only)	●	Option
Automatic forwarding to remote mail servers via dial-up connection?	●	●	●	●	●	●	●	●	●
MESSAGE CREATION									
Text editor	●	●	●	●	●	●	●	●	●
Graphics editor (formats supported)	● (cc:Mail)	○	○	○	● (PICT)	○	○	○	○
Voice-mail capability	Third-party option	○	○	○	●	○	○	●	○
Message attachment types supported:									
Text	●	●	●	●	●	●	●	●	●
Graphics	●	●	●	●	●	●	●	●	●
Binary	●	●	●	○	●	●	●	Mac only	●
Attachments per message	20	1	Unlimited	Unlimited	1	Unlimited	Unlimited	16	10
Can assign message priority?	●	○	●	●	●	●	●	●	●
Message-delivered acknowledgment?	●	○	●	●	●	●	●	●	●
MESSAGE RECEIPT									
Message alert (beep, pop-up window, text prompt)	All	None	All	All	All	Beep, text, icon	All	Beep or blinking icon	Beep, text prompt
Notification via workstation TSR	●	●	●	●	●	●	TSR or NetBIOS	●	Vines redirector
TSR memory required (K bytes)	<15	8	3	3.5	25	18	78	<15	N/A
View attachments	Text only	Text only	○	○	Mac Word, Excel, PageMaker files	○	○	○	Text only
ADMINISTRATION									
Read any message	○	●	●	○	○	●	○	●	●
Delete any message	○	●	●	○	○	●	○	●	●
Purge old messages	●	●	●	●	○	●	●	●	●
Define user mail space	○	●	●	●	○	●	●	○	●

help you find the package with the features you're looking for.

Special Delivery

Anytime a mail message has to be sent off-site, there has to be a way of converting it from a local LAN message to something better suited for travel. An E-mail bridge connects two similar E-mail systems. Let's say your company has offices on the East and West coasts. If someone on the East Coast tries to send E-mail to the West Coast, the East Coast mail server, using the companywide mail list, will dial up the West Coast office and transfer the message via modem. The West Coast server simply routes the incoming message to the appropriate mailbox.

E-MAIL SYSTEMS: FEATURES SUMMARY (CONTINUED)

Product Name and version	cc:Mail 3.15	The Coordinator 2.1	eMail 1.07	Higgins Mail 2.3	Microsoft Mail 2.0	InBox Plus 3.0	The Network Courier 2.1	QuickMail 2.2.3	Network Mail for Vines 4.0
SECURITY									
User account password	●	●	●	●	●	●	●	●	●
Message/attachment encryption	●	○	●	●	○	●	●	○	○
GATEWAYS									
MHS	Option	Option	Option	Option	Third-party	Option	Third-party	Option	Third-party
User-definable gateway via scripting language?	Option	●	○	Option	○	○	●	●	○
X.400	Option	Third-party	Option	Option	Third-party	Third-party	Third-party	●	Third-party
Fax	Option	Third-party	Option	Option	Third-party	Option	Third-party	●	Third-party
SMTP	Option	Third-party	Option	Option	Third-party	Option	Third-party	●	Option
Public E-mail services:									
MCI Mail	Option	Third-party	Option	Third-party	Third-party	○	Option	●	Third-party
Western Union EasyLink	Option	Third-party	Option	Third-party	○	○	○	○	Third-party
AT&T Mail	○	Third-party	Option	Third-party	○	○	Third-party	●	Third-party
CompuServe	○	Third-party	Option	Third-party	○	○	○	●	Third-party
Sprint Mail	Option	Third-party	○	Third-party	○	○	Third-party	●	Third-party
Other E-mail gateways:									
DEC All-In-One	Third-party	Third-party	Option	Third-party	Third-party	●	○	●	Third-party
IBM PROFS	Option	Third-party	Option	Option	Third-party	●	Third-party	○	Third-party
IBM DISOSS	Third-party	Third-party	Option	Option	Third-party	●	Third-party	○	Third-party
Banyan Vines Mail	○	Third-party	Option	Third-party	Third-party	○	Third-party	●	N/A
DEC VMS Mail	Third-party	Third-party	Option	Third-party	Third-party	●	○	●	Third-party
Wang Mailway	Third-party	Third-party	Option	Third-party	Third-party	○	○	○	Third-party
Others	UUCP	None	QuickMail, VoxMail, Network Scheduler	3+Mail	None	None	AppleLink	UUCP	Mac Vines Mail
SUPPORT									
On-line help	●	●	●	●	●	●	●	●	●
Support line (800# or toll call)	Toll	800#	800#	800#	Toll	Toll	800#	Toll	Toll
Telephone-support policy	Unlimited	3 years	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited[2]	Unlimited	Through VAR/dealer
On-site training available?	●	●	●	●	○	Through VARs	●	○	●
Site license available?	●	●	●	●	○	○	●	●	○
Price	$695.25 for DOS users; Mac or OS/2: $495 per server	$1800 for 10 users; $4500 for 50 users	$995/server w/DOS interface; $1195/server w/Windows, DOS, OS/2 interface; $195/NewWave user	$295 for 8 users; $695 site license	$1329 for 20 users	20-user InBox license $329; 50-user DOS Administrator: $995; 50-user Mac Administrator: $995	Single-server: $295 for six users; $695 for 150 users Inter-Network version: $995 per server[3] Additional interfaces: $595 per server	Mac: $499.95 for 10 users; DOS: $469.95 for 10 users	$995 per server

DOS front-end software requires running document conversion utility to attach text files.
Support contract required for gateway assistance.
Inter-Network Courier is required for multiserver or inter-LAN connections. Server licenses include one user interface.

If the West Coast office uses a different type of mail system, you need to have a gateway to translate between the two message formats. The gateway's task can be as easy as rearranging the headers from one format to another, or it may require parsing through gobs of ASCII messages and prompts. Consumers Software and cc:Mail offer many such gateways as extra-cost options.

You may also need a gateway if you do business through commercial E-mail services, such as Western Union's EasyLink or AT&T Mail. The gateway collects outgoing messages and calls the E-mail provider periodically to send and receive messages. Some services also provide their own gateway software that routes

messages between LAN-based E-mail systems by way of the E-mail service.

The international E-mail interexchange standard, X.400, is so complex and costly to implement that currently only large enterprisewide networks and commercial E-mail service providers use these gateways. Action Technologies' Message Handling Service is less sophisticated but more widely implemented in smaller workgroup environments that need to interconnect dissimilar E-mail systems. MHS runs on a dedicated file server. Novell includes a copy of MHS with NetWare. Most of the E-mail vendors offer gateway software as an option that runs in conjunction with the MHS server.

The Arena

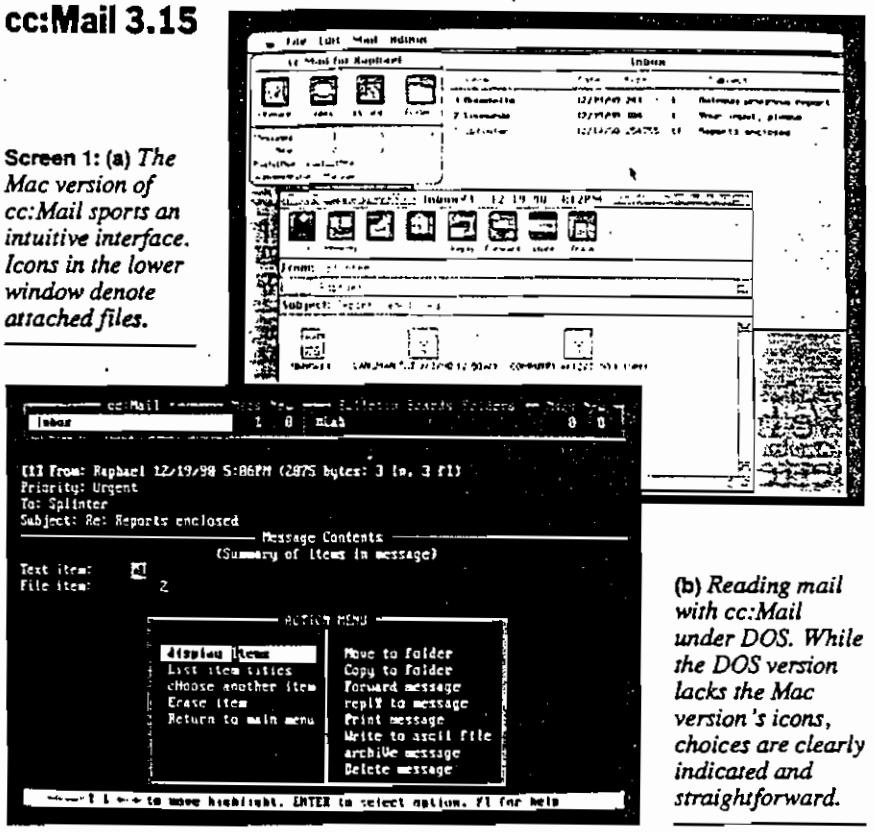
We concentrate here on nine best-selling packages that run on a variety of systems and networks. Most of them support Action Technologies' MHS, the current standard on PC LANs for exchanging messages between dissimilar E-mail systems (see the text box "MHS Gets the Mail Through" on page 231). Enable Software's Higgins Mail, Action Technologies' The Coordinator, and Da Vinci Systems' eMail run only on PC LANs. The rest of the packages we tested—cc:Mail, from cc:Mail, Inc.; The Network Courier, from Consumers Software; Sitka's InBox Plus; Microsoft Mail; and CE Software's QuickMail—support mixed DOS and Macintosh environments. If you can get your machines to share files, you'll be able to share E-mail, too.

Banyan Systems' Network Mail for Vines didn't meet our criteria because it works only on Vines networks, but it has a following among Vines users. We discuss it in the text box "Banyan's Network Mail for Vines" on page 234.

We put these nine E-mail packages to work on three test networks. We used a LocalTalk PC card and interface software to connect a 386 clone running DOS to our AppleShare network. We also tested all the E-mail packages on PC LANs running Vines and NetWare.

None of the packages was particularly easy to install or maintain. You should consider E-mail software to be in the same class as file-server software. Your network administrator should install it, set up the user lists, and get the bridges connected. A system administrator should be able to easily manage any of these E-mail systems, but for large installations that require gateways, help from an experienced installer is invaluable.

cc:Mail 3.15



Screen 1: (a) *The Mac version of cc:Mail sports an intuitive interface. Icons in the lower window denote attached files.*

(b) *Reading mail with cc:Mail under DOS. While the DOS version lacks the Mac version's icons, choices are clearly indicated and straightforward.*

The cc:Mail package comes in DOS, OS/2, and Mac versions and offers optional gateways to many other E-mail systems. cc:Mail uses your network file server to provide mail services. It encrypts messages and stores them as data files on the server's hard disk. Installation and administration aren't easy. There's no installation program—just a fat administrator's manual full of instructions.

A PC needs an AppleTalk-compatible network card and the appropriate network connector (in our case, LocalTalk) to access an AppleTalk network. We used an Apple LocalTalk PC card connection to add a 25-MHz 386 PC to our Mac network. The card's AppleTalk software provides services for printing and remote file access. These services are memory hogs, taking from 107K bytes to 170K bytes of RAM, depending on the network services you use. However, the card allowed us to place the data files in a folder on our AppleShare file server.

On the Mac, a desk accessory (DA) provides notification services, and an application manages your mailbox. When you first launch cc:Mail, you use a Standard File dialog box to locate the mail files on the server; cc:Mail then creates a Post_Office file. Once you've done this, from then on you simply double-click on this file, which launches cc:Mail, and information (i.e., the path to the server and your user name, stored as STR resources) in this file helps establish the connection. It feels a bit kludgey, but it works.

PC users run the Mail and Notify programs to manage their mailboxes and to install a TSR program that alerts users to incoming messages. The Messenger program also provides notification and sets up Alt-2 as a hot key to access mail services from DOS. When you run each of these programs, you must supply the mail directory's path, your mail name, and your password. cc:Mail should remember the message directory path: Users will be tempted to build a batch file to supply the path and other information, but this may compromise the security of their mailboxes. Under Windows 3.0, a postage-stamp icon of a minimized Notify program lets you list the messages in your mailbox and can switch you into cc:Mail.

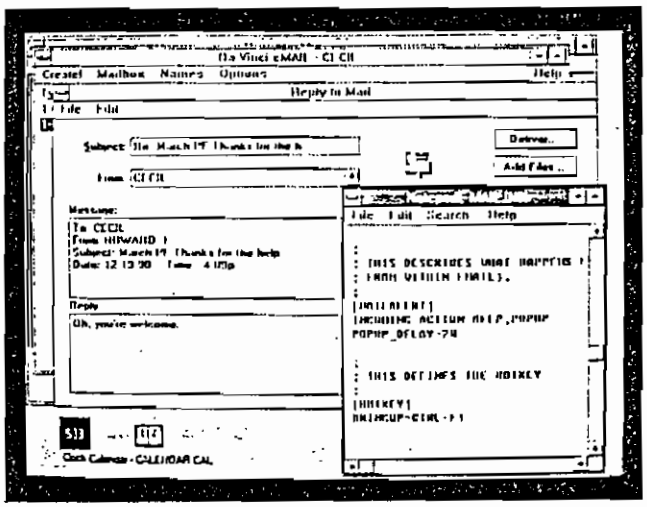
The Mac interface is simple and clean and makes good use of color. Of all the Mac E-mail packages, this one had the best interface. Various icons represent buttons that you click on to provide mail services such as reading, composing, and deleting messages. Each button has

of your current messages broken down by classification. You open a message by moving the cursor to it and pressing the Return key. A new window pops open, but, unfortunately, the cursor isn't there. In order to scroll through the message text, you must manually change to that window. The F5 and F6 keys switch between windows, or you can use the Scroll Lock key to modify the operation of the cursor.

IBM intended the Scroll Lock key on the PC to constrain the cursor from moving off the page of a document. But no one ever programs it this way. Usually, the Scroll Lock key is left undefined because no one knows what to use it for. Action Technologies set up the Scroll Lock key so that when you enable it, the up-arrow and down-arrow keys can scroll only the text within the current window. Pressing the key to disable Scroll Lock allows the cursor to leave the current window and move to the next one. Of course, once you're in the new window, you can't scroll until you reactivate Scroll Lock. It felt awkward to use the key the way it was intended—perhaps that's why no one else does.

Other keys are inconsistent from screen to screen. When you're selecting a message to operate on, for example, the Delete key deletes (or marks for deletion) the message. If you're composing a new message or reply, the Delete key opens up the addressing window.

eMail 1.07



Screen 3: *Da Vinci Systems' eMail running under Windows 3.0. The MAIL.INI file lets you customize eMail to your tastes.*

Da Vinci Systems offers versions of eMail for DOS, Windows, OS/2, and NewWave environments. The DOS interface uses control keys, and if you forget what to press, the F8 key brings up options. Besides that, the screen is essentially blank and offers no obvious hints. The addition of a few messages to the DOS screen would make eMail easier to use. The Windows version is cleaner and puts the functions where you'd expect them. It was necessary to read the manual to figure out the DOS version.

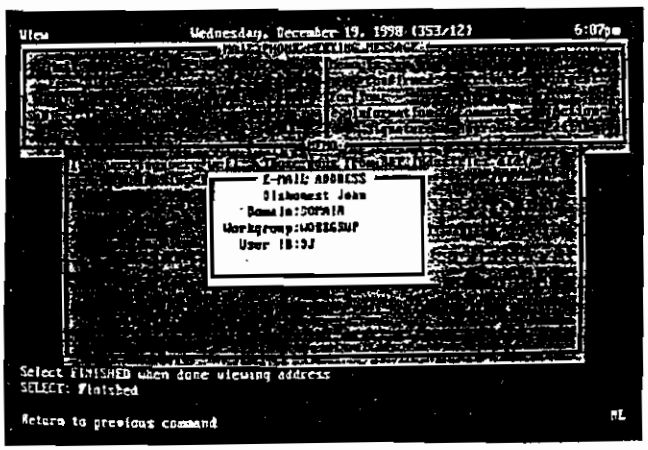
eMail lets you attach files to messages. Under Windows, you can send the contents of the Windows Clipboard to other Windows users. You copy something to the Clipboard and attach it, and the recipient pastes it into an application.

Security-conscious administrators may have a problem with eMail. Message files are easy to locate on the file server and remain unencrypted unless the sender specifically requests encryption. If you encrypt a file, the message sits on the server in unreadable form, and the recipient must type a password in order to accept the message.

Users have personal information files that define how eMail operates on their systems. They can change the polling frequency for incoming messages and the alert procedure, and they can customize their message alert sounds by changing the MAIL.INI file. The latter procedure makes it easier to tell whose machine received mail in offices where machines are closely grouped. We configured one of our machines to play reveille. That sounds like an obvious idea, but none of the other packages do it.

DOS users can run eMail as a standalone application or as a TSR program. The "micro TSR" format uses a swap file and takes up only 10K bytes of RAM. You define a hot-key sequence that swaps out your current application and loads eMail. When you exit eMail, it restores the interrupted application where it left off. Alerts can come through the Novell Send mechanism, or you can load a TSR that presents a one-line message at the bottom of the screen. Windows alerts will appear for a definable amount of time (the default is 20 seconds) and then disappear.

Higgins Mail 2.3



Screen 4: *The simple and efficient layout of Higgins Mail. Note the extended addressing capabilities that support E-mail over wide-area networks.*

Higgins Mail is the E-mail-only version of Enable Software's workgroup scheduler software. It runs on DOS and OS/2 machines.

Unlike The Coordinator, Higgins presents E-mail as an electronic version of slips of paper. We ran the user software on both NetWare and Vines without any problems. The administration software is heavily based on an ASCII menuing system that proved to be too large for the Vines workstations. Running the administrative menus resulted in an "insufficient memory" message.

Higgins Mail uses a shared database on the file server. The file structure is proprietary, and the message files them-

MHS Gets the Mail Through

Before Action Technologies introduced its Message Handling Service, there were no workable interexchange standards in the LAN E-mail world. Bundled with every copy of NetWare, an MHS gateway requires its own dedicated server and is a convenient way of moving information between E-mail systems. Because of widespread support for MHS, the product has become the least common denominator for interconnecting workgroup E-mail systems.

MHS provides a standard structure on the file server where your mail application can drop off messages; it puts the incoming messages in specific locations and manages the physical flow of messages between mail centers. When you install MHS, you create a structure in a publicly accessible spot. Anyone on the network can create a message packet and drop it in the MHS *in box*. Once you've created the message, the MHS utility software grabs the message and then processes it.

A standard MHS packet is an ASCII file containing several vital pieces of information. A version number (65 for MHS 1.2) tells MHS that this is an MHS mail packet. The next line has the "To:" field, and the following line has the "From:" field. Your E-mail front end is responsible for handling the addressing and providing complete MHS addresses.

If you have addressed the message to a user on the same MHS server, the server simply copies the file to that user's MHS mailbox. Periodically, an MHS E-mail front end has to poll the mailbox, looking for new messages. When it finds one, the software copies it from the MHS mailbox to the E-mail mailbox. If the address is for another mail center, MHS moves the message to an *out box* for further processing. At some time that is determined by the MHS *scheduler*, the server picks up the outbox mail and sorts it by destination. It then establishes a connection to the mail center and transfers the messages to the remote MHS site.

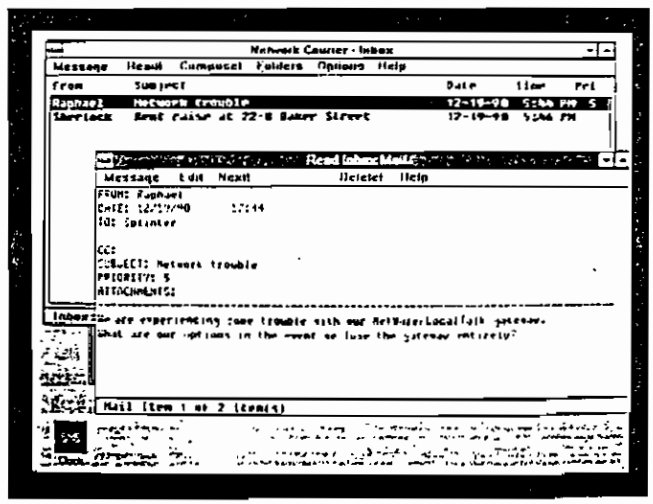
The remote MHS server then picks up and sorts the messages by address. From this point on, it's the same as if the mail were sent within the LAN. As far as a user at the remote site is concerned, the only difference is that the mail takes a bit of time to arrive. The E-mail software doesn't know about gateways or bridges. It just puts an address on the mail and sends it out. MHS takes care of the dirty work.

MHS server gateways work differently from other E-mail gateways. The MHS scheduler can execute programs as part of the scheduled process. These programs are usually file converters or message formatters, much like the ones the gateway software would use in some other mail program. MHS defines a gateway as one of these special programs and can dispatch it to each message in the in box.

ager icon blinks in the Apple menu. If you're using MultiFinder, you can let the InBox Plus application run in the background, which leaves a small, movable "hot window" when you switch to another application. Clicking on this hot window gets you back into InBox Plus, where you can read, delete, store, and print letters. Templates for memos and phone messages are built in. Several buttons with icons let you select certain operations (e.g., printing, deleting, composing new mail, and enclosing files) rapidly.

On the PC, you get a "crawler" message across the top of the screen stating who sent you mail. It moves across the screen once and sounds a chime, but it won't reappear if you miss it. The menu layout resembles the Mac's, and you use the Tab and Alt keys to navigate through the menus. Copious use of function keys takes the place of Mac buttons. This provides a consistent interface that lets you quickly read and write letters on either platform. However, there are differences. On the Mac, a paper-clip icon indicates that a message has an attached file; on the PC, an ampersand appears next to the message. Finally, InBox won't erase letters marked for deletion until you exit the program, so you can recover accidentally deleted messages.

The Network Courier 2.1



Screen 6: *The Network Courier's Windows 3.0 interface isn't fancy, but it works well—especially its Monitor feature.*

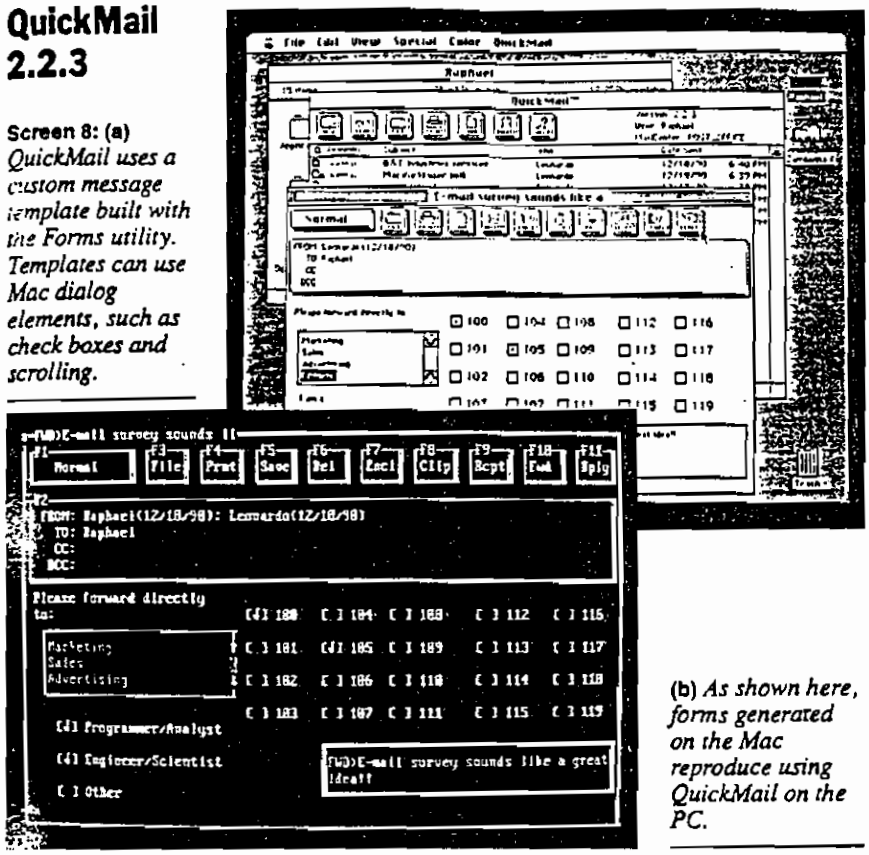
The Network Courier provides E-mail services for DOS, Mac, OS/2, and Windows users. Consumers Software also offers an extensive array of gateway options for interconnecting diverse computing environments.

Users exchange messages through virtual "post offices" that can in turn exchange messages. The Network Courier relies on the file services provided by network file-server software, such as NetWare, LAN Manager, and Vines, to operate.

The Network Courier includes a scripting language for writing programs that access, send, and receive messages from other on-line services via modem. Optional gateway software provides access to other mail systems, such as DEC VMS mail and MHS servers. Messages reside in subdirectories on the network's file server. The program uses the Department of Defense's Data Encryption Standard scheme to protect messages.

The Network Courier's install programs place data files and PC software

QuickMail 2.2.3



Screen 8: (a) *QuickMail uses a custom message template built with the Forms utility. Templates can use Mac dialog elements, such as check boxes and scrolling.*

(b) *As shown here, forms generated on the Mac reproduce using QuickMail on the PC.*

Like Microsoft Mail, QuickMail supports Macs and PCs but requires a Mac server and an AppleShare network. QuickMail was the only package we tested, except for Network Mail for Vines, that supports real-time conferencing—a handy feature. It's also one of the few packages to support voice mail.

QuickMail's Mac software loads as an INIT and installs a quick-access menu in the menu bar. Installing the user software is incredibly easy. The character-based DOS software doesn't mind running from a .PIF file under Windows.

Public messages appear as a BBS of sorts. Anyone on the network can read messages addressed to "public," but only the message creator or the administrator can delete them. We'd like this feature even better if QuickMail would let administrators assign expiration dates for public messages.

You create a new message by selecting the appropriate form. Standard forms are memos, notes, and "While You Were Out," but you can use QuickMail's form designer to create your own. Forms include a collection of check boxes, text objects, and, on the Mac, bit-mapped graphics. You draw a new form and then install it with a menu choice. Even better, if you attach the form as a mail message, the recipient's machine can automatically install it as soon as it arrives. It's a handy way to move new forms from one place to another.

Before you send a message, you must choose a priority level. QuickMail uses priority levels primarily for sorting messages, but the Urgent messages serve a special purpose. The DOS user interface has a separate alert for Urgent messages, and any messages sent through a gateway bypass the gateway's standard batch mode schedule and are sent immediately.

We expected the DOS software to be harder to use than the Mac software. Boy, were we wrong. CE Software has laid out the buttons in the same configuration as the Mac version and has defined the menus in the same way. Even the forms defined on the Mac translate directly to PC screen format. Mouse support on the PC is limited, and we found ourselves using the function keys most of the time. As a mimicry of a Mac interface, it's the best we've seen on a character-based screen.

On both platforms, incoming mail or conference activity automatically brings up the mail package. That can be a little disconcerting at first, and you can disable this function if it bothers you. Conferences display a multiwindow screen. One window shows the list of participants and lets you selectively target messages. A second screen shows the conversation thread; the third shows your input. We found conferencing to be one of QuickMail's strongest features, and one we'd use.

The only bug we found has to do with multiple registrations. When we set up a conference between Macs, we'd occasionally see one of the Macs appear on the registration list more than once. The Refresh menu option cleared this up, but it shouldn't have happened in the first place. The PC software didn't have this problem.

One last feature that you may find interesting is voice mail. Using a Farallon MacRecorder, you can digitize a voice message and attach it to your mail message. Anyone receiving the message on a Mac can play the message back. The feature is fun, but we wonder if it has much practical value.

The performance of our Mac LC, which did double duty as a mail server and a workstation, wasn't affected significantly, despite heavy mail-server activity. Still, we'd recommend that any installation with heavy mail-server activity use a dedicated machine. Dedicated servers aren't as likely to crash from broken applications software. Also, QuickMail can share a machine with your AppleShare server—a great way to get the most out of your dedicated file server.

Connecting remote mail sites requires that you run a modem from the server's modem port. We chose to set up the QuickMail server as a workstation and wanted to get the Telecom bridge running on the server. The manuals aren't clear on all the details, and we found ourselves spending several hours on the phone with CE Software's technical support.

We finally managed to use the generic gateway to grab our mail from BIX and route it to our QuickMail mailboxes. *Aliasing* is a way of having mail sent to one user name forwarded to another name. For example, if Theodore Logan wants to be known as "Ted," the aliasing functions provide for that. Getting the aliasing to divert the mail correctly under all circumstances would have taken a bit more time than we were willing to spend.

Do You Need E-Mail?

Maybe, and maybe not. According to the vendors of the packages we reviewed, everyone in the office needs E-mail. One

COMPANIES MENTIONED

Action Technologies
(The Coordinator)
1145 Atlantic Ave., Suite 101
Alameda, CA 94501
(415) 521-6190
fax: (415) 769-0596
Circle 1105 on Inquiry Card.

Banyan Systems, Inc.
(Network Mail for Vines)
120 Flanders Rd.
Westborough, MA 01581
(508) 898-1000
fax: (508) 898-1755
Circle 1106 on Inquiry Card.

cc:Mail, Inc.
(cc:Mail)
2141 Landings Dr.
Mountain View, CA 94043
(800) 448-2500
(415) 961-8800
fax: (415) 961-8400
Circle 1107 on Inquiry Card.

CE Software
(QuickMail)
P.O. Box 65580
West Des Moines, IA 50265
(800) 523-7638
(515) 224-1995
fax: (515) 224-4534
Circle 1108 on Inquiry Card.

Consumers Software, Inc.
(The Network Courier)
Seventh Floor
73 Water St.
Vancouver, BC
Canada V6B 1A1
(800) 663-8935
(604) 688-4548
fax: (604) 682-1378
Circle 1109 on Inquiry Card.

Da Vinci Systems Corp.
(eMail)
4200 Six Forks Rd., Suite 200
P.O. Box 17449
Raleigh, NC 27609
(800) 328-4624
(919) 881-4320
fax: (919) 787-3550
Circle 1110 on Inquiry Card.

Enable Software/ Higgins Group
(Higgins Mail)
1150 Marina Village Pkwy.
Suite 101
Alameda, CA 94501
(800) 888-0684
(415) 865-9805
fax: (415) 521-9779
Circle 1111 on Inquiry Card.

Microsoft Corp.
(Microsoft Mail)
1 Microsoft Way
Redmond, WA 98052
(800) 426-9400
(206) 882-8080
fax: (206) 883-8101
Circle 1112 on Inquiry Card.

Sitka Corp.
(InBox Plus)
950 Marina Village Pkwy.
Alameda, CA 94501
(800) 445-8677
(415) 769-9669
fax: (415) 769-8771
Circle 1113 on Inquiry Card.

Soft•Switch, Inc.
(Mailbridge and Soft•Switch Central E-mail gateways)
640 Lee Rd.
Wayne, PA 19087
(215) 640-9600
fax: (215) 640-7550
Circle 1114 on Inquiry Card.

VoxLink Corp.
(VoxVoice, VoxMail)
1516 Tyne Blvd.
Nashville, TN 37215
(615) 331-0275
fax: (615) 331-2057
Circle 1115 on Inquiry Card.

right around the corner, you don't need E-mail. But it can be a godsend if your company is geographically dispersed. BYTE has its main editorial offices in New Hampshire, with news offices spread out around the globe. Trying to keep in touch with all these sites without using E-mail would be almost impossible, especially considering time-zone differences.

The Perfect E-Mail Package

In business, good communication can often mean the difference between profit and loss. If you can't get messages to your remote sales staff, rest assured that other companies can reach *their* people. Playing phone tag is frustrating. A good E-mail package effectively bypasses the phone and puts the message right on your contact's desktop. Most of these packages also let you enclose files that contain graphics, a software update, or a lengthy report.

Most E-mail packages aren't cheap. In a small workgroup environment, price may influence your decision. But if you are trying to bridge multiple E-mail systems, computer architectures, and networks, support and training are more critical. Vendors who sell their own gateways are probably better positioned to support your entire E-mail network than those vendors who refer you to third-party products.

During our evaluation, we found that most of these packages had annoying quirks or limitations. Having your E-mail messages sit unprotected on the server can be a problem for some installations. If you decide on Microsoft Mail or QuickMail, you'll want to keep your mail server in a secure place. We'd suggest that you beef up your file server and run either QuickMail or Microsoft Mail as a process on the file server. Lock the server in a secure place, and security should no longer be an issue.

If you're running an AppleShare network, check out QuickMail. The user interface is clean and intuitive. Factor in the wealth of gateways available and the built-in voice mail, and you've got a winner.

Of course, if you are not running AppleShare, you can't use QuickMail. In that case, cc:Mail should do the trick. It's easy to use and has all the features most workgroups will need. cc:Mail's front end was the best of any of the Mac packages. We also liked the built-in graphics editor; PCs are not well endowed with drawing software, and having it right there makes it easy to annotate your messages.

Finally, there is The Coordinator. This is the only package reviewed that treats your messages the way you intend them to be—as part of a communication thread. It runs only on the PC, but you can share messages with Mac E-mail systems through an MHS gateway. The user interface is somewhat obscure, but don't let that deter you.

Neither rain, nor snow, nor stray magnetic fields will keep your mail from getting there. As E-mail becomes more popular, we hope to see a real standard emerge. Until then, it will take some creative effort to forge the connections. Get your network administrator involved early—installing any one of these packages is harder than it looks, especially if gateways or bridges are involved. ■

Howard Eglowstein is a testing editor/engineer in the BYTE Lab. Tom Thompson is a senior editor at large. You can reach them on BIX as "heglowstein" and "tom_thompson," respectively.

NFPA 75

Standard for the Protection of

Electronic Computer/Data Processing Equipment

1992 Edition

This edition of NFPA 75, *Standard for the Protection of Electronic Computer/Data Processing Equipment*, was prepared by the Technical Committee on Electronic Computer Systems and acted on by the National Fire Protection Association, Inc. at its Annual Meeting held May 18-21, 1992 in New Orleans, LA. It was issued by the Standards Council on July 17, 1992, with an effective date of August 14, 1992, and supersedes all previous editions.

The 1992 edition of this document has been approved by the American National Standards Institute.

Origin and Development of NFPA 75

The Committee on Electronic Computer Systems was formed by the action of the NFPA Board of Directors in January, 1960, following a request for standardization of fire protection recommendations by the computer industry.

The Committee first submitted the *Standard for the Protection of Electronic Computer Systems* to the 1961 NFPA annual meeting, and it was tentatively adopted. At the 1962 Annual Meeting it was officially adopted as an NFPA standard. Revisions were adopted in 1963, 1964, 1968, 1972, 1976, 1981, 1987, and 1989. The document was completely rewritten for this 1992 Edition.

Technical Committee on Electronic Computer Systems

Richard B. Swartz, *Chairman*
Chase Manhattan Bank, NY

Kathy A. Vernot, *Secretary*
Reliable Automatic Sprinkler Co. Inc., PA

rl F. Baldassarra, Schirmer Engineering Corp., IL
rnhard G. Bischoff, ASCOA Fire Systems, IL
rl A. Caves, Damascus, MD
n Chaiyabhat, Kemper Nat'l Insurance Cos., IL
Rep. The Alliance of American Insurers
omas M. Child, Alexander & Alexander, Inc., NJ
ge F. Clark, Cerberus Technologies, SC
...p. Nat'l Electrical Manufacturers Assn.
gust F. DiManno, Hanover Insurance Co., NY
chard H. Field, Royal Insurance Co., NC
Rep. American Insurance Services Group, Inc.
vid L. George, UNISYS Corp., PA
omas O. Gibson, The Dow Chemical Co., MI
Rep. Chemical Manufacturers Assn.
omas Goonan, Tom Goonan Associates, VA
. A. Haas, Underwriters Laboratories Inc., IL
seph J. Humphrey, Digital Equipment Corp., MA
onald J. Keigher, Los Alamos, NM
eorge A. Krabbe, Automatic Suppression Systems Inc., IL
Rep. Halon Research Institute
Howard C. Kubsch, IBM Corp., NJ
Stephen G. Leeds, Lawrence Livermore Nat'l Laboratory, CA
Edward D. Leedy, Industrial Risk Insurers, IL
Rep. Industrial Risk Insurers
Lawrence A. McKenna, AT&T Co., NJ
William F. Ramonas, Johnson & Higgins, NJ
Donald Reilly, M&M Protection Consultants, NY
James Retzloff, The Viking Corp., MI
Rep. Nat'l Fire Sprinkler Assn.
Earl E. Robisheaux, Corpus Fire & Safety, Inc., TX
Rep. Nat'l Assn. of Fire Equipment Distributors, Inc.
C. B. Shippey, Southern California Edison Co., CA
Rep. NFPA Industrial Fire Protection Section
Thomas D. Stilwell, Kidde-Fenwal Protection Systems, NC
Rep. Fire Equipment Manufacturers' Assn., Inc.
Thomas J. Wysocki, Guardian Services, Inc., IL
Rep. Technical Committee on Halogenated Fire Extinguishing Systems

Alternates

mes L. Kidd, Fire Equipment Inc., MA
(Alternate to B. G. Bischoff)
anley G. Kowalski, Electronic Data Systems Corp., MI
(Alternate to C. B. Shippey)
bert L. Langer, Ansul Fire Protection, WI
(Alternate to T. D. Stilwell)
' E. Lingenfelter, American Insurance Services Group
c. ,NY
(Alternate to R. H. Field)
onald J. Megasko, Marsh & McLennan Protection
onsultants, PA
(Alternate to D. Reilly)
Gary R. Milton, Emerson Electric Co., CA
(Alternate to G. F. Clark)
Melvyn Musson, Johnson & Higgins, MO
(Alternate to W. F. Ramonas)
John E. Roche, Industrial Risk Insurers, CT
(Alternate to E. D. Leedy)
Mark L. Rochholz, Schirmer Engineering Corp., CA
(Alternate to C. F. Baldassarra)
David J. Vandeyar, Nat'l Fire Sprinkler Assn.
(Alternate to J. Retzloff)

Nonvoting

Robert C. Everson, Calabash, NC
(Member Emeritus)

rk T. Conroy, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the text of this edition. Since that time, changes in the membership may have occurred.

NOTE: Membership on a Committee shall not in and of itself constitute an endorsement of the Association or any document developed by the Committee on which the member serves.

nt or materials and by whose labeling the manufacturer ıicates compliance with appropriate standards or perfor- ıce in a specified manner.

Listed. Equipment or materials included in a list pub- ed by an organization acceptable to the "authority hav- jurisdiction" and concerned with product evaluation, t maintains periodic inspection of production of listed ipment or materials and whose listing states either that equipment or material meets appropriate standards or been tested and found suitable for use in a specified ıner.

NOTE: The means for identifying listed equipment may ary for each organization concerned with product evalua- ion, some of which do not recognize equipment as listed s it is also labeled. The "authority having jurisdiction" should utilize the system employed by the listing organiza- ion to identify a listed product.

Master Record. A record of information on a medium t can be referred to whenever there is a need to rebuild ata base.

Noncombustible. A material that, in the form in which used and under the conditions anticipated, will not aid ıbustion or add appreciable heat to an ambient fire. terials, when tested in accordance with ASTM E136, *ıdard Test Method for Behavior of Materials in a Vertical e Furnace at 750°C*, and conforming to the criteria con- ed in Section 6 of the referenced standard, shall be sidered as noncombustible.

Program. Instructions to direct system operation.

Raised Floor. A platform with removable panels on ch equipment is installed, with the intervening space ween it and the main building floor used to house the erconnecting cables and at times as a means for supply- ditioned air to the data processing equipment and room. (Sometimes referred to as a false floor or second- floor.)

Records, Important. Records of which a reproduction ld be obtained only at considerable expense and labor nly after considerable delay.

Records, Vital. Records that are irreplaceable, such as: ords of which a reproduction does not have the same ue as an original; records needed to sustain the business mptly or to recover monies with which to replace build- s' equipment, raw materials, finished goods, and work rogress; and records needed to avoid delay in restora- of production, sales, and service.

Separate Fire Division. A portion of a building cut off n all other portions of the building by fire walls, fire rs, and other approved means adequate to prevent any that may occur in one fire division from extending to ther fire division.

Shall. Indicates a mandatory requirement.

Should. Indicates a recommendation or that which is ısed but not required.

Smoke Detector. A device that detects the visible or invisible particles of combustion.

Supervision. Continuous surveillance of a system or operation by special supervisory equipment or personnel to alert those responsible that failure has occurred or that a hazardous condition is being approached.

Water Sensor. A device or means that will detect the presence of water.

1-5 Equivalency Concepts.

1-5.1 Nothing in this standard is intended to prevent the use of systems, methods, or devices of equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety to those prescribed by this standard, provided technical documentation is submitted to the authority having jurisdiction to demonstrate equivalency.

1-5.2 Equivalent protection features accepted by the authority having jurisdiction shall be considered as conforming with this standard.

Chapter 2 Risk Considerations

2-1* Risk Factors. The following factors shall be considered when determining the need for protecting the environment, equipment, function, programming, records, and supplies:

(a) Life safety aspects of the function (e.g., process controls, air traffic controls);

(b) Fire threat of the installation to occupants or exposed property;

(c) Economic loss from loss of function or loss of records; and

(d) Economic loss from value of equipment.

2-2 Telecommunications Risks. In assessing and evaluating the damage and interruption potential of the loss of computer room operations, attention shall be given to the impact of the loss of data and communications lines. The complexity and scope of on-line computer operations make it necessary to link the computer to access terminals and other computers to perform a wide variety of functions.

If this is vital to the operation, rooms housing the services shall be constructed in accordance with Chapter 3 and protected in accordance with Chapter 6. These rooms shall be secured, locked, and free of extraneous combustibles.

Chapter 3 Construction Requirements

3-1* Building Construction.

3-1.1 The computer area shall be housed in one of the following:

eption No. 1: Small supervisory offices and similar light haz- occupancies directly related to the electronic equipment opera- s shall be permitted within the computer room if noncombusti- containers are provided for combustible material.

eption No. 2: Records shall be permitted in the computer n to the extent allowed in Chapter 7.

.2 Office furniture in the computer room shall be of tal construction.

eption No. 1: Metal frame chairs with integral seat cushions ll be permitted.

eption No. 2: Insulated or controlled conductive coverings ll be permitted on surfaces of chairs, tables, desks, etc.

.3 Only approved self-extinguishing-type trash recep- hall be used in the computer room.

General Storage.

.1 Paper stock, inks, unused recording media, and ier combustibles within the computer room shall be tricted to the absolute minimum necessary for efficient eration. Any such materials in the computer room shall kept in totally enclosed metal file cases or cabinets or, if ovided for in individual machine design, shall be limited the quantity prescribed and located in the area desig- ed by the equipment manufacturer.

.2 Reserve stocks of paper, inks, unused recording dia, and other combustibles shall be stored in one or re rooms outside of the computer room.

.3 The space beneath the raised floor shall not be used storage purposes.

.4* Abandoned cables shall not be allowed to accumu- e. Cables not identified for future use shall be removed.

hapter 5 Construction of Computer Equipment

Computer Equipment.

.1 Equipment and replacement parts shall meet the uirements of UL 478, *Standard for Safety Information- cessing and Business Equipment*, or UL 1950, *Standard for ety Information Technology Equipment Including Electrical iness Equipment.*

.2 Listed equipment shall be considered as meeting requirements of 5-1.3.

.3* Each individual unit shall be constructed in such a that by limiting combustible materials, or by use of losures, fire is not likely to spread beyond the unit in ch the source of ignition is located. Automatic protec- shall be provided for all units not so constructed.

.4 Enclosures of floor-standing equipment having ernal surfaces of combustible materials of such size that ght contribute to the spread of an external fire shall e a flame spread rating of 50 or less. (*See NFPA 255, ndard Method of Test of Surface Burning Characteristics of lding Materials.*)

5-2 Construction Features.

5-2.1* Cables. Interconnecting cables and wiring between units, power cords, plugs, and connectors shall be listed. They shall be considered as part of the computer system and suitable for installation on the floor or under a raised floor as described in Section 3-4.

5-2.2 Cords. Approved flexible cord and plug assemblies used for connecting computer equipment to the branch circuit to facilitate interchange shall not exceed 15 ft (4.57 m) in length.

5-2.3 Filters. Air filters for use in the cooling systems of individual units shall be listed. They shall be arranged in such a way that they can be readily removed, inspected, cleaned, or replaced when necessary.

5-2.4 Liquids. If the design of the unit is such that oil or equivalent liquid is required for lubrication, cooling, or hydraulic purposes, it shall have a closed-cup flash point of 300°F (149°C) or higher, and the container shall be of a sealed construction, incorporating automatic pressure relief devices.

5-2.5 Acoustical Materials. All sound-deadening material used inside of computer equipment shall be of such material or so arranged that it does not increase the potential of fire damage to the unit or the potential of fire propagation from the unit.

Chapter 6 Fire Protection and Detection Equipment

6-1* Automatic Sprinkler Systems.

6-1.1 An automatic sprinkler system shall be provided to protect the computer rooms or computer areas where:

(a) The computer room construction contains any combustible materials other than permitted in 3-3.1, or

(b) The enclosure of a unit in a computer system, or the unit's structure, is built all or in part of a significant quantity of combustible materials, or

(c) The operation of the computer room involves a significant quantity of combustible materials, or

(d) The building is otherwise required to be sprinklered.

6-1.2 Automatic sprinkler systems protecting computer rooms or computer areas shall be installed in accordance with NFPA 13, *Standard for the Installation of Sprinkler Systems.*

NOTE: To minimize damage to electronic computer equipment located in sprinkler protected areas, it is important that power be off prior to the application of water on the fire.

6-1.3 Sprinkler systems protecting computer rooms shall be valved separately from other sprinkler systems.

6-1.4* AISS units containing combustible media shall be protected by automatic sprinklers within each unit.

ecords Stored outside of the Computer Room.

Vital and important records that have not been cated shall be stored in fire-resistive rooms. The e of fire resistance shall be commensurate with the xposure to the records but not less than two hours. *ection 7-3.*)

The records storage room shall be used only for the ge of records. All other operations including splicing, ring, erasing, reproducing, cataloging, etc., shall be bited in this room.

tion: Spare media shall be permitted to be stored in this if they are unpacked and stored in the same manner as the containing records.

Portable extinguishing equipment and hose lines ecord storage rooms or areas shall be installed in dance with 6-3.1 through 6-3.5.

Duplication of Records. All vital and important ds shall be duplicated or protected and located in dance with NFPA 232, *Standard for the Protection of ds*. Duplicate records shall be stored in an area that is ubject to the same fire, or its associated effects, as the nals.

Chapter 8 Utilities

Heating, Ventilating, and Air Conditioning (HVAC). ir conditioning system shall be provided for the com- r room/media storage room and shall comply with one e following:

An HVAC system that is dedicated for electronic puter/data processing equipment use and is separated her areas of occupancy shall be used.

Any HVAC system that serves other occupancies also be permitted to serve the computer room/media ge room. The air ducts shall be provided with auto- fire and smoke dampers.

Dampers in HVAC systems serving computer s/media storage rooms shall operate upon activation oke detectors and by operation of the disconnecting s required by NFPA 70, Section 645-10.

Air ducts serving other rooms either shall not pass gh the electronic equipment rooms or fire dampers be provided in the ducts.

All duct insulation and linings, including vapor bar- and coatings, shall be noncombustible.

* Air filters for use in air conditioning systems shall ncombustible and installed in accordance with manu- rer's instructions.

Coolant Systems. If a separate coolant system is red for operation of a computer installation, it shall ovided with a suitable alarm to indicate loss of fluid.

dition

8-3* Electrical Service.

8-3.1 All wiring shall conform to NFPA 70, *National Electrical Code*.

8-3.2 Service equipment supplying the main power requirements of the computer area shall be of a type arranged for remote control or located to fulfill the requirements of Section 8-4.

8-3.3* Premise transformers installed in the computer area shall be of the dry type or type filled with a nonflammable dielectric medium. Such transformers shall be installed in accordance with the requirements of NFPA 70, *National Electrical Code*.

8-3.4 Service entrance transformers shall not be permitted in the electronic computer area.

8-3.5* Protection against lightning surges shall be provided in accordance with the requirements of NFPA 70, *National Electrical Code*.

8-3.6* Junction boxes shall be approved, completely enclosed, easily accessible, and properly grounded. They shall be securely fastened. No splices or connections shall be made in the underfloor area except within junction boxes or approved-type receptacles and connectors.

8-3.7 Emergency lighting shall be provided in the computer area.

8-4 Emergency Power Controls. An emergency disconnect accessible to the operator at each principal exit door shall be provided. These disconnects shall shut off power to all electronic equipment in the computer room.

8-4.1 An emergency disconnect accessible to the operator at each principal exit door shall be provided. These disconnects shall shut off power to the air conditioning system serving the computer area.

Chapter 9 Emergency and Recovery Procedures

9-1* There shall be a management-approved written, dated, and annually tested emergency fire plan.

9-2* There shall be a management-approved written, dated, and annually tested damage control plan.

9-3* There shall be a management-approved written, dated, and annually tested plan covering recovery procedures for continued operations.

Chapter 10 Electrical†

NOTE: The text of Chapter 10 was extracted from NFPA 70, Article 645. Only editorial changes were made to make the text consistent with this standard.

10-1 [645-1] General. This chapter covers equipment, power-supply wiring, equipment interconnecting wiring, and grounding of electronic computer/data processing equipment and systems, including terminal units, in the computer area.

..1 **NFPA Publications.** National Fire Protection ciation, 1 Batterymarch Park, P.O. Box 9101, Quincy, 02269-9101.

FPA 10, *Standard for Portable Fire Extinguishers*, 1990 ion

FPA 12, *Standard on Carbon Dioxide Extinguishing Sys-*, 1989 edition

FPA 12A, *Standard on Halon 1301 Fire Extinguishing ms*, 1992 edition

FPA 13, *Standard for the Installation of Sprinkler Systems*, l edition

FPA 14, *Standard for the Installation of Standpipe and tems*, 1990 edition

FPA 70, *National Electrical Code*, 1993 edition

FPA 72E, *Standard on Automatic Fire Detectors*, 1990 edition

FPA 220, *Standard on Types of Building Construction*, 2 edition

FPA 232, *Standard for the Protection of Records*, 1991 edition

FPA 253, *Standard Method of Test for Critical Radiant of Floor Covering Systems Using a Radiant Heat Energy ce*, 1990 edition

FPA 255, *Standard Method of Test of Surface Burning racteristics of Building Materials*, 1990 edition

..2 **Other Publications.**

1.2.1 **ASTM Publications.** American Society for Test- and Materials, 1916 Race Street, Philadelphia, PA 05.

STM E136-1982, *Standard Test Method for Behavior of 's in a Vertical Tube Furnace at 750°C*

STM E814-1988, *Standard Method of Fire Tests of ough-Penetration Fire Stops*

1.2.2 **UL Publications.** Underwriters Laboratories , 333 Pfingsten Road, Northbrook, IL 60062.

L 478-84, *Standard for Safety Information-Processing and ness Equipment*

L 1950-89, *Standard for Safety Information Technology pment Including Electrical Business Equipment*

Appendix A

his Appendix is not a part of the requirements of this NFPA document included for information purposes only.

2 This standard does not cover installation of elec- ic computer/data processing equipment and areas that be made without special construction or protection. It , however, be used as a management guide for the llation of electrically powered mechanical data pro- ing equipment, small tabletop or desk-type units, and ronic computer/data processing equipment.

The strategic importance placed upon electronic computer/data processing equipment and areas by the user is vitally tied to uninterrupted operation of the system. Consequently, by the partial or entire loss of this equipment, an entire operation of vital nature could be temporarily paralyzed.

Not to be overlooked are the "one-of-a-kind" electronic computer/data processing systems. These are the custom-made models that are designed to perform specific tasks. Replacement units for this type of equipment are not available, and the probability of the existence of duplicate facilities, which could be used to perform vital operations in the event that the one-of-a-kind systems are partially or totally impaired by a fire, is remote.

A-2-1 Risk Considerations. Electronic computer/data processing equipment is a vital and commonplace tool for business, industry, government, and research groups. The use of such equipment is a direct result of the increased complexity of modern business, industrial, governmental, and research needs. Particularly pertinent are the increasing number of variables that must be taken into consideration in everyday decisions — overlooking any one item may spell the difference between profit and loss, success or failure, life or death. To keep track of all these variables, electronic computer/data processing equipment offers practical answers.

This equipment has become the accepted tool to process large amounts of statistical, problematical, or experimental information and to print out or display answers or information in very short periods of time. Reliance is being placed on the equipment to perform the repetitive, the experimental, and, in some cases, even the whole programming operation for business, industry, government, and research groups.

Risk considerations include the selection of proper equipment, checking and planning for areas to receive the equipment, utility requirements, orientation and training of personnel to operate the equipment, as well as consideration for expansion of the initial facility. One other factor should be included in this vital study — namely, protection against fires of either accidental or deliberate origin, i.e., sabotage and incendiary.

Computer equipment and materials for data recording and storage may incur damage when exposed to elevated sustained ambient temperatures. The degree of such damage will vary depending upon exposure, equipment design, and the composition of materials for data recording and storage.

Business Interruption. Planning for fire protection is vital due to an organization's dependence upon the electronic computer/data processing equipment. Once management commits itself to a program of dependence on any such equipment, simple economics dictate doing away with former methods and procedures. The personnel, equipment, and facilities are no longer available to pick up the load assumed by the data processing equipment if it is put out of operation by fire or other unforeseen occurrences.

for beams and pipes should be sealed to watertight- Where drainage is installed in an area containing an rfloor extinguishing system, provisions should be for maintaining the drain piping as a closed system s water is present. This is required to ensure the rity of a gaseous extinguishing system and allow for enance of the necessary concentration level. As water vaporate from the standard plumbing trap, mineral another substitute should be considered.

derfloor spaces should be provided with leak detec- vhen any utility or computer auxiliary cooling fluids ïped into the computer room or are capable of enter- ie room from adjoining areas.

The determination of the depth of the raised floor .ake into consideration air movement and fire tion and extinguishing systems requirements (if led), as well as building construction restrictions.

.4 Openings in raised floors for electric cables or uses should be protected to minimize the entrance of s or other combustibles beneath the floor.

.1 Support equipment such as high-speed printers ilize large quantities of combustible materials should be d outside of the computer room whenever possible.

.4 Abandoned cable will potentially interfere with w and extinguishing systems. Abandoned cable also to the fuel loading.

.3 All nonelectrical parts, such as housings, frames, orting members, and the like, should not constitute ional fire hazard to the equipment.

.1 Cables that are listed as part of an electronic r/data processing equipment system may not carry .te listing mark on the cable.

Automatic sprinkler systems protecting computer s or computer areas should be maintained in accor- with NFPA 13A, *Recommended Practice for the Inspec- Testing and Maintenance of Sprinkler Systems.* In facilities are under the supervision of an operator or other n familiar with the equipment (during all periods that ment is energized), the normal delay between the ini- utbreak of a fire and the operation of a sprinkler sys- vill provide adequate time for operators to shut down ower by use of the emergency shutdown switches as ribed in Section 8-4. In other instances when a fire operate sprinkler heads before discovery by person- method of automatic detection should be provided to natically de-energize the electronic equipment as y as possible.

.4 It is not intended that small automatic media rs or AISS units be provided with protection within nit. The decision of whether to install protection the unit must be made on the combustible load added to the room or area. In the absence of further nation it is reasonable to assume that units that han- the range of 27 cu ft of combustibles storage space or less need not be provided with protection within the unit. The 27 cu ft volume assumes that no single dimension is larger than 3 ft (e.g., 3 ft × 3 ft × 3 ft).

A-6-2 Fire detection and extinguishing systems shall be selected after a complete evaluation of the exposures. The amount of protection provided shall be related to the building construction and contents, equipment construction, business interruption, exposure, and security need.

NOTE: For amplification of the important need of fire protection, see Chapter 2.

A-6-2.1 The detection system selection process should evaluate the ambient environmental conditions in determining the appropriate device, location, and sensitivity. In high airflow environments, air sampling detection devices should be considered.

A-6-4.1 If major concerns over potential fire loss to specific critical data or equipment or of serious interruption to operations cannot be resolved or alleviated by equipment redundancy, subdivision of the computer area, or the use of leased facilities, automatic gaseous agent total flooding may be the only feasible approach to handling an incipient fire situation with an acceptable minimum amount of damage. At the same time, this sophisticated protection approach requires that all environmental design criteria (e.g., damper closure, fan shutdown, sealed openings, etc.) be carefully maintained to ensure that the needed concentration for extinguishment will be achieved.

A-6-4.2 The gaseous extinguishing system may be actuated by the automatic fire detection system required in Section 6-2 when designed to do so.

A-6-4.3 This requires that all environmental design criteria (e.g., damper closure, fan shutdown, sealed openings, etc.) be carefully maintained to ensure that needed concentration for extinguishment will be achieved. It is preferable but not essential to de-energize computer equipment prior to discharge if computer shutdown does not cause major service interruptions.

A-7-1.2 The evaluation of records should be a joint effort of all parties concerned with the safeguarding of computer operations. The amount of protection provided for any record should be directly related to its importance in terms of the mission of the computer system and the reestablishment of operations after a fire.

NOTE: It is assumed that computer equipment capable of properly using the records will be available. (*See Chapter 9.*)

A-7-2.1 The size of record storage rooms should be determined by an engineering evaluation of the operation, followed by the application of sound fire protection engineering principles. The evaluation should include, but not be limited to:

(a) Classification of records.

(b) Quantity of plastic-based records and type of container.

(c) Type and capacity of fire suppression system.

dition

Appendix B Example of a Computer Area

his Appendix is not a part of the requirements of this NFPA document included for information purposes only.

he rooms shown in Figure B-1 are symbolic and do not ote size, shape, or location, nor are the rooms in Figure necessarily required in the computer area (*see definition omputer Area*).

upervisor and maintenance rooms normally are adja- to and have direct access to the computer room. Com- er rooms normally have a raised floor. (*See Figure B-1.*)

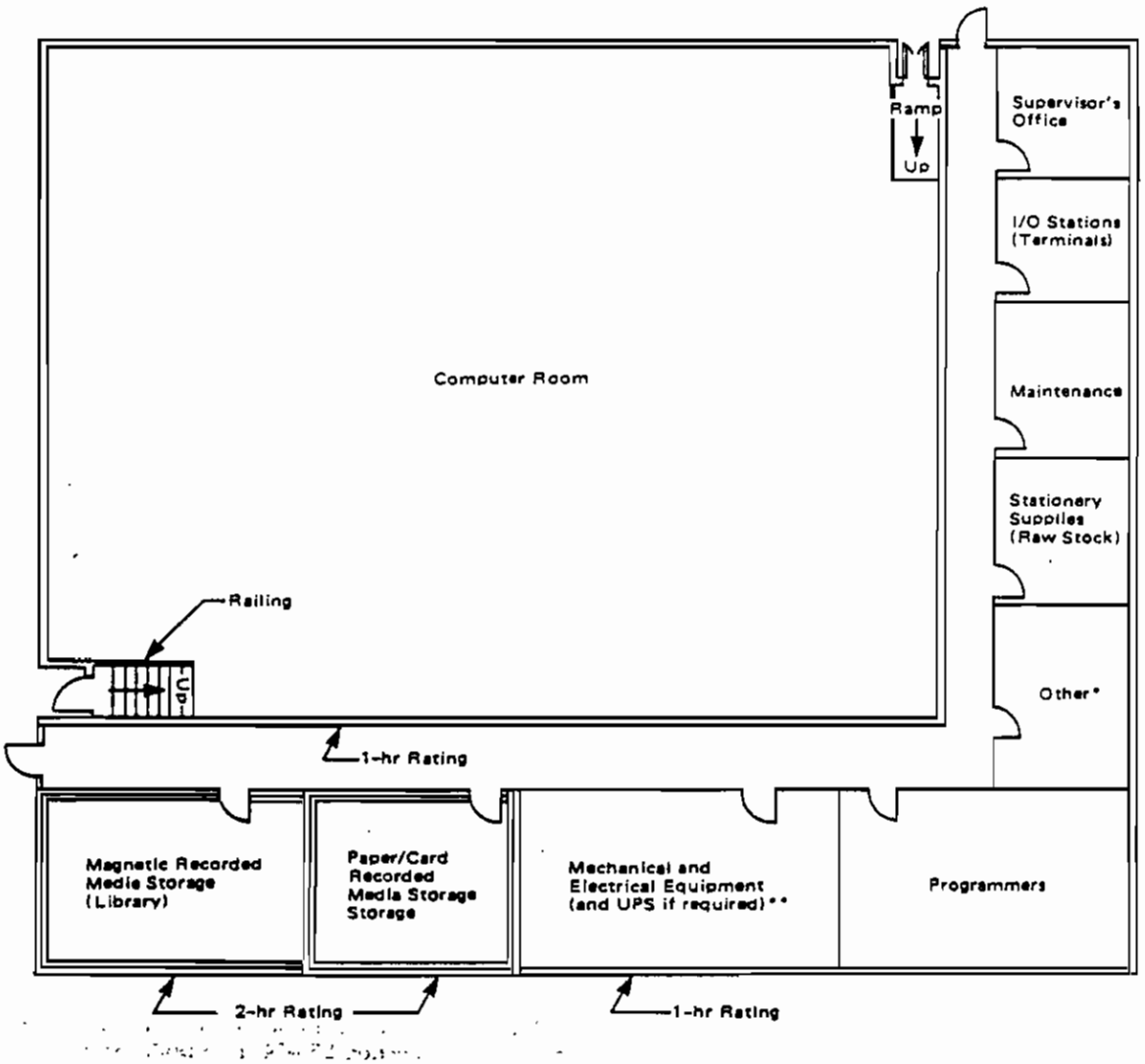
Appendix C

The following was extracted from the Blackmon-Mooring-Steamatic Publication "Electronics & Magnetic Media Recovery" (see D-1.2.3).

What to Do in the First 24 Hours

for Damaged Electronic Equipment and Magnetic Media

This plan attempts to detail the necessary recovery steps to be taken after a disaster has occurred to electronic equipment. The plan considers fire, heat, smoke, and water damage and is designed to limit and mitigate potential losses. The equipment under discussion includes office computers, word processors, telephone switching equipment, test equipment, audio-video equipment, and other electrical and electronic apparatus.



*Other: Security Station, Communications, Control Rooms
**UPS: Uninterruptable Power Supply (Motor/Generator or Solid State Systems)

Figure B-1 Diagram of computer area.

Edition

253, *Standard Method of Test for Critical Radiant Floor Covering Systems Using a Radiant Heat Energy* 990 edition

780, *Lightning Protection Code*, 1992 edition

ther Publications.

CSA Publication. Canadian Standards Association, dale Blvd., Rexdale, Ontario, Canada M9W-1R3.

C22.2, *Test Methods for Electrical Wires and Cables*

DOE Publication. U.S. Dept. of Energy, EH-34, gton, DC 20545.

P-0108-1986, *Standard for Fire Protection of DOE omputer/Data Processing Systems*, Appendix B, "Reconditioning of Flooded and Smoke-Contaminated Equipment"

D-1.2.3 UL Publication. Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062.

Standard Method of Test for Flame-Propagation Classification of Flooring and Floor Covering Materials

ANSI/UL 1581-1985, *Standard for Electrical Wires, Cables, and Flexible Cords*

D-1.2.4 Other Publication. Appendix C was extracted from: *Electronics and Magnetic Media Recovery*, Blackmon-Mooring-Steamatic Catastrophe, Inc., International Headquarters, 303 Arthur, Fort Worth, TX 76107, (817) 332-2770, FAX (817) 332-6728.

Index

ANEXO 6

ADMINISTRACION DE LA RED

Organización de Directorios y Volúmenes

En esta sección se muestra la estructura general de directorios y volúmenes que tiene el servidor Netware de archivos.

Están definidos cuatro volúmenes de acuerdo a las necesidades y al tipo de información que en ellos se almacena:

SYS Este volumen contiene la información de Netware a nivel del sistema operacional y utilitarios que vienen con éste. También se mantienen los paquetes o software aplicativo que utilizan los diferentes usuarios de la red (supervisores, operadores y usuarios normales). Adicionalmente se tiene el software de comunicaciones de ccMail, y el software para respaldos TNA.

VOL1 En este volumen se mantienen los datos que son generados por los usuarios de los diferentes departamentos. El volumen se encuentra dividido en directorios por departamentos.

VOL2 En este volumen se almacena toda la información que los usuarios de los departamentos de Operations, Drilling y Exploration, información que manejan con las diferentes aplicaciones instaladas en la red.

VOL3 Este volumen ha sido creado para almacenar aplicaciones que funcionan en ambiente WINDOWS.

NET36PRD En este volumen se almacena toda la información sobre los sistemas MAXI, de contabilidad y OPICS para materiales.

A continuación se puede observar como se organiza el contenido en cada uno de los volúmenes mencionados.

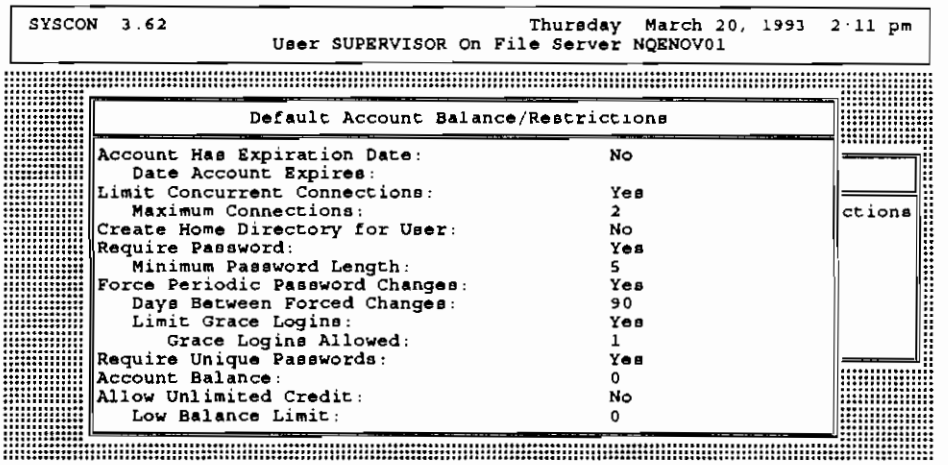
servidor se debe establecer está cuota (en el volumen VOL1 y VOL2).

DIRECTORIOS	CONTENIDO
VOL3:	Volumen
TNA	Ejecutables del Sistema Operacional
WINDOWS	Archivos necesarios para entrar y salir de la red
MSAPPS	Menú para el manejo de aplicaciones
LICENSER	Correo y archivos de control de Netware
WINAPPS	Directorio con las aplicaciones para los usuarios
MSPUB	Ejecutables de Lotus versión 2.4
TASKFORC	Ejecutables de Lotus versión 2.2
WP51	Ejecutables de WordPerfect versión 5.1
WPWIN	Ejecutables de WordPerfect para Windows versión 5.2
GMKW	Ejecutables de Grammatik versión 5
PDOX35	Archivos de Paradox
WINPROJ	Ejecutables de Microsoft Project
QPRO	Ejecutables de Quattro Pro versión 4.0
QPW	Ejecutables de Quattro Pro para Windows versión 1.0
NETHQ	Ejecutables de Network H. Q.
FOXPW	Ejecutables de FoxPro para Windows versión 2.5
FL	Archivos de Freelance Plus Versión 3.1
FLW	Archivos de Freelance para Windows Versión 2.0
LOTSHARE	Directorio para control de Lotus
123.V22	Para Lotus versión 2.2
123.V24	Para Lotus versión 2.4
TNA	Archivos para el TNA (The Network Archivist)
UTIL	Directorio de Utilitarios
PKZIP	Ejecutables del Pkzip
NORTON	Archivos de Norton
ME	Archivos de Multi Edit
BATCH	Archivos Batch para usuarios de la red
MISC	Varios utilitarios y programas
VSCAN	Ejecutables de antivirus
XTREE	Ejecutables de Xtree
REMOTE	Ejecutables de cc:Mail Remote
PROCOMM	Ejecutables de Procomm
PHONE	Directorio Telefónico
AUTOMENU	Archivos del Menu para la red
CCMAIL	Ejecutables del programa ccMail
CCADMIN	Archivos para la administración del ccMail
CCDATA	Directorio para la base de datos del ccMail
CCGATE	Ejecutables para el ccMail Gateway

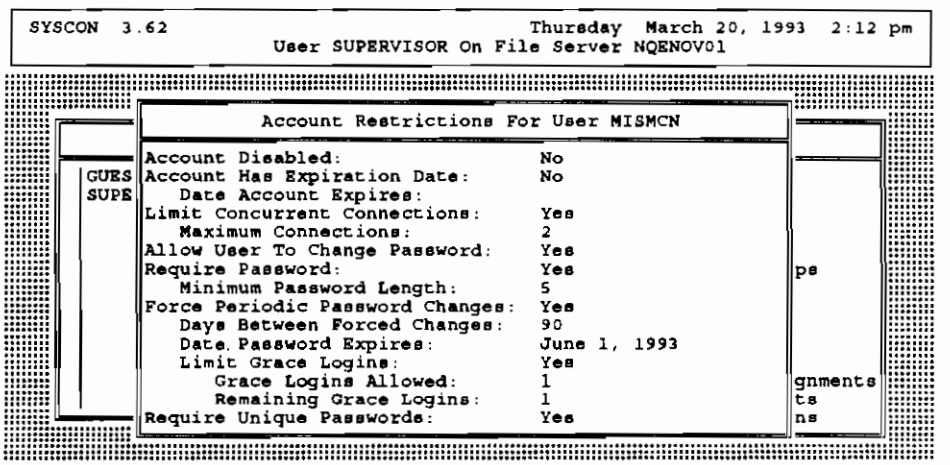
Definición de Restricciones de Contabilidad

Existen una serie de variables que afectan la contabilidad y la seguridad de la red y que deben determinarse para los usuarios normales.

Es posible encontrar diferentes usuarios especiales, que necesiten tratamientos diferentes a los normales a nivel de la contabilidad. A continuación se muestra la pantalla de la utilidad **SYSCON** en donde se establecen los valores que deben tener las variables que afectan la contabilidad de un usuario normal en la Compañía (Default Account Balance/Restrictions).



Teniendo en cuenta las definiciones anteriores, para cada usuario la definición normal debe ser la siguiente, utilizando el utilitario **SYSCON** en la sección de restricciones de contabilidad para cada uno de los usuarios:



Administración de Grupos y Usuarios

A continuación se muestran los pasos que se deben seguir para la adición de grupos y de usuarios a la red Netware haciendo uso de la utilidad **SYSCON**.

Adición de grupos

Los pasos necesarios para crear un grupo **XXX** son los siguientes:

- Entrar al programa SYSCON e incluir el grupo con los integrantes que se deseen y que estén definidos.

- Crear el archivo **XXX.LOG** en el subdirectorio PUBLIC\SCRIPT con el correspondiente Login Script del grupo **XXX**. Es posible copiar uno existente (diferente del grupo SUPPORT) y modificarlo con un editor de texto.

- Cambiar el Login Script del sistema adicionando la línea que corresponde al grupo y colocarle el correspondiente **XXX.LOG**. Hay que tener en cuenta el orden en que están colocadas ya que es un INCLUDE y el último es el que quedará operando para los usuarios que se encuentren en varios grupos.

- Crear el directorio **XXX** en la raíz del volumen con los permisos [R F] para el grupo **XXX**.

- Crear el directorio **SHARE** como subdirectorio del directorio **XXX** con los permisos [RWCEMFA] para el grupo **XXX**.

Adición de usuarios

Para efectuar la adición de un usuario **EXPZZZ** a la red deben efectuar los siguientes pasos:

- El grupo o los grupos a los que se va adicionar el usuario deben existir.

- Verificar con el administrador del AS\400 el "USER ID" (**EXPZZZ**) del usuario que se desee adicionar.

- Entrar como supervisor copiar el archivo que corresponde al grupo, donde el usuario estará perteneciendo, con el nombre de EXPZZZ.USR.

- Ejecutar el utilitario MAKEUSER, tomar la segunda opción de "xxxxxx" editar el archivo EXPZZZ, cambiar la última línea poniendo el "user id", "Full name" y el nombre del grupo. Luego se ejecuta la última opción del menu "xxxxxxx" con el archivo modificado EXPZZZ, inmediatamente se creará el nuevo usuario, con todas sus caracteristicas.

- Para revisar que el proceso se ejecutó bien, mire el archivo EXPZZZ.RPT donde le indicará si todo salio bien.

- Adicionalmente se debe crear el **Login Script** del usuario colocando como mínimo las siguientes instrucciones:

Consideraciones Especiales para las Estaciones

Para que una estación trabaje correctamente en la red, es necesario tener en cuenta las siguientes consideraciones:

- Debe tener una tarjeta de comunicación Token Ring que puede ser de tipo IBM ó PROTEON.

- Se debe revisar si hay lugar en el MSAU para instalar un nuevo cable, hasta el lugar donde se pondra la nueva estación.

- La tarjeta de comunicación debe estar debidamente configurada (Velocidad, nivel de interrupción, dirección de memoria ROM y RAM) y conectada a la red por medio de cable Token-Ring.

- Se debe revisar la configuración en el **AUTOEXEC.BAT**, lo mínimo que debe tener es los comandos **IPX, NETX y MENUS** o cuando es una estación especial que administra algún servicio para la red debe tener el comando **RPRINTER** para indicar que la impresora conectada a la estación será compartida.

- El archivo **CONFIG.SYS** debe también revisarse y debe tener las siguientes líneas como mínimo:

```
SHELL=C:\DOS\COMMAND.COM /P /E:512
LASTDRIVE=H
```

- Debe existir el sub-directorio **SYS\DRIVERS** en el directorio raíz del disco duro de cada estación.

- En el directorio **C:\SYS\DRIVER** se deben tener los archivos que necesita la estación para accesar a la red y los archivos que configuran el equipo para algunas aplicaciones de la red, como administradores de memoria. Los archivos necesarios para accesar la red son:

	IPX.COM	(Es diferete para IBM o PROTEON)
	NETx.COM	(x Depende de la versión de DOS)
o	NETX.COM	(Standard para cualquier versión de DOS)
	SHELL.CFG	

El único archivo editable es el **SHELL.CFG** que debe contener como mínimo las siguientes líneas:

```
IPX PACKET SIZE LIMIT=4096
IPX RETRY COUNT=50
SHOW DOTS=ON
SPX ABORT TIMEOUT=2000
```

RPRINTER <Print-Server-Name> ##

Donde, ## representa el número de impresora que va ha ser inicializada, cuando la estación arranque.

6. Se debe editar los archivos Batch básicos de la estación (AUTOEXEC.BAT y CONFIG.SYS) para verificar en el primero que se ejecuten los comandos IPX y NETX, y en el segundo para que la líneas de LASTDRIVE=H y SHELL con ENVIRONMENT de 512 existan.

   La siguiente es una configuración típica del CONFIG.SYS

```
FILES = 30
BUFFERS = 20
BREAK = ON
LASTDRIVE = H
SHELL=C:\DOS\COMMAND.COM /P /E:512
```

   Se puede añadir otra instrucción como se mencionó anteriormente, por ejmplo un administrador de memoria expandida, así:

```
DEVICE = C:\SYS\DRIVERS\ASTEMM.SYS NOXRAM ON EMS=####
```

   La siguiente es una configuración típica del AUTOEXEC.BAT

```
ECHO OFF
PATH=C:\;C:\DOS;C:\BATCH;C:\UTIL;
PROMPT $P$G
SET BOOT=NOVELL
C:\SYS\DRIVERS\IPX
C:\SYS\DRIVERS\NETX
MENUS
```

   Al igual que en el config.sys, en el archivo AUTOEXEC.BAT, tambien se puede añadir mas instrucciones, como variables de ambiente, comandos para cargar Windows posteriormente, entre otros.

Vale la pena anotar que una estación conectada a la red debe tener definidos los sub-directorios locales (Disco C:) que corresponden a cada usuario, de la estación, en el directorio **/MISC** estos le servirán para mantener información confidencial del usuario, programas propios del usuario, o como respaldo de información especial.

Impresión

En esta sección se explican los puntos que debe tener en cuenta el administrador de Netware 3.11 para implementar el sistema de impresión.

Es importante aclarar que la versión 3.11 de Netware contiene el software de impresión o el software que necesita el servidor de impresión, éste software sirve para un servidor local (en el file server) o servidor dedicado (en alguna estación dedicada).

Para poner en funcionamiento el servidor de impresión es necesario ejecutar el **PSERVER**, para hacerlo en el file server se utiliza el archivo PSERVER.NLM y para un servidor de impresión dedicado es un PSERVER.EXE.

Cada vez que se utilice el PSERVER es necesario dar el nombre del servidor de impresión, según los estándares de la Compañía, así por ejemplo, debe ser **ECU-PS#**, donde **#** corresponde a una identificación única para los servidores de impresión en Ecuador.

Una vez se tenga definido el servidor de impresión, se debe adicionar al sistema a través del utilitario **PCONSOLE**. Adicionalmente, se deben adicionar las impresoras y las colas de impresión. En general, para cada impresora existe una cola de impresión, con pocas excepciones.

Los nombres que deben llevar las impresoras deben ser cortos y deben especificar el modelo o clase de la impresora y la ubicación (Departamento) o piso donde ésta se encuentre. Para ilustrar mejor la nomenclatura de las impresoras, aquí unos ejemplos:

FIN1	Impresora Hewlett Packard III para Finanzas,
OPR1	Impresora Hewlett Packard III para Operaciones.
MAXI	Impresora Hewlett Packard III SI para MAXI,

La nomenclatura de las colas asociada a cada impresora tiene el mismo nombre de la impresora con el prefijo **PRINT_**. En caso de que existan varias colas para ser atendidas por una misma impresora se debe colocar como postfijo una letra para diferenciar las diferentes colas. Ejemplos:

PRINT_MAXI	Cola de la impresora MAXI de Finanzas y para FOAS ubicada en el piso 1°,
PRINT_FIN2	Cola de la impresora HP III ubicada en el piso 2°,
PRINT_ADMIN	Cola de la impresora HP III ubicada en el piso 6°.

La lista de las impresoras con sus respectivas colas es la siguiente:

Nombre de Impresora	**Cola de Impresión**	**Departamento**
PRINT_ADM1	PRINT_ADM1	ADMINISTRACION
PRINT_OPICS	PRINT_OPICS	MATERIALES

PRINT_MAXI	PRINT_MAXI	FINANZAS
PRINT_FIN1	PRINT_FIN1	FINANZAS
PRINT_FIN2	PRINT_FIN2	FINANZAS
PRINT_FIN3	PRINT_FIN3	FINANZAS
PRINT_MIS	PRINT_MIS1	MIS
PRINT_OPR1	PRINT_OPR1	OPERACIONES
PRINT_OPR2	PRINT_OPR2	OPERACIONES
PRINT_OPR3	PRINT_OPR3	OPERACIONES
PRINT_OPR4	PRINT_OPR4	O P E R A C I O N E S
PRINT_EXPL1	PRINT_EXPL1	EXPLORACIONES
PRINT_EXPL2	PRINT_EXPL2	EXPLORACIONES
PRINT_ADM2	PRINT_ADM2	RECURSOS HUMANOS
PRINT_LEGAL	PRINT_LEGAL	LEGAL
PRINT_GOVT	PRINT_GOVT	GOBIERNO
PRINT_ENVR	PRINT_ENVR	MEDIO AMBIENTE
PRINT_GM	PRINT_GM	GERENCIA GENERAL

ANEXO 7

DESASTRE Y RECUPERACION

Consideraciones Generales

Este procedimiento Para ejecutar el proceso de backup se debe seguir el siguiente procedimiento. Es importante conocer la configuración existente así como las herramientas en software de las que disponemos para facilitar el manejo y control del Sistema de Respaldo (backup).

Para facilitar el proceso se ha definido un usuario en la red con caracteristicas suficientes para realizar el backup, adicional a esto se ha asignado un computador exclusivamente para la tarea de respaldos y recuperación, así también se han desarrollado batch files (ver anexos) para ofrecer los servicios básicos en el manejo del sistema, reduciendo al máximo la interacción del operador y automatizando su servicio.

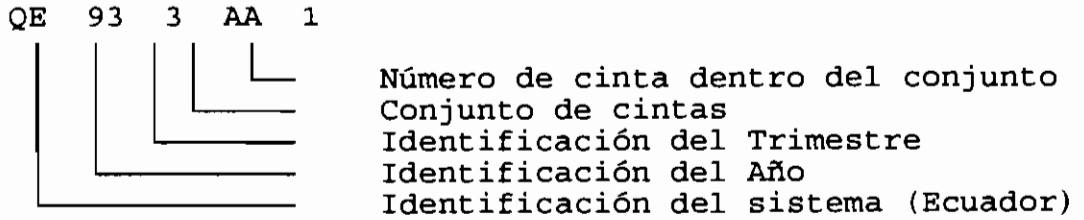
HARDWARE

El Sistema de Respaldo físicamente se encuentra localizado en el Centro de Cómputo y es el equipo identificado con el número 001. Lo compone un computador IBM AT 286, una tarjeta controladora interna (SCSI) y un "TAPE BACKUP" de carga frontal marca Palindrome, el cual utiliza cartuchos de 8mm con capacidad de almacenamiento de 2 GB. Posee dos bombillos indicadores, uno verde que muestra que el equipo esta prendido, y uno amarillo que indica cuando el sistema está operativo (leyendo, grabando o simplemente transportando la cinta).

Posee también un botón de control para abrir la puerta del compartimiento donde se coloca la cinta la cual solo funciona si el usuario se encuentra en alguno de los menús del sistema. Normalmente el software abre automáticamente dicha puerta indicando que el proceso ha terminado, que se requiere una diferente, una nueva o que la cinta montada no corresponde al proceso en curso.

SOFTWARE

El sistema posee de la misma casa fabricante del hardware un software denominado TNA (The Network Archivist) que administra y controla los procesos de backup. La administración del sistema indica, cómo se debe manejar la rotación de cintas y donde deben encontrase ellas. La identificación de las cintas será:



de la cinta. Sin embargo, si por algún motivo se coloca una cinta que no corresponda, el proceso no continuará hasta tanto no sea cambiada por la cinta correcta.

Básicamente, el sistema de rotación maneja la utilización de las cintas tomando como base el número de veces que cada cinta se ha utilizado y una solicitud secuencial para su uso. Toda cinta utilizada será solicitada dos veces más que el número de veces que el sistema utiliza la cinta anterior por ejemplo: si la cinta "QE933AP1" fué utilizada ocho veces la siguiente cinta "QE933AQ1" será utilizada diez y seis veces más que la anterior.

Después de cada proceso de backup el sistema siempre terminará con un resumen del estado de las cintas, que está utilizando o que en un corto período podrá llegar a utilizar. Indica el "Tape set" de la cinta utilizada (Last Archive Update: QE933AP1), la cinta que utilizará durante el siguiente proceso (Continue with tape: QE933AP1) y la fecha de la próxima rotación (cambio de cinta).

En adición y dado que el sistema de rotación efectúa una mayor utilización de las cintas cuyo "tape set" corresponde a los últimos, (en estricto orden ascendente) el TNA diferencia y divide en dos grupos todo el conjunto de cintas así:

IN-VAULT
Indica que todas las cintas dentro de esta categoría, estarán en un lugar seguro (por ejemplo en el Off-Site Backup) por su mínima utilización durante las próximas semanas.

IN-HAND
Son todas aquellas cintas con las que normalmente el sistema estará trabajando o de las cuales eventualmente (a corto plazo) se requerirá.

Se entiende, que cualquier proceso de Recuperación **podrá** requerir cualquiera de las cintas que se encuentren "IN-VAULT" por lo que todo proceso de recuperación puede tomar más de una hora, o en algunos casos inclusive más de un día.

Igualmente el sistema siempre que, en su proceso normal de backup, requiera un cambio en la ubicación física de las cintas terminará el proceso indicando:

Please move to vault: **QE933AP1**
Please retrieve from vault: **QE933AQ1**

Dicha solicitud será oportuna y se repetirá al menos 2 veces antes de físicamente requerir dicha cinta.

Solamente hay dos posibilidades en los que el sistema acepte una cinta que no corresponda al proceso de "Rotación, manejo y administración de cintas". Primero, si eventualmente se coloca una cinta en blanco, el sistema la acepta aunque previamente hará una advertencia al respecto (este hecho alterará el ciclo normal de rotación de cintas). El segundo caso se presenta si en un proceso de backup la cinta de trabajo se llena y por lo tanto será el sistema el que explícitamente hará la solicitud. (**713 NOTE: The mounted tape is full**). Es de anotar, que en el último caso la cinta llena volverá ha ser utilizada únicamente en procesos de Restaure (recuperación) de información.

indicado en el equipo descrito así:

1. Al prender el computador, este automáticamente ingresará a la red, para esto se ha añadido al AUTOEXEC.BAT las instrucciones necesarias para poder ingresar a la red. El nombre del USERID con el cual accesa a la red es **ECU-ARC**, el password como se explica en el manuál de Administración de la Red, es cambiado cada 90 días.

2. Al ingresar a la red se ejecuta un batch file GO.BAT (ver en anexos) que carga en memoria el ejecutable de TNA para su posterior ejecución.

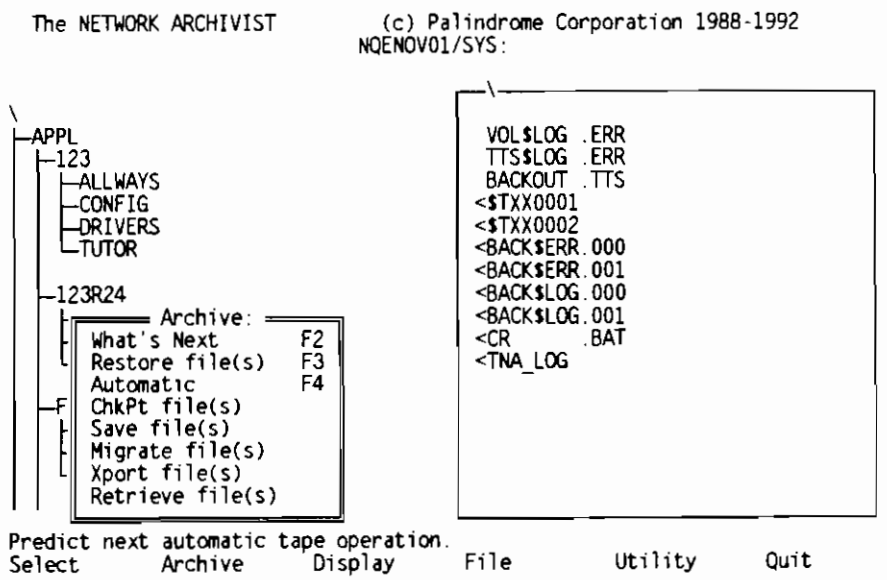
3. Las instrucciones que estan en el batch GO se realizaran a las 22:00 horas, todos los días motivo por el cual hay una restricción a los usurios a partir de las 00:00 horas, primero se realiza in respaldo de la base de datos del cc:Mail luego el respaldo de la información de cada volumen, en los anexos se explica el batch file.

4. El sistema dará el acceso a la red y terminará mostrando la hora a la cual se relizará el proceso de respaldos. Al dejar la el computador preparado para realizar los respaldos es importante tener presente las siguientes indicaciones.

   4.1 Verifique que el Dispositivo de cinta esté prendido (foco verde en la esquina inferior izquierda del dispositivo de cinta).

   4.2 Verifique que la cinta sea la correcta. (eje. QE933AP1) Si tiene duda, utilize la opción F2 del TNA llamada **"NEXT TAPE SCHEDULE"**. Para verificar la identificación correcta de la cinta.

   4.3 Si usted quiere verificar la cinta que le toca para el respaldo, ingrese al utilitario TNA, este es un software que administra al Palindrome, cuando se ingresa a parece un menú en pantalla, si toma la opción F2 el TNA le responde indicandole cual cinta es la que corresponde.



5. Como se mencionó anteriormente Estos procesos deben ser iniciados entre las 11:00 pm y las 4:00 am, con el fin de poder garantizar un ágil backup (sin perjuicio en el tiempo de respuesta para los usuarios) y la garantía de que ningún archivo quedará pendiente de copia (Este horario siempre deberá corresponder al período de más baja actividad en la Red).

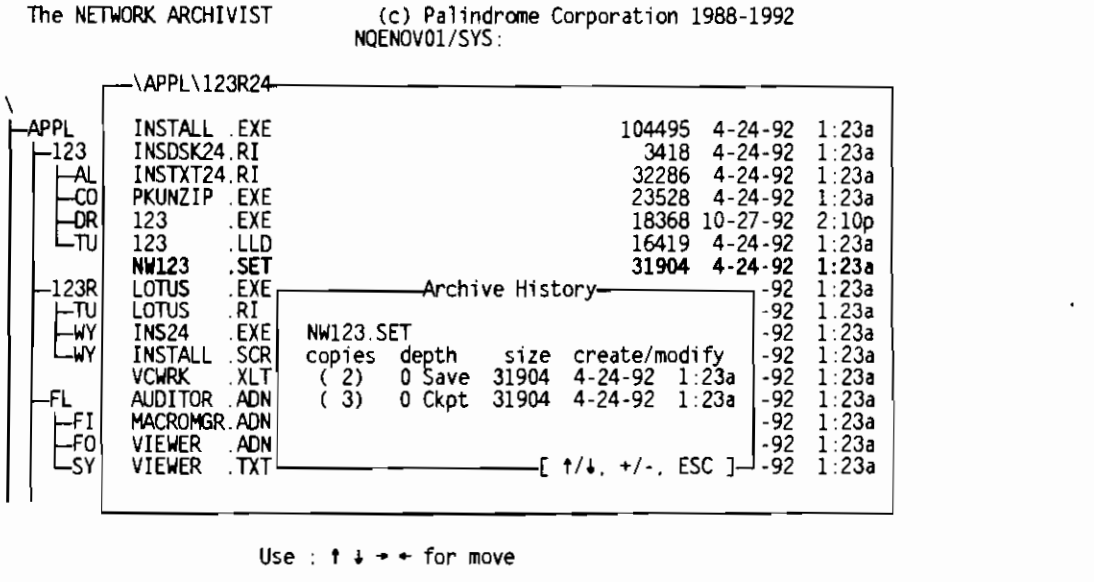
PROCEDIMIENTO DE RECUPERACION DE INFORMACION.

Este procedimiento debe ser realizado preferiblemente en horas de más baja actividad en la red. Si la solicitud de recuperación y su prioridad requiere que el proceso sea ejecutado en horas hábiles se deberá coordinar el acceso con el administrador de la red. Para el proceso de recuperación de información se debe tener los siguientes datos: Nombre completo y exacto del archivo(s)/directorio(s), User ID, Drive en el cual se encontraba el archivo, nombre de subdirectorios adicionales.

1. Para realizar este proceso se debe considerar el primer paso del proceso anterior, es decir trabajar desde el computador que tiene conectado la unidad Palindrome, e ingresar a la red.

2. Ejecute el programa **TNA**, seleccione el volumen con el cual va a trabajar, para esto utilize la opción "S" para el menú **Select** y luego la opción **New Volume**, el sistema le responderá pidiendole el nombre del volumen con el cual quiere trabajar.

3. Una vez ingresado el nombre del volumen, en pantalla estará la estructura de directorios del volumen, usted seleccione el directorio o directorios, archivo o archivos con la tecla "+". Con la tecla "-" puede eleminar algo seleccionado. Para moverse entre los directorios y archivos puede usar las teclas "Page Up", "Page Down", y las flechas ↑ ↓ → ← .



4. Como se puede mirar en el gráfico una vez seleccionado el archivo, se puede escojer una versión del mismo, si este lo tiene, las versiones corresponden a las diferentes modificaciones que se realizaron a un determinado archivo. Seleccionado el o los objetos a restaurarse, tome la opción "A" de **Archive**, en pantalla saldrá el menú de Archive, tome la opción **Restore file(s)** ó la tecla **F3** para proceder con la restauración.

5. Dependiendo de la última fecha de modificación el sistema exigirá una o más cintas anteriores, la información (oportuna y completa) del usuario será importante por si se requieren cintas localizadas fuera del Centro de Cómputo .

   5.1 El sistema efectúa el proceso automáticamente, indicando el tiempo que tomará dicho proceso (se estima que el tiempo total de restaure puede ser un poco largo, cerca de 15 minutos, dado que el sistema requiere recorrer toda la cinta para verificar contra sus bases de datos y recuperar el archivo más reciente o que no se encuentre marcado como sospechoso si al ser copiado estaba en uso).

   5.2 El proceso finaliza indicando que el restaure ha sido satisfactorio, en caso contrario comuníquese con el Administrador de las RED, previa verificación del nombre correcto del archivo y de la información suministrada por el usuario o el Help Desk según el caso.

PROCESOS ESPECIALES

A. ROTACION DE CINTAS.

Para consultar la cinta que corresponde en el próximo ciclo de backup (llamada "**NEXT TAPE SCHEDULE**") puede hacerlo utilizando el menú del TNA. Recuerde que la cinta indicada corresponde a los procesos del servidor.

```
The NETWORK ARCHIVIST        (c) Palindrome Corporation 1988-1992

                Last Archive update:  Modified checkpoint.
                        Using tape:  QE933AQ1.
                        Updated on:  Wed 08/04/93 00:48:46.
                      Notes logged:  Review c:\tna\tna-log!

                   QE933AQ1 Summary:  Percent     Bytes
                     Permanent saves:     0%           0
                Reusable checkpoints:    60%        1.33G
                            Unused:      39%   920,258,560

               Next scheduled update:  Modified checkpoint.
                 Continue with tape:  QE933AQ1.

            For next scheduled rotation:  Sat 08/07/93 02:30:00.
                    You will need tape:  BLANK TAPE to become QE933AR1.

                   Please move to vault:


                        [ Strike any key to continue! ]
```

D. PRECAUCIONES

1. Una alternativa especial y de manejo del Administrador de la Red, que se emplea para configuración y cambios en el sistema TNA, no se encuentra en este manual por ser u proceso restringido debe ser manipulado de manera especial garantizando la integridad de los procedimientos.

2. Cualquier proceso de backup y o manejo diferente a los anteriormente mencionados será manejado directamente con el Menú de TNA, y deberá ser coordinada con el Administrador de la Red.

3. Al final del presente documento existe un apéndice que corresponde a los diferentes y más comunes mensajes de error que se pueden presentar y los cuales pueden fácilmente ser solucionados, así como los batch files mencionados durante la explicación de los procesos.

ANEXO 7-A

THE NETWORK ARCHIVIST (c) Palindrome Corporation 1988-1990

Release 2 0 MAIN MENU All Rights Reserved

Welcome to The NETWORK ARCHIVIST highly automated librarian for networks.

Help is available at all times by pressing F1.

F1 for Help

F2 for Tape Schedule and Status

F3 to Restore an Entire Disk Drive

F4 to Perform Automatic Archiving to Tape

F10 to Quit

ENTER for All Other Archive Operations

TNA 20

ANEXO 7-B

BATCH FILE PARA PROCEDIMIENTO AUTOMATICO DE RESPALDOS DE APLICACIONES.

Existe el procedimiento automático para los respaldos que se van a realizar diariamente en la red de area local (LAN). Estos respaldos, de manera general, solo sirven para recuperar los datos de OPICS, MAXI, ACCOUNTS PAYABLE, hasta el estado en que se encontraban el día anterior al problema. Para recuperar los datos a un estado previo al desastre, existen otros procedimientos de respaldos que están a cargo de los responsables de cada área dentro de OPICS, MAXI y ACCOUNTS PAYABLE.

Para realizar este proceso de backup el usuario que tiene los atributos de realizar ciertas operaciones en el sistema, dentro del grupo de SUPPORT es el ECU-ARC.

Para iniciar este procedimiento se debe correr en el computador que está a cargo de realizar los respaldos de forma automática, el archivo **GO.BAT** que está en J:\TNA\GO.BAT.

A continuación se detalla el archivo go.bat.

```
@echo on
:start
be trigger 22:00
z:\ccadmin\ccbackup z:\ccdata\mlandata j:\ccbackup\mlandata
be trigger 00:30
c:\backup\dlybck1.bat
goto :start
```

Este archivo es un lazo infinito que ejecuta automáticamente dos procesos:

1. El respaldo de la base de datos del CCMAIL, y
2. El respaldo de OPICS, MAXI, ACCOUNTS PAYABLE, y el TNA (el TNA es el respaldo de toda la red).

Para el disparo de cada uno de los dos procesos se utiliza el TRIGGER que es una opción del Batch Enhancer de NU versón 4.5.

1. El primer proceso, el Backup de la base de datos del CC:MAIL, se lo realiza a las 22h00, y se utiliza el VOL1: que está con un MAP de M:, en el directorio CCBACKUP, el archivo que contiene dicha base de datos es el MLANDATA.

2. Para el segundo proceso, se corre un bat (a las 0h30) que está en el drive C:\BACKUP\dlybck1.bat.

A continuación detallo el DLYBCK1.BAT:

```
@ECHO OFF
REM
REM  BACKUP MAXI DATA FILES
REM
REM  PKZIP WILL RETURN THE FOLLOWING ERRORLEVELS
REM
REM       0 - NO ERROR
REM       1 - BAD FILE NAME OR FILE SPECIFICATION
REM       2,3 - ERROR IN ZIP FILE
REM       4-11 - INSUFFICIENT MEMORY
REM       12 - NO FILES TO PROCESS
REM       13 - FILE NOT FOUND
REM       14 - DISK FULL
REM       15 - ZIP FILE IS READ-ONLY
REM       16 - BAD/ILLEGAL PARAMETERS
REM       17 - TOO MANY FILES
REM       18 - UNABLE TO OPEN ONE OR MORE FILES
REM
MAP N:=NET36PRD:
N:
DEL C:\BACKUP\MAXI\B36BKPMX.ZIP
REM
N:\#LIBRARY\PKZIP -A= C:\BACKUP\MAXI\B36BKPMX OXY_*.*
REM
rem BACKUP C:\BACKUP\MAXI\B36BKPMX.ZIP C:\BACKUP\MAXI
REM
REM  THIS IS A BACKUP OF THE -MAXI- DATA FILES
REM  LABEL THE DISKETTES(S) WITH THE DATE AND TIME
REM
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !      PKZIP HAS REPORTED AN ERROR      !
IF ERRORLEVEL 1 ECHO !      BACKUP MAY NOT BE ACCEPTABLE     !
IF ERRORLEVEL 1 ERASE C:\BACKUP\MAXI\b36bkpmx.ZIP
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 GOTO :SKIP1
rem IF ERRORLEVEL 1 PAUSE
COPY C:\BACKUP\MAXI\B36BKPMX.ZIP K:\MAXI\LEONM\BKUP\B36BKPMX.ZIP
REM
```

```
:SKIP1
REM
@ECHO OFF
REM
REM  A/P DATA FILE BACKUP
DEL C:\BACKUP\ACCOUNT\B36BKPAP.ZIP
REM
N:\#LIBRARY\PKZIP -A= C:\BACKUP\ACCOUNT\B36BKPAP AP?_*.*
REM
rem BACKUP C:\BACKUP\ACCOUNT\B36BKPAP.ZIP C:\BACKUP\ACCOUNT
REM
REM  THIS IS A BACKUP OF THE -A/P- DATA FILES
REM  LABEL THE DISKETTES(S) WITH THE DATE AND TIME
REM
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !      PKZIP HAS REPORTED AN ERROR      !
IF ERRORLEVEL 1 ECHO !      BACKUP MAY NOT BE ACCEPTABLE     !
IF ERRORLEVEL 1 ERASE C:\BACKUP\ACCOUNT\b36bkpap.ZIP
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
rem IF ERRORLEVEL 1 PAUSE
REM
IF ERRORLEVEL 1 GOTO :SKIP2
COPY C:\BACKUP\ACCOUNT\B36BKPAP.ZIP
K:\MAXI\LANDAZUR\BKUP\B36BKPAP.ZIP
REM
:SKIP2
REM
@ECHO OFF
DEL C:\BACKUP\MATERIAL\B36BKPMT.ZIP
REM
N:\#LIBRARY\PKZIP -A= C:\BACKUP\MATERIAL\B36BKPMT MTR_*.*
REM
rem BACKUP C:\BACKUP\MATERIAL\B36BKPMT.ZIP C:\BACKUP\MATERIAL
REM
REM  THIS IS A BACKUP OF THE -OPICS- DATA FILES
REM  LABEL THE DISKETTES(S) WITH THE DATE AND TIME
REM
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !     PKZIP HAS REPORTED AN ERROR     !
IF ERRORLEVEL 1 ECHO !     BACKUP MAY NOT BE ACCEPTABLE    !
IF ERRORLEVEL 1 ERASE C:\BACKUP\MATERIAL\b36bkpmt.ZIP
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
rem IF ERRORLEVEL 1 PAUSE
IF ERRORLEVEL 1 GOTO :SKIP3
COPY C:\BACKUP\MATERIAL\B36BKPMT.ZIP
K:\OPICS\ENDERICA\BKUP\B36BKPMT.ZIP
REM
:SKIP3
REM
j:
j:\tna\tna2tape /a /q
J:\TNA\TNAWHAT
j:\tna\go.bat
```

Este **DLYBCK1.BAT** contiene 2 procesos:

2.1. El repaldo de OPICS, MAXI, y ACCOUNTS PAYABLE.

2.2. El respaldo de todos los volúmenes de la red, utilizando el TNA.

2.1 Este bat realiza una compresión (con el PKZIP versión 2.0) de los datos de MAXI, ACOUNT PAYABLE, y OPICS al drive C:,y se obtienen los siguientes archivos:

C:\BACKUP\MAXI\B36BKPMX.ZIP
C:\BACKUP\ACCOUNT\B36BKPAP.ZIP
C:\BACKUP\MATERIAL\B36BKPMT.ZIP

Luego, copia cada uno de estos archivos al VOL1:, que para el usuario ECU-ARC es el drive k: en el directorio de Marcos León, Rubén Landazuri, y Jeannette Enderica respectivamente.

Se ha implementado el BK.BAT que es un archivo batch para ser utilizado por Marcos, Rubén y Jeannette, que copia del drive I: (VOL2:) de cada uno de estos usuarios los archivos B36BKP*.ZIP al drive c: de la computadora local que ellos estén utilizando, para luego hacer un backup (del DOS) a diskette, una vez transferida

la información a diskette.

BK.BAT

```
COPY I:\BKUP\B36BKP*.ZIP C:
BACKUP C:\B36BKP*.ZIP A:
DEL C:\B36BKP*.ZIP
```

2.2 Una vez hecho los backup de CCMAIL, MAXI, ACCOUNT PAYABLE, y OPICS, se realiza el backup de la red a las 4h00, y vá a respaldar todo lo hecho anteriormente.

Existe elaborado un diskette y una copia en poder del SUPERVISOR de la red y el OPERADOR del sistema respectivamente, con todos estos archivos bat, para en caso de tener problemas con el computador destinado a los respaldos, pueda destinarse otro computador provisionalmente para realizar dichas tareas.

PROCEDIMIENTO AUTOMATICO DE RESTAURACION EN OPICS, MAXI, ACCOUNTS PAYABLE.

En caso de necesitarse restaurar archivos del sistema de Baby 36, que es el ambiente en el que se desarrollan MAXI, OPICS,y ACCOUNTS PAYABLE, estos pueden ser restaurardos desde el TNA.

Los siguientes pasos describen el procedimiento para recuperar archivos de datos después de una contingencia.

Primero, debemos identificar cual de los tres sistemas tiene el problema (OPICS, MAXI o A/P), dependiendo de eso podemos aplicar el archivo batch que corresponda.

B36RSTMX.BAT	Para restaurar MAXI.
B36RSTMT.BAT	Para restaurar OPICS.
B36RSTAP.BAT	Para restaurar A/P.

Estos archivos realizan una descompresión de los archivos de datos utilizando el PKUNZIP versión 2.0, luego los copia en el volúmen NET36PRD: cuyo mapeo es el drive N:.

Estos archivos se encuentran en el computador de respaldos en el drive c:, subdirectorio BACKUP, y en el diskette que tiene el SUPERVISOR de la red.

A continuación detallamos cada uno de los archivos batch:

B36RSTMX.BAT

```
@ECHO OFF
REM
REM  RESTORE MAXI DATA FILES
REM
REM  PKUNZIP WILL RETURN THE FOLLOWING ERRORLEVELS
REM
REM      0 - NO ERROR
REM      1 - BAD FILE NAME OR FILE SPECIFICATION
REM      2,3 - ERROR IN ZIP FILE
REM      4-8 - INSUFFICIENT MEMORY
REM      9 - FILE NOT FOUND
REM      10 - BAD PARAMETERS
REM      11 - NO FILES TO EXTRACT
REM      50 - DISK FULL
REM      51 - UNEXPECTED EOF
REM
MAP N:=NET36PRD:
N:
```

```
RESTORE A: C:  /S
REM
N:\#LIBRARY\PKUNZIP -O C:\BACKUP\B36BKPMX *.*
REM
ERASE C:\BACKUP\B36BKPMX.ZIP
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !     PKUNZIP HAS REPORTED AN ERROR   !
IF ERRORLEVEL 1 ECHO !     RESTORE MAY NOT BE ACCEPTABLE   !
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 PAUSE
```

B36RSTMT.BAT

```
@ECHO OFF
REM
REM  RESTORE OPICS DATA FILES
REM
REM  PKUNZIP WILL RETURN THE FOLLOWING ERRORLEVELS
REM
REM      0 - NO ERROR
REM      1 - BAD FILE NAME OR FILE SPECIFICATION
REM      2,3 - ERROR IN ZIP FILE
REM      4-8 - INSUFFICIENT MEMORY
REM      9 - FILE NOT FOUND
REM      10 - BAD PARAMETERS
REM      11 - NO FILES TO EXTRACT
REM      50 - DISK FULL
REM      51 - UNEXPECTED EOF
REM
MAP N:=NET36PRD:
N:
RESTORE A: C: /S
REM
N:\#LIBRARY\PKUNZIP -O C:\BACKUP\B36BKPMT *.*
REM
```

```
ERASE C:\BACKUP\B36BKPMT.ZIP
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !     PKUNZIP HAS REPORTED AN ERROR   !
IF ERRORLEVEL 1 ECHO !     RESTORE MAY NOT BE ACCEPTABLE   !
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 PAUSE
```

B36RSTAP.BAT

```
@ECHO OFF
REM
REM  RESTORE A/P DATA FILES
REM
REM  PKUNZIP WILL RETURN THE FOLLOWING ERRORLEVELS
REM
REM      0 - NO ERROR
REM      1 - BAD FILE NAME OR FILE SPECIFICATION
REM      2,3 - ERROR IN ZIP FILE
REM      4-8 - INSUFFICIENT MEMORY
REM      9 - FILE NOT FOUND
REM      10 - BAD PARAMETERS
REM      11 - NO FILES TO EXTRACT
REM      50 - DISK FULL
REM      51 - UNEXPECTED EOF
REM
MAP N:=NET36PRD:
N:
RESTORE A: C:  /S
REM
N:\#LIBRARY\PKUNZIP -O C:\BACKUP\B36BKPAP *.*
REM
ERASE C:\BACKUP\B36BKPAP.ZIP
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !     PKUNZIP HAS REPORTED AN ERROR   !
IF ERRORLEVEL 1 ECHO !     RESTORE MAY NOT BE ACCEPTABLE   !
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 ECHO !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
IF ERRORLEVEL 1 PAUSE
```

110 NOTE: Drive reported excessive soft errors %9.99 < when >

When: indica la operación en proceso (restaure, copia a cinta, etc)
El mensaje indica que durante el proceso en curso se han detectado un cierto porcentaje (%9.99) de problemas de software durante la ejecución (when) del comando seleccionado por lo que se requiere solicitar mantenimiento preventivo (especialmente de limpieza) a la cinta "Palindrome". Si el problema persiste, por favor coordine con el administrador de la Red un reemplazo de la cinta correspondiente, en tanto se le brinda un mantenimiento mas a fondo.(Después de cada limpieza se recomienda utilizar una cinta nueva para efectuar las pruebas y nunca una del juego de backup) Se estima que al menos cada 3 meses se debe efectuar limpieza a las cabezas de lectura del "Tape backup"

450 ERROR: To little memory for TNA o run

La memoria (RAM) disponible para ejecutar los comandos de TNA no es suficiente y por lo tanto no puede continuar (o efectuar) con el proceso.
Favor verificar si existen programas residentes, o si previamente ejecutaron programas con opción de salir al sistema temporalmente. TNA requiere 490KB de memoria disponible para poder trabajar. De ser posible la solución mas fácil será dar "BOOT" al sistema (Alt + Ctrl + Del) o apagar y prender el equipo.

573 NOTE: Deferred protection - file in use: [path\filename]

El archivo que en ese momento quería salvarse no pudo ser copiado, por tener atributos de "No sharable" el proceso continua pero en esta sesión este archivo no será copiado. Como medida de seguridad durante el siguiente proceso de backup TNA automáticamente intentará hacer la copia pendiente de este archivo y así sucesivamente seguirá intentando hasta tanto no logre obtener una copia (confiable) en cinta de dicho archivo. Este mensaje aparecerá tantas veces como archivos sean encontrados como no disponibles. Solo en caso de ser este un proceso "Especial" en el que se requiera la seguridad absoluta de tener toda la información de los servidores de archivos, el mensaje no será considerado como grave. Para obviar lo anterior se recomienda que ningún usuario se encuentre trabajando en la Red. Sin embargo como medida preventiva se ha determinado como horario de backup de los volúmenes, directorios y archivos de la red un período entre las 10 PM y 12 PM, con lo cual se garantiza que este mensaje no será muy común.

586 NOTE: File open - suspect file protection [source]

El archivo indicado en "source" fue copiado a cinta, pero dado que está en uso el archivo quedará marcado como sospechoso y dos situaciones indican

que su contenido no será confiable. El archivo puede estar corrupto si en el momento en que el sistema lo leía para copiarlo a cinta este estaba siendo grabado por quien lo tenía "OPEN", el segundo caso sería si el archivo fue cambiado después del proceso de backup y por tanto la copia en cinta no es exactamente la última por lo que en un eventual proceso de recuperación a este archivo no se puede garantizar la integridad de su información.

712 NOTE: The mounted tape is full

TNA requiere una cinta diferente ya que la que es utilizada en este momento se llenó o simplemente ya estaba llena, esta nueva cinta se requiere para poder terminar la presente operación. (Debe ser una cinta totalmente en blanco) En adición, esta nueva cinta será incluida en el sistema y las futuras referencias se harán siempre a esta nueva cinta, salvo que este "set" este involucrado en un proceso de recuperación, en cuyo caso se puede requerir también la primera. (ver el mensaje "713 ERROR")

713 ERROR: The mounted tape is full

En la última operación realizada la cinta se llenó o se montó una cinta que no corresponde al proceso elegido. Seleccione el paso de consulta para averiguar cual es la próxima cinta y poder así iniciar el proceso. Este mensaje se encuentra correlacionado con el "712 NOTE"

752 ERROR: During QUIET operation, mounted tape was unformatted

La cinta colocada para el proceso de backup No Atendido no está formateada, favor colocar un cinta previamente formateada. Normalmente el sistema no requiere cintas preformateadas, favor reportar este hecho al Administrador del la Red.

753 ERROR: No tape installed during quiet operation.

No se ha colocado una cinta en la unidad.
La cinta montada no es reconocida por el sistema.
La cinta no es compatible con los sistemas "Palindrome".
El compartimiento no fue cerrado.
El equipo no esta prendido.

769 NOTE: Please remove tape and label it:[BOGARC_xx]

Después de cada proceso de backup en el que fue montada una cinta nueva este mensaje solicitará que dicha cinta sea rotulada, ya que TNA internamente siempre identificará esta cinta con este nombre. La marcación de esta cinta es de suma importancia dado que el sistema siempre hará referencia a la cinta mediante esta identificación y en todo caso deberá corresponder al nombre interno que el sistema asignó a la cinta ya que ella lo valida.

ANEXO 8

HELP DESK

ANEXO 8

HELP DESK

OBJETIVO

El objetivo de este documento es el de implementar la ayuda que el departamento de MIS dará a los usuarios de la red (LAN), para solucionar problemas que día a día tienen en diversas areas que involucran al departamento de MIS.

Para tener un registro de las llamadas, se ha diseñado un formulario de control de llamadas, el mismo que debe ser llenado antes y después de atender una llamada. Este formulario permitirá al Departamento de MIS mantener estadísticas de los problemas atendidos y ubicar las áreas débiles que requieren mayor atención.

PROCEDIMIENTO

Para poder dar una mejor atención a los usuarios de los PC's, se ha visto conveniente la implementación del HELP-DESK. El departamento de MIS ha asignado una extensión de la central telefónica **444**, este número estará siempre a disposición de los usuarios. Así mismo, se ha instalado un contestador automático para esta extensión, en donde los usuarios pueden indicar su problema. MIS tiene asignado a una persona para atender los problemas.

- Al recibir una llamada de ayuda, ésta debe ser registrada en el formulario de HELP-DESK, este formulario tiene diseñado los campos necesarios para el efecto.
- La coordinadora de MIS será la encargada de notificar al HELP-DESK sobre los problemas registrados.
- Al ser notificada la persona encargada del HELP-DESK, ésta deberá acudir donde el usuario y solucionar el problema.
- A su retorno al Departamento de MIS, el encargado del HELP-DESK debe llenar el formulario, detallando el problema encontrado, las causas y la solución que se dio al mismo; además indicará el tiempo aproximado que le tomó resolver el problema.

REPORTES DE ATENCIONES

Como se mencionó anteriormente en base a la información recopilada en los formularios llenados del servicio prestado por el HELP-DESK, se deberán preparar reportes semanales y mensuales. Estos reportes serán de mucha ayuda para el departamento de MIS.

Reporte Semanal.

En este reporte se deberá registrar bajo que aplicación ocurrió el problema, si en hardware ó software. Para facilitar este reporte existe un diseño en blanco que se debe llenar.

Al final del reporte hay una tabla para registrar a los usuarios que llamaron por ayuda más de una vez.

Reporte Mensual

El reporte Mensual es una recopilación de los reportes semanales. Así mismo, para este reporte hay un formato preestablecido que debe ser llenado cada mes.

Al analizar estos reportes, se pueden identificar varios aspectos importantes para el departamento de MIS. Por ejemplo, cuál es la aplicación más compleja para los usuarios, cuál es el nivel de conocimiento de los usuarios sobre ciertos programas, que dispositivos son los que se dañan con más frecuencia, el tiempo que gasta la persona de HELP-DESK en solucionar los problemas, cuál es el usuario con más problemas, entre otros. De esta manera MIS podrá considerar otras alternativas para ayudar a los usuarios, como el dictar cursos o charlas sobre determinados programas, realizar controles periódicos sobre ciertos dispositivos, y más alternativas que incrementen el nivel de conocimientos y buen uso de computadores y programas que están disponibles para todos los usuarios.

LLAMADAS DE AYUDA EN FINES DE SEMANA

OBJETIVO

El objetivo de este documento es el de implementar la ayuda que el Departamento de MIS dará a los usuarios de la red (LAN), durante los fines de semana o días festivos, para solucionar problemas en diversas areas que involucran al departamento de MIS.

PROCEDIMIENTO

Cuando una persona (usuario de la red) tiene problemas debe comunicarlos al departamento de MIS, para dejar registrado su problema. El departamento de MIS ha creado para HELP-DESK un número especial (444), con un contestador automático. Adicionalmente MIS tiene asignado un BEEPER (2097) con Metro Quito que es portado por la persona de MIS que esté de turno. Se ha distribuido un Memorándum para dar a conocer a todos los usuarios de este servicio que MIS esta dando, así como la forma de ubicar a una persona de MIS.

Para implementar la ayuda de los fines de semana o días feriados, MIS asignó turnos para cada una de las personas. La responsabilidad del turno es por una semana completa (7 días), es decir de lunes a lunes, esto significa que la ayuda no solo es para los fines de semana o días feriados sino, aún entre semana por las noches.

- El operador de la central telefónica es la primera persona que recibe el mensaje de ayuda. El será quien comunique a la persona de turno de MIS, por medio del receptor (# 2094), dándole el mensaje inmediatamente.

- Al ser notificado la persona de turno, ésta deberá hablar con el operador para pedir información adicional del problema reportado. Esto es, preguntará quien es la persona con el problema, de que departamento es y, exactamente, a qué hora se produjo la llamada de ayuda.

- Inmediatamente la persona de turno de MIS, debe acudir a las oficinas a solucionar el problema. Puede haber ocasiones en las que se puede solucionar problemas por teléfono. Si así lo hace, la persona de turno volverá a llamar luego de un momento para asegurarse que realmente el problema está solucionado. De preferencia el problema debe ser solucionado en las oficinas de OXY.

- Al llegar a las oficinas la persona de MIS de turno, debe verificar el problema reportado. El personal de MIS está capacitado para poder solucionar cualquier problema hasta cierto nivel. Hay personas responsables y expertas en cada area de sistemas, por lo tanto si el problema no puede ser solucionado, inmediatamente el responsable del area involucrada deberá ser notificado.

- Al terminar el turno se debe firmar y anotar las observaciones que hubo en el mismo, en el formulario que existe para control de turnos.

- El receptor asignado a MIS debe ser entregado a la persona que continúa en la lista de turnos.

ACTIVIDADES IMPORTANTES

Esta es un lista de las actividades que deben ser realizadas por la persona que está de turno.

- Mirar la consola del SERVER, si hay mensajes de error.
- Ver el monitor del cc:Mail Gateway, si esta activo, es decir enviando y recibiendo mensajes de Tulsa.
- Ver el monitor del DIALIN, si esta recibiendo y enviando mensajes al CPF.
- Mirar el monitor del computador que tiene conectado el Tape BACKUP, ver el status del backup.
- Ver la temperatura del centro de cómputo.

ANEXO 9

PLAN DE CONTINGENCIA PARA REDES LOCALES

1. OBJETIVO

Este procedimiento tiene por objeto el recuperar la información, y más que eso, el tener siempre operativo el sistema de información de Occdental Ecuador. Esto implica el poner en marcha un plan en casos de catástrofes, es decir situaciones imprevistas, que interrumpen el funcionamiento del sistema de información. Las causas conocidas o desconocidas deben ser tratadas con mucha cautela, un olvido o demora en realizar este procedimiento puede producir resultados impredecibles. La interrupción del sistema de información no solo implica la pérdida de datos, sino también fallas en Hardware y en Software. Las causas que pueden obligar a caer es este estado pueden ser varias como la falla del Hardware, el daño de una tarjeta interna del equipo central, falla de los discos duros, o causas más fuertes como atentados, incendios, terremotos, entre otros.

2. RECUPERACIONES

En este tema se consideran varios niveles de recuperación de información. Empezando con la recuperación total, esto es cuando hay pérdida total; Recuperación de datos, cuando hay pérdida de información; Recuperación de dispositivos, cuando hay problemas con adaptadores y/o discos duros; Recuperación de Comunicación, cuando hay problemas con adaptadores de comunicaciones; Recuperación por problemas en tarjetas básicas; Recuperación por problemas en otros tipos de dispositivos.

2.1 Pérdida Total

La Pérdida Total del sistema de información, es el daño más grande que hay en los desastres que puede ocurrir. Nosotros hemos tomado las siguientes precausiones para estos casos.

2.2 Pérdida de Información

Se ha clasificado en varios niveles la pérdida de información, dando su respectiva importancia se debe tratar a cada nivel.

2.2.1 Nivel de Usuario/Grupo

Se debe considerar como pérdida de información a nivel de usuario o de grupo, cuando un usuario o más de un mismo grupo de usuarios, reportan la perdida de información. Es decir el no poder consultar un archivo de datos, o no poder utilizar un aplicación. Para

2.2.2 Nivel de Volumen

Se considera que ha existido pérdida de información en un volumen, cuando dos o más usuarios de diferentes grupos o departamentos reportan falta de archivos, archivos que no se pueden consultar o la imposibilidad de consultar sus datos en diferentes aplicaciones. Los siguientes son los pasos a seguir para tal evento:

a. Evaluar la magnitud del problema (cuantos volúmenes están involucrados en el daño). Esta operación se puede efectuar rápidamente mediante la ejecución de la utilidad Novell "VREPAIR" así:

   Desde la consola del servidor afectado y en la modalidad de System Console cargar el módulo VREPAIR "**LOAD VREPAIR**". Si previamente el volumen SYS ha sido desmontado el módulo Vrepair puede ser cargado desde el drive A o B montado el diskette número 2 de Netware marcado "Netware Operating System-2".

   Desmontar los volúmenes afectados "**DISMOUNT XXX**" donde XXX debe ser SYS, VOL1, VOL2, VOL3 y/o NET36PRD.
   Si más de un volumen esta desmontado se podrá observar una lista de ellos y se deberá seleccionar el volumen deseado. Inmediatamente se indique cual, el proceso de diagnóstico detección y corrección de errores inicia. Cada vez que un error sea detectado el proceso genera una pausa e indica el error, esta parada puede ser eliminada mediante un cambio de SET vía la tecla "F1" en la opción 1, así mismo con la opción 2 se puede almacenar un log de las reparaciones efectuadas (una y otra opción permitirán agilitar el presente test). Este proceso puede tomar 5 y 30 minutos dependiendo del tamaño del disco y la cantidad de errores detectados (la experiencia previa en estos eventos sugiere, si la urgencia en el tiempo lo permite, repetir el proceso sobre los volúmenes que presenten un porcentaje importante de errores).

b. Si el problema involucra una falta de sincronismo en la definición de Mirroring (Out of Sync) lo cual genera un proceso de Remirroring este puede tomar hasta 4 y media horas, período en el cual no es recomendable ofrecer ningún servicio por lo que se debe seguir el siguiente proceso para desactivar el Mirroring y activarlo en horas de la noche.
Desde la consola del servidor afectado y en la modalidad de System Console cargar el módulo de instalación "**LOAD INSTALL**".

Inmediatamente se observa un menú el cual consta de 5 opciones: Seleccionar la primera opción, la cual conduce al menú **Partition Mirroring Status**. Esta pantalla permite observar la situación exacta de los volúmenes.

Seleccionar la primera opción, la cual conduce al menú **Partition Mirroring Status.** Esta pantalla permite observar la situación exacta de los volúmenes.

Seleccione la partición que aparece **Mirrored**, y aparecerá la lista **Mirrored Netware Partitions**. Borre la partición "**Out of Sync**", lo cual causará dos efectos: el primero cancelara inmediatamente el proceso de Remirroring y el segundo que para todos los efectos el proceso de Mirror estará inhabilitado.

NOTA: La opción de Mirroring debe activarse a la mayor brevedad, preferiblemente en horas de la noche, se estima para un disco de 1 Gigabyte que el proceso para sincronizar las particiones (Remirroring) tarda 4 horas, cuando éste se encuentre ocupado en un 70%. Para cumplir este propósito se debe ejecutar el proceso inverso al planteado en el punto anterior (b.):

* Para restablecer el sincronismo en la definición de Mirroring se podrá observar el mensaje de no sincronismo (Out of Sync) al indicar nuevamente que quiere hacer "Mirroring" el sistema genera el proceso de Remirroring (el cual puede tomar hasta 4 y media horas), se recomienda activarlo en horas de la noche siguiendo los siguientes pasos.
  Desde la consola del servidor afectado y en la modalidad de System Console cargar el módulo de instalación "**LOAD INSTALL**". Inmediatamente se observa un menú **Partition Mirroring Status**. Esta pantalla permite observar la situación exacta de los volúmenes (Mirrored, Not Mirrored y/o Out of Sync).

  Seleccione la partición que usted requiere dejar efectuando el proceso de Espejo. Para este caso deberá ser la partición No. 1. Esta selección conduce a nueva pantalla **Mirrored NetWare Partitions** que mostrará una lista de los volúmenes

que están haciendo Espejo.

Finalmente presione la techa Insert para obtener la lista de particiones disponibles pantalla llamada "**Mirrored NetWare Partitions**" y seleccione el volumen deseado.

Una vez se selecciona la partición deseada, en la parte de consola se observará un mensaje de sincronización informando que esta opción está habilitada así como que el proceso de sincronización se inicia, por lo que la lista mostrará "Out of Sync" hasta que dichas particiones queden sincronizadas momento en el cual mostrará "In Sync".

c. Cuando el problema reporte inconsistencias en el sistema operacional, este debe ser reinstalado de la siguiente manera:

Desde la consola del servidor afectado y en la modalidad de System Console cargar el módulo de instalación "**LOAD INSTALL**".

Seleccionar la tercera opción "System Options" la cual conduce al menú "Available System Options" del cual se debe seleccionar la opción "**Copy System and Public Files**". Con esta selección se inicia el restaure del sistema operacional Netware solicitando el diskette No. 2 llamado "Netware Operating System-2", el sistema así sucesivamente ira indicando el diskette requerido. Al finalizar este proceso, se recomienda bajar y subir el servidor, finalmente se debe renombrar en el directorio Public del volumen SYS el archivo MENU.EXE por ejemplo como MENUNOV.EXE.

d. Como última opción la información se podrá recuperar de la más reciente cinta de backup que para tal fin se encuentra en el Centro de Cómputo. Cualquier información sobre los pasos a seguir o cualquier necesidad al respecto debe ser consultado en el Procedimiento de Backup en Red. A pesar de ser esta una de las opciones más confiable y seguras se ha dejado como última en vista del excesivo tiempo necesitado para poder restablecer cualquier cantidad de información.

2.2.3. Nivel de Disco

Toda pérdida de información a nivel de disco involucra dos componentes a tener en cuenta, el primero define todos los elementos de Hardware que permiten el trabajo en disco y el segundo que tiene que ver son el manejo y administración de datos.

Para el primer criterio de análisis más adelante el punto "2.3 Problemas en Adaptadores y/o Discos" establece las pautas y criterios a seguir para el diagnóstico y pronta solución de todos los inconvenientes de Hardware que se presentasen.

Para el segundo criterio, el punto "2.2.2 Nivel de Volumen" incluye los pasos básicos a seguir en caso de establecer que la pérdida de información fue a nivel de Disco, pero no involucra daño físico de los diferentes dispositivos de almacenamiento. Sin embargo y así los parámetros de información lo indiquen es necesario programar un diagnóstico exhaustivo de dichos dispositivos una vez la información se halla recuperado y se obtenga un nuevo y actualizado backup.

2.2.4 Pérdida Total

Se considera pérdida total de información cuando por ningún método o utilidad conocida es posible consultar y/o recuperar la información almacenada en los diferentes discos del Servidor.

Para llegar a la anterior conclusión se deben haber seguido las diferentes pruebas y pasos enumerados en el numeral "2.2.2 Nivel de Volumen" así como todas las pruebas y diagnósticos planteadas en el punto "2.3 Problemas en Adaptadores y/o Discos".

Es indispensable entender que los diferentes problemas presentados a este nivel motivan un diagnóstico completo y exhaustivo de la totalidad del hardware que compone el Servidor de Archivos así como del sistema de potencia, para ello se deben seguir los siguientes pasos:

a. Una vez la Red esté inoperativa, dar BOOT al equipo con el diskette de configuración correspondiente en el Drive "A" (asegurarse que el diskette esté perfectamente identificado con el número del equipo ya que este almacena la última configuración dada).

b. El proceso de inicialización desde el diskette finaliza mostrando el menú principal que suministra AST llamado "Configuration Utility" que en un punto 5 direcciona las rutinas de diagnóstico "Test Computer".

c. Al seleccionar el anterior punto se direcciona lo que se conoce como Diagnósticos Confidenciales, nivel más bajo (completo) de pruebas.

d. La rutina que puede tomar hasta 15 minutos indicará los problemas detectados y permitirá establecer las acciones a tomar.

e. De existir otro software de test para el hardware, se recomienda efectuar pruebas con este otro software dado que tener más de una opinión sobre el estado real de los equipo permite a su vez garantizar una solución duradera y confiable.

2.3 Problemas en Adaptadores y/o Discos

2.3.1 Diagnóstico de Adaptadores y Cables

Los diagnósticos de los adaptadores Procom 1990 se ejecutan automáticamente (Power-On Self Test, chequeo de integridad del sistema) cuando el equipo se prende. Por ser tarjetas EISA el sistema en el momento de boot efectúa una verificación de la existencia de estos adaptadores y hace inmediatamente la configuración.

Normalmente, los mensajes de error generados en la consola y por este tipo de problemas son consistentes con la naturaleza del problema. Cuando se presentan varios errores en el servidor, vale la pena analizarlos cronologicamente, ya que en algunos casos se generan reacciones en cadena y la documentación mostraría que el problema es generado por varias fuentes.

Un problema en un adaptador o en un cable puede generar daños en la información de los discos que manejan. Algunas veces, como en el caso de los cables, para encontrar una falla es necesario efectuar reemplazos y por prueba y error encontrar el elemento que esté fallando.

2.3.2 Reemplazo de Adaptadores y Cables

El reemplazo de un adaptador o de un cable debe realizarse de manera muy cuidadosa, vale la pena anotar que antes de realizar este tipo de reemplazos de be existir un backup (a lo menos) de la información.

El reemplazo de un cable SCSI se debe hacer con el equipo y los discos apagados, teniendo en cuenta que el orden en la cadena debe conservarse de menor a mayor. El primer dispositivo o disco debe ser el 0 y el último de la cadena debe llevar un terminador SCSI. El cable que conecta dos dispositivos SCSI es diferente a el cable que conecta el adaptador y el dispositivo 0.

Las tarjetas Procom 1990 que tienen instalados los servidores se encuentran físicamente configuradas igual a como vienen de fábrica. Lo único que varia es su configuración en el ambiente EISA. Para efectuar el reemplazo rápido de un adaptador de estos, se debe efectuar sobre el mismo slot donde se encuentra. Si se desea cambiar el slot, es necesario efectuar también la modificación en la configuración del equipo (Ver el manual de configuración de equipos EISA).

En caso de que se efectué el cambio de la configuración se recomienda tener en cuenta la forma en que se encuentran configuradas las tarjetas para que no se creen conflictos internos (Ver anexos de configuración del sistema).

2.3.3 Diagnóstico de Discos

Desafortunadamente no existen herramientas rápidas para chequear la integridad de un disco de 1 Gigabyte. Si por algún motivo se detecta información corrupta, o que en la consola se presenten mensajes de error aludiendo errores físicos en el disco es necesario ejecutar alguna herramienta de test. Es natural que hay que descartar el adaptador y el cable en la etapa de análisis inicial.

Netware ofrece la posibilidad de efectuar una recuperación de bloques malos efectuando un test de superficie (Surface Test). Esta opción se puede ejecutar de dos formas **destructiva** o **no destructiva**, ambas se encargan de encontrar e inhabilitar los bloques dañados. La diferencia consisten en que una destruye los datos y la otra no lo hace, eso repercute en el tiempo de ejecución. La primera es 20% más rápida que la segunda. En pruebas realizadas en la Compañía la segunda tarde del orden de 2 minutos 20 segundos por cada Megabyte, y haciendo los cálculos correspondientes un disco de 1 Gigabyte puede tardar aproximadamente 40 horas y 36 si se efectúa destructivo.

De todas maneras se recomienda efectuar este tipo de trabajos en el servidor de TEST ya que degradan completamente el tiempo de respuesta. No sobra decir que el ejecutar este tipo de tests a discos de uso diario, y que presentan problemas constantes, en una buena opción.

El procedimiento general para ejecutar el **SURFACE TEST** es el siguiente:

a. Primero se deben desmontar los volúmenes que componen el disco, buscando aislarlo.

b. Haciendo uso del **INSTALL.NLM** se debe seleccionar la opción **Surface Test Options** del menú **Disk Options**. Estando en el menú Surface Test Options se comienza el Test seleccionando **Begin Surface Test**, el sistema preguntará el Tipo de Test: **Destructive** o **Nondestructive**. Y se comienza a realizar el Test. Este puede ser interrumpido en cualquier momento desde el mismo menú.

Paralelo al Test se pueden ejecutar otros o simplemente trabajar en el servidor, teniendo en cuenta que el tiempo de respuesta se degrada.

2.3.4 Reemplazo de Discos

El cambio de disco consiste en eliminar de la cadena SCSI un disco y adicionar uno nuevo de las mismas características. El proceso a seguir es el siguiente:

a. Apagar el servidor y los discos.

b. Verificar la dirección dentro de la cadena SCSI del disco que se va a reemplazar. Colocar la dirección encontrada en el disco nuevo.

c. Desconectar el disco y colocar el nuevo efectuando las mismas conexiones.

No olvidar el terminador SCSI en el caso que sea el último de la cadena.

d. Prender los discos y el servidor. Si el disco reemplazado es el disco con el cual es sistema inicia, se debe verificar que la partición de DOS del disco nuevo sea la primaria, tenga el sistema y esté activada (bootable); y que se encuentren los directorios y archivos necesarios para iniciar el servidor, es de especial importancia verificar las diferentes versiones instaladas en este dispositivo de todos y cada uno de los programas. En caso de no estar así, se debe preparar el disco con anterioridad.

e. Iniciar o arrancar el servidor con el fin de preparar el disco para su funcionamiento normal, siguiendo el procedimiento necesario que se explica en la sección **Pérdida de Información**.

3. ANEXOS

3.1 Lista de Configuración

Las configuraciones que se debe tener para poder configurar el equipo principal (Server de la Red), o para el equipo de respaldo (Backup Server), son la siguientes:

- Especificaciones Técnicas del computador, características físicas como tipo de monitor, floppy, disco duro, puertos seriales o paralelos, memoria, interrupciones, etc.

- Archivos de configuración, como el config.sys, autoexec.bat, startup.cnf, autoexec.cnf.

3.2 Especificación Técnica

Para utilizar el Server, hay que observar la configuración del equipo. Para observar o modificar parámetros de la configuración, se utiliza el diskette con la etiqueta de "EISA SYSTEM CONFIGURATION" marcado para el SERVER. La configuración que debe tener el SERVER principal (AST POWER PREMIUM SE/50), es la siguente:

System - AST Premium SE System Board (MAIN SERVER - 50/66 Mhz)

Parallel Port Configuration
Parallel Port 3BCh, IRQ5

Serial Port Configuration
Serial Ports ..... Port 1=3F8h, 2=2F8h

Floppy-Disk Adapter ..... Integrated

```
Floppy-Disk Type
     Floppy Disk A ..............................  1.44 MB 3.5"
     Floppy Disk B ..............................  None

Hard-Disk Adapter ...............................  Add-in

Hard-Disk Type
     First Hard-Disk Type .......................  None
     Second Hard-Disk Type ......................  None

User-Defined Type for First Hard-Disk
     Number of Heads (1--16) ....................  0
     Number of Cylinders (1--1024)...............  0
     Number of Sectors Per Track (1--63) ........  0
     Write Precompensation (1--1023) ............  0
     Landing Zone (1--1024) .....................  0

User-Defined Type for Second Hard-Disk
     Number of Heads (1--16) ....................  0
     Number of Cylinders (1--1024)...............  0
     Number of Sectors Per Track (1--63) ........  0
     Write Precompensation (1--1023) ............  0
     Landing Zone (1--1024) .....................  0

Video Adapter ...................................  EGA/VGA
Integrated Mouse Port ...........................  Disable
CPU   ..................................................   Type   =
80486DX, Speed = 50 MHz
Math Coprocessor Type ...........................  None
Memory Configuration
     Conventional Memory ........................  640 KB
     Processor Board Memory .....................  16M
     Limit Access to 16 MB ......................  Disable
     Cache Memory ...............................  Enable

Integrated VGA Video Output
     800 x 600 Mode .............................  56 Hz, non-
interlaced
     1024  x  768  Mode  ..........................  87  Hz,
interlaced

Slot 4 - Proteon ProNET 4/16 Token Ring Adapter
Token Ring Network Controller
     Interrup  ..................................  IRQ11,  Edge
triggered
     Speed ......................................  4 Mbps
     Media Type .................................  Shielded

Slot 8 - AST Processor Board

Slot 10 - AST Cupid Memory Expansion Board (32-MB Maximun)
Cupid Memory Configuration
     Total Memory ...............................  8 MB
```

USED RESOURCES

Resource	Slot	Function
IRQ 0	System	System Resources
IRQ 1	System	System Resources
IRQ 3	System	Serial Ports
IRQ 4	System	Serial Ports
IRQ 5	System	Parallel Port
IRQ 6	System	Floppy-Disk Adapter
IRQ 8	System	System Resources
IRQ 11	Slot 4	Token Ring Network Controller
IRQ 13	System	System Resources
DMA 2	System	Floppy-Disk Adapter
Port 2F8h - 2FFh	System	Serial Ports
Port 3BCh - 3BEh	System	Parallel Port
Port 3F0h - 3F7h	System	Floppy-Disk Adapter
Port 3F8h - 3FFh	System	Serial Ports

Memory Address	Amount		
0	640K	System	Conventional Memory
0F0000h	64K	System	System Rom BIOS
1M	15M	System	Processor Board Memory
1040000h	8M	Slot 10	Total Memory

Available Resources

IRQs	DMAs	ISA I/O Ports	Amount	Address
7	0	100h - 2F7h	64K	0A0000h
2 (9)	1	300h - 3BBh	64K	0B0000h
10	3	3BFh - 3EFh	64K	0C0000h
12	5		64K	0D0000h
14	6		64K	0E0000h
15	7			

System - AST Power Premium System Board (BACKUP SERVER - 33 Mhz)

Parallel Port Configuration
    Parallel Port 3BCh, IRQ5

Serial Port Configuration
    Serial Ports ..... Port 1=3F8h, 2=2F8h

Floppy-Disk Adapter ..... Integrated

Floppy-Disk Type
    Floppy Disk A ..... 1.44 MB 3.5"
    Floppy Disk B ..... 1.2 MB 5.25"

Hard-Disk Adapter ..... Add-in

Hard-Disk Type
    First Hard-Disk Type ..... None
    Second Hard-Disk Type ..... None

User-Defined Type for First Hard-Disk
    Number of Heads (1--16) 0
    Number of Cylinders (1--1024)..... 0
    Number of Sectors Per Track (1--63) 0
    Write Precompensation (1--1023) 0
    Landing Zone (1--1024) 0

User-Defined Type for Second Hard-Disk
    Number of Heads (1--16) 0
    Number of Cylinders (1--1024)..... 0
    Number of Sectors Per Track (1--63) 0
    Write Precompensation (1--1023) 0
    Landing Zone (1--1024) 0

Video Adapter ..... EGA/VGA
Integrated Mouse Port ..... Disable
CPU ..... Type = 80486DX, Speed = 33 MHz
Math Coprocessor Type ..... None
Memory Configuration
    Conventional Memory ..... 640 KB
    Processor Board Memory 16M
    Limit Access to 16 MB ..... Disable
    Cache Memory ..... Enable

Integrated VGA Video Output
    800 x 600 Mode ..... 56 Hz, non-interlaced
    1024 x 768 Mode ..... 87 Hz, interlaced

Slot 4 - Proteon ProNET 4/16 Token Ring Adapter
Token Ring Network Controller

Interrup ..... IRQ11, Edge triggered
Speed ..... 4 Mbps
Media Type ..... Shielded

Embedded - AST Integrated VGA

Integrated VGA ..... Enable : Color Display

USED RESOURCES

Resource	Slot	Function
IRQ 0	System	System Resources
IRQ 1	System	System Resources
IRQ 3	System	Serial Ports
IRQ 4	System	Serial Ports
IRQ 5	System	Parallel Port
IRQ 6	System	Floppy-Disk Adapter
IRQ 8	System	System Resources
IRQ 11	Slot 4	Token Ring Network Controller
IRQ 13	System	System Resources
DMA 2	System	Floppy-Disk Adapter
Port 2F8h - 2FFh	System	Serial Ports
Port 3BCh - 3BEh	System	Parallel Port
Port 3C0h - 3C8h	Embedded	Integrated VGA
Port 3CAh	Embedded	Integrated VGA
Port 3C0h - 3C8h	Embedded	Integrated VGA
Port 3CAh	Embedded	Integrated VGA
Port 3CCh	Embedded	Integrated VGA
Port 3CEh - 3CFh	Embedded	Integrated VGA
Port 3DEh - 3CFh	Embedded	Integrated VGA
Port 3D4h - 3D5h	Embedded	Integrated VGA
Port 3DAh	Embedded	Integrated VGA
Port 3F0h - 3F7h	System	Floppy-Disk Adapter
Port 3F8h - 3FFh	System	Serial Ports
Port 46E8h	Embedded	Integrated VGA

Memory Address	Amount		
0	640K	System	Conventional Memory
0B8000h	32K	Embedded	Integrated VGA
0C0000h	32M	Embedded	Integrated VGA
0F0000h	64M	System	System ROM BIOS
1M	15616K	System	Processor Board Memory

Available Resources

IRQs	DMAs	ISA I/O Ports	Amount	Address
7	0	100h - 2F7h	64K	0A0000h
2 (9)	1	300h - 3BBh	64K	0B0000h
10	3	3BFh	64K	0C0000h
12	5	3C9h	64K	0D0000h
14	6	3CBh	64K	0E0000h
15	7	3CDh		
		3D0h - 3D3h		
		3D6h - 3D9h		
		3DBh - 3EFh		

3.3 Archivos de Configuración

3.3.1 Config.sys

3.3.2 Autoexec.bat

```
PAUSE
SERVER.EXE
```

3.3.3 Startup.ncf

3.3.4 Autoexec.ncf

```
file server name NQENOV01
ipx internal net 1525F
mount NET36PRD
mount VOL1
mount VOL2
mount VOL3
load c:3nw990r slot=4
bind IPX to 3NW990R net=1525E
set allow unencrypted passwords=on
set maxium packet received buffers=200
load UPS TYPE=MOUSE DISCHARGE=3 RECHARGE=60
load PSERVER ECU-PS1
load REMOTE
load RSPX
load MONITOR
```

NOTA: Para que el server trabaje con memoria sobre los 16 MB se debe ejecutar la

siguiente instrucción en modo de CONSOLA.

:REGISTER MEMORY 1000000 800000

Donde el 1000000 reprensenta los 16MB de base, y los 800000 son los 8MB adicionales que tiene el Server principal (24MB).

Las tarjetas controladoras de disco SCSI están en los slots, número 1 y número 2 respectivamente. Cada una de estas tarjetas deberá estar con diferentes direcciones, para esto se utilizan los jampers que

BIBLIOGRAFIA

- ALCATEL, MANUAL DE LA CENTRAL TELEFONICA ALCATEL 100.
- APIKI Steve, DIEHL Standford y GREHAM Rick, Redes Locales: Batalla entre estrellas", REVISTA BINARY, Junio 1991.
- BEST INC, MANUAL DE OPERACION DEL FERRUPS FD18KVA, 1993.
- CURRID Cheryl C. - GILLET Craig A., DOMINE NOVELL NETWARE. MACROBIT, 1991.
- CHAMORRO Rafael, "La interconexión de sistemas abiertos OSI", REVISTA PC WORLD, Junio 1992.
- EGLOWSTEIN Howard y THOMPSON Tom, "Please Mr. Postman", REVISTA BYTE, Marzo 1991.
- GARCIA MARQUEZ Rogelio, LA PUESTA A TIERRA DE INSTALACIONES ELECTRICAS Y EL R.A.T..MARCOMBO S.A. 1991.
- GRUPO WAITE, REDES LOCALES, TEORIA Y PRACTICA.. ED ANAYA 1987.
- KAPLAN Gadi, "Data Communications", REVISTA SPECTRUM de la IEEE, Agosto 1991.
- IBM, AS/400 SYSTEM ADMINISTRATION AND CONTROL, 1993.
- IBM, FOLLETO DE RECOMENDACIONES E INSTALACIONES FISICAS PARA EL AS/400.
- ITT, MANUAL DE LA CENTRAL TELEFONICA ITT 3100.
- LOTUS, MANUAL DEL ADMINISTRADOR DEL CC:MAIL.
- LOTUS, MANUAL DEL USUARIO DEL CC:MAIL.

LOTUS, MANUAL DEL ADMINISTRADOR DEL CC:MAIL GATEWAY.

NFPA, NORMAS DE LA NFPA, 1992.

NOVELL, MANUAL DE INSTALACION DE NETWARE 3.11, 1991.

OCCIDENTAL OIL AND GAS CORPORATION, ORGANIZATION MANUAL,1992.

PALINDROME, MANUAL DE OPERACION DEL "TAPE BACKUP", 1993.

- TANENBAUM Andrew, REDES DE ORDENADORES. PRENTICE HALL, 2DA EDICION, 1991.
- TIMEPLEX, MANUAL DE OPERACION DEL MINILINK/2+, 1992.
- TIMEPLEX, MANUAL DE MANTENIMIENTO DEL MINILINK/2+, 1992.
- TIMEPLEX, MANUAL DE OPERACION DEL MICROLINK/2+, 1992.
- TIMEPLEX, MANUAL DE MANTENIMIENTO DEL MICROLINK/2+,1992.
- Apuntes de clase: Comunicación Digital y Telemática.