39

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

INGENIERIA

"SISTEMA DE COMUNICACIONES MOVILES VIA TERRESTRE Y SATELITAL MOVISAT"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N :

JAIME ESTRADA HERNANDEZ

ARTURO ISLAS BLANCO

DIRECTOR DE TESIS: ING. ROBERTO REYES CHALICO

MEXICO, D. F. 1996

Por el gran apoyo que siempre he recibido dedico este trabajo con cariño para :

Mi madre y hermano

Laura y Alejandro

"Gracias por haberme dado una gran oportunidad en la vida"

Leticia

"Por estar conmigo en todos los momentos"

Mis tios y primos

"Por sus valiosos consejos"

Arturo

Con cariño para :

Mis padres :

Alicia y Javier

"Para que de alguna manera vean reflejados sus esfuerzos e ilusiones. Gracias".

Mis hermanos :

Javier, Reyna, Armando y Guadalupe

"Consideren mi trabajo como un ejemplo de lo que se puede lograr con entusiasmo y dedicación en lo que uno se propone, ánimo".

Jaime

Indice

CAPITULO 3 Administración del Sistema de Trabajo 82

Introducción

Las comunicaciones hoy en día son esenciales para el desarrollo de un país, México se encuentra en el umbral de una nueva era, esto es, el desarrollo de una sociedad informática, en el que las telecomunicaciones serán una parte esencial de la infraestructura básica para alcanzar la modernización productiva del país, al apoyar la descentralización y crear nuevas opciones de desarrollo en cada una de las regiones por más lejanas que sean.

En los últimos años México ha experimentado avances en este sector y su rápido desarrollo tecnológico hacen del campo de trabajo en computación y telecomunicaciones una fuente creciente de empleos. A este campo pertenecen sistemas telefónicos, redes digitales de servicios integrados, radio y microondas, redes de computadoras de área local y expandida, sistemas basados en fibra óptica, redes de computadoras y teleinformática, sistemas de transmisión analógica, digital, satelital y áreas de radiocomunicación.

Dentro de las comunicaciones vía satélite Telecomunicaciones de México ha introducido al país un sistema de comunicaciones móviles, que permite facilidades a las actividades empresariales que requieran mantener un control permanente de sus unidades de transportación para comunicarse con el personal móvil y localizar los movimientos de sus vehículos; a las industrias de recursos naturales para mantenerse en contacto con el personal de obras y controlar los bienes y equipos remotos. La comunicación móvil también es utilizada para que el personal de ventas y servicio de una organización puedan crear su propia oficina realmente móvil. A los servicios de emergencia (Policía Federal de Caminos, Policía Judicial, Cruz Roja, Bomberos, entre otros) y las agencias gubernamentales, les facilita una comunicación segura para atender y resolver las necesidades que presente una determinada población.

La cobertura del servicio MOVISAT, le permite a un usuario comunicarse a lo largo y ancho de todo el territorio nacional con sus unidades móviles (equipo con el cual se puede realizar el proceso de comunicación), las cuales pueden estar ubicadas en las más aisladas carreteras, en el más inhóspito desierto y en la más lejana selva de nuestro país.

MOVISAT esta formado por varios sistemas, uno de los cuales es el Sistema de Cómputo formado fundamentalmente por procesadores VAX de DIGITAL EQUIPMENT, estos requieren de una eficiente administración de recursos de hardware y software para mantener el procesamiento de la información en óptimas condiciones y así poder ofrecer servicios con información altamente confiable.

Por lo anterior consideramos relevante tratar un tema que nos permita conocer y proponer los alcances que una buena administración de recursos computacionales pueda ofrecer a un sistema tan importante como lo es MOVISAT.

La Administración del Equipo Computacional bajo Plataforma VAX del Sistema de Comunicaciones Móviles MOVISAT para Telecomunicaciones de México, es el tema a desarrollar en este trabajo, en el cual tratamos con aspectos que nos ayudarán a comprender una de las áreas de desarrollo del Ingeniero en Computación.

CAPITULO 1

Introducción al Sistema de Comunicaciones Inmarsat

1.1 Introducción al sistema de comunicaciones Inmarsat-C
1.2 Componentes básicos del sistema Inmarsat
1.3 Diferencias de Inmarsat-C con otros sistemas de Inmarsat
1.4 Servicios de Inmarsat-C
1.5 Configuración del sistema MOVISAT
    1.5.1 Segmento espacial
    1.5.2 Segmento terrestre
    1.5.3 Estación terrena LES-TELECOMM
        1.5.3.1 Equipo de radiofrecuencia (RF)
        1.5.3.2 Equipo de Señalización y Control de Acceso (ACSE)
    1.5.4 Estaciones móviles
1.6 Sistema de comunicaciones LES-TELECOMM
1.7 Configuración física del ACSE
1.8 Software del ACSE
1.9 Tipos de datos generados por el ACSE

CAPITULO 1

Introducción al Sistema de Comunicaciones Inmarsat

Un consorcio de signatarios de todo el mundo estableció Inmarsat (Organización Internacional de Comunicaciones Móviles vía Satélite) en 1969, para ofrecer los servicios de comunicación vía Satélite a usuarios marítimos en una base global. En años recientes este servicio se ha extendido para incluir comunicación con unidades móviles terrestres. Inmarsat lanza sus propios Satélites y opera sus propios centros de control de red para coordinar el acceso a ellos por medio de Terminales Móviles y Estaciones Terrestres. Las unidades móviles se comunican con los usuarios terrestres vía Estación Terrena (LES, Land Earth Station).

Inmarsat ofrece servicios de comunicación de voz y datos a través de varias redes independientes que comparten los satélites y las Estaciones Terrenas (LES). Actualmente, la red principal es Inmarsat-A, la cual ha sido empleada principalmente para comunicaciones de voz y desde unidades móviles en el mar y en las partes inhóspitas del mundo o bien en lugares donde no existen redes telefónicas adecuadas. Otras redes están en vías de desarrollo incluyendo comunicaciones aeronáuticas y una versión mejorada de Inmarsat-A conocida como Inmarsat-B, que pone mucho más énfasis en la transmisión de información a gran velocidad y otros servicios de información. La tabla 1.1 muestra los servicios que son provistos por Inmarsat.

Estándar	Servicios provistos por Inmarsat
A	Voz, FAX, Datos y TELEX
B	Servicio Digital, reemplaza al Estándar-A
C	Sólo datos de baja velocidad, almacenamiento y envío
M	Voz, FAX y Datos
P	Servicio a Futuro
Aeronáutico	Operaciones de Voz y Datos a pasajeros

Tabla 1.1 Servicios provistos por Inmarsat

1.1 Introducción al sistema de comunicaciones Inmarsat-C

Inmarsat-C, es un servicio de bajo costo que opera bajo la filosofía de almacenamiento y transmisión de mensajes que puede proporcionar hacia y desde las terminales terrestres y marítimas en unidades móviles, faros, plataformas petroleras, etc., o hacia y desde unidades móviles terrestres, dentro de los alcances de los Satélites utilizados por el sistema.

El sistema Inmarsat se constituye de cuatro regiones oceánicas sobre la Superficie Terrestre de cobertura para los servicios de Inmarsat-C controladas por la Estación Coordinadora de Red (NCS, Network Coordinate Station) dichas regiones oceánicas son:

- Atlántico Este
- Atlántico Oeste
- Pacífico
- Indico

Cada región sirve para una o más Estaciones Terrenas (LES), cada una de las cuales está conectada a una o más redes terrestres locales, como por ejemplo a una red telefónica.

De acuerdo a los protocolos de Inmarsat-C, el control de cada región Oceánica se lleva a cabo mediante una Estación Coordinadora de Red (NCS). Cada NCS se comunica con la LES en su Región Oceánica, usando para ello el Satélite apropiado.

En la figura 1.1 se observa la relación entre dos regiones oceánicas: la región 1 cuenta con su LES y su grupo de terminales móviles terrestres y marítimas, la cual se comunica con la región 2 por medio del Sistema de Procesamiento y Control (SCP).

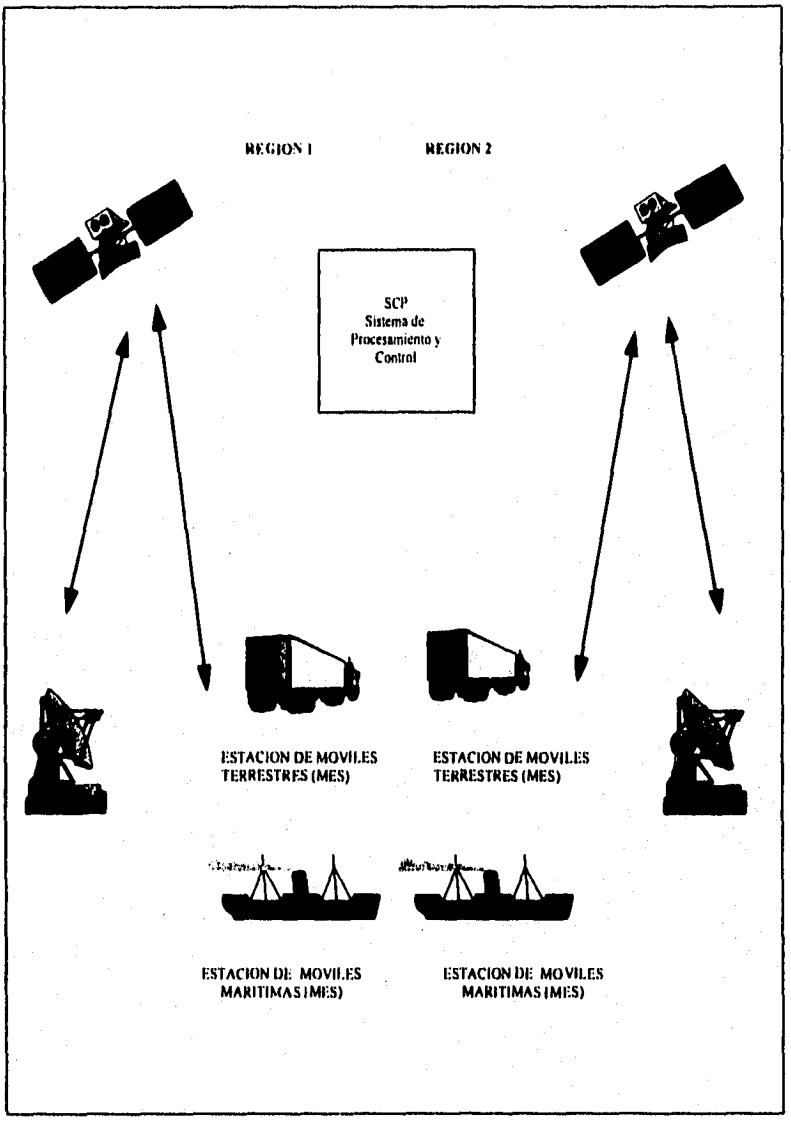

Figura 1.1 Regiones oceánicas dentro de Inmarsat-C

1.2 Componentes básicos del sistema Inmarsat-C

El Sistema de Comunicaciones de Inmarsat-C esta dividido fundamentalmente en:

- Usuarios Terrestres, típicamente este concepto está formado por terminales de TELEX, Redes Conmutadas de Paquetes de Datos (PSDN, Packed Switched Data Network), máquinas de FAX, red telefónica y correo electrónico, que son básicamente las redes de comunicación que un usuario utiliza para sus diferentes necesidades de comunicación.

- La Estación Terrena (LES, Land Earth Station), la cual provee la interface entre los datos (mensajes) y el satélite.

- El satélite geoestacionario cuya cobertura es una región específica.

- Las terminales móviles (MES, Maritime Earth Station) con su equipo de comunicaciones: transmisores, receptores y terminales de datos, dichas terminales son el hardware que un usuario requiere para poder enviar mensajes, esto es, entablar comunicación.

- El NCS (Network Coordinate Station), el cual administra todos los recursos del satélite y coordina todas las actividades entre las MES y las LES.

En la figura 1.2 se muestra el esquema del Sistema de Comunicaciones de Inmarsat-C, en este se pueden observar cada uno de los elementos que forman parte del mismo.

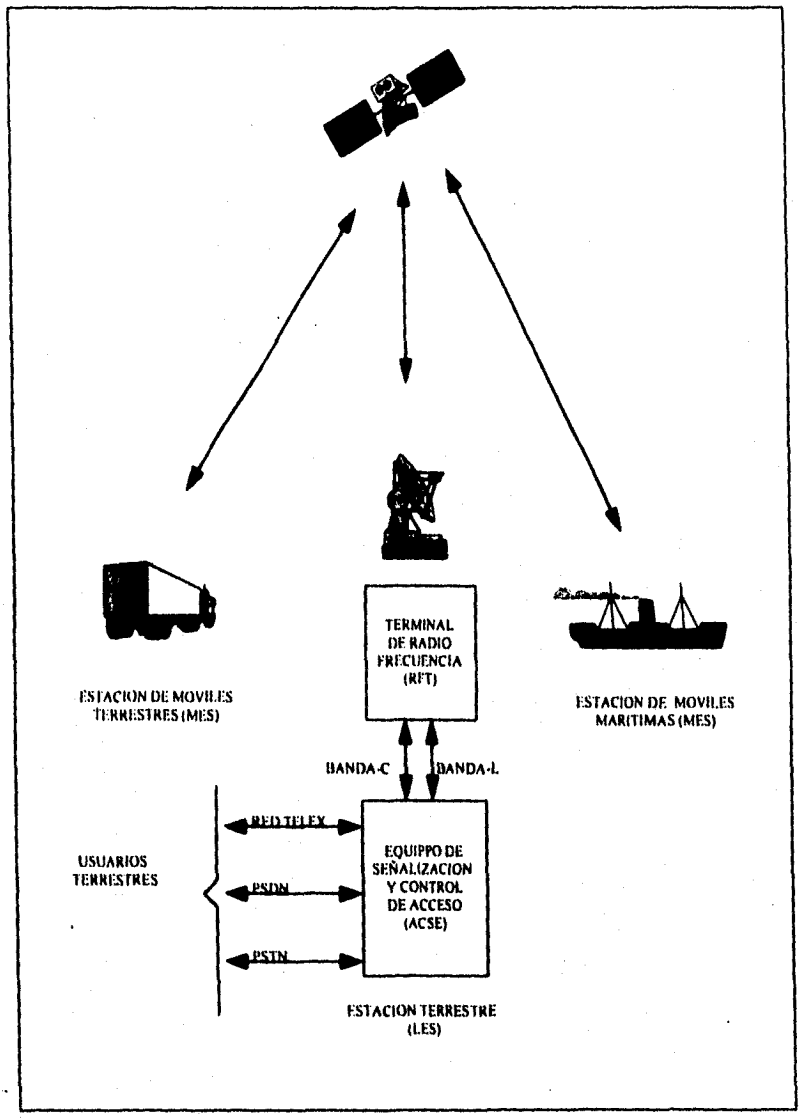

Figura 1.2 Sistema de comunicaciones de Inmarsat-C

Cada LES consiste de los siguientes sistemas, los cuales se observan en la figura 1.3:

- Un Equipo de Señalización y Control de Acceso (ACSE, Access Control and Signalling Equipment), para el manejo de las comunicaciones, este provee la interconexión al equipo de radio frecuencia a través de las interfaces especializadas para el manejo de las señales de comunicación. Por otra parte permite la interconexión al conjunto de redes terrestres mediante interfaces de TELEX, PSDN, PSTN, etc.

- Equipo Terminal de Radio Frecuencia (RFT, Radio Frecuency Terminal).

1.3 Diferencias de Inmarsat-C con otros sistemas de Inmarsat

La principal diferencia entre Inmarsat-C y otros sistemas de Inmarsat, así como Inmarsat-A, Inmarsat-C facilita el almacenamiento y envío de mensajes. En los sistemas Inmarsat-C, un mensaje de un usuario terrestre es transmitido sobre una ruta terrestre y almacenado (seguramente en el ACSE), después este es transmitido vía satélite. Similarmente, un mensaje de una terminal móvil es transmitido por el satélite y almacenado en el ACSE para después ser transmitido sobre una red terrestre.

Cada uno de los mensajes transmitidos es asegurado por el ACSE, deliverándolo exitosamente si este toma su destino final en caso contrario la LES retornará un valor en donde se indique que no se ha entregado.

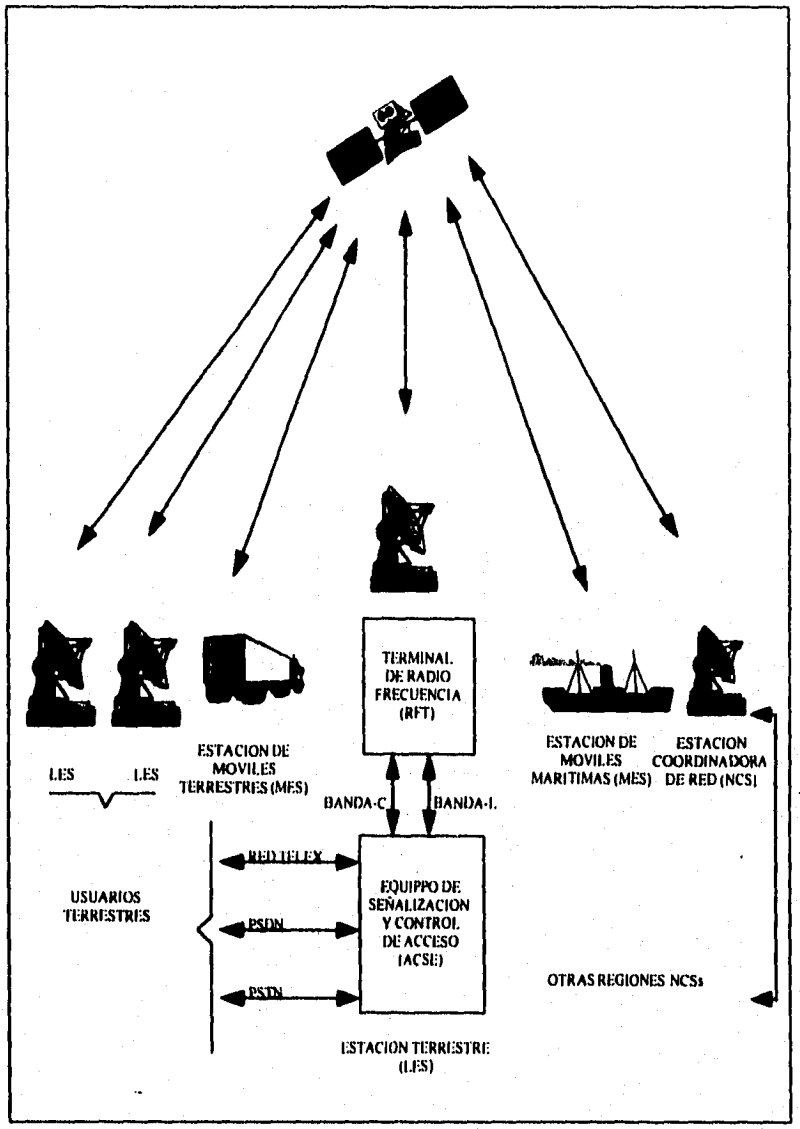

Figura 1.3 Estación terrestre (LES)

1.4 Servicios de Inmarsat-C

Los servicios que ofrece Inmarsat-C y que son soportados por una LES son:

- **Almacenar y transmitir los mensajes a y desde las terminales móviles**

  Este servicio permite aceptar mensajes de cualquier longitud, como por ejemplo mensajes de TELEX, los cuales serán almacenados y enviados posteriormente a su destino final.

  Las interfaces terrestres soportadas incluyen : Télex, Datos, Red Telefónica de Paquetes Conmutados (PSTN, Packet Switched Telephone Network), FAX y PSDN (X25). El FAX está disponible solamente en la dirección proveniente de una unidad móvil. Si por cualquier razón no se envía algún mensaje, se regresará un aviso de no enviado (NDN, No Delivery Notification) explicando la razón. Para los suscriptores inscritos al servicio, se puede solicitar un aviso de entrega positiva (PDN, Positive Delivery Notification).

- **Alerta de Emergencia de unidad móvil terrestre**

  Este servicio está únicamente disponible para los vehículos terrestres, de manera similar que la alerta de socorro, esto es, para casos de emergencia como lo puede ser un accidente en la unidad móvil (asalto, choque, etc.).

- **Llamada grupo amplificada (EGC)**

  En este servicio de EGC (Enhanced Group Call, por sus siglas en inglés) la información de interés a usuarios móviles, tales como el estado del tiempo, advertencias sobre riesgos de inundación, sismos, etc. se envía a los usuarios suscritos a este servicio mediante un canal especial de comunicación. Los mensajes pueden transmitirse a una flota de unidades móviles o a un grupo de unidades móviles dentro de una área geográfica definida.

Las unidades móviles deben estar equipadas con un receptor EGC para así poder tener el servicio. Las amplificaciones incluyen información del manejo de la flota de unidad móvil terrestre.

- **Reporte de Datos y llamadas selectivas (poleo)**

Los reportes de datos son mensajes cortos de hasta 32 bytes, los cuales se envían desde una unidad móvil sin el procedimiento normal de establecer llamada requerido para almacenar y transmitir mensajes, este tipo de mensajes por ejemplo nos indican la posición de una terminal móvil.

La llamada selectiva es un procedimiento que se emplea en la dirección hacia la unidad móvil para solicitar el envío de reportes de datos.La llamada selectiva puede enviarse a una unidad móvil individual o a todas las unidades móviles en un grupo o área geográfica en particular. Este servicio se encuentra únicamente disponible vía acceso Red de Paquetes de Datos Conmutados (PSDN, Packet Switched Data Network).

- **Pruebas de Verificación**

La LES proporciona una serie de pruebas diseñadas para checar cuál es el estado de operación de la terminal móvil.

- **Registros de llamadas**

La LES mantiene registros completos de todas las transmisiones de mensajes para poder a partir de estos generar los registros de facturación.

1.5 Configuración del sistema MOVISAT

El sistema MOVISAT (Comunicaciones Móviles Satelitales) surge como una solución a los problemas de comunicación que en nuestros días presentan las empresas en sus unidades de transportación (camiones, barcos, aviones, etc.). MOVISAT es un sistema de comunicaciones móviles vía satélite que cuenta con el respaldo de una tecnología probada a nivel internacional en la que se incluye la infraestructura terrestre y espacial, propiedad de TELECOMM (Telecomunicaciones de México).

Bajo la modalidad de almacenamiento y envío de mensajes, el servicio MOVISAT ayuda a establecer un puente de comunicación con las unidades móviles, a través de un centro de despacho que, debidamente equipado, permite conocer el estado en que se encuentra la flota (conjunto de unidades móviles), para precisar aspectos de especial interés para la empresa como la velocidad del vehículo, variación de temperatura de la carga, gasto de combustible, modificación de rutas, etc.

La cobertura del servicio MOVISAT permite comunicarse a lo largo y ancho de todo el territorio nacional, esto quiere decir que las unidades móviles pueden estar ubicadas desde la más aislada carretera, en el más inhóspito desierto o en la más alejada selva de nuestro país.

Los elementos principales del sistema MOVISAT de Telecomunicaciones de México son los siguientes:

- Segmento Espacial
- Segmento Terrestre
- Estación Terrena (LES-TELECOMM)
- Estaciones Móviles

1.5.1 Segmento espacial

Compuesto por el satélite Solidaridad 1, que incluye los transpondedores de banda Ku y L, con sus respectivos filtros y trasladadores de frecuencia de Ku a L y de L a Ku.

1.5.2 Segmento terrestre

Se debe considerar a los sistemas que provee el medio para entregar y recibir mensajes de usuarios terrestres. Cualquier medio que transmita datos a baja velocidad, se puede considerar adecuado. Por ejemplo el ACSE maneja los mensajes de usuarios registrados a la red TELEPAC.

1.5.3 Estacion terrena LES-TELECOMM

En el mes de abril de 1994 TELECOMM publicó una licitación internacional con el fin de adquirir una Estación Terrena, LES (Land Earth Station) compatible con el servicio de INMARSAT en su modalidad estándar C. La empresa Hughes Network Systems Ltd (HNS) obtuvo a su favor dicha licitación por considerarse entre otros aspectos su experiencia con redes de sistemas móviles tipo Inmarsat-C.

La LES-TELECOMM es un sistema que sirve como un medio de comunicación entre las redes terrestres mediante interfaces TELEX, redes de datos (PSDN) red telefónica (PSTN), etc. y las terminales móviles (MES), así como el enlace entre móvil y móvil dentro del área de cobertura del satélite. Es importante mencionar que la LES se encarga de enrutar los mensajes entre móviles y usuarios terrestres. Se constituye de dos unidades generales :

- Equipo de Radiofrecuencia (RF)
- Equipo de Señalización y Control de Acceso (ACSE)

1.5.3.1 Equipo de radio frecuencia (RF)

El equipo de radiofrecuencia (RF) opera en bandas Ku y L hacia el satélite. La sección de banda Ku opera con una antena de 7.2 m, incluye el equipo de potencia para proveer la amplificación redundante en ambas direcciones (TX/RX), así como los convertidores de frecuencia de subida y bajada.

Adicionalmente se presentan trasladadores de frecuencia de banda C a Ku y de banda Ku a C entre la etapa de potencia y los convertidores para la operación con el satélite Solidaridad 1 (los satélites de Inmarsat operan en banda C).

1.5.3.2 Equipo de Señalización y Control de Acceso (ACSE).

El Equipo de Señalización y Control de Acceso (ACSE), se puede considerar el corazón de la LES-TELECOMM, ya que posee todo el software y el hardware computacional con capacidad redundante para realizar sus funciones como administración de red, señalización, almacenamiento y envío de mensajes, categorización, etc.

El ACSE no resulta tan sencillo de seleccionarlo para su análisis, como es el caso del equipo de RF. Existen varias formas de representar sus elementos desde diversos puntos de vista: físico, lógico y de comunicación.

1.5.4 Estaciones móviles

Como unidad móvil nos referimos a cualquier medio que pertenezca a una flotilla de transportación como por ejemplo camiones, automóviles, barcos, aviones, etc. El equipo a bordo de la unidad móvil consta de un transreceptor, una antena para banda L (que generalmente se monta en el techo de la cabina) con un sistema de posicionamiento global (GPS, Global Position System) integrado y una terminal de datos con teclado para envío de mensajes.

La terminal es muy pequeña y con frecuencia se basará en una computadora personal pequeña. Existen diversas compañías que fabrican dichas terminales. Es importante mencionar que las terminales se deben dar de alta en la Base de Datos de la LES-TELECOMM.

1.6 Sistema de comunicaciones LES-TELECOMM

El sistema de comunicaciones LES-TELECOMM es compatible con el servicio de Inmarsat-C facilita la transferencia de datos a baja velocidad para el envío de mensajes, mensajes TELEX y alfanuméricos entre estaciones móviles de bajo costo.

El modo básico de operación del sistema Inmarsat-C aplicado a la LES-TELECOMM es mediante el almacenamiento y envío de mensajes (Store and Forward), lo cual significa que la comunicación se realiza en dos fases:

- **Fase 1**

Cuando se recibe la información desde una red terrestre o un móvil, se almacena en un archivo en el disco de la computadora principal del ACSE (Equipo de Señalización y Control de Acceso).

- **Fase 2**

Cuando se envía la información a su destino considerando que el circuito terrestre o el espacio en el satélite esta disponible, así como el destinatario.

1.7 Configuración física del ACSE

En la figura 1.4 se representa un esquema a bloques del ACSE, en el cual se incluyen los equipos duplicados para efectos de redundancia así como a los dos subsistemas que forman parte del equipo del ACSE:

- Sistema de Procesamiento y Control (SCP)
- Unidades de Canal (CU)

El SCP puede ser dividido en dos áreas funcionales (que no necesariamente coinciden con la localización física dentro de los racks del ACSE) excepto por el equipo conectado directamente al BAP (procesador VAX), como por ejemplo los discos, unidades de cintas y consolas de operación VMS, todos los componentes del SCP son conectados a una red Ethernet. El SCP comprende:

- **Procesador de Aplicación de Respaldo** (BAP, Background Aplication Processor) con medios de almacenamiento como unidades de cinta magnética y discos, este es el corazón del sistema. El BAP provee las funciones de almacenamiento y envío de mensajes, de mantener la base de datos del sistema y control para restablecer el ACSE en caso de fallas o servicios.

- **Interfaces Terrestres**, son proporcionadas por varios procesadores, conectados vía Ethernet ligados por el BAP, estos comprenden:

  - **Controlador de Interfaz Terrestre o TIC**. Este subsistema ubicado en el SCP proporciona el bajo nivel de proceso para cada interfaz terrestre por lo que el medio entre las interfaces terrestres (tales como telex y líneas para X.25) y el ACSE son interconectadas por este subsistema.

  - **DEMSA**, interface con una o más redes PSDN (para comunicaciones X.25) o con la Red Telefónica de Paquetes Conmutados (PSTN, Packet Switched Telephone Network, para comunicaciones asíncronas), vía un Ensamblador y Desensamblador (PAD, Packed Assembler/Deassembler).

- **PC de FAX**, interface con la red PSTN para el propósito de envío de FAX. El ACSE puede soportar un mínimo de cuatro máquinas de FAX.

- **Controladores de Unidades de Canal** (CUC, Channel Unit Controller), este subsistema que pertenece al SCP realiza el proceso de adecuación de la señal para la interfaz al satélite incluyendo la implementación de protocolos del lado del satélite. El ACSE tiene la capacidad para soportar cuatro pares de CUCs.

- **Consola del Operador del Sistema** (SOC, System Operator Console) que provee el control día a día de la configuración del sistema, tiene la capacidad de actualizar la amplia variedad de parámetros y permite la visibilidad del tráfico en el sistema. Así mismo puede desplegar los mensajes de desastre y alarmas, además de dar las facilidades de post-proceso para el análisis del sistema y preparación de las cintas (en cartucho) de facturación.

- **Impresoras** las cuales son usadas para la salida de eventos y reportes, en conjunción con las interfaces hombre-máquina que el SOC proporciona. Están conectadas a la red Ethernet vía un servidor de terminal (terminal server).

- **Consola de monitoreo VMS**, es la interface al sistema operativo de los procesadores centrales. Existe una terminal por cada BAP.

- **Racks de Unidades de Canal**, este genera y recibe datos para canales satelitales en uso.

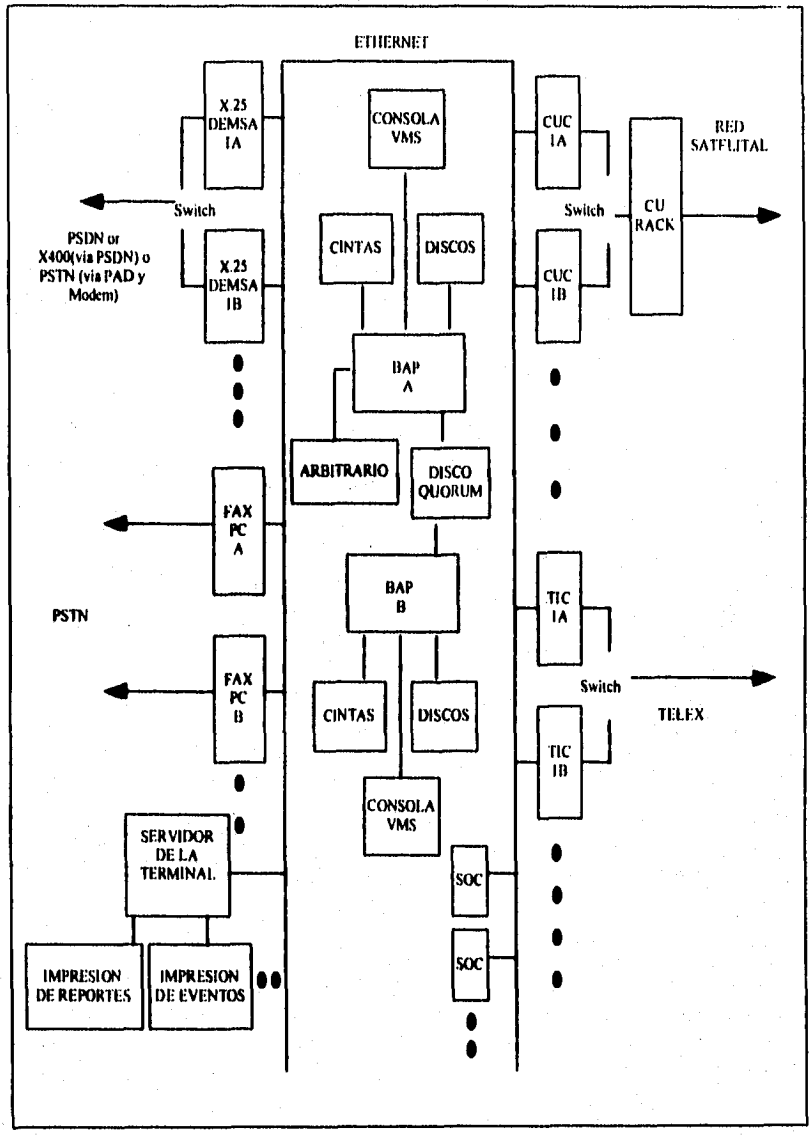

Figura 1.4 Configuración física del ACSE

1.8 Software del ACSE

El software que forma parte del Sistema de Procesamiento y Control (SCP), corre en los Procesadores de Aplicación y Respaldo (BAPs), en las unidades de TELEX y en las máquinas de FAX. El software está dividido en los siguientes subsistemas:

- **Sistema de Administración (SM, System Menager)**

  Es una colección de componentes los cuales proveen las funciones asociadas con la comunicación de procesos, control de redundancia y administración de recursos, arranque del sistema y control de los mensajes de error.

- **Sistema de Base de Datos (DB, System Database)**

  Es una colección de elementos de software que permiten la administración y el control de los datos adicionados dentro de la base de datos de la LES. La base de datos está soportada por el manejador relacional SYBASE.

- **Interface Hombre-Máquina (MMI, Man-Machine Interface)**

  Este subsistema da los medios con los cuales un operador monitorea y controla la LES. Una parte importante de este subsistema es la Consola del Operador del Sistema (SOC, System Operator Console) que corre independientemente en una estación de trabajo DIGITAL (VAX 4000-60) sobre el sistema operativo VMS. Además proporciona información sobre eventos sucedidos, controla la creación y uso de estadísticas, todo esto mediante una serie de opciones de menús.

- **Control de Mensajes (MH, Message Handler)**

  Este es el responsable para la validación de direcciones y enrutamiento de los mensajes entre los controladores terrestres y satelitales. Otra actividad importante es la canlendarización de la entrega de mensajes.

- **Controlador Terrestre (TD, Terrestrial Driver)**

  Esta compuesto por uno o más de los siguientes controladores, dependiendo de como este configurado el ACSE: controlador de X.25, TELEX y FAX.

  - El controlador de TELEX maneja la entrega de llamadas de TELEX desde la LES hasta la red terrestre de TELEX.
  - El controlador de FAX maneja la configuración del FAX, distribuye carga sobre los circuitos, mantiene el estado de las líneas e interactúa con el servidor de FAX.
  - El controlador X.25 trabaja con las llamadas X.25 desde la LES a la red PSDN.

- **Controlador Satelital (SD, Satellite Driver)**

  Provee la ruta de comunicación entre el satélite y las terminales móviles, asi como el procesamiento de una llamada.

- **Base de Datos fuera de línea (OFDB, Offline Database)**

  La base de datos fuera de línea esta relacionada con la generación de una base de datos que se produce con los archivos de registro (LOG FILES) para generar la cinta de facturación y los reportes del sistema MOVISAT.

En la figura 1.5 se representa la organización funcional del software ilustrando a los subsistemas y las relaciones entre estos.

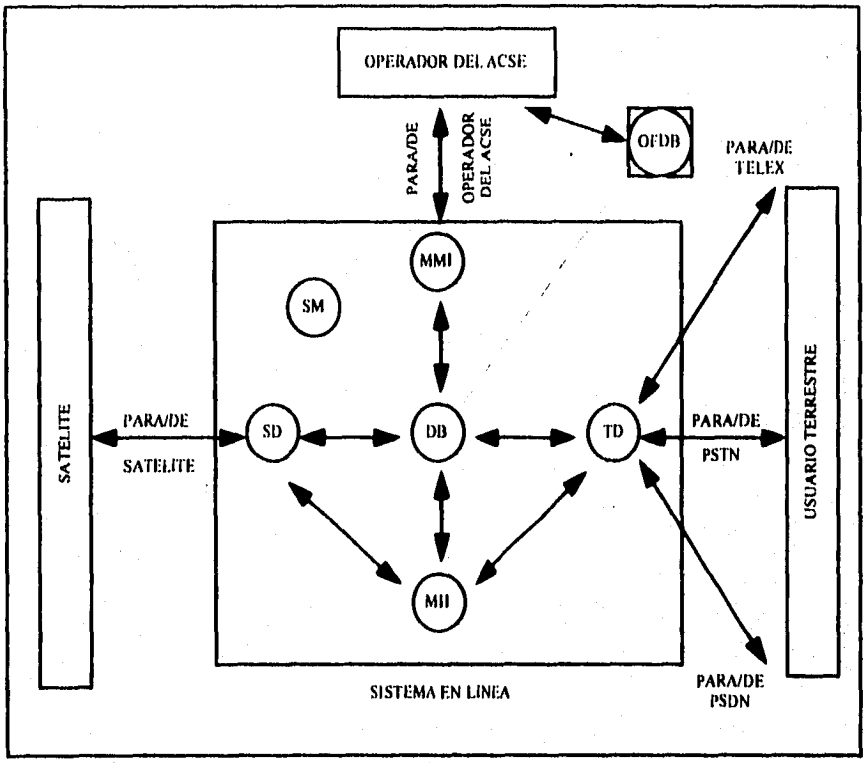

Figura 1.5 Software del ACSE

1.9 Tipos de datos generados por el ACSE

Existen dos principales categorías de datos pertenecientes al funcionamiento del ACSE (por sus siglas en inglés, Access Control and Signaling Equipment) y son las que a continuación se muestran :

- **Datos en Línea (ONLINE DATA)**

Consiste de una serie de tablas y valores de configuración que se tienen para la operación del ACSE, muy en particular son necesarios para administrar la red de móviles y usuarios terrestres junto con el equipo que forma al ACSE. Algunos datos en línea son aquellos que se generan debido a la actividad del sistema, en particular los detalles de mensajes.

Algunos de estos datos son dados de alta cuando el sistema es instalado por primera vez y/o después cuando el ACSE es operacional, por el operador, utilizando para ello el apropiado comando (MMI, Man Machine Interface). Otros campos son el resultado de la actividad del sistema (incluyendo al operador), en particular como resultado de los mensajes que pasan a través del sistema, o los cambios físicos hechos al estado del hardware.

Los datos en línea son controlados por el software comercial SYBASE RELATIONAL DATABASE MANAGER. Dicho software accesa a los datos por medio de rutinas SYBASE de manera íntegra y eficiente todo esto a través del software del ACSE.

- **Archivos de Registro (Log Files)**

Almacenan información perteneciente a varios tipos de datos pertenecientes a la actividad del sistema y son abiertos cada hora o bien en caso de que se rebasara el límite de tamaño del archivo, dichos tipos de datos son : registros de llamadas, eventos, "distress" (mensajes de desastre) y estadísticas.

- **Registros de llamadas**

Cada mensaje que entra y sale del ACSE genera un registro de llamada, con esto se tiene información relacionada con dicha llamada como puede ser el origen y destino de la llamada ; este tipo de registros se utilizarán posteriormente para generar cintas de facturación y reportes fuera de línea.

- **Eventos**

Son generados normalmente por ocurrencias irregulares en el funcionamiento y operación del ACSE. Ejemplo de este tipo de datos puede ser el apagado de alguna computadora o impresora del ACSE.

- **Estadísticas**

Sirven para tener referencias sobre: las llamadas efectuadas a través del Sistema, sucesos de falla, utilización de circuitos, etc.

Los Archivos de Registro están por debajo del control del Sistema Operativo VMS. Dichos archivos son la base para el Procesamiento fuera de Línea (OFFLINE PROCESSING) dentro del cual la Base de Datos fuera de línea (OFFLINE DATABASE) es formada.

La Base de Datos fuera de Línea es fundamental para la generación de los registros de facturación así como también de varios reportes relacionados con la actividad del sistema. Como su nombre lo dice, la creación y procesamiento de esta base de datos es fuera de línea, es decir, no se afectan recursos que actualmente se estén ocupando dentro del procesamiento de tráfico.

No es importante que el usuario tenga conocimiento de las estructuras de las base de datos. Realmente son necesarios algunos conocimientos de manejo de interfaces para la operación del ACSE, se cuenta con herramientas con las que podemos ver, modificar, agregar o eliminar elementos de la base de datos.

- **Identificadores**

Existen algunos campos que sirven a nivel de Base de Datos de llaves para el funcionamiento del ACSE, dichos campos son :

- **Número de Serie** . Es responsabilidad del fabricante e identifica a una terminal móvil (MES, Mobile Earth Station). El software del ACSE por cuestiones de seguridad no muestra este número.

- **FORWARD MES ID.** Número de 24 bits, está en el rango de 0 a 16777215 y es usado por la LES para seleccionar una MES en particular y entablar comunicación vía satélite.

- **RETURN MES ID.** Al igual que el anterior es un número de 24 bits, con el mismo rango y es utilizado por la MES para identificar comunicaciones con el satélite.

Cada uno de los números anteriores es único, hablando mundialmente, y sólo son mostrados por el ACSE.

- **Número de Móvil.** Es un número de 9 dígitos y sirve para identificar a la móvil, principalmente cuando comienza a ser direccionada a redes terrestres.

- **PIN (Personal Identification Number).** Sirve para identificar a los usuarios terrestres. Es una combinación de seis a ocho dígitos, con una combinación de números y/o letras.

- **Número de Referencia de Mensaje.** Los mensajes son identificados por este número de seis dígitos.

- **ENID.** Número de cinco dígitos para móviles que soportan llamadas a grupo (EGC).

- **DNID.** Es un archivo al cual se le asigna un número que sirve para identificar móviles con los servicios de poleo y reportes de datos, está formado por cinco dígitos.

CAPITULO 2

Configuración del Sistema de Trabajo

2.1 Procesamiento distribuido
- 2.1.1 Ventajas del procesamiento distribuido
- 2.1.2 Desventajas del procesamiento distribuido
- 2.1.3 Dimensiones del procesamiento distribuido

2.2 Redes de computadoras
- 2.2.1 Redes de área local
- 2.2.2 Redes de cobertura amplia

2.3 Protocolos de comunicación y el modelo OSI
- 2.3.1 Modelo OSI
- 2.3.2 Protocolo TCP/IP

2.4 Ambiente VAX y sistema operativo VMS
- 2.4.1 Tipos de sistemas operativos
  - 2.4.1.1 Sistemas operativos de lotes
  - 2.4.1.2 Sistemas operativos de multiprogramación
  - 2.4.1.3 Sistemas operativos de multiprocesamiento
  - 2.4.1.4 Sistemas de tiempo real
  - 2.4.1.5 Sistemas operativos distribuidos
  - 2.4.1.6 Sistema operativo VMS
- 2.4.2 Lenguaje de comandos digital (DCL)
- 2.4.3 Lenguaje intérprete de comandos (CLI)
- 2.4.4 Programas imágenes y utilerías
- 2.4.5 Procesos
- 2.4.6 División implícitas y explícita de tareas
- 2.4.7 Los procesos desde la visión del sistema operativo
- 2.4.8 Los procesos en VMS
- 2.4.9 Estado de los procesos en VMS

CAPITULO 2

Configuración del Sistema de Trabajo

La evolución de los sistemas de cómputo, ha cambiado radicalmente la manera de efectuar nuestro trabajo, incluso ha cambiado nuestra manera de pensar.

En los últimos años el trabajo en redes ha pasado a ser fundamental en la productividad de toda empresa, incrementando notablemente las actividades de cada departamento, presentándose como una integración cooperativa dentro de las funciones empresariales.

La parte más difícil de la comunicación de computadoras, se concentra en los diseñadores o administradores de redes. Estos diseñan arquitecturas de redes para que a los usuarios les sea más fácil implementarlas, además requieren capacidad para resolver cualquier tipo de problema en misión crítica, requerimientos de hardware, transferencia de datos entre estaciones de trabajo y servidores, topología de redes, sistemas operativos de redes (NOS), protocolos de comunicación, así como estar actualizados en lo último de la tecnología.

2.1 Procesamiento distribuido

Un sistema de cómputo distribuido es una colección de sistemas informáticos autónomos capaces de comunicarse a través de interconexiones de hardware y software.

Para llegar a una red distribuida exitosamente, se deben conjuntar elementos administrativos y de diseño con conceptos de distintas aplicaciones, no importando su localización física y el modo de acceso, es decir, una distribución de acceso lógico sin posibilidad de error o caída, una gran diversidad de protocolos de transmisión, así como el soporte a múltiples plataformas operativas.

La conjunción de estos tópicos, da como resultado el alojamiento y aplicaciones de negocio corriendo simultáneamente en diferentes máquinas y lugares de manera lógica.

2.1.1 Ventajas del procesamiento distribuido

El procesamiento distribuido ofrece características importantes como las siguientes :

- **Compartición de recursos**, la cual es una de las más importantes ventajas potenciales de los sistemas distribuidos, podemos citar ejemplos tales como la potencia de procesamiento, capacidad de almacenamiento, información procedente de bases de datos, etcétera, todas estas características pueden ser equilibradas para obtener ventajas del sistema distribuido.

- **Comunicación y compartición de información** son formas de compartición de recursos. La necesidad y el deseo de los usuarios de comunicar y compartir la información fue uno de los descubrimientos resultantes del uso de los sistemas compartidos, los sistemas distribuidos atienden generalmente a usuarios que pueden estar separados geográficamente y representar por tanto una oportunidad atractiva para la comunicación y compartición de información.

- **Crecimiento incremental** puede conseguirse en un sistema distribuido mejorando gradualmente los equipos conforme se modifiquen las necesidades de las aplicaciones y los requisitos de los usuarios. Además, la distribución permite actualizaciones selectivas haciendo posible añadir recursos cuando se tengan problemas de comunicación en el sistema. De igual modo pueden existir las modificaciones de software sin afectar a las aplicaciones existentes, como por ejemplo la adición de nuevas funciones, de actualizaciones de software, etc.

- **Fiabilidad**, esta característica proviene de la duplicación de los equipos y de la posibilidad de almacenar información en lugares diferentes, esto puede conseguirse de una manera gradual configurando la capacidad incremental en exceso o replicando los datos importantes.

- **La disponibilidad** puede ser mejorada previniendo múltiples copias de los recursos para que estas sean utilizadas en caso de sobrecarga o de que se presenten fallas.

Existen otras ventajas potenciales de los sistemas distribuidos como el rendimiento (cuando múltiples nodos cooperan en la resolución de un único problema), reducción de costos, su mayor capacidad en comparación con un único procesador, etc.

2.1.2 Desventejas del procesamiento distribuido

El procesamiento distribuido también tiene algunas desventajas entre las que podemos mencionar:

- Aumento de la dependencia con respecto al rendimiento y la fiabilidad de la red.

- Debilidad en esquemas de seguridad.

- Se requiere de un plan de administración y mantenimiento más completo para el sistema.

2.1.3 Dimensiones del procesamiento distribuido

La distribución se extiende básicamente en tres dimensiones:

- Hardware
- Control
- Datos (Software)

Los recursos del sistema caen generalmente dentro de dos categorías: recursos físicos, como por ejemplo los procesadores y los dispositivos (impresoras, discos, memorias, etc.), y los recursos lógicos, como los archivos y los procesos.

El control centralizado de la información se caracteriza por tener solo un nodo para organizar los recursos del sistema de cómputo. Para accesar a cualquier miembro del sistema se requiere que las peticiones sean enviadas al nodo de control para que este de la autorización.

Es interesante comparar a los sistemas distribuidos con los sistemas centralizados, en estos últimos la información es localizada en un solo punto, el cual es el centro de los datos. Esto a diferencia de un modelo distribuido, donde la información puede estar repartida en distintos servidores o centros de datos, y el procesamiento de la información se efectúa de acuerdo a cada petición en colaboración con los distintos servidores.

Los sistemas centralizados pueden soportar actualizaciones de hardware y el de software sólo hasta que se alcance el límite del equipo existente. El crecimiento posterior para acomodar crecientes necesidades de usuarios y aplicaciones es sólo posible por medio de llevar a cabo una sustitución de equipo y posiblemente también de software.

El distribuir correctamente los datos (información) optimizará el rendimiento y la disponibilidad debido a que se colocarían los elementos más frecuentemente utilizados cerca de sus puntos de procesamiento.

2.2 Redes de computadoras

Las máquinas autónomas que ejecutan programas de aplicación y constituyen el recurso computacional de un sistema distribuido se suelen denominar *hosts*. Están conectadas para comunicarse por medio de una red de comunicación o subred. Dependiendo de la distancia física que alcanzan las redes de comunicación, las redes de computadoras se clasifican generalmente como:

- Redes de Cobertura Amplia (WAN, Wide Area Network)
- Redes de Area Local (LAN, Local Area Network)

No se tiene una distancia específica para distinguir unas de otras, es razonable que una red de área local abarca espacios pequeños como por ejemplo un edificio. Las redes de cobertura amplia, por otro lado, pueden conectar *hosts* que están separados por varios kilómetros, incluso incluyendo distancias internacionales. Por razones de tecnología las WAN tienden a tener anchos de banda comparativamente bajos y retardos de comunicación elevados. Las LAN suelen estar caracterizadas por sus elevados anchos de banda y bajos retardos de comunicación.

2.2.1 Redes de área local

Las redes de área local (LAN), es un grupo de computadoras conectadas entre sí por cable, fibra óptica o en algunas ocasiones por radio frecuencia, se caracterizan por enlaces de comunicación con elevado ancho de banda y bajo retardo. Una LAN típica, consiste en una computadora denominada servidor, que alberga el sistema operativo de red (NOS), información contenida en bases de datos, así como aplicaciones de software, independientemente de las conexiones necesarias para soportar a los clientes o estaciones de trabajo.

Las velocidades de comunicación en redes de área local pueden ser desde el orden de varios Mbps (megabits por segundo) hasta el orden de Gbps (gigabytes por segundo) con cableado especial o con fibras ópticas. Estas velocidades se aproximan a las velocidades de transferencia de otros periféricos de alta velocidad, como los discos. Debido al acceso potencialmente rápido a los recursos en cualquier punto de la red, las LAN presentan la tarea de ubicar tanto a los periféricos como a los servicios dentro del sistema.

En las LAN, las funciones de comunicación y procesamiento las proporcionan los nodos (las máquinas *host*), directamente o mediante coprocesadores de comunicación dedicados. La topología de red es generalmente un ducto (bus) o un anillo.

En los sistemas basados en anillo, los mensajes circulan alrededor del anillo, los mensajes así son conocidos y copiados por sus destinatarios. La topología en anillo parece ser muy vulnerable a disfunciones de nodos y enlaces, ya que cualquier falla por muy simple que sea rompe con el anillo y por lo tanto paraliza el tráfico. Hablando comercialmente se evita este problema utilizando relés para conectar los nodos del anillo. El relé está diseñado para permitir que el tráfico fluya a través del nodo asociado. Si existieran fallas, el relé se cierra y forma un puente, evitando así el nodo fallido, así habrá continuidad en el anillo.

La topología de ducto (bus) o ETHERNET es muy común en las redes de área local, esta arquitectura, se podría decir que es la más utilizada en el mundo de las redes de cómputo actualmente, además presenta el mejor balance entre velocidad y precio. En una topología de ducto típica, un conductor pasivo transporta el tráfico de mensajes. Todos los nodos tienen una toma de conexión al ducto, escuchan todo el tráfico y extraen los mensajes que les son dirigidos.

Las LAN orientadas a ducto son confiables y capaces de sostener comunicación entre nodos sanos en presencia de múltiples fallas en nodos, ejemplo de este tipo de red se presenta en la figura 2.1, en ella se tienen cuatro *hosts* comunicándose a través de un solo ducto.

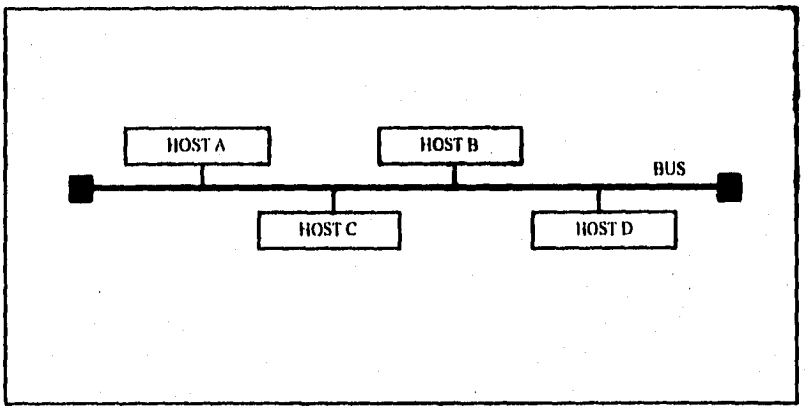

Figura 2.1 LAN orientada a ducto (BUS)

2.2.2 Redes de cobertura amplia

Las redes de cobertura amplia actúan o funcionan de la misma manera que las redes LAN, la diferencia se basa en que este tipo de redes se comunican vía telefónica o vía conmutada mediante un cable dedicado que corre grandes distancias geográficas para conectar dos o más puntos.

En la figura 2.2 se muestra una arquitectura de una red de cobertura amplia, en ella podemos observar que la subred de comunicaciones consta de una serie de procesadores de comunicación conectados mediante líneas de comunicación físicas. Los procesadores de comunicación dedicados actúan como elementos de conmutación entre dos o más líneas de comunicación, las cuales también son llamadas líneas de transmisión, circuitos o canales.

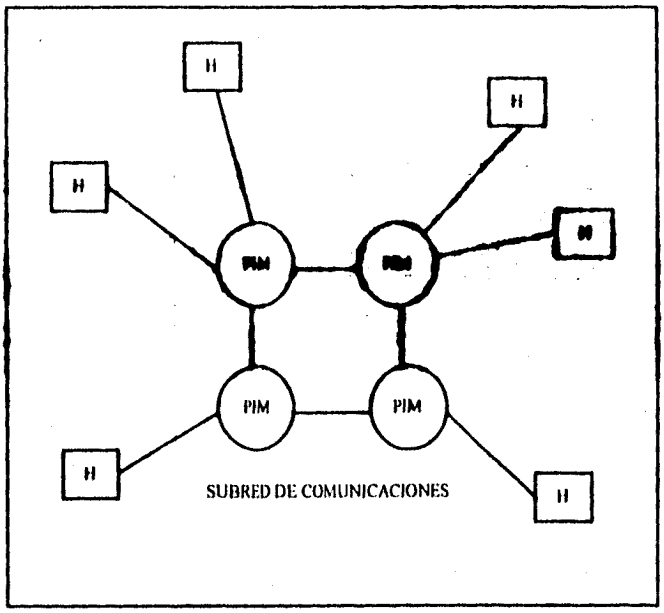

Figura 2.2 Red de Cobertura Amplia (WAN)

Un procesador *host* que desee comunicarse con otro *host* presenta típicamente su petición de comunicación al procesador de interfaz de mensajes (PIM, nombre que recibe el procesador de comunicación). Generalmente cada *host* aprovecha los servicios de un PIM específico, aunque un mismo PIM puede atender a varios *host*. Los canales de PIM a PIM pueden ser de una estructura llamada enlace de punto a punto.

Los enlaces punto a punto son líneas físicas dedicadas, utilizadas para conectar un par específico de PIM. A continuación se explican las topologías de redes de los circuitos físicos que conectan directamente a un PIM. Estas topologías son:

- **Topología de estrella**

La configuración en estrella encamina a todas las comunicaciones a través de un único punto central, que puede ser un nodo o un conmutador. La estrella tiene un retardo fijo de comunicación entre *hosts*, pero el gran inconveniente que tiene es que cuenta con un punto de fallo único. La figura 2.3 ilustra un diagrama típico de una red estrella.

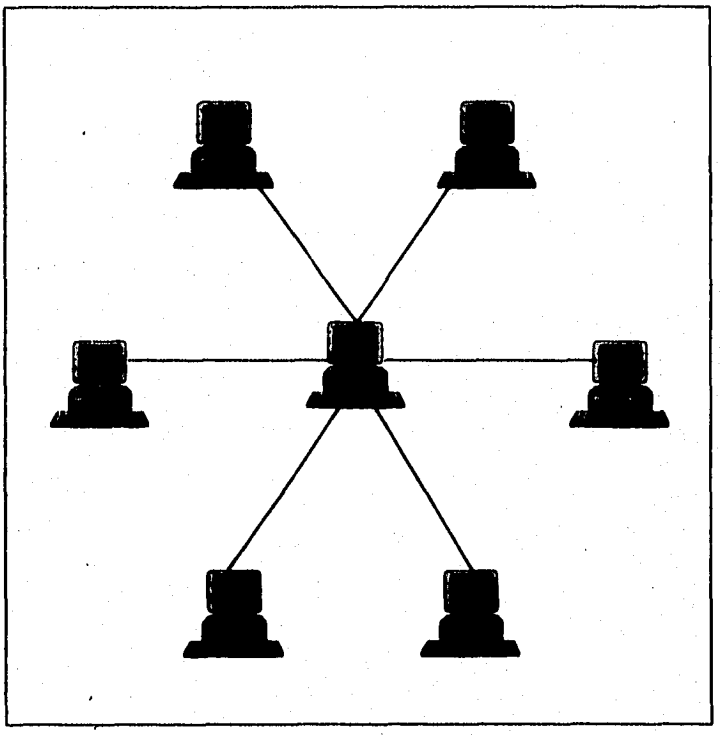

Figura 2.3 Topología de Estrella

- **Redes totalmente conexas**

Los sistemas totalmente conexos son rápidos y fiables pero costosos ya que el número de enlaces crece como el cuadrado del número de *hosts*, los cuales están conectados entre sí. En la figura 2.4 se tiene una red de este tipo.

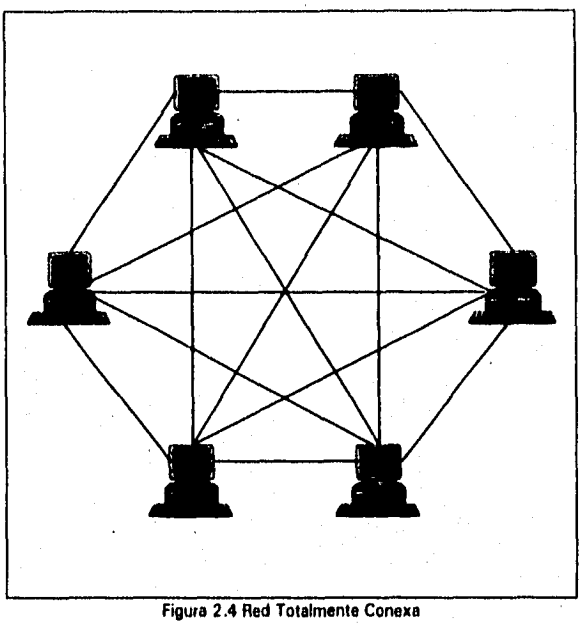

Figura 2.4 Red Totalmente Conexa

- **Redes parcialmente conexas**

Las redes parcialmente conexas y en malla tienen enlaces directos entre algunos de los nodos pero no de todos. Si las conexiones físicas se reducen, con los costos pasará lo mismo.

El inconveniente que tienen este tipo de redes es que se requiere de un encaminamiento de mensajes intercambiados entre *hosts* que no están directamente conectados aumentando así el peligro de particionamiento de la red, en donde si se presentara una falla en cualquier enlace se rompería la subred de comunicación de dos o más subconjuntos disjuntos incapaces de comunicarse entre sí. En la figura 2.5 se muestra el esquema de los sistemas parcialmente conexos.

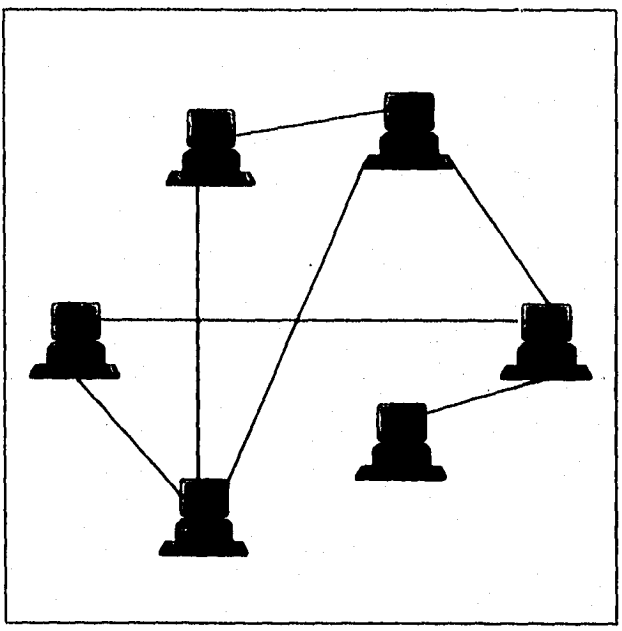

Figura 2.5 Red Parcialmente Conexa

- **Topología de anillo**

Las redes anillo de un solo enlace tienen un costo bajo, pero retardos variables y potencialmente largos, especialmente cuando un *host* desea comunicarse con su vecino inmediato en dirección opuesta a la del flujo del anillo. Los anillos generalmente son sensibles a fallas de enlace. En la figura 2.6 se tiene un ejemplo de la configuración de red en anillo.

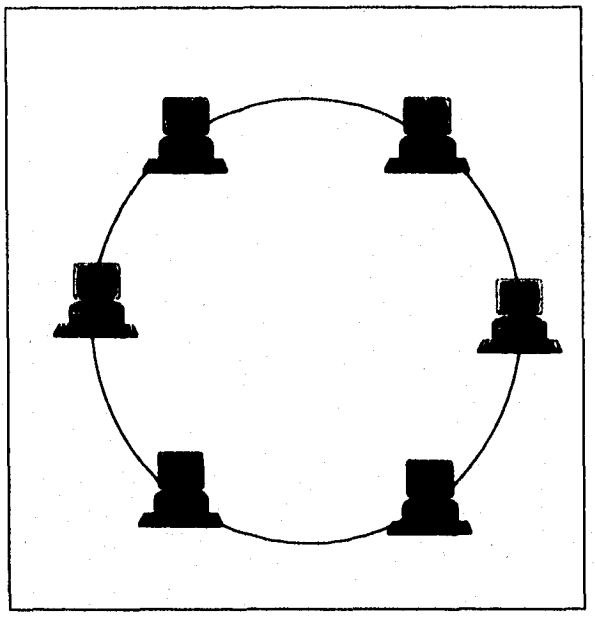

Figura 2.6 Configuración de Anillo

- **Topología jerárquica**

Las conexiones jerárquicas pueden ser adecuadas para ciertos tipos de organizaciones y sistemas, tales como el control de procesos, en donde la comunicación fluye de manera natural de una manera jerárquica (ordenada). Esta configuración de red (figura 2.7) es pobre en sistemas con frecuentes interacciones entre nodos de un mismo nivel, ya que deben ser encaminadas arriba y abajo de la jerarquía.

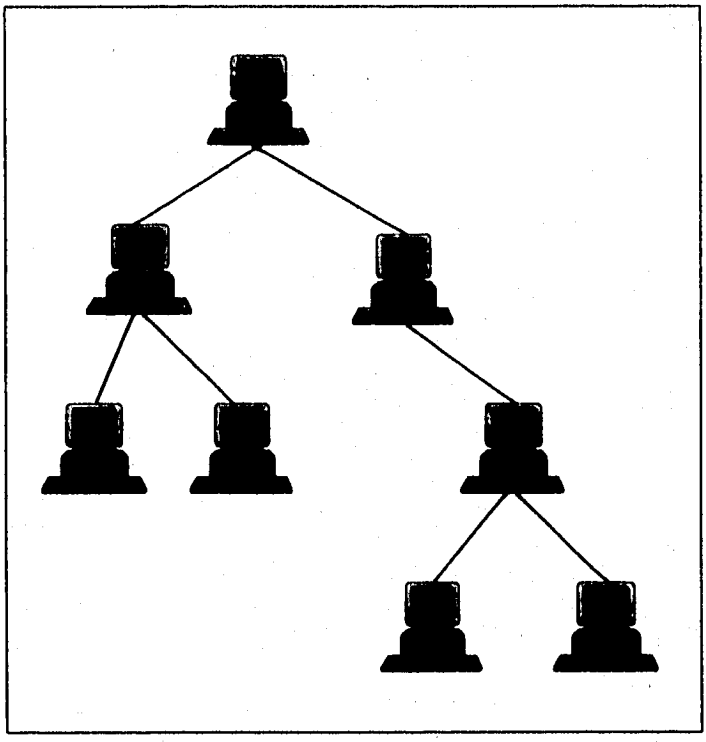

Figura 2.7 Topología de una red Jerárquica

En un sistema con un número fijo de *hosts*, el incremento en el número de circuitos físicos de comunicación produce un aumento en la disponibilidad y en la velocidad, y una disminución en los retardos. Pero también se tiene un aumento en el costo del sistema.

Un aspecto muy importante del diseño de la subred de comunicación es la estrategia de conexión , la cuestión en este punto es durante cuánto tiempo deberá estar dedicado un enlace de comunicación a un par determinado de emisor-receptor. Las estrategias más comunes son:

- Conmutación de circuitos
- Conmutación de mensajes
- Conmutación de paquetes

Conmutación de circuitos

La conmutación de circuitos se asemeja a un sistema telefónico. Funciona estableciendo y manteniendo un circuito físico dedicado de extremo a extremo entre los *hosts* de comunicación durante la sesión de comunicación entera.

Conmutación de mensajes

En la conmutación de mensajes se establece un enlace físico temporal entre el emisor y el receptor durante la transferencia de un solo mensaje. Los enlaces físicos son asignados a los usuarios durante breves períodos de tiempo y se conmutan rápidamente con objeto de incrementar la utilización de la línea de comunicación.

Las ventajas de la conmutación de mensajes son : incremento de la eficiencia del canal de comunicación, reducción de la congestión al almacenar temporalmente los mensajes y el envío de un mensaje a varios destinos.

La conmutación de mensajes presenta las siguientes desventanjas : se requieren dispositivos de almacenamiento-reedexpedición con gran capacidad de memoria y no es compatible con sistemas de tiempo real.

Conmutación de paquetes

La conmutación de paquetes intenta incrementar aún más la utilización de las líneas de comunicación (enrutamiento de mensajes en caso de congestión de canal de comunicación), la productividad del sistema y algunos aspectos de la gestión de memoria de los procesadores de interfaz de paquetes dividiendo los mensajes largos en trozos de un tamaño fijo denominados paquetes. Teniendo los paquetes estos son enviados a través de rutas diferentes y son reunidos en el destino para su entrega al receptor.

La posibilidad de que los paquetes de información se pierdan y el punto de que los protocolos para la conmutación de paquetes sean relativamente más complejos son las desventajas que este tipo de conmutación tiene.

2.3 Protocolos de comunicación y el modelo OSI

Los protocolos de redes son estándares que entablan comunicación entre computadoras, estos, identifican a una computadora de otra dentro de una red, por ejemplo los bloques de información que transitan dentro de la red, así como el proceso que se debe de dar a la información cuando llega a su destino final. Algunos ejemplos de protocolos son : TCP/IP (Transmission Control Protocol/Internet Protocol, desarrollado por el Departamento de la Defensa de los Estados Unidos para la comunicación de computadoras), DECnet (protocolo de comunicaciones de Digital Equipment Corporation), AppleTalk (protocolo utilizado en plataforma MACINTOSH), X.25, entre otros.

El método tradicional de conmutación de paquetes se origina a mediados de los años 60´s y se basa en el estándar X.25 aprobado por la CCITT (International Telegraph and Telephone Consultative Committee). Su enfoque inicial fue principalmente en la detección y corrección de errores en cada nodo de la red pública.

Los protocolos internet son medios para conectar redes bajo el sistema operativo UNIX, Internet es una colección de redes de paquetes conmutados interconectadas por GATEWAYS (dispositivos o unidades de software que habilitan a redes de diferentes proveedores a comunicarse entre sí), con protocolos que presentan al usuario como si se tratase de una sola red. Fundamentalmente los protocolos utilizados en este tipo de redes con el TCP y el IP (TCP/IP) los cuales interactúan en la capa transporte y red del modelo de OSI respectivamente.

2.3.1 Modelo OSI

El software de comunicación entre computadoras de conexión por red es generalmente muy complejo. Para que sea manejable, el software de conexión se diseña e implementa generalmente por capas. Cada capa proporciona a las capas superiores un conjunto de servicios que pueden ser invocados a través de un interfaz bien definido.

La Organización de Normas Internacionales (ISO, International Standards Organization) creó el modelo de referencia de Interconexión de Sistemas Abiertos u OSI (Open Systems Interconnection).

La meta de OSI, es habilitar computadoras de múltiples vendedores para compartir información más fácilmente en un ambiente de "sistemas abiertos". OSI es un conjunto de reglas organizadas en capas describiendo los formatos y protocolos para la interconexión de sistemas de cómputo.

Este modelo considera siete capas que cubren todos los aspectos de flujo de información requeridas para la comunicación entre un sistema final y otro sistema final, desde la comunicación de dispositivos al medio físico hasta servicios relacionados con las aplicaciones de los usuarios. A continuación se da una breve descripción de cada una de ellas y en la figura 2.8 se tiene un esquema a bloques de este modelo.

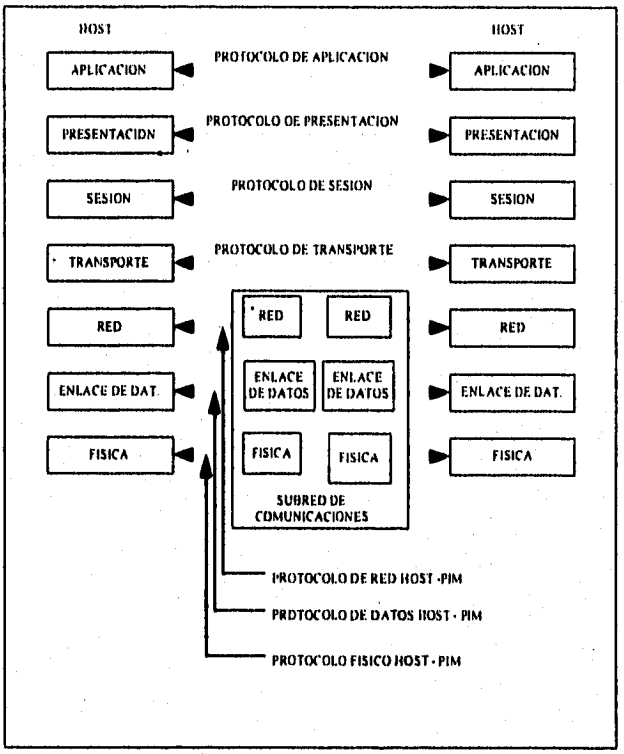

Figura 2.8 Arquitectura de Protocolos ISO

Capa física

Está encargada de transmitir flujos de bits a través del canal de comunicaciones. Se ocupa principalmente de los circuitos de comunicación y de sus interfaces físicas y de procedimiento con el medio de transmisión físico subyacente.

Capa de enlace de datos

La capa de enlace de datos toma la facilidad de transmisión de flujo de bits en bruto y la mejora para proporcionar aparentes líneas de comunicación libres de errores entre computadoras que están conectadas directamente. La capa de enlace de datos está encargada de resolver los problemas relativos a los mensajes dañados, perdidos y duplicados. También está encargada del control de flujo, un mecanismo diseñado para evitar el desbordamiento de los nodos que pueden resultar de, entre otras cosas, las discrepancias de velocidad entre emisores y receptores.

Capa de red

Sus funciones principales son el encaminamiento de paquetes, el mantenimiento y congestión. Las consideraciones y problemas entre redes resultantes de la reunión de redes heterogéneas están también confiadas a la capa de red. Estas pueden incluir conversiones entre diferentes esquemas de direccionamiento y diferentes tamaños de paquetes.

Capa de transporte

La tarea de la capa de transporte es proporcionar como su nombre lo dice transporte de mensajes independientes de la red entre pares de extremos de la red, o puertos.

La capa de transporte es la primera que proporciona una conexión verdadera entre fuente y destino. En las capas inferiores, la comunicación se efectúa entre una máquina y sus vecinos inmediatos, y no necesariamente entre los *host* fuente y destino.

La capa de transporte acepta datos procedentes de la capa de sesión, los divide en unidades más pequeñas tales como paquetes si es necesario y asegura que todas las piezas sean reunidas adecuadamente en el extremo receptor. El transporte efectivo de los trozos de información lo efectúa la capa de red. La capa de transporte soporta dos modos de comunicación :

- **Circuito virtual**

  Un circuito virtual se asemeja a un sistema telefónico. Es un canal de comunicación lógica establecido entre dos *hosts* con objeto de mantener una conversación. Un circuito virtual entrega fiablemente mensajes en el orden en que son enviados. El modo de comunicación que utiliza circuitos virtuales se denomina servicio orientado a conexión ya que requiere que las entidades interesadas establezcan implícitamente un enlace de comunicación con objeto de intercambiar los mensajes.

- **Datagrama**

  Un datagrama se considera un mecanismo no fiable de entrega de mensajes, ya que no reconoce la recepción de los mensajes. En el servicio de datagrama los mensajes individuales son enviados individualmente y sin acuerdo previo, debido a esto los mensajes enviados como datagramas pueden ser perdidos o recibidos fuera de orden. El servicio de datagrama tiene menos retardo que el circuito virtual y generalmente es más rápido ya que no requiere la preparación del enlace. Los datagramas son populares en redes de área local, cuya fiabilidad puede ser lo suficientemente buena para reducir las preocupaciones con respecto a la pérdida de mensajes.

Capa de sesión

La capa de sesión permite que los procesos residentes en *hosts* diferentes se comuniquen entre sí. Esta capa establece sesiones entre procesos que determinan transporte ordinario de datos y algunos servicios adicionales tales como aperturas de sesiones remotas y transferencia de archivos.

La capa de sesión también está encargada de proporcionar sincronización y gestión de testigos para soportar interacciones entre procesos a través de los circuitos virtuales que establece.

Capa de presentación

La capa de presentación efectúa algunas funciones habituales que pueden requerir conocimiento de la sintaxis y de la semántica de la información transmitida. Un ejemplo, es la codificación de los datos en algún formato estándar, independiente de la máquina. Esta codificación permite conversiones de formatos de datos, tales como ordenación de octetos (bytes) y presentación de coma flotante, para permitir la comunicación entre máquinas heterogéneas.

Además esta capa proporciona, opcionalmente el cifrado y compresión de datos. La codificación necesaria es efectuada por la capa de presentación del extremo receptor.

Capa de aplicación

La capa de aplicación proporciona una variedad de protocolos habitualmente requeridos por los procesos de aplicación que corren en computadoras separadas a cuenta de las tareas del usuario. Los protocolos pueden incluir correo electrónico, admisión de trabajos remotos y transferencia de archivos que ocultan las posibles diferencias de denominación y presentación entre los usuarios de los extremos.

La capa de presentación también ofrece una abstracción de terminal denominada terminal virtual de red. Esto permite a los proveedores de aplicaciones escribir código, por ejemplo un editor de pantalla, para un único tipo de terminal (la terminal virtual) y confiar en la capa de aplicación para traducir las órdenes relevantes por secuencias de control apropiadas para el tipo o tipos de terminales específicos.

2.3.2 Protocolo TCP/IP

El protocolo Internet (IP) está sobre la capa de red (capa 3 del modelo OSI) y fue desarrollado por el Departamento de la Defensa de los Estados Unidos, está diseñado para la interconexión de redes de paquetes. Para nombrar a una computadora dentro de una red se le asigna una dirección llamada IP, la cual es usada en todas las comunicaciones que pueda tener la máquina y es única dentro de la red.

El protocolo IP trabaja con el protocolo TCP (Transmission Control Protocol), el cual está en la capa 4 del modelo OSI. TCP provee una comunicación punto a punto y tiene tres características muy importantes : establece la conexión, transfiere y mantiene datos en el proceso de comunicación y termina con la conexión.

2.4 Ambiente VAX y sistema operativo VMS

El hardware y el software siempre han estado en una delicada simbiosis: uno carece de sentido sin la existencia del otro y sólo si ambos trabajan en perfecta coordinación, es posible un rendimiento óptimo.

Dentro del software el sistema operativo es el programa más importante de una computadora. Es el encargado de controlar los programas y administrar todos y cada uno de los recursos de hardware disponibles. Sus capacidades y alcances definen (y a veces limitan) todo lo que se puede realizar en una computadora.

Otros programas se apoyan en las facilidades proporcionadas por el sistema operativo para obtener acceso a los recursos del sistema informático, tales como archivos y dispositivos de entrada/salida (E/S). Los programas invocan generalmente los servicios del sistema operativo por medio de llamadas al sistema operativo. Además, los usuarios pueden interactuar con el sistema operativo directamente por medio de órdenes del sistema operativo. En cualquier caso, el sistema operativo actúa como interfaz entre los usuarios y el hardware de un sistema informático.

El rango y la extensión de los servicios proporcionados por un sistema operativo dependen de varios factores. Entre otras cosas, las funciones visibles al usuario de un sistema operativo están en gran medida determinadas por las necesidades y características del entorno objetivo que el sistema operativo está destinado a soportar.

Internamente un sistema operativo actúa como gestor de los recursos del sistema informático, tales como el procesador, la memoria, los archivos y los dispositivos de E/S. En esta función, el sistema operativo lleva la cuenta del estado de cada recurso y decide quién obtiene un recurso, durante cuánto tiempo y cuándo. En sistemas que soportan ejecución concurrente de programas, el sistema operativo resuelve las peticiones conflictivas de recursos de manera que preserva la integridad del sistema y al hacerlo intenta optimizar el rendimiento final.

En general, el objetivo primario de los sistemas operativos es incrementar la productividad de un recurso de proceso tal como el hardware de la computadora, o los usuarios del sistema informático.

2.4.1 Tipos de sistemas operativos

Los sistemas operativos han sido clasificados de la manera que a continuación presentamos :

2.4.1.1 Sistemas operativos de lotes

El procesamiento por lotes precisa generalmente que el programa, los datos y las órdenes adecuadas al sistema sean remitidos todos juntos en forma de trabajo. Los sistemas operativos por lotes permiten poca o ninguna interacción entre los usuarios y los programas en ejecución. El procesamiento por lotes tiene un mayor potencial de utilización de recursos que el procesamiento serie simple en sistemas informáticos que dan servicio a múltiples usuarios. Debido a los retardos en los tiempos de retorno y a la depuración fuera de línea, el procesamiento por lotes no es muy conveniente para desarrollo de programas.

Los programas que no requieren interacción y los programas que tienen largos tiempos de ejecución pueden estar bien servidos por un sistema operativo de lotes.

La planificación en sistemas de lotes es muy sencilla. Los trabajos son típicamente procesados en orden de llegada, es decir, el modo primero en llegar, primero en ejecutarse.

La gestión de memoria en sistemas de lotes es también muy sencilla. La memoria se suele dividir en dos áreas. Una de ellas está permanentemente ocupada por la parte residente del sistema operativo y la otra es utilizada para cargar programas transitorios durante su ejecución. Cuando un programa transitorio termina se carga un nuevo programa en la misma área de memoria.

Los sistemas por lotes suelen proporcionar formas sencillas de gestión de archivos. Puesto que el acceso a los archivos es también seria, se requiere poca protección y ningún control de concurrencia para tal acceso.

2.4.1.2 Sistemas operativos de multiprogramación

A una instancia en ejecución se le denomina tarea o proceso. Un sistema operativo multitarea se distingue por su capacidad para soportar la ejecución concurrente de dos o más procesos activos.

El término programación designa a un sistema operativo que, además de soportar multitarea, proporciona formas sofisticadas de protección de memoria y forza el control de la concurrencia cuando los procesos acceden a dispositivos de E/S y archivos compartidos.

Los sistema operativo de multiprogramación soportan múltiples usuarios, en cuyo caso también se les denomina sistemas multiusuarios, los cuales proporcionan facilidades para mantenimiento de usuarios individuales, requieren revalidación de usuario para seguridad de protección y proporcionan contabilidad de uso de los recursos por cada usuario.

2.4.1.3 Sistemas operativos de multiprocesamiento

Los sistema operativo de Multiprocesamiento gestionan la operación de sistemas informáticos que incorporan varios procesadores. Los sistemas multitarea por definición soportan la ejecución simultánea de múltiples tareas sobre diferentes procesadores.

2.4.1.4 Sistemas de tiempo real

Los sistema operativo de tiempo real se utilizan en entornos en donde deben de ser aceptados y procesados un gran número de sucesos, la mayoría externos al sistema informático. Tales aplicaciones incluyen control industrial, control de comunicaciones, control de vuelo y simulaciones de tiempo real.

2.4.1.5 Sistemas operativos distribuidos

Un sistema operativo distribuido es una colección de sistemas informático autónomos capases de comunicación y cooperación mediante interconexiones de hardware y software. Un sistema operativo distribuido gobierna la operación de un sistema informático distribuido y proporciona una abstracción de máquina virtual a sus usuarios, esto es, proporciona transparencia.

Los sistema operativo distribuidos proporcionan generalmente medios para la compartición global de los recursos del sistema, tales como la capacidad computacional, los archivos y los dispositivos de E/S.

2.4.1.6 Sistema operativo VMS

Las computadoras VAX operan bajo el control del Sistema Operativo VMS (Virtual Memory System). El sistema operativo VMS controla los recursos de las computadoras VAX así como programa los accesos a dichos recursos. VMS es un sistema operativo interactivo. El sistema operativo VMS maximiza las funciones siguientes :

- Provee la comunicación entre los usuarios del sistema y los dispositivos.
- Crea y protege el ambiente de trabajo para cada usuario.
- Planifica el uso de los recursos del sistema, para que los usuarios los utilicen de manera más óptima.

2.4.2 Lenguaje de comandos digital (DCL)

Para tener comunicación con la VAX, el sistema operativo VMS ofrece un Lenguaje de Comandos (DCL, Digital Command Language) para tener dicha interactividad. Se tienen arriba de 200 comandos y funciones, los cuales son palabras escritas en inglés. Se puede utilizar el DCL de los dos modos siguientes :

- Interactivo, el usuario da el comando en la terminal y para la ejecución de otro, el primero tiene que terminar.

- BATCH, en este modo el sistema crea un proceso para ejecutar una serie de comandos. Cuando se está ejecutando el usuario tiene la posibilidad de seguir interactuando con el sistema.

Los tres tipos de comandos DCL caen en cualquiera de las siguientes divisiones:

- **Comandos construidos.** Son los comandos que están construidos dentro del intérprete de DCL y son ejecutados internamente.

- **Comandos de invocación.** Son comandos que invocan la ejecución de un programa.

- **Comandos Externos.** Un símbolo que ejecuta una imagen (programa invocado para ejecutarse).

2.4.3 Lenguaje intérprete de comandos (CLI)

Las principales características del lenguaje intérprete de Comandos (CLI) de VMS son:

- Traslada los comandos (palabras en inglés) a lenguaje que pueda entender el CPU.

- Despacha los comandos trasladados para su ejecución.

2.4.4 Programas, imágenes y utilerías

Un programa es un archivo que contiene una serie de instrucciones escritas para realizar alguna tarea. Se tienen programas que son llamados imágenes o no imágenes.

Una imagen es un programa ejecutable cuya extensión es EXE, tiene instrucciones con direccionamiento de información y es el resultado de la compilación del programa fuente (lenguaje entendible por el ser humano). Está asociado con un comando DCL. Un programa de no-imagen no está relacionado con un comando DCL y para invocarlo es necesario utilizar este programa como un parámetro del comando RUN.

Las utilerías son programas que provee VMS para ofrecer un servicio. Son invocadas por un comando DCL. Se puede trabajar de manera interactiva con estas herramientas y casi siempre tienen su propio DCL, un ejemplo de utilería lo es el correo electrónico (MAIL).

También se tienen utilerías no interactivas las cuales realizan una tarea específica y después retornan al ambiente de trabajo.

2.4.5 Procesos

La multiprogramación es esencialmente la multiplexación de los recursos del sistema, tales como el procesador, la memoria y los dispositivos de E/S entre una serie de programas activos.

Un proceso o tarea es una instancia de un programa en ejecución. Es la unidad más pequeña de trabajo individualmente planificable por un sistema operativo. Un sistema operativo de multiprogramación se encarga de seguir la pista a todos los procesos activos y les asigna recursos del sistema de acuerdo a las políticas ideadas para satisfacer objetivos de rendimiento.

Un sistema operativo en la definición de Denning incluye lo siguiente:

- La creación y eliminación (destrucción) de procesos.
- El control del avance de los procesos, es decir, el garantizar que cada proceso lógicamente activo progresa hasta su terminación.
- La actuación sobre condiciones excepcionales que aparecen durante la ejecución de un proceso, incluidas interrupciones y errores aritméticos.
- La asignación de los recursos de hardware entre los procesos.
- La provisión de medios para la comunicación de mensajes o señales entre los procesos.

2.4.6 División implícita y explícita en tareas

Dependiendo del sistema operativo la división del trabajo en tareas que serán ejecutadas como procesos independientes y la asignación inicial de los atributos de los procesos puede ser efectuada o bien por el sistema operativo o por el programador de sistemas. Lo que constituirá un proceso separado en tiempo puede provenir de:

- Una división implícita en tareas (definida por el sistema), se aplica en sistema operativo multitarea para multiplexar la ejecución de una serie de programas.
- Entre las razones comunes para aplicar la división explícita (definida por el programador) se incluyen: ganancia de velocidad, el uso de dispositivos de E/S que tienen latencia (mientras una tarea espera que acabe la E/S, otra parte de la aplicación puede progresar si contiene otras tareas que pueden hacer trabajo útil mientras tanto), conveniencia del usuario, multiprocesarniento y computación distribuida.

2.4.7 Los procesos desde la visión del sistema operativo

Desde el punto de vista del sistema operativo un proceso es la entidad más pequeña planificable, formada por código y datos, y caracterizada por atributos y un estado dinámico. El código se compone de las instrucciones máquina y de las llamadas de servicio al sistema (llamadas al sistema operativo). Los atributos asociados con un proceso son asignados por el programador del sistema o por el mismo sistema operativo., incluye aspectos tales como la prioridad de software y los derechos de acceso. El sistema operativo contempla la ejecución de un proceso típico en el curso de su actividad en forma de progresión a través de una sucesión de estados.

En forma general el diagrama de transición de estados de los procesos es el que aparece en la figura 2.9. Un proceso creado (dado a conocer al sistema operativo) está en ejecución, listo para ejecutarse, o suspendido esperando un suceso.

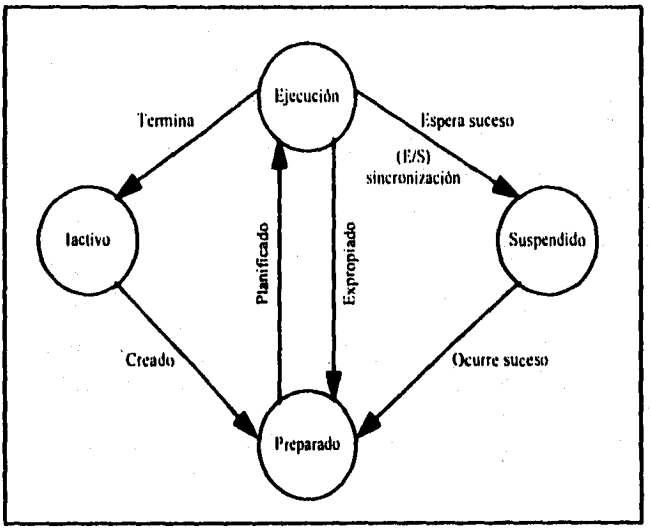

Figura 2.9 Transición de Estados de los Procesos

Las cuatro categorías generales de los estados de un proceso son:

- **Inactivo**

El estado inactivo es en cierta medida periférico, ya que se refiere a los procesos que aún no son conocidos y por tanto no son contabilizados por el sistema operativo. Todas las plantillas de procesos en espera de activación, además de los programas aún no remitidos al sistema operativo, pueden ser considerados como inactivos en esta clasificación.

- **Preparado**

Un proceso preparado posee todos los recursos necesarios para su ejecución, excepto el procesador. Los procesos asumen generalmente el estado preparado inmediatamente después de ser creados. Todos los procesos preparados están esperando que el sistema operativo les asigne el procesador para poder ejecutarse. Un módulo del sistema operativo denominado planificador selecciona uno de los procesos separados para ser ejecutado cada vez que el sistema operativo toma control del procesador y está en disposición de transferirlo a un proceso de usuario.

- **En ejecución**

Un proceso en ejecución posee todos los recursos necesarios para su ejecución, incluyendo el procesador. En un sistema de un solo procesador, sólo puede estar ejecutándose un proceso como máximo en cada instante. El proceso en ejecución ejecuta su secuencia de instrucciones máquina y puede invocar al sistema operativo para que efectúa servicios tales como una operación de E/S o una sincronización mediante intercambio de señales en su nombre. Dependiendo de la política de planificación particular aplicada, el sistema operativo puede devolver control al proceso en ejecución después de realizar el servicio, o puede planificar otro proceso si hay alguno preparado para ejecutarse.

- **Suspendido**

Un proceso suspendido carece de algunos recursos además del procesador, como por ejemplo de una señal de sincronización. Tales procesos están normalmente excluidos de la competencia por la ejecución hasta que desaparezca la condición de suspensión. El proceso en ejecución puede quedar suspendido al invocar una rutina de E/S cuyo resultado necesite para proseguir, o por la espera de una señal que aún no se haya producido. El sistema operativo anota entonces la razón de la suspensión de modo que pueda reanudar el proceso cuando la condición de suspensión desaparezca por efecto de las acciones de algunos otros procesos o por la llegada de un suceso externo.

2.4.8 Los procesos en VMS

El ambiente de trabajo del sistema operativo VMS está definido en términos de procesos:

- Todo el trabajo sobre el sistema se lleva a cabo dentro de procesos.
- El sistema utiliza información asociada con los procesos para determinar : el orden en el que los trabajos se ejecutarán, los recursos que serán designados para un trabajo.
- Un proceso contiene información relacionada con su identificación y estado, esto el sistema lo requiere para ejecutar programas.

Dentro del ambiente VMS existen cuatro tipos de procesos : procesos separados, subprocesos, BATCH y de red. Existen varias razones para crear los tres primeros tipos de procesos, esto es, pueden servir para cargar un programa muy extenso sin que suspendamos una sesión, para accesar al sistema sin interrumpir lo que esté realizando y aún más se realizará un mejor uso de los recursos del sistema.

Procesos separados :

- Son creados cuando se entra a una sesión en la VAX.
- Termina al finalizar la sesión.
- Puede ser interactivo
- No afecta los recursos de otros procesos.

Subprocesos

- Creados y apropiados por otros procesos, los cuales reciben el nombre de procesos padres.
- Usa algunos de los recursos que utiliza el proceso padre.
- Puede ser o no un proceso interactivo.

Procesos BATCH

- Creados por el sistema para ejecutar un procedimiento de comandos.
- Crean un archivo de registro de sus actividades (a este archivo se le llama LOG).
- Es no interactivo.

Procesos de red

- Son creados por un sistema remoto cuando el nombre del nodo es especificado con un comando DCL.
- Crean un LOG llamado NETSERVER.LOG en el directorio del nodo remoto.
- Es no interactivo.

2.4.9 Estado de los procesos en VMS

En el sistema operativo VMS, un proceso se encuentra siempre en uno de los tres estados siguientes:

- **Current (actua).** Proceso que esta usando el CPU para realizar su tarea.

- **Computable.** Proceso listo para correr y esperando para obtener acceso al CPU.

- **Espera.** Estado en el cual un proceso puede estar en "espera" del CPU de forma voluntaria o forzada.

2.4.10 Estados de espera voluntaria

Un proceso en estado de espera voluntaria se tiene cuando dicho proceso requiere de algún tipo de servicio del sistema, esto es, esperará por un recurso. Ocurre frecuentemente, dependiendo del diseño de la aplicación y puede ser de larga duración. En este estado se definen los siguientes tipos:

- **LEF** (Local Event Flag), espera por un evento local.
- **CEF** (Common Event Flag), espera a un evento común.
- **HIB** (Hiebernación), espera para ser despertado.
- **SUSP** (Suspendido), espera para ser reanudado.

2.4.11 Estados de espera involuntarios

Un estado de espera involuntario, no es explícitamente requerido por el proceso, esto es, el proceso es forzado a caer en este estado. Los estados de espera involuntarios pueden ser:

- **COM.** Espera por el CPU.
- **FPG** (Free Page), proceso que espera por una pagina de memoria libre.
- **MWAIT.** Espera por diferentes recursos.

Los estados de espera involuntarios que ocurren frecuentemente tienen una larga duración, pueden indicar un embotellamiento del sistema.

A continuación se presenta la figura 2.10 con algunos de los procesos que ocurren bajo el Sistema Operativo VMS.

VAX/VMS V5. 5-2H4 on node MEBAPB 2-MAY-1996 20:01:15.13 Uptime 6:00:01:05

Pid	Process Name	State	Pri	I/O	CPU	Page flts	Ph.Mem
20200201	SWAPPER	HIB	16	0	0 00:00:01.59	0	0
2020020C	OPCOM	HIB	8	695	0 00:00:00.59	420	178
20200213	NETACP	HIB	9	1661	0 00:00:01.70	157	398
20200214	EVL	HIB	6	163	0 00:00:00.11	131469	88
20200215	LES$ACP	HIB	10	144	0 00:00:00.28	383	601
20200237	BAPSYS_01	LEF	9	26245	0 00:00:13.71	29168	286
202002A8	BAPSYS_03	CUR	4	383	0 00:00:01.19	6872	584

Figura 2.10 Procesos en el Sistema Operativo VMS

2.4.12 Configuraciones en VAX

En esta sección se analiza a la plataforma VAX dentro de las redes de computadoras, un sistema VAX estará conectado a una red de cómputo cuando éste tiene alguna o todas las características siguientes :

- El sistema VAX (computadora) es parte de una configuración VAXCLUSTER.

- La computadora se comunica con otras (por ejemplo para compartir datos, correr aplicaciones o utilizar el correo electrónico).

- La computadora es una estación de trabajo con software DECWINDOWS.

Como ya hemos explicado una red permite la comunicación entre computadoras no importando su localización. Las computadoras DIGITAL con el sistema operativo VMS (Virtual Memory System) utilizan para conectarse a una red de computadoras el protocolo de comunicaciones llamado DECnet-VAX.

DECnet es el nombre que recibe la familia de productos de comunicaciones (software y hardware) que permiten a los sistemas operativos de DIGITAL trabajar en el ambiente de las redes.

Una red con DECnet consiste de dos o más computadoras comunicadas entre sí para compartir recursos e intercambiar información. Algunas características adicionales de este tipo de red son :

- Los sistemas VMS utilizan el software DECnet-VAX para participar en redes DECnet.

- Todos los sistemas conectados con DECnet son similares.

- Cada sistema en la red es llamado nodo.

- Las redes DECnet pueden variar en tamaño desde 2 hasta 64,000 nodos. Cuando se tiene un máximo de 1023 nodos es posible mantener sin división a la red, pero cuando se cuenta con redes muy amplias, estas podrán ser divididas en múltiples áreas de trabajo. Pueden ser hasta de 63 áreas, cada una de ellas puede tener hasta 1023 nodos y es importante hacer notar que cada área trabaja como si se tratara de una red independiente (subred).

- Las redes DECnet soportan una variedad de configuraciones incluyendo :

    - Redes de área local (LAN), usando para este tipo de configuración : fibra óptica (FDDI, Fiber Distribuited Data Interface) con altas velocidades de comunicación (100Mb/s), también utilizan la configuración de redes tipo ETHERNET (IEE 802.3) de muy bajo costo y alta flexibilidad de conexión (10 Mb/s).

    - Redes de área amplia (WAN) utilizando conexiones punto-punto, conexiones síncronas y asíncronas así como conexiones multipunto.

    - Conexiones a través de redes de conmutación de paquetes (PSDN).

    - Comunicación con distintas plataformas como por ejemplo IBM, HP, etc.

2.5 Hardware de red

Una red DECnet puede comprender diferentes tipos de hardware. A continuación se explican algunos componentes comunes.

2.5.1 Conexiones punto a punto

Una conexión punto a punto utiliza tecnología de redes de cobertura amplia (WAN) para conectar dos nodos de manera directa, esta tecnología utiliza :

- Comunicaciones síncronas o asíncronas

  La comunicación asíncrona maneja cada carácter como una entidad separada, con un bit de arranque y uno más de parada. Los bits de arranque y parada indican al receptor los límites de cada carácter enviado a través de la línea de comunicación.

  En la comunicación síncrona los caracteres se transmiten en bloques a intervalos de tiempo precisos con un bit de inicio por bloque, de tal forma que el dispositivo receptor se encuentra listo para recibir grandes cantidades de información con mayor eficiencia y velocidad. Otra característica importante de la transmisión síncrona, es la adición de correctores de error, lo cual reduce en forma drástica la probabilidad de falla en el proceso transmisión-recepción.

- Un módem para modular la señal de digital a analógica para su transmisión sobre una línea de comunicación y para demodular la señal de analógica a digital para su destino final.

- Líneas telefónicas (comunicación por cable).

La figura 2.11 muestra una red sencilla, la cual consiste de dos nodos VAX unidos por una conexión punto a punto.

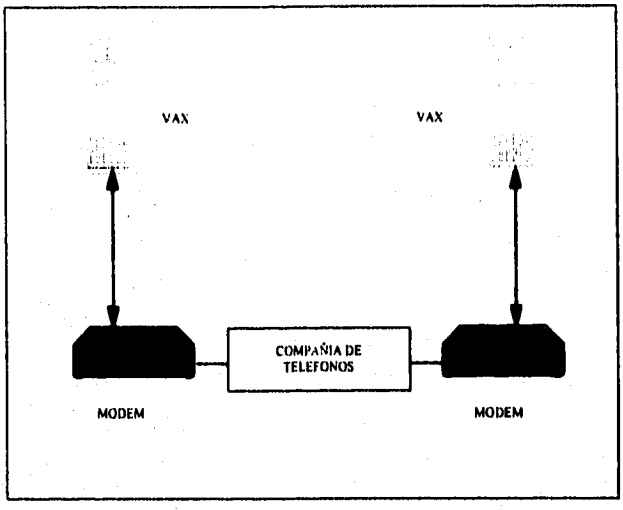

Figura 2.11 Conexión punto a punto

2.5.2 Redes de fibra óptica

FDDI (Fiber Distribuited Data Interface) es la primera LAN estandarizada para fibras ópticas. Puede operar a una velocidad de 100 Mb/s. Este tipo de red puede ser un canal dedicado de alta velocidad para el manejo de múltiples subredes (802.3 ETHERNET) así como trabajar simultáneamente con interconexiones VAXCLUSTER.

La figura 2.12 muestra un esquema de este tipo de redes, en ella se puede observar el anillo que está conectando dos redes de trabajo.

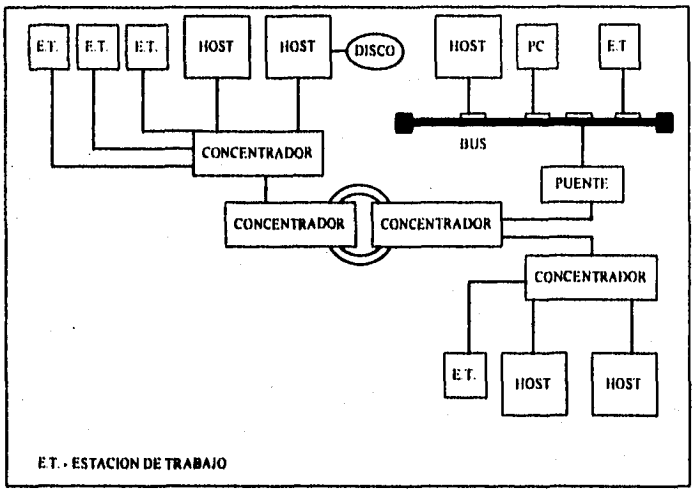

Figura 2.12 Vista de una Red FDDI

Soporta un máximo de 500 estaciones de red (concentradores o puentes), un radio de 100 km.

2.5.3 Redes LAN (802.3/ETHERNET)

DIGITAL soporta el estándar de la IEEE 802.3/ETHERNET (figura 2.13), este es el estándar que más se ha utilizado para las redes de área local. Esto se debe a las características siguientes :

- La distancia que puede existir entre dos estaciones de la red ETHERNET es de 2800 metros aproximadamente.
- Si un segmento es mayor a 500 metros, deberá trabajarse con un repetidor para refrescar y regenerar la señal.
- Se pueden soportar hasta 8000 estaciones.
- Con la configuración 802.3 ETHERNET puede soportar algunos otros protocolos de comunicación simultáneamente con DECnet.

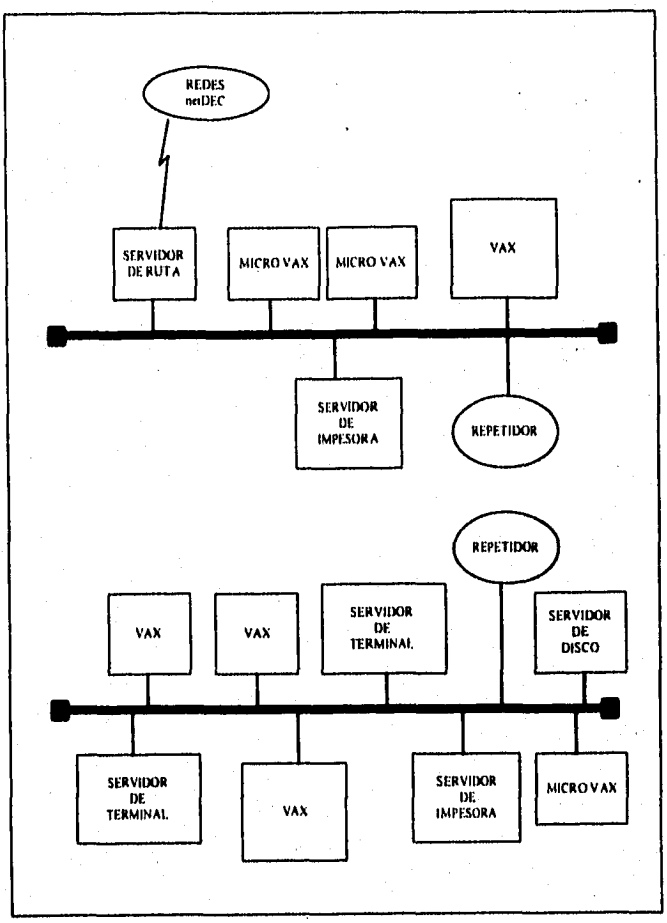

Figura 2.13 LAN ETHERNET

2.5.4 Configuración de LANs extendidas

Este tipo de redes son creadas utilizando diferentes tipos de puentes (BRIDGES), estos se utilizan para :

- Unir dos o más LAN y así formar una LAN extendida.
- Conectar diferentes tipos de LAN (por ejemplo una LAN 802.3/ETHERNET con una red FDDI)
- Para unir LANs que estén situadas remotamente, con esto se logra que los recursos de una red sean compartidos con la otra red.
- En una LAN 802.3/ETHERNET, un repetidor remoto puede extender la red solamente por 1000 metros. Con redes de fibra óptica y micro-ondas se extienden hasta 22000 metros y pueden incluir hasta 8000 nodos.
- Existen puentes que en la actualidad soportan tecnología satelital obteniendo así alcances de comunicación mayores.

En la figura 2.14 se tiene una configuración de LAN extendida

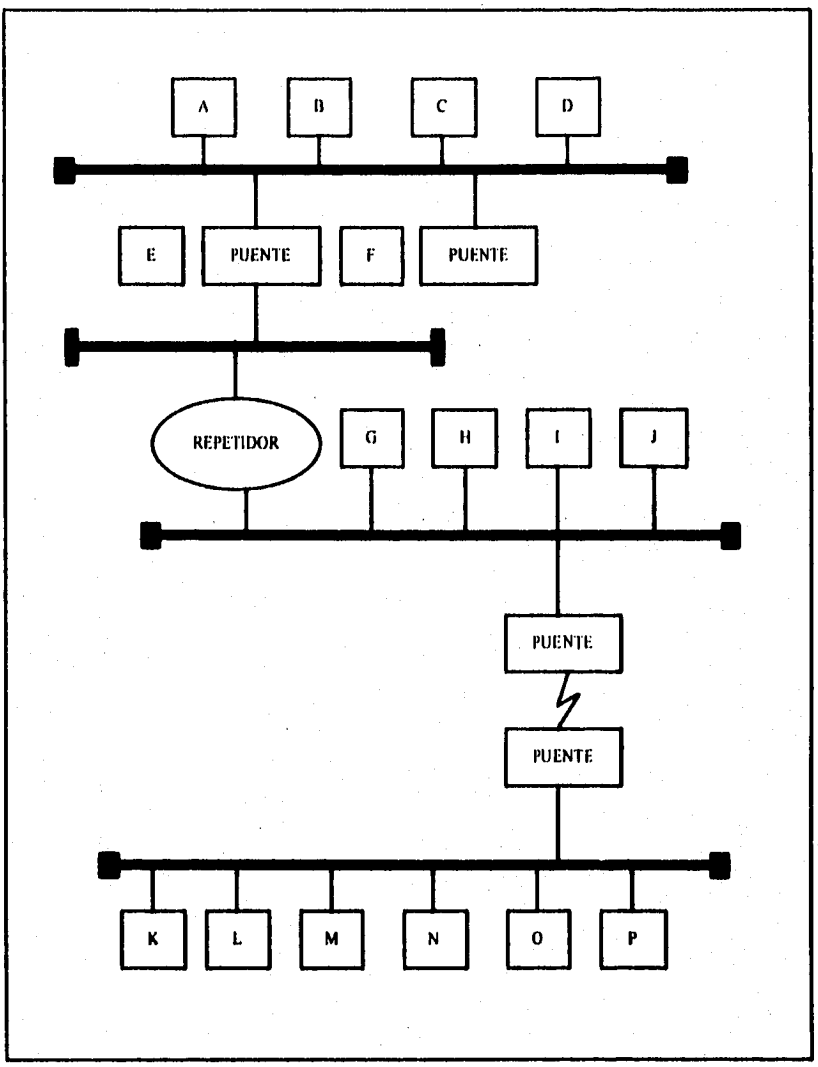

Figura 2.14 Configuración de una LAN extendida

2.5.5 Redes MULTIVENDOR

DECnet es lo suficientemente flexible para soportar redes MULTIVENDOR (redes que están integradas por sistemas de diferentes proveedores), como se puede observar en la figura 2.15. Se requiere de un software especial que trabaje sobre sistemas VMS para comunicarse con otras redes, llamado GATEWAY este sirve para la conversión de protocolos entre las diferentes redes. Ejemplos de GATEWAY son :

- DECnet/SNA para la comunicación con equipos IBM.
- DECnet/X.25router como interface con redes de transmisión de paquetes usando redes X.25.
- UCX es el gateway para la comunicación con redes UNIX.

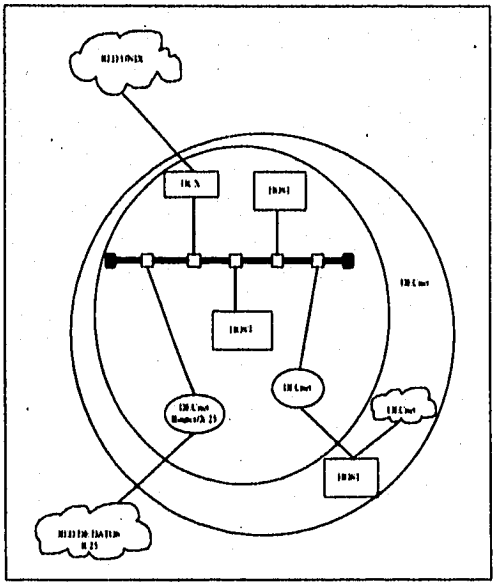

Figura 2.15 Ambiente de Redes Multivendor

2.5.6 Ruteo con DECnet

Si existen dos nodos como los que se muestran en la figura 2.16 que no están directamente conectados y necesitan comunicarse, DECnet encamina la información entre ellos. Selecciona el mejor camino entre ambos nodos, esto es, el de menor costo (dinero, tiempo, etc.). En caso de que dos caminos tuvieran el mismo costo los paquetes toman alternadamente cualquiera de ellos. Algunos conceptos utilizados en el encaminamiento (ruteo) son lo siguientes :

- Una línea de comunicación es un canal físico entre dos nodos, se llaman nodos adyacentes si estos se comunican entre sí, por una línea.

- Un circuito es un canal lógico entre nodos adyacentes, múltiples circuitos pueden compartir una línea de comunicación.

- Costo del circuito es un entero positivo asociado con el uso del circuito.

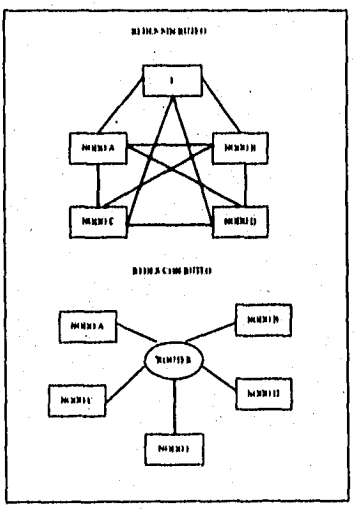

Figura 2.16 Redes sin y con ruteo

En una red con múltiples áreas, existen dos tipos de ruteo : ruteo de nivel 1 tiene la característica de enviar los paquetes de información dentro de una sola área, al contrario del ruteo de nivel 2 el cual se efectúa entre diferentes áreas.

2.5.7 Tipos de nodos

Existen dos tipos de nodos en una red DECnet :

- Nodo final, el cual tiene exactamente un circuito activo y puede comunicarse solo a través de su nodo adyacente.

- Nodo de ruteo, tiene más de un circuito activo, recibe y transmite información direccionada a otros nodos de la red.

2.5.8 Configuraciones de doble procesamiento

La configuración doble consiste de un par de unidades centrales de procesamiento dentro de un mismo sistema de cómputo, este tipo de arquitectura tiene las características siguientes :

- Las Unidades Centrales de Procesamiento comparten el mismo Sistema Operativo.

- Las Unidades Centrales de Procesamiento no pueden operar independientemente una de la otra.

- La administración y operación es manejada como si se tuviera solo una máquina.

- Este ambiente de trabajo provee de un alto rendimiento.

Para comprender este concepto exponemos a continuación un ejemplo, con las VAX series 6000 se pueden tener dos o más unidades centrales de proceso compartiendo la misma memoria por medio de un ducto de alta velocidad y la configuración multiprocesador actúa como un simple sistema para los usuarios y administradores.

2.5.9 Sistemas VAXCLUSTER

Un sistema VAXCLUSTER es un grupo de dos o más computadoras las cuales comparten algunos o todos sus recursos. Cuando un grupo de computadoras VAX comparten sus recursos en un ambiente VAXCLUSTER, los medios de almacenamiento de todas ellas son combinados, esto incrementa la capacidad de procesamiento, comunicaciones y disponibilidad del sistema de cómputo.

2.5.9.1 Miembros de un VAXCLUSTER

Un VAXCLUSTER puede tener por miembros :

- Recursos compartidos : procesadores, colas de impresión o batch, discos de almacenamiento, unidades de cinta, entre otros.
- Puede usar un sólo dominio de Seguridad y Administración.
- Arranque (BOOT) independiente para cada procesador.
- Comunicación entre los procesadores que intervienen en el VAXCLUSTER para coordinar las actividades de este.
- Alto potencial en las entradas y salidas (I/O) a cualquiera de los medios de almacenamiento ya sean discos o unidades de cinta.
- Se ejecuta una copia privada del sistema operativo VMS en memoria de la computadora.

Se identifican algunos elementos del VAXCLUSTER dependiendo de la función que realizan : servidor de arranque (BOOT SERVERS), satélites, servidores de disco, servidores de cinta y miembros de ethernet.

Servidor de Arranque

Con el concepto de servidor de arranque nos referimos a la máquina más poderosa en el VAXCLUSTER, esta computadora contiene los archivos de arranque del sistema para los satélites, también los archivos comunes de inicialización para el VAXCLUSTER (STARTUP FILES) así como los directorios raíz de los satélites.

Satélites

Son estaciones de trabajo o MICROVAX miembros del VAXCLUSTER, no tienen discos locales de sistema por lo que arrancan a partir del Servidor de arranque (BOOT SERVER) sobre ETHERNET.

Servidores de Disco

Son dispositivos que sirven para que nodos de otros sistemas VAXCLUSTER tengan acceso a discos con los cuales no tengan conexión directa. También sirve para el manejo de discos mediante HSC.

Un HSC (Hierarchical Storage Controller), es un controlador de discos inteligente que optimiza las operaciones físicas del disco. Es un nodo pasivo que cuenta con memoria y unidad central de proceso; es importante mencionar que un VAXCLUSTER soporta hasta quince controladores HSC.

Otro concepto utilizado en plataforma VAX es el de MSCP (Mass Storage Control Protocol), el cual es un protocolo de acceso lógico a discos y cintas. Existe un dispositivo llamado MSCP SERVER el cual proporciona la capacidad de compartir volúmenes, manejar discos locales a miembros CI, servidores de boot y servidores de disco en el VAXCLUSTER, discos controlados por HSC, etc.

Servidor de Cinta

Este dispositivo se utiliza para que los nodos de otro VAXCLUSTER tengan acceso a unidades de cinta con las cuales no se tenga conexión directa.

También se encuentra el concepto de MSCP SERVER (servidor de cintas MSCP), cuando una cinta es accesada a través de MSCP, algún procesador en el VAXCLUSTER puede accesar y montar la cinta (únicamente un procesador puede utilizar una unidad a la vez).

Miembros ETHERNET

Usan el disco local del sistema y pueden servir así como discos locales a otros miembros.

2.5.9.2 Tipos de configuración de los sistemas VAXCLUSTER

El tipo de configuración del VAXCLUSTER está determinada por la forma en que están conectados sus dispositivos. Se tienen los siguientes tipos :

CI DUCTO

Las características de un ducto CI (Computer Interconnect) son las siguientes : incluye una velocidad de 70 megabytes por segundo, doble comunicación serial (DUAL PATH) conecta unidades HSC y procesadores VAX.

Esta configuración cuenta con las ventajas siguientes :

- **Alta Disponibilidad.** Se utiliza redundancia de hardware y software, esto se realiza para que el sistema soporte fallas de manera automática.

- **Compartir Recursos y Datos.** Se refiere a la utilización de múltiples discos y unidades de cinta vía controladores. Los discos son disponibles para todos los nodos del sistema.

- **Aumentar los recursos de la Computadora.** Esta ventaja se debe a que se pueden combinar las características de varios sistemas VAX, para el usuario esto es transparente, ya que para él este es un sólo sistema.

- **Administración Centralizada.** El Administrador del sistema puede llevar a cabo sus tareas desde un nodo del VAXCLUSTER, ve al sistema como si fuera uno solo.

VAXCLUSTER de área local (ETHERNET)

Las características principales de este tipo de conexión son la baja velocidad de transmisión (10 megabytes por segundo), simple canal de comunicación (SINGLE PATH), capacidad para la transmisión de múltiples protocolos de comunicación entre los que podemos mencionar DECNET, TCP/IP, X25, etc. Esta configuración presenta las siguientes ventajas :

- Se comparten los recursos del sistema VAXCLUSTER.

- Los periféricos también se comparten.

- Un punto muy importante lo son las Bases de Datos de aplicación o configuración del sistema que puedan estar almacenadas en el sistema, estas también se pueden compartir.

- En resumen proporciona todas las ventajas que da una red de área local (LAN).

DUCTO DSSI (Digital Standard Storage Interconnect)

Diseñado para distancias cortas (6 metros), la velocidad de transmisión gira alrededor de los 4 megabytes por segundo y utiliza un ducto paralelo.

Red FDDI

La red FDDI (Fiber Distributed Data Interface, por sus siglas en inglés), se pueden llevar a cabo conexiones hasta de más de 40 km y al igual que ETHERNET soporta varios protocolos de comunicación.

DUCTO MI

Un DUCTO MI (Mixed Interconnect) este es una combinación de las distintas formas de interconexión.

2.5.10 Nombre de los dispositivos en un sistema VAXCLUSTER

Debido a que los nodos en un sistema VAXCLUSTER pueden compartir recursos (dispositivos), estos dispositivos deben ser nombrados sin redundancias o ambigüedades. Existen dos formas de nombrar a los dispositivos en un ambiente VAXCLUSTER :

- **nodo$dispositivo.** Usado por dispositivos que están directamente conectados solamente a un nodo.

- **$localización-clase$dispositivo.** La clase de localización es un parámetro que se instala sobre un nodo y sirve para los discos o cintas. Este es un controlador HSC o un nodo corriendo el servidor MSCP. Para cualquier disco o cinta todos los nodos dentro de VAXCLUSTER deberán tener el mismo parámetro de localización clase.

No pueden existir dos dispositivos con el mismo nombre, ya que habría conflictos de reconocimiento por parte del usuario que requiera del servicio de dicho dispositivo.

En la figura 2.17 se muestra un esquema de la configuración VAXCLUSTER.

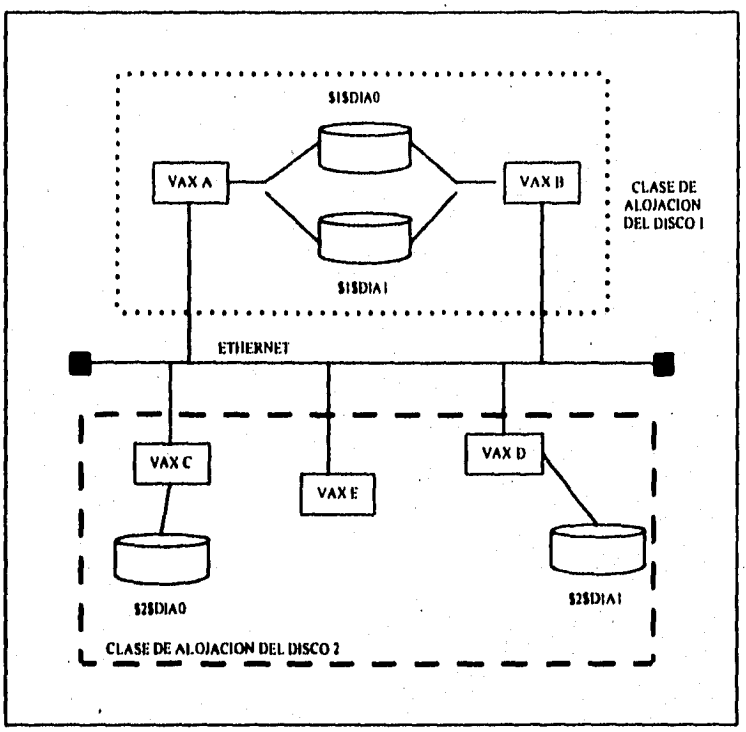

Figura 2.17 Configuración de un VAXCLUSTER

2.6 Hardware del ACSE

El corazón del Sistema de Procesamiento y Control es un par de computadoras VAX (Digital Equipment Corporation, DEC), corriendo bajo el sistema operativo VMS, nos referimos a los BAPs (Background Aplication Processors). Estas computadoras proveen todas las funciones principales del sistema, en particular el almacenamiento y envío de mensajes. Están conectadas vía ETHERNET a otros elementos del sistema.

Conectadas directamente a cada VAX existen unas consolas de monitoreo (opcionalmente una impresora para el registro de eventos a través de la red ETHERNET), se les llama consolas VMS, todos los mensajes del sistema operativo VMS se presentan en ellas.

Cada BAP soporta unidades de almacenamiento tanto de cinta como de disco. Todos los discos son accesados por ambos BAPs. Existen dos pares de discos uno por cada BAP para el almacenamiento del software y de las bases de datos del sistema.

Las unidades de cinta son accesadas desde cada BAP, por lo regular existen dos tipos de unidades de cinta :

- Unidad de cinta de carrete, usada principalmente para efectos de generación de archivos de facturación de servicios.

- Unidad de cinta de cartucho (DAT), esta es utilizada para la realización de respaldos y carga de nuevo software para el sistema.

Se cuenta con facilidades para la operación del sistema, en la red ETHERNET se tienen conectadas dos estaciones de trabajo (máquinas VAX) las cuales proveen el acceso a toda la red. Cada una de ellas recibe el nombre de Consola de Operador del Sistema (System Operating Console, SOC). Tienen asociadas dos impresoras para el registro de eventos relacionados con el sistema.

En el área que ocupa el ACSE, se cuenta con una impresora especial para la salida de reportes y estadísticas.

2.6.1 Redundancia en la VAX

Los procesadores principales (VAX) trabajan bajo un esquema de redundancia, esto quiere decir, que se tiene un equipo adicional por cada procesador para que en caso de falla, entre el otro a cubrir al que ha fallado.

Cuando el procesador está a cargo del procesamiento de la información en tiempo real se dice que éste es el procesador MASTER, en caso contrario cuando el procesador está en espera de que pueda ocurrir alguna falla, se dice que el procesador está en STANDBY. Se puede cambiar de un estado a otro manualmente o bien desde el software de control.

2.6.2 Interface hombre-máquina

El operador del sistema tiene varios medios de comunicación con el equipo. Los elementos que permiten esto son :

- Consola de Operador del Sistema (software)
- Panel de Alarmas
- Impresora de Alarmas
- Impresora de reportes
- Consola VMS

En la figura 2.18 se muestra el diagrama físico del equipo que forma al ACSE en el centro de control MOVISAT.

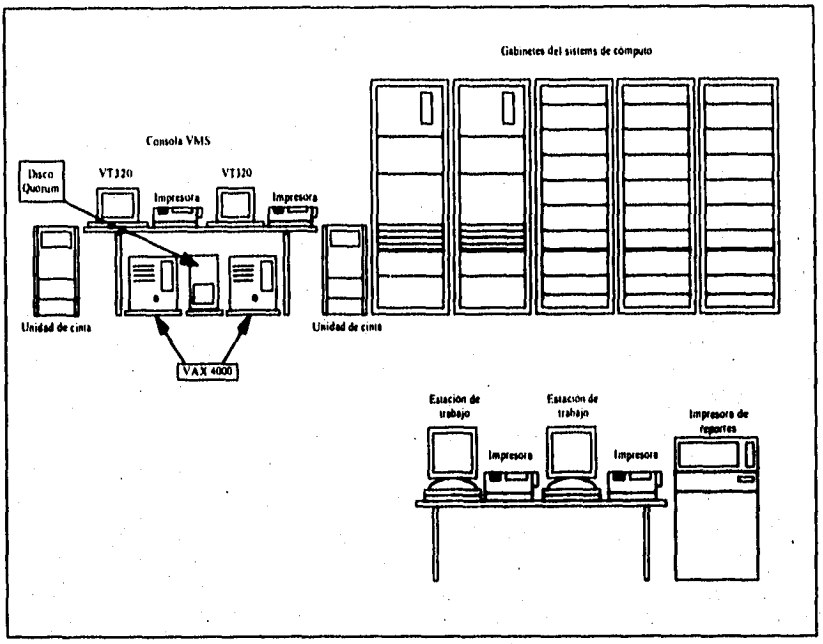

Figura 2.18 Configuración física del ACSE

CAPITULO 3

Administración del Sistema de Trabajo

CAPITULO 3

Administración del Sistema de Trabajo

3.1 Administración de usuarios en ambiente VAX

El Sistema Operativo VMS y algunas otras utilerías de software bajo la plataforma VAX, ofrecen una serie de capacidades de cómputo para llevar a cabo las tareas que se requieren para Administrar correctamente un sistema de cómputo. Dichas tareas de administración son : control de acceso al sistema de cómputo, mantenimiento de la seguridad, definición de los tiempos de acceso, control de procesos, manejo de recursos (software y dispositivos), etc. En este capítulo nos ocuparemos del análisis de la Administración de los Usuarios en el Procesador de Aplicación de Respaldo (BAP, Background Aplication Processor), el cual dentro del ACSE (Access Control and Signalling Equipment) de MOVISAT es una computadora VAX 4000.

Es trabajo del Administrador del Sistema crear y dar mantenimiento a las cuentas que corresponden a los usuarios del sistema de cómputo. Para crear dichas cuentas para los usuarios y dar un uso efeciente al sistema, se tiene que determinar cuáles son las necesidades de acceso al sistema de los usuarios y qué recursos requieren ellos.

El sistema operativo VMS provee una utilería llamada Archivo de Autorización de Usuarios (UAF, User Authorization File) para como su nombre lo indica autorizar y controlar el uso de los recursos del Sistema Operativo para los usuarios individuales del sistema. Nos permite realizar las tareas siguientes:

- Crear cuentas para usuarios
- Modificar cuentas existentes
- Borrar cuentas (usuarios) del sistema
- Listar las cuentas de los usuarios

3.1.1 Archivo de autorización de usuarios (UAF)

Se administra a los usuarios sobre el sistema operativo VMS, creando y manteniendo en buenas condiciones cada una de las cuentas pertenecientes a estos, para ello se requiere de la utilería AUTHORIZE, la cual es un software que corre sobre VMS y permite realizar las tareas de administración sobre los usuarios del sistema, consta de varios comandos que son los que permiten realizar todas las tareas de administración de usuarios bajo VMS.

Para ejecutar el software de la utilería AUTHORIZE se tienen que tener los privilegios necesarios para ello (los cuales se explicarán más adelante); A continuación se explican los comandos que se utilizan para correr el AUTHORIZE. Se puede observar que se necesita estar en el directorio SYS$SYSTEM, para llegar a este se utiliza el comando SET DEFAULT (nos permite cambiar de directorio). Ya estando en el directorio antes mencionado se ejecuta la utilería con el comando RUN (correr) y para salir de AUTHORIZE se ejecuta el comando EXIT (salida).

```
$SET DEFAULT SYS$SYSTEM:
$RUN AUTHORIZE
.
.
.
UAF>
```

El ambiente de trabajo de la utilería AUTHORIZE considera los siguientes puntos:

- Crea registros nuevos y modifica los existentes, sobre un archivo llamado SYSUAF.DAT; y cuando trabaja con usuarios en una red en el archivo NETPROXY.DAT

- Crea y modifica los registros en un archivo de base de datos del sistema operativo VMS llamado RIGHTSLIST.DAT

La utilería AUTHORIZE contiene un conjunto de comandos para asignar valores a cualquier campo de un registro.

Se tiene dentro de este software (AUTHORIZE) cuatro tipos diferentes de registros o cuentas:

- **DEFAULT (por defecto)**

  Sirve como plantilla para la creación de los registros o cuentas de un usuario en el UAF. Un nuevo registro de usuario tiene asignado los valores que el sistema ya tiene en la cuenta DEFAULT, excepto los que el administrador del sistema asigne a la nueva cuenta. De esta manera, cuando se quiera agregar una nueva cuenta se necesita especificar únicamente los valores de los campos que se quieran diferentes.

  Para poder cambiar los valores que la cuenta DEFAULT tiene es importante conocer los parámetros a modificar en el registro, ya que puede afectar al sistema de cómputo. La cuenta de DEFAULT no puede ser borrada o renombrada, porque esta es importante para el manejo de las nuevas cuentas sobre el sistema VAX en cuestión.

- **FIELD (Campo de servicio)**

  Permite al personal de campo de DIGITAL el poder verificar un sistema computacional, en caso de fallas reportadas. Este registro puede ser habilitado o bien deshabilitado cuando el sistema es instalado.

- **SYSTEM (Cuenta del Sistema)**

  La cuenta SYSTEM provee los medios para entrar al sistema con todos los privilegios. Puede ser modificado este registro, pero no borrado o renombrado desde el UAF, porque desde esta cuenta se tiene todo el control de privilegios y algunas otras tareas como puede ser bajar el sistema, realizar respaldos, la instalación de nuevo software, etc.

- **SYSTEST (Cuenta de pruebas)**

  La cuenta SYSTEST provee un ambiente para la ejecución de una utilería de pruebas para el sistema. Esta cuenta puede ser habilitada cuando el sistema es instalado.

3.1.2 Agregando una cuenta de usuario al sistema

El administrador del sistema de cómputo VAX tiene que analizar los requerimientos de los posibles usuarios del sistema, esto con la finalidad de determinar las características de la cuenta que se le va a asignar, por ejemplo tiene que ver el espacio en disco que se le va a proporcionar, qué privilegios va a tener, a que disco físico va a tener acceso, etc. En el ambiente de trabajo VAX existen dos tipos de cuentas:

- **Cuenta interactiva**

  Una persona que utiliza una cuenta interactiva tiene acceso al software del sistema y puede trabajar de manera muy natural utilizando como por ejemplo un programa de desarrollo, un editor, pero dentro de todo el ambiente de trabajo del equipo VAX. Usualmente este tipo de cuenta es considerada como una cuenta individual ya que por lo general solamente una persona puede utilizarla.

- **Cuenta Cautiva**

  Este tipo de cuenta se asigna a un usuario que tiene un acceso limitado en el uso de los recursos del sistema y es usada para personas que tienen una función específica dentro del mismo.

Las cuentas que se administran dentro del ACSE (en la VAX principal, esto es, dentro de cada uno de los BAPs) son de tipo interactivo y son las que se muestran en la tabla 3.1

OWNER	USERNAME	VIC	ACCOUNT	PRIVS	PRI	DIRECTORY
BAPSYS	BAPSYS	[126,1]	BAPSYS	ALL	4	LES$DISK0:[BAPSW]
BAPV	BAPV	[126,2]	BAPV	ALL	3	LES$DISK0:[BAPSYS]
CESTST	CESTST	[125,2]	CESTST	ALL	4	LES$DISK0:[CESTST]
DECNET DEFAULT	DECNET		DECNET	NORMAL	4	SYS$SPECIFIC:[FAL$SERVER]
	DEFAULT	[376,376]		NORMAL	4	DISUSER
		[200,200]				
FAL$SERVER DEFAULT	FAL$SERVER		DECNET	NORMAL	4	SYS$SPECIFIC[FAL$SERVER]
		[376,373]				
FIELD SERVICE	FIELD	[1,10]	FIELD	ALL	4	SYS$SYSROOT:[SYSMAINT]
MAIL$SERVER	MAIL$SERVER		DECNET	NORMAL	4	SYS$SPECIFIC:[MAIL$SERVER]
DEFAULT		[376,374]				
NML$SERVER	NML$SERVER		DECNET	NORMAL	4	SYS$SPECIFIC:[NML$SERVER]
DEFAULT		[376,371]				
PCFS	PCFS$ACCOUNT	[369,1]		NORMAL	4	SYS$SYSDEVICE:[PCSA]
PCSA$RMI	PCSA$RMI	[360,2]		NORMAL	4	SYS$COMMON:[PCSA]
PHONE$SERVER	PHONE$SERVER		DECNET	NORMAL	4	SYS$SPECIFIC:PHONE$SERVER]
DEFAULT		[376,372]				
	SYBASE	[400,4]		ALL	4	SYS$SYSDEVICE:[SYBASE_491. SYBASE]
HUGHES NETWORK SYSTEM	SYBASE_401P3	[300,3]	SYBASE	ALL	4	SYS$SYSDEVICE:[SYBASE_401P 3.SYBASE]
SYSTEM MANAGER	SYSTEM	[1,4]	SYSTEM	ALL	4	SYS$SYSROOT:[SYSMGR]
SYSTEST-UETP	SYSTEST	[1,7]	SYSTEST	ALL	4	DISUSER
SYSTEST-UETP	SYSTEST_CLIG	[1,7]	SYSTEST	ALL	4	DISUSER

Tabla 3.1 Cuentas del ACSE

Para tener un buen desarrollo al momento de dar de alta una nueva cuenta en el sistema el administrador debe considerar los puntos siguientes:

- **Determinar el nombre del usuario**

El nombre del usuario por lo general se define con el apellido o nombre del usuario de la cuenta a dar de alta, si por cuestiones de seguridad se requiere de un nombre más sofisticado, esto es, con algún formato en especial, se puede dar.

El nombre del usuario es una cadena que va desde 1 hasta 12 caracteres, incluyendo letras, números y guiones bajos. El signo de dólar ($) es permitido, pero usualmente está reservado para los nombres que el sistema utiliza. Un nombre de usuario definido solamente con números no está permitido.

- **Definir la clave de acceso (password)**

  La clave de acceso es una palabra que va a permitir, como su nombre lo dice, la entrada a la cuenta del usuario, le sirve a este para mayor seguridad de su ambiente de trabajo. Solamente es conocida esta clave de acceso por el usuario y el Sistema Operativo. Las claves de acceso son asignadas por el Administrador del Sistema y su longitud va de 0 a 31 caracteres, puede incluir letras, números, guiones bajos y también el signo de dólar.

- **Determinar el código de identificación del usuario (UIC, User Identification Code).**

  El Código de Identificación del Usuario (UIC) se especifica en formato octal y además está formado por dos números: el primero representa a un grupo (conjunto de usuarios del sistema, con alguna característica en común por ejemplo área de ingeniería, cobranza, departamento, proyecto, etc.), y el segundo a un miembro de ese grupo, ambos separados por una coma y encerrados con paréntesis cuadrados. El grupo es un número que tiene que estar en el rango de 1 a 37776, el miembro en el rango de 0 hasta 177776. Un ejemplo de esta notación del UIC es el siguiente: si el UIC de una cuenta fuera [200,26] tendríamos que se trata de un usuario que pertenece al grupo 200 y que de ese grupo él es el miembro número 26.

- **Asignación del dispositivo por defecto**

  Seleccionar el dispositivo (disco) que tenga el espacio suficiente para que el usuario de la cuenta pueda tener sus archivos de trabajo.

- **Directorio por defecto**

  Crear un directorio base a nivel comando desde VMS, utilizando para ello CREATE/DIRECTORY (crear directorio), debe de residir en su dispositivo por defecto.

- **Privilegios**

  Determinar las necesidades de seguridad de la cuenta (niveles de protección, privilegios y control de acceso).

Después de realizado el análisis anterior acerca del propósito de la nueva cuenta, el Administrador del Sistema decide cuáles serán los atributos y cuáles los recursos que el usuario requiere. Definido esto se utiliza la utilería AUTHORIZE para crear la nueva cuenta, desde el prompt que se tiene al correr dicha utilería (UAF) se usa el comando ADD y enseguida se especifican todas las características que el usuario tendrá.

3.1.3 Modificación de una cuenta de usuario

Para cambiar en una cuenta del sistema características tales como: el espacio en disco, el directorio base, la clave de acceso (password), los privilegios o cualquier otra característica asignada con AUTHORIZE, se utiliza el comando MODIFY (modificar). Resumiendo, se tiene que con el comando anterior se modifican los campos existentes en una cuenta del sistema VAX.

Para comprender el uso de este comando tenemos el ejemplo siguiente: cuando a un usuario se le olvida su clave de acceso (password) para poder accesar a su cuenta, el Administrador del Sistema con ayuda de la utilería AUTHORIZE y el comando MODIFY (modificar) puede cambiar la clave de acceso y así el usuario podrá trabajar con una nueva clave.

En la VAX principal del ACSE, esto es, en el Procesador de Aplicación de Respaldo (BAP, Background Aplication Processor), se requiere del comando MODIFY para tener un constante manejo de las claves de acceso y privilegios, por motivos de seguridad.

3.1.4 Listado de las cuentas de los usuarios

Dentro de AUTHORIZE se tiene un comando llamado LIST (lista), que nos permite listar todas las cuentas que están dadas de alta en el Procesador de Aplicación de Respaldo del ACSE. Al correr este comando, el listado de las cuentas se guarda en un archivo de texto que tiene por nombre SYSUAF.LIS, el cual, es un reporte que después puede ser analizado desde un editor de texto de VMS (el editor de texto más común en el Sistema Operativo VMS es el EDIT).

Por defecto, el comando LIST produce un reporte (archivo tipo texto) con la información siguiente:

- Nombre del dueño de la cuenta
- Nombre del usuario
- Los privilegios de la cuenta
- Prioridad de los procesos de la cuenta
- Disco y directorio por defecto

Si se requiere de un reporte con toda la información relacionada con las cuentas dadas de alta al comando LIST se le agrega el calificativo /FULL (completo) de la manera siguiente: LIST/FULL.

3.1.5 Borrado de las cuentas de los usuarios

Para efectuar el borrado de una cuenta del sistema de cómputo se utiliza el comando REMOVE de la utilería AUTHORIZE, con este el registro se pierde del UAF. En el siguiente ejemplo se muestra el comando REMOVE para eliminar al usuario [nombre del usuario].

```
UAF> REMOVE [nombre del usuario]
UAF> EXIT
```

3.2 Administración de los discos de almacenamiento en el ACSE

3.2.1 Organización de archivos

La Organización de Archivos del Sistema Operativo está encargada de manejar los datos que residen en el almacenamiento secundario. Los datos lógicamente relacionados ubicados en el almacenamiento secundario se organizan generalmente en colecciones caracterizadas por un nombre y son llamados archivos. Un archivo suele aparecer ante los usuarios como un arreglo lineal de caracteres o de estructuras de tipo registro.

Las reponsabilidades más comunes del Sistema de Organización de Archivos son las siguientes:

- Traducción de las peticiones de acceso desde el espacio lógico de direcciones hacia el archivo físico.
- Transmisión de elementos de archivo entre almacenamiento principal y secundario.
- Organización del almacenamiento secundario, como por ejemplo, llevar control del estado, asignación y desasignación de espacio en disco.
- Soporte para protección de archivos.
- Recuperación y posiblemente restauración de archivos después de que el sistema pueda tener fallas.

Los servicios básicos del sistema de organización de archivos, tales como la transmisión de bloques de datos, son necesarios para soportar el manejo de memoria virtual y el intercambio (swapping), aspectos bajo los cuales trabaja el sistema operativo VMS y que serán detallados más adelante.

3.2.2 Organización del disco

En un sistema informático se pueden utilizar una gran variedad de dispositivos de entrada/salida (E/S) para el almacenamiento de archivos. Su característica general es la direccionabilidad y la transmisión de datos en bloques, en contraposición con la conexión entre el procesador y la memoria principal, en donde la unidad de transferencia de datos es típicamente una palabra. A diferencia de la memoria principal, los dispositivos de almacenamiento de archivos experimentan generalmente una pronunciada varianza en el tiempo medio necesario para acceder a un determinado bloque de datos. El orden de magnitud de esta varianza depende de la implementación física de un dispositivo particular, y es bastante diferente para discos, cintas magnéticas y memorias de burbuja.

El medio físico para el almacenamiento de datos es la película de óxido magnético, un plato de disco que se asemeja a una grabación fonográfica. En una sola unidad de disco puede haber disponible uno o más de tales platos para almacenamiento y recuperación de datos. Dependiendo de si los platos de grabación pueden o no ser extraídos de la unidad, los discos se dice que son extraíbles o fijos (discos duros). Los discos extraíbles suelen estar alojados en alguna forma de paquete, como por ejemplo un cartucho de disco o una cubierta de disco flexible.

Una vez alojado un cartucho en la unidad, los discos fijos (duros) y flexibles funcionan de manera similar . A diferencia de las cintas magnéticas, los platos de discos son obligados a girar constantemente por el mecanismo de la unidad a una velocidad de 3.000 revoluciones por minuto (rpm) o mayor; los discos flexibles giran a 300 rpm aproximadamente, y pueden ser detenidos completamente entre un acceso y otro. Los datos son leídos y escritos por medio de cabezas de lectura/escritura montadas en un conjunto de cabezas de tal modo que puedan ser puestas en contacto íntimo con la parte del disco en donde residen los datos requeridos.

3.2.2.1 Conceptos básicos de discos

La grabación de información en el disco ocurre sobre ambas superficie de cada plato. La superficie del extremo superior e inferior del mismo disco no son utilizadas para la grabación. Los principales conceptos utilizados bajo el Sistema Operativo VMS son los siguientes:

- **Pista**

  Los datos se almacenan en la superficie magnética del disco en forma de círculos concéntricos llamados pistas.

- **Cilindro**

  Se denominan cilindro a la colección de pistas en el mismo radio sobre la superficie del disco que están a la misma distancia del eje del disco.

- **Sector**

  Se denomina sector a la porción de una pista. Se utiliza el concepto de bloques en VMS, cada uno de ellos equivale a 512 octetos (bytes)

En la figura 3.1 se muestra las características usadas bajo las plataforma VAX.

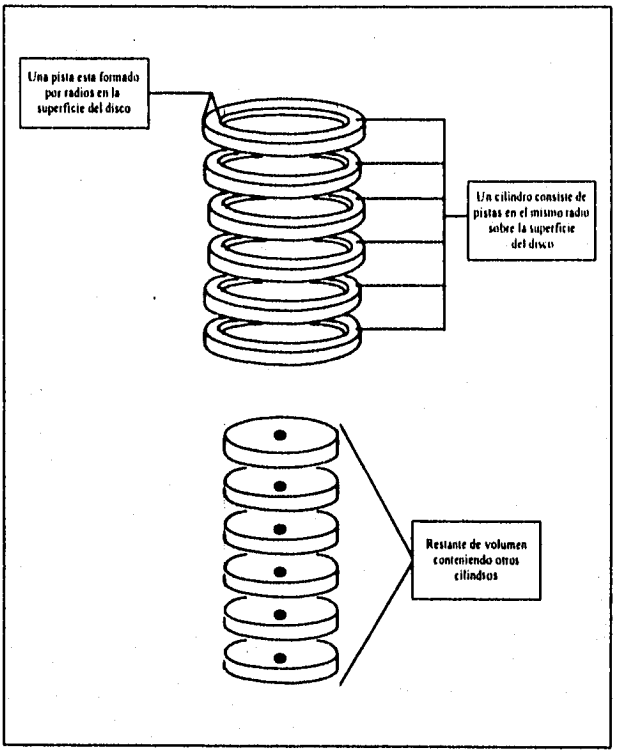

Figura 3.1 Características físicas de un disco de almacenamiento

3.2.2.2 Tiempo de acceso al disco

Dependiendo del número de cabezas de lectura/escritura disponibles, los discos se pueden clasificar como:

- Discos de cabeza fija
- Discos de cabeza móvil

Discos de cabeza fija

Los discos de cabeza fija tienen generalmente una cabeza de lectura/escritura distinta por cada pista. Un determinado sector es accedido activando la cabeza sobre la pista apropiada cuando el sector requerido pasa bajo ella.

El tiempo necesario para acceder al sector deseado se denomina latencia rotacional. En promedio, es igual a la mitad del tiempo de revolución del disco , que es del orden de milisegundos (ms) para las velocidades de rotación típicas de un disco.

Discos de cabeza móvil

Los discos de cabeza móvil se caracterizan por tener una o unas pocas cabezas de lectura/escritura por superficie. Los discos flexibles son generalmente del tipo de cabeza móvil con el fin de permitir al montaje de cabezas apartarse del cartucho antes de que éste sea reemplazado. Con cabezas móviles, la lectura de un sector requiere que el montaje de las cabezas sea en primer lugar desplazado hasta el cilindro correspondiente. Una vez conseguido esto, se activa la cabeza sobre la pista buscada cuando el sector objetivo pasa bajo ella. Así, el tiempo de acceso de un disco de cabeza móvil incluye el tiempo de posicionammiento de la cabeza, o tiempo de búsqueda (movimiento circunferencial) y la latencia rotacional, descrita anteriormente.

Los fabricantes de discos suelen especificar el tiempo medio de búsqueda requerido para que el montaje de la cabeza atraviese la mitad de la superficie del disco. Este parámetro varía en un rango mayor que el de la latencia rotacional. Su orden de magnitud es de milisegundos (ms), y puede ir desde casi 10 ms a por encima de 60 ms en unidades de menor rendimiento.

Estas dos componentes del tiempo de acceso de disco son las responsables de su variabilidad en unos dos órdenes de magnitud, desde menos de 1 ms hasta del orden de 100 ms. Una vez que se accede al sector deseado, los datos se transfieren a una velocidad del orden de 0.25 a 5 MB/s. Suponiendo que el tamaño de un sector a 5 megabytes por segundo (MB/s) de aproximadamente 98 microsegundos (μs). Esto es obviamente varios órdenes de magnitud más rápido que el tiempo medio de acceso al disco. Dado que las velocidades de transferencia de datos a disco son elevadas, el método de Acceso Directo a Memoria (DMA, Direct Memory Access) es el único casi exclusivamente utilizado para transferir datos entre los discos y memoria principal.

Los retardos relacionados con el hardware en la transferencia de datos entre disco y memoria principal son una combinación de tres factores principales:

- **Tiempo de búsqueda**

  Es el tiempo necesario para que las cabezas de lectura/escritura se desplacen hasta el cilindro buscado.

- **Latencia rotacional**

  Es el tiempo empleado en esperar a que el sector deseado aparezca bajo las cabezas de lectura/escritura.

- **Tiempo de transferencia**

  Es el tiempo necesario para transferir un sector entre el disco y la memoria.

Los dos primeros componentes representan el tiempo de acceso a disco o la latencia cuando se accede a un sector de disco. Sólo el tiempo de transferencia, que es generalmente el más pequeño de los tres, es función del tamaño del sector. Generalmente es más eficiente transferir grandes cantidades de datos en cada acceso a disco ya que el gasto por acceso a disco se amortiza entonces para un número mayor de octetos (bytes). esta es la razón por la cual la eficiencia de transporte de páginas y la eficiencia de lectura /escritura de disco aumentan generalmente al aumentar los tamaños de los tamaños de página y sector.

3.2.2.3 Controlador y rutina de disco

Debido a que los discos son dispositivos electromagnéticos, sólo son capaces de obedecer ordenes bastante primitivas. En la figura 3.2 se muestran las señales de interface típicas entre una unidad de disco y el controlador de disco de un sistema informático. Dado que un controlador es generalmente capaz de manejar varias unidades de características similares, se necesitan algunas líneas de control para seleccionar la unidad designada que participa en una operación dada.

En la figura 3.2 se indican como líneas sector de unidad. Análogamente, las líneas sector de cabeza se utilizan para activar una cabeza específica en la unidad seleccionada. La señal dirección, necesaria para las unidades de cabeza móvil, se utiliza para designar la dirección, hacia dentro o hacia fuera, en que se desplazarán las cabezas desde la posición actual. La línea paso se utiliza para proporcionar una secuencia temporizada de impulsos de paso. Generalmente un impulso mueve la cabeza un cilindro, y un número predeterminado de impulsos lleva el montaje de cabezas desde el cilindro actual hasta el cilindro objetivo.

Las señales de leer y escribir se utilizan para activar la cabeza de lectura/escritura seleccionada. Las líneas entrada de datos y salida de datos transportan generalmente el flujo de bits de entrada o de salida cuando se realiza una operación de leer o de escribir, respectivamente. Pista 00 es una señal suministrada por la unidad que indica que el montaje de cabezas se encuentra en el cilindro 0 pista 0, la posición más externa u origen. La señal índice indica el momento en que la electrónica de la unidad detecta la marca de dirección del cilindro o de la pista (el agujero índice en discos flexibles). La señal cambio de volumen, proporcinada generalmente en medios extraíbles, alerta al sistema operativo sobre cambios en el medio magnético.

Después de detectar este suceso, el sistema opertivo debe invalidar toda la información almacenada en la memoria principal relativa a la unidad asociada, tal como entradas de directorio y tablas de espacio libre.

Otras señales incluyen reinicializar y la indicación de fallo y unas pocas señales adicionales específicas del dispositivo colectivamente indicadas como entrada miscelánea y salida miscelánea. Algunos ejemplos de estas señales son modo de codificación, puerta abierta, motor encendido y protección frente a escritura.

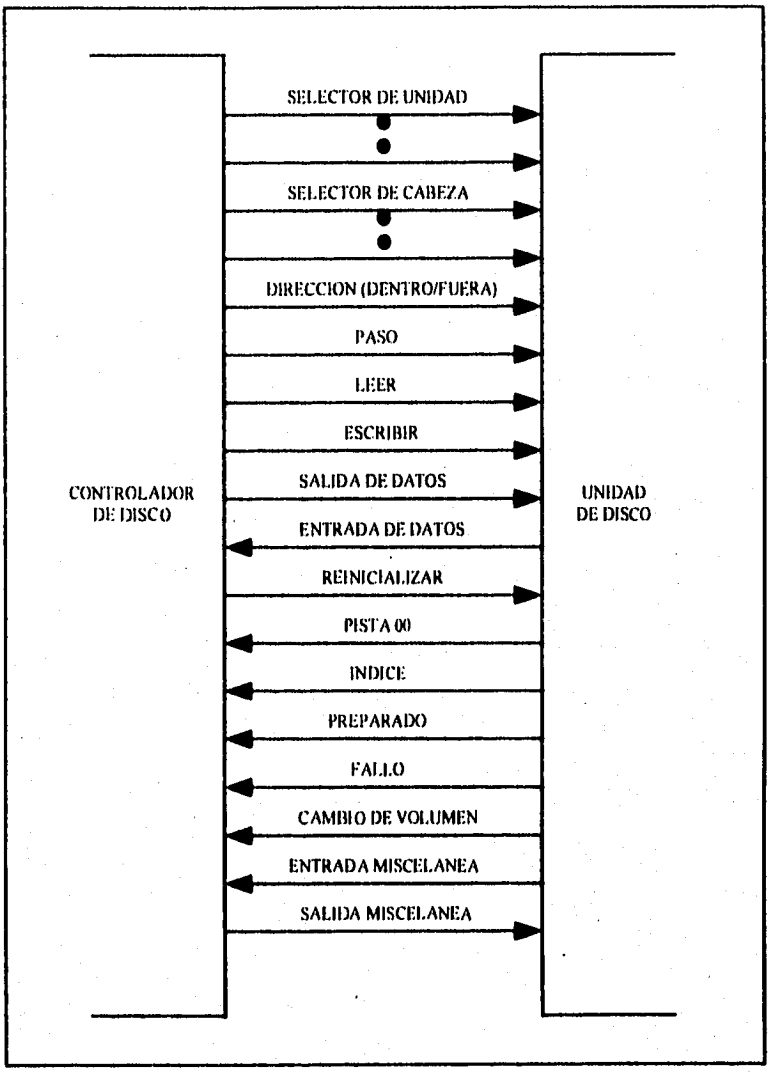

Figura 3.2 Señales del controlador/unidad de disco

Las principales funciones de un controlador básico de disco son:

- Convertir órdenes de nivel superior, tales como buscar o leer un sector, en una secuencia adecuada temporizada de órdenes específicas de la unidad.

- Proporcionar conversión serie a paralelo y acondicionamiento de señales necesarias para pasar de un formato de byte o palabra, requerido por la comunicación DMA con la memoria principal, a los flujos análogos de bits esperados y producidos por las unidades de disco.

- Efectuar verificación y control de errores. El control de errorres es necesario para detectar errores transitorios provocados por ruidos e interferencias electromagnéticas y para manejar los defectos del medio de almacenamiento. Cada vez que escribe un bloque de datos en disco, el controlador calcula los valores de los bits de chequeo de los datos y los añade. Puesto que los errores de disco suelen ocurrir en ráfagas, que producen errores en cadena de bits sucesivos, los controladores de disco suelen utilizar mecanismos de detección de errores capaces de tratar tales errores como los códigos de redundancia cíclica (CRC). Durante las operaciones de lectura, el controlador calcula los bits de chequeo calculados con los recibidos desde el disco. Cualquier discrepancia es inicio de error.

Dependiendo de su causa, un error de disco puede ser transitorio o permanente. Los errores transitorios son tratados generalmente mediante la relectura del sector en cuestión un número predeterminado de veces. a este parámetro se le suele denominar contador de reintentos. Si el error persiste después de unos pocos reintentos, se supone que es permanente. Supuesto que la unidad es, en los restantes aspectos, totalmente funcional, los errores permanentes se producen por defectos del medio de almacenamiento. Los sectores defectuosos se suelen denominar bloques malos.

Los discos pueden contener bloques defectuosos, particularmente los discos de bajo costo y de elevada densidad. La práctica habitual es excluir del uso los bloques malos, por ejemplo, marcándolos como permanentemente utilizados. La misión de evitar el uso de los bloques malos se delega generalmente a una capa de bajo nivel del sistema de control de archivos con el fin de evitarle a los usuarios esa tarea. Los bloques defectuosos pueden ser detectados inicialmente en tiempo de inicialización del disco.

Excepto las funciones básicas descritas hasta ahora, hay una gran variación en cuanto a la sofisticación de los controladores de disco cada vez más "inteligentes" que se encargan de muchas funciones tradicionales delegadas al software, tales como el formateo, el almacenamieto en memoria y la agrupación de los datos de bloques. Algunos controladores también proporcionan caché de sectores, optimizadores de búsqueda y búsquedas asociativas en disco. Implementaciones VLSI de controladores de disco flexible y disco rígido son comúnmente empleadas en los diseños más novedosos, que también suelen disponer de microprocesadores dedicados y grandes memorias RAM (Ramdon Access Memory).

Por otra parte, muchos controladores clásicos o "tontos" permanecen al nivel funcional de rendimiento descrito anteriormente. Por tanto éstos dependen en gran medida del software para proporcionar el resto de funciones necesarias.

Puesto que las transferencias de datos entre discos y memoria principal utilizan acceso directo a memoria (DMA), la rutina de disco no devuelve datos explícitamente a sus invocadores, excepto la información referente al resultado de la operación en cuestión. Cuando se detecta una excepción (como por ejemplo un error de lectura o un fallo de la unidad), la rutina de disco suele indicar el número real de octetos (bytes) que han sido transferidos correctamente antes de producirse el error. Otras órdenes de la rutina pueden incluir algunos modos de manejo de la unidad de almacenamiento, tal como formatear una pista, y marcar un bloque como defectuoso escribiendo en él una marca especial de supresión de datos.

Algunas rutinas y controladores de disco son capaces de transferir múltiples sectores e incluso pistas, en respuesta a una sola orden. Una ventaja de este modo de operación es que las cabezas se posicionan sólo una vez, de modo que el recargo del tiempo medio de acceso puede amortizarse para muchos sectores. Las operaciones multisector y multipista requieren generalmente que todos los datos transferidos ocupen direcciones consecutivas de disco. En particular, no suelen estar permitidos movimientos de cabezas o salto de sectores entre medio.

3.2.3 Sistemas de archivos

Las funciones básicas del Sistema de Archivos en un Sistema Operativo incluye:

- Tener conocimiento de todos los archivos del sistema.
- Controlar la compartición y forzar la protección de los archivos.
- Organización del espacio en disco, asignación y designación.
- Traducir las direcciones lógicas de los archivos a direcciones físicas de disco.

Esta lista supone que las funciones de bajo nivel, tales como organización del dispositivo y del medio de almacenamiento así como el manejo de errores, son proporcionadas por la rutina de disco como hemos descrito anteriormente.

El sistema de archivos tiene conocimiento de los archivos por medio de los directorios. La protección de los archivos requiere forzar la separación de los distintos archivos. Esto significa que a cada usuario sólo se le concede acceso a aquellos archivos para los cuales tiene permiso explícito de uso.

Además, los usuarios autorizados sólo tienen permitido acceso a los archivos en el modo especificado por la autorización asociada, por ejemplo, sólo-lectura o sólo-escritura. La compartición de archivos, cuando está soportada, permite a varios usuarios autorizados a acceder al mismo archivo concurrentemente. Con el fin de preservar la integridad de los archivos compartidos, el sistema puede imponer algunas restricciones temporales adicionales necesarias para propósitos de sincronización.

Los cambios dinámicos en el número y el tamaño de los archivos necesitan frecuentes asignaciones y designaciones de espacio en disco. El sistema de archivos contabiliza generalmente el espacio de disco no utilizado por medio de un depósito de bloques libres. Las peticiones de bloques de disco necesarias para el crecimiento y la creación de archivos se satisfacen normalmente a partir de ese depósito.

Aunque es posible la traducción directa lógica a física de las direcciones de disco, la mayoría de los sistemas lo realizan por etapas. Una de las razones principales para ello es la gran variabilidad en estructura y otras características físicas de los diferentes dispositivos de almacenamiento secundario. Incluso dispositivos similares, tal como las unidades de disco que pueden variar en el número y capacidad de los platos, tamaños de los sectores, número de cabezas de lectura/escritura, etc.

Los tres niveles de direccionamiento de almacenamiento en disco son habitualmene identificables en implementaciones del sistema de organización de archivos, y caen en los esquemas siguientes :

- **Direccionamiento lógico relativo a archivo**

  En el nivel más elevado de la abstracción, el sistema de almacenamiento se contempla como una colección de archivos con nombres. Los elementos contenidos en almacenamiento secundario se direccionan por medio de una dirección con dos componentes de la forma (nombrearchivo, desplazamieto), La mayoría de las aplicaciones y llamadas al sistema relativas a archivo utilizan esta forma de direccionamiento.

- **Direccionamiento lógico relativo a volumen**

  Muchas rutinas de dispositivo de disco proporcionan una abstracción del disco como array lineal de sectores. Las partes independientes de dispositivo del sistema de archivos utilizan esta forma de direccionamiento (sector, desplazamiento). Los dispositivos de interfaz de sistemas informáticos pequeños (SCSI, Small Computer System Interface) proporcionan esta forma de abstracción de disco directamente por medio de controladores hardware integrados en las propias unidades.

- **Direccionamiento físico relativo a unided**

  Este nivel utiliza las direcciones físicas de tres componentes de la forma <cilindro, cabeza, sector>. Este nivel de direcionamiento es producido por las rutinas de dispositivo software que las traducen a señales reales de control de la unidad tales las mostradas en la figura 3.1

  Sólo el nivel inferior, el tercero, de abstracción de disco utiliza las direcciones físicas de tres componentes, que dependen de la estructura y geometría específicas de la unidad. Debido a la traducción de direcciones por capas, el conocimiento específico del dispositivo puede quedar confinado a las rutinas de dispositivo de bajo nivel mientras que el resto del sistema de archivos opera utilizando formas generales de direccionamiento de disco independientes del dispositivo.

3.2.4 Archivos en el sistema operativo VMS

Como se mencionó anteriormente un archivo es una colección de información, la cual puede ser código entendible por la computadora o bien texto que un usuario puede interpretar. Un archivo de tipo texto puede contener una carta, un programa escrito en cualquier lenguaje de programación, una lista de direcciones, la salida de un comando DCL, etc. En el Sistema Operativo VMS el nombre de los archivos pueden constar de cadenas de hasta 39 caracteres, formados con letras, números y guiones. Los archivos también constan de un tipo y de una versión, para el tipo se tienen las mismas características que para el nombre. Las versiones que se pueden tener de un archivo son de hasta 32767.

Para el Administrador del Sistema existen archivos que le ayudan a realizar su tarea de manera más sencilla, tales archivos son :

- **Archivo de Autorización de Usuarios** (UAF, User Authorization File), el cual contiene información acerca de los usuarios dados de alta en el sistema.

- **Archivo de Parámetros del Sistema,** este contiene las características de configuración del sistema.

3.2.5 Control del Espacio en Disco

Un método para administrar el espacio en disco es utilizando el comando SET FILE, con el cual se modifican las características de un archivo en VMS. Dichas características son:

- **Fecha de expiración**

  Se realiza con el comando /EXPIRATION= <fecha> asigna una fecha de finalización de uso del archivo. Después se podrá borrar el archivo cuya fecha de expiración ha pasado .

- **Límite de versiones**

  En VMS se pueden generar distintas versiones para un archivo, con el comando /VERSION=<n> se especifica el número de versiones que se quiere sobre un archivo, si el número de versión se excede al límite, el último archivo ocupa el lugar de la versión más antigua.

- **Dueño del archivo**

  Con el comando /OWNER=<identificador de dueño> especifica el dueño de un archivo, esto es, quién lo puede utilizar. El dueño inicial es el proceso sobre el que actualmente está el archivo.

3.2.6 Directorios

Los directorios son básicamente tablas de símbolos de archivos. Un solo directorio plano puede contener una lista de todos los archivos del sistema. Cuando se utilizan directorios jerárquicos, la colección de todos los directorios y entradas de subdirectorios definen la totalidad de los archivos del sistema. Los directorios planos pueden ser considerados como una forma degenerada, sin subdirectorios y en la cual el directorio raíz contiene a todos los archivos del sistema.

En el Sistema Operativo VMS, la información está almacenada en una estructura hereditaria (forma de árbol), el tope de la estructura es el directorio maestro (MFD, Master File Directory), colgados a este se tienen los directorios de usuarios (UFD, User File Directory). El concepto de subdirectorios también es manejado para organizar la información de cada usuario en el sistema, se pueden tener hasta siete niveles para crear subdirectorios

3.2.7 Organización del espacio en disco

Una función importante del sistema de archivos es organizar el espacio en el almacenamiento secundario. Esto incluye llevar la cuenta de los bloques de disco asignados a los archivos y de los bloques libres disponibles para asignación. El crecimiento de los archivos consume bloques libres, y la eliminación y truncación de archivos produce bloques libres para asignación. Así además de los directorios que describen los archivos existentes, el sistema de archivos debe mantener un depósito de bloques libres. Una buena estrategia de asignación de espacio debe tener en cuenta varios factores relacionados e interactivos, tales como:

- La velocidad de procesamiento de los accesos secuenciales a archivos, los accesos aleatorios a archivos y la asignación y designación de bloques.
- La capacidad de realizar transferencias multisector y multipista.
- La utilización del espacio de disco.
- Los requisitos de memoria principal de un algoritmo dado.

3.2.7.1 Asignación contigua

Es generalmente sencilla de implementar y proporciona acceso secuencial y aleatorio eficiente a los archivos. En el lado negativo, la asignación contigua del espacio del almacenamiento secundario sufre de fragmentación externa e interna, lo cual puede hacer disminuir la utilización del disco a menos que se efectúen costosas compactaciones para reclamar el espacio en disco fragmentado.

3.2.7.2 Asignación encadenada

Es un esquema de asignación de espacio no contiguo conceptualmente similar a una lista enlazada. El encadenamiento elimina la fragmentación externa, facilita el manejo de los bloques defectuosos y es relativamente sencillo de implementar. Las desventajas del encadenamiento incluyen la lentitud del acceso aleatorio a los archivos y la sensibilidad al daño en los punteros. La indexación es una forma de asignación no contigua que proporciona acceso aleatorio más rápido manteniendo la mayoría de las ventajas del encadenamiento. La principal ventaja de la indexación es el recargo de acceso del disco impuesto por la necesidad de buscar en los bloques índice para localizar los bloques de datos de un archivo. Este problema puede ser aliviado manteniendo en memoria principal los índices más frecuentemente utilizados.

3.2.8 Características de los archivos en disco

Los archivos utilizan bloques virtuales para mapear a bloques lógicos sobre el disco. Un bloque virtual esta orientado hacia un archivo y se encuentran al principio del mismo, con esto queremos decir que el primer bloque en un archivo es siempre un Bloque Virtual (VBN, Virtual Block Number). Un Bloque Lógico (LBN, Logical Block Number) está orientado a disco y es el primer bloque que se tiene almacenado en un disco. En la figura 3.3 se muestra la relación entre Bloques Virtuales y Lógicos, en ella se observa que el encabezado (Header) del archivo es el punto medio entre el disco y el archivo.

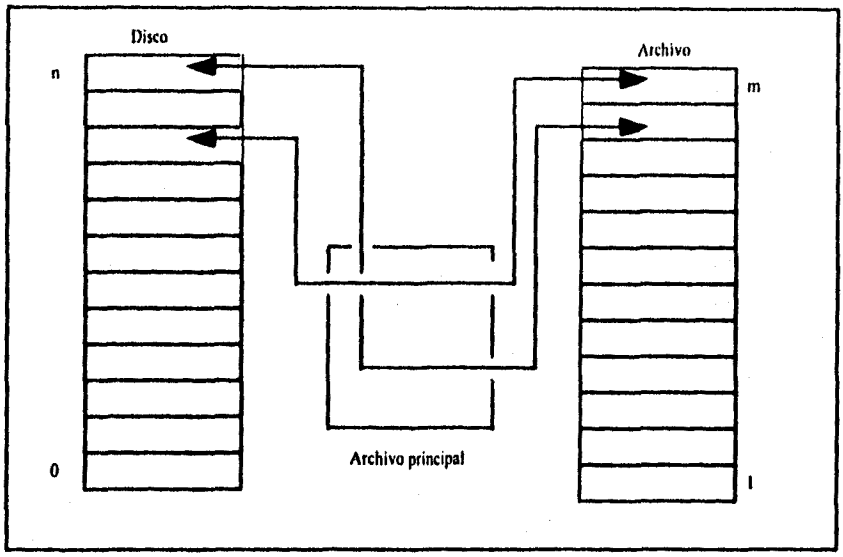

Figura 3.3 Relación entre bloques virtuales y lógicos

3.2.9 Discos del ACSE

El ACSE cuenta con una serie de discos en cada una de sus máquinas VAX principales. Debido a que se cuenta con un sistema de cómputo redundante, esto es, que en caso de que se presente una falla en una computadora VAX, automáticamente entraría la otra a trabajar, se tienen dos procesadores principales. En el ACSE se identifica a cada VAX 4000-105A como BAP A y BAP B. Los discos de cada VAX tienen los nombres que a continuación se presentan:

- **BAP A (VAX4000-105A)**

Disco 1DIA0: El cual es el disco en donde se encuentra el Sistema Operativo VMS, el software de comunicaciones para la operación y control del ACSE y la Base de Datos del Sistema MOVISAT.

- **BAP B (VAX400-105A)**

Disco 1DIA4: En este disco se almacena la misma información que en el disco del BAP A

Se cuenta con discos en espejo a causa de la redundancia de las computadoras, estos discos reciben el nombre de 1DIA1 y 1DIA3, los cuales se localizan en ambas computadoras.

En un gabinete exterior a las computadoras se tiene un disco llamado QUORUM, el cual es común a los dos sistemas VAX, su nombre es 1DIA2 y se utiliza para todo el procesamiento de la información del Sistema MOVISAT, por mencionar algunos ejemplos: generación de la cinta de facturación (para el cobro de los servicios proporcionados por el Sistema), elaboración de reportes y estadísticas de la actividad del Sistema, etc.

En la figura 3.4 se tiene la configuración de los discos con que cuenta el ACSE, se indica cuales son los discos espejo y su relación en ambas máquinas VAX, también se puede observar al disco QUORUM. Es importante hacer notar que las computadoras principales están conectadas vía ethernet.

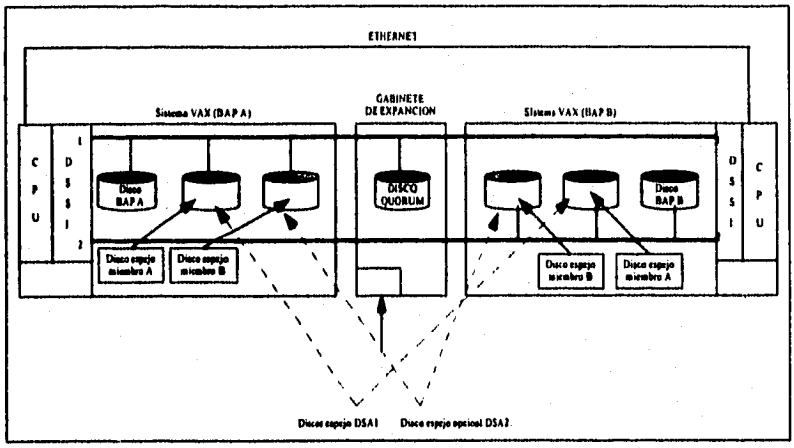

Figura 3.4 Discos de almacenamiento del ACSE

3.2.9.1 Respaldos de los discos del ACSE

Se deben de realizar una serie de respaldos de la información contenida en los discos del ACSE de manera sistematizada, esto es, sobre un esquema planeado de realización. Existen dos tipos principales de respaldos de archivos :

- Respaldos completos (image full backups)
- Respaldos incrementales (incremental backups)

Respaldos completos (image full backups)

En los respaldos completos se guarda una copia de todos los archivos contenidos en un medio de almacenamiento (en nuestro caso, los discos del ACSE), es mucho más rápido de restaurar que un respaldo incremental.

Para realizar un respaldo completo de archivos hacia una cinta o un disco se tienen que realizar los pasos siguientes :

- Utilizar el comando BACKUP de VMS con el calificador /IMAGE (este calificador le indica al comando BACKUP que se realizará una copia total de la información). También se especifica el identificador /RECORD para guardar información que será necesaria para respaldos posteriores.

- Dar el nombre del dispositivo origen, seguido de dos puntos.

- Indicar el medio en donde será almacenada la información, especificando qué tipo de medio de almacenamiento se utilizará.

Para comprender la idea anterior analicemos el ejemplo que se muestra a continuación :

```
$BACKUP/IMAGE/RECORD $1$DIA0: MKA500:RESP.SAV
```

Se realizará un respaldo completo del disco 1DIA0: el cual se almacenará en una unidad de cinta bajo el nombre de RESP.SAV, existen otras opciones para optimizar este comando.

Respaldos incrementales (incremental beckups)

En este tipo de respaldo se guardan los archivos que fueron creados o modificados desde la última copia que se realizó, una ventaja de este tipo de respaldo es que se requiere de menos espacio de almacenamiento (destino) que en el completo.

Para realizar un respaldo incremental, se debe de tomar en cuenta lo siguiente :

- Se utiliza el calificador /SINCE=BACKUP para el comando BACKUP.

- La sintaxis para los respaldos incrementales es la misma que la de los respaldos completos, excepto por el calificador /IMAGE.

- Se pueden especificar los archivos a ser guardados.

El ejemplo es :

```
$BACKUP/RECORD/SINCE =BACKUP $1$DIA0: [*...] -
$_MKA500:RESP.SAV/LABEL=JUN01
```

Es un respaldo incremental, los archivos se guardan desde el último respaldo efectuado (gracias al calificador /RECORD se obtiene esta información), se muestra el calificador /LABEL (etiqueta) se utiliza para cuando se inicializa una cinta (es una especie de proceso de formateo) para indicar al sistema que la cinta tendrá ese nombre.

Los periodos para efectuar respaldos en un sistema VAX se definen de la manera siguiente : si se realizan respaldos completos, una vez a la semana, en caso contrario, esto es, respaldos incrementales deberían realizarse diariamente. En el sistema de cómputo del ACSE se ha implantado un programa de respaldos completos cada mes, por las características del sistema, ya que se tienen que respaldar distintos discos y no se pueden dar de baja las máquinas principales de manera periódica, se aprovechan los mantenimientos preventivos para realizar este tipo de tareas.

3.2.9.2 SAVE SETS

Cuando se realiza un respaldo los archivos son almacenados en unidades llamadas SAVE SETS, las cuales son creadas al momento de ejecutar el comando BACKUP, un SAVE SET puede ser :

- Un archivo sobre cinta
- Un archivo de disco en el mismo sistema
- Un archivo de disco en otro sistema (en una red por ejemplo)

3.2.9.3 Restauración de respaldos

Para restaurar (bajar a disco la información respaldada en una unidad de cinta o bien en otro disco) se sigue el mismo procedimiento que se utiliza para efectuar el respaldo. Se debe de considerar si la información respaldada se almacenará en un disco, en un directorio específico, etc.

3.2.10 Directorios en VMS

Los directorios en VMS están asociados con un nombre simbólico con un identificador (ID, Identification), los directorios de archivos de usuario (UFD, User File Directory) surgen desde el directorio principal (MFD, Master File Directory), el cual se representa así [000000]. Los subdirectorios al igual que en otros Sistemas Operativos se originan desde un directorio padre.

Los directorios y subdirectorios se nombran de la misma forma que los archivos en VMS. En la figura 3.5 se indica la estructura de los directorios y subdirectorios.

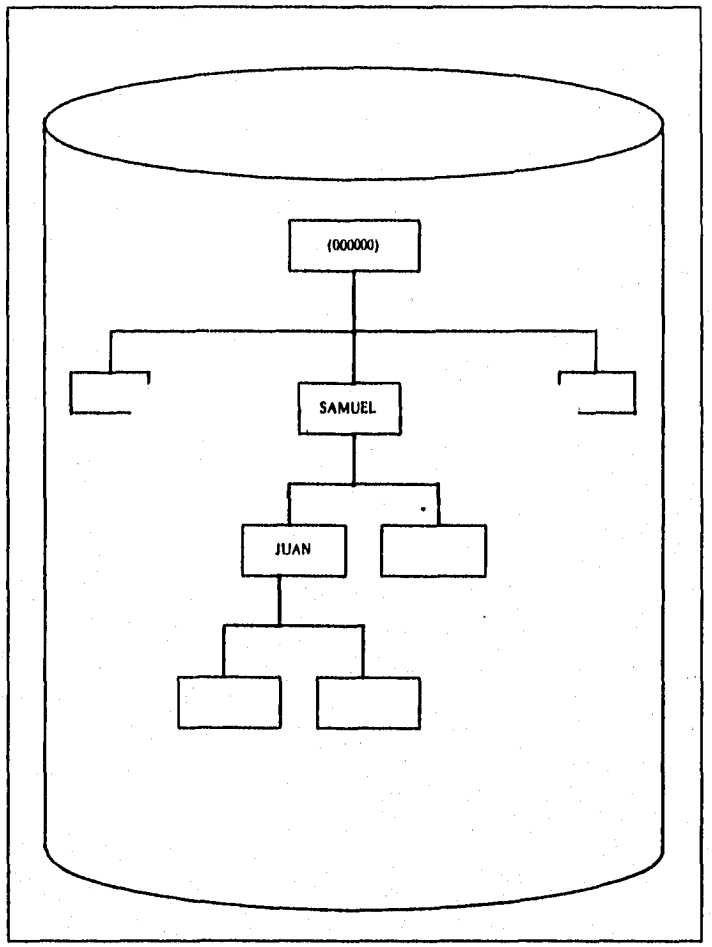

Figura 3.5 Estructura de los directorios y subdirectorios

3.2.11 Nombre de dispositivos en VMS

Cada dispositivo dentro del ambiente de VMS tiene un único nombre en el formato: **ddcu**, en donde :

dd Código del dispositivo simbolizado con dos letras.

c Código de una letra que especifica el controlador de hardware para el dispositivo (el controlador provee la interface entre el BUS y el dispositivo, entre dos ductos (BUSES).

El controlador de hardware:

- Identifica el controlador del dispositivo
- Esta representado por una letra de la A a la Z
- Es asignado por el sistema

u El número unitario del dispositivo

El número unitario:

Indica la posición del dispositivo sobre el controlador, puede ser cambiado por:

- Instalando un botón o interruptor sobre el dispositivo.
- Instalando un tapón individual sobre el dispositivo.

El código del dispositivo especifica el tipo de dispositivo tales como: consolas, terminales, unidades de cinta, unidades de disco compacto y óptico, discos, etc.

3.2.12 Servidor MSCP

El servidor de protocolo de control de almacén de volumen (MSCP, Mass Storage Control Protocol), es un dispositivo (disco) que localiza conexiones de discos para un procesador VAX o un procesador inteligente; MSCP controla los recursos a ser compartidos. Estos discos incluyen:

- Discos locales para miembros de un VAXCLUSTER.
- Discos sobre servidores de arranque, y servidores de discos en cualquier VAXCLUSTER.
    - Discos sobre servidores de discos en un VAXCLUSTER, incluyendo satélites.
    - Discos HSC en interconexiones mezcladas.

EL Servidor MSCP decodifica y da servicios de entrada/salida para enviar a las diferentes clases de discos o a los nodos remotos de un VAXCLUSTER. Cada dispositivo es servido por el MSCP, cualquier procesador puede ser montado en el VAXCLUSTER y accesar al MSCP.

3.2.13 Volúmenes

Para montar volúmenes de disco en un ambiente de trabajo referido a un sistema VAXCLUSTER se siguen los pasos siguientes:

- Hacer dispositivos locales a través del servidor MSCP
- Montar el HSC
- Montar DSSI

- Montar el MSCP y discos locales en todos los nodos, el comando MOUNT/CLUSTER monta un disco sobre todos los nodos que pertenece al VAXCLUSTER.

Para montar todos los dispositivos antes mencionados se utiliza el comando MOUNT/SYSTEM. Para desmontar discos se utiliza el comando DISMOUNT/CLUSTER. Los discos no serán desmontados si otro sistema los esta ocupando, por tal motivo se tiene que realizar un SHUTDOWN al sistema, esto es, dar de baja el sistema.

El Administrador del Sistema puede obtener toda la información relacionada con los discos del sistema, utilizando los comandos siguientes:

- **SHOW DEVICE**, lista todos los dispositivos del sistema

- **SHOW DEVICE/FULL**, muestra el estado completo del dispositivo y se utiliza para la determinación de la configuración de los discos en un VAXCLUSTER.

- **SHOW DEVICE/FILES**, este comando lista todos los archivos que actualmente están abiertos y siendo utilizados por el sistema. Además únicamente muestra los archivos que están abiertos sobre el nodo en el que se da el comando.

- **SHOW DEVICE D**, sirve para observar los discos instalados en el sistema.

3.2.14 Creación de un SET VOLUMEN

Si los archivos o directorios llegaran a ser muy largos para un solo volumen, se puede crear lo que se conoce como un SET VOLUMEN. El sistema operativo VMS trata al SET VOLUMEN como un volumen muy grande, además almacena archivos sobre cualquier espacio libre que tenga.

3.2.15 Administración del espacio en disco

En el ambiente VMS existe una herramienta conocida como archivo de autorización de usuario (UAF, User Authorization File), que nos permite restringir el uso de los recursos del sistema, para ello existe un campo para indicar el espacio en disco que se le proporcionará a un usuario del sistema.

La restricción del espacio en disco es manejada a través de QUOTAS de disco, las cuales son manejadas por la utilería SYSMAN (System Manager), con esta se especifica la cantidad de espacio en disco que se proporcionará a la cuenta sobre el sistema.

El sistema operativo VMS tiene como unidad de espacio de almacenamiento a lo que se conoce como un bloque, el cual equivale a 512 bytes.

3.3 Administración de trabajos en colas (BATCH y de impresión)

El Sistema Operativo VMS provee facilidades que dinámicamente ayudan al Administrador del Sistema a realizar la administración de los trabajos en colas, esto es, de impresión y en BATCH. En el ACSE se cuenta con este tipo de objetos definidos en cada uno de los procesadores principales (BAPs), se requiere de un buen control de este tipo de recursos ya que para efectos de operación de MOVISAT son necesarios, por ejemplo la obtención de impresiones de reportes y estadísticas, programas, archivos de tipo texto como lo puede ser uno de correo electrónico (MAIL) o bien la ejecución de procedimientos (imágenes) en BATCH.

Un trabajo en BATCH (en lotes) se refiere al conjunto de programas que estén esperando algún evento para que se ejecuten, como lo puede ser la asignación de CPU, memoria, disco, etc. Un trabajo de impresión se tiene cuando desde una terminal del sistema se ha solicitado el uso de una impresora para obtener en papel un archivo.

3.3.1 Proceso QUEUE

En el Sistema Operativo VMS corre un proceso llamado QUEUE (QUEUE_MANAGER, Administrador de Cola), controla los trabajos en colas BATCH y los trabajos de impresión. Dicho proceso presenta las características siguientes:

- Automáticamente corre cuando un nodo de la red o de un VAXCLUSTER se levantan. Este proceso se automatiza desde un programa de arranque del sistema, especificando en alguna de sus líneas el comando START/QUEUE/MANAGER.

- Para detener la ejecución del proceso QUEUE se tiene el comando STOP/QUEUE/MANAGER/CLUSTER.

- Si el nodo en donde el proceso está corriendo falla, un nuevo proceso comenzará automáticamente en otro nodo que resida en la red o VAXCLUSTER.

- Coordina los trabajos sobre el sistema, esto es, como se mueven de una cola genérica a una de ejecución (se detallará más adelante).

La administración de trabajos en colas se apoya en una Base de Datos que consiste de tres archivos:

- SYS$SYSTEM:QMAN$MASTER.DAT, archivo maestro
- SYS$SYSTEM:SYS$QUEUE_MANAGER.QMAN$QUEUES, archivo de colas
- SYS$SYSTEM:SYS$QUEUE_MANAGER.QMAN$JOURNAL, archivo de jornal

El proceso de administración de trabajos en colas se comunica con el proceso que controla este tipo de trabajos llamado JOB_CONTROL, sobre cada sistema VAX, este proceso optimiza y controla actividades de asignación de recursos para que el trabajo se lleve a cabo.

3.3.2 Tipos de Colas

El Sistema Operativo VMS soporta dos clases generales de colas:

- Colas de Ejecución
- Colas Genéricas

Colas de Ejecución

Una cola de ejecución mejora el procesamiento de un trabajo, se llaman de ejecución porque llevan a cabo el procedimiento de la información para poder realizar cada trabajo. Existen dos tipos de colas de ejecución:

- **Colas BATCH**

  Aceptan solamente trabajos en lotes (programas de aplicaciones de usuarios, de administración para poder realizar por ejemplo un respaldo, etc.).

- **Colas de Salida**

  Aceptan típicamente trabajos de impresión para su procesamiento y realización. Hay dos principales salidas para este tipo de colas:

  - Impresora, la salida se tiene en una impresora, esto es, el resultado es la obtención de un archivo en papel.

  - Terminal, la salida está direccionada a una terminal de trabajo.

Colas Genéricas

Este tipo de colas contienen los trabajos pendientes hasta que son asignados y transferidos a una cola de ejecución. Existen dos tipos de colas genéricas:

- **Cola Genérica BATCH**

  Definida para mantener únicamente trabajos en BATCH y es usada en sistemas VAXCLUSTER para distribuir la carga de trabajo sobre todo el sistema.

- **Cola Genérica de Impresión**

  Mantiene los trabajos de impresión para enviarlos a su respectiva cola de ejecución.

La relación de las colas de ejecución con las genéricas es mediante una lista (archivo) que se define cuando las colas son inicializadas. En el ACSE se tiene una cola para impresión llamada REPORT$PRINTER y dos colas para trabajos en BATCH, llamadas SYBASE$BATCH (para uso del manejador de bases de datos del ACSE, esto es, SYBASE) y SYS$BATCH la cual es la cola por defecto del sistema, en esta es donde entran los trabajos que un usuario trabaja en lotes.

Es importante mencionar que las colas que están definidas en el ACSE, se encuentran en cada BAP (VAX 4000-105A). Desde cada máquina se pueden administrar.

3.3.3 Trabajos de impresión por el sistema operativo VMS

Una impresora es controlada por un proceso llamado SYMBIONT si está asociada con una cola. Con relación a una impresora se puede:

- Tener una impresora y enviarle datos interactivamente con el comando COPY (copia).

- Tener una impresora y enviarle datos desde un programa utilizando para ello el comando WRITE (escribe).

- La última opción y la más utilizada es usando el comando de VMS llamado PRINT (imprime).

Los comando COPY y WRITE (copia y escribe) tienen algunas desventajas. Si se tiene en el sistema de cómputo un número limitado de impresoras, el usuario tendría que esperar hasta que se disponga de una, esto llevaría a serios problemas de tiempo si se tienen varios usuarios. Además no se tiene la capacidad de controlar la impresión de trabajos dependiendo del tamaño o importancia de éstos. Se imprime el trabajo que llegó primero.

Los problemas anteriores se resuelven en parte por las colas de ejecución para trabajos de impresión. Para ello el comando PRINT (imprime) es utilizado, este causa que el proceso QUEUE_MANEGER tome su lugar en una cola. El sistema entonces decide cuándo y en dónde se realizará un trabajo de impresión. Las colas de impresión solucionan problemas de tiempo y calendarización.

En la figura 3.6 se muestran los procesos JOB_CONTROL y un SYMBIONT (el cual indica que existe un trabajo de impresión). Esta salida se obtiene con el comando SHOW SYSTEM (muestra sistema).

VAX/VMS V5.5-2H4 on node MEBAPB 2-SEP-1995 19:01:22.13 Uptime 6:00:01:05

Pid	Process Name	State	Pri	I/O	CPU	Page flts	Ph.Mem
20200201	SWAPPER	HIB	16		0 00:00:01.59	0	0
2020020C	OPCOM	HIB	8	69	0 00:00:00.59	420	178
2020020E	JOB_CONTROL	HIB	8	14	0 00:00:00.19	179	338
20200213	NETACP	HIB	9	166	0 00:00:01.70	157	398
20200214	SYMBIONT_1	HIB	5	6912	0 00:00:00.56	307	204
20200214	EVL	HIB	6	16	0 00:00:00.11	131469	88
20200215	LES$ACP	HIB	10	14	0 00:00:00.28	383	601
20200237	BAPSYS_01	LEF	9	2624	0 00:00:13.71	29168	286
202002A8	BAPSYS_03	CUR	4	38	0 00:00:01.19	6872	584

Figura 3.6 Procesos JOB_CONTROL y SYMBIONT

3.3.4 Calendarización de los trabajos de impresión

Después de que los trabajos son puestos en una cola utilizando el comando PRINT, el proceso QUEUE_MANAGER calendariza dichos trabajos usando:

- **Prioridad**

  Un trabajo con una prioridad alta es ejecutado primero. La prioridad de los trabajos en colas está limitada por dos parámetros: el primero de ellos es el que define la prioridad del trabajo y se llama DEFQUEPRI (Define Queue Priority), la prioridad por defecto para todos los trabajos de impresión es de 100 y es asignada por el Sistema Operativo VMS; el segundo parámetro define la máxima prioridad dentro de un rango de 0 a 255, se llama MAXQUEPRI (Maximium Queue Priority).

- **Tamaño del trabajo**

  Los trabajos pequeños de impresión son ejecutados antes que los más grandes (dentro de la misma prioridad de grupo).

- **Sumisión de Tiempo**

  Los trabajos son ejecutados en orden de sumisión de tiempo, esto es, se ejecuta un trabajo aleatoriamente si es que ellos tienen el mismo tamaño y la misma prioridad de ejecución.

3.3.5 Creación de Colas de Impresión

Para crear una cola de impresión se establecen los siguientes puntos:

- Instalar los atributos físicos del dispositivo, en nuestro caso los de una impresora, para ello se utiliza el comando SET PRINTER.

- Inicializar y arrancar la cola de ejecución para cada dispositivo de impresión.

- Inicializar y correr la cola genérica de impresión.

Se pueden crear y arrancar colas de impresión con los comandos que se muestran a continuación:

- **INITIALIZE/QUEUE (nombre de la cola).** Crea la cola. Si la cola está corriendo, este comando no la afecta. Si existe la cola pero está detenida, se utiliza este comando para modificar los parámetros de dicha cola de impresión. Este comando es muy utilizado en las impresoras del ACSE, debido a la carga de trabajo que ellas tienen, por lo mismo, en algunas ocasiones se salen de línea las impresoras y en ese momento hay que inicializarlas.

- **START/QUEUE (nombre de la cola).** La función de este comando es poner a funcionar de nueva cuenta una cola de impresión que hubiera estado detenida. Si la cola está trabajando correctamente, solamente se despliega un mensaje de error en pantalla.

3.3.6 Monitoreo de las colas de impresión y BATCH

El Administrador del Sistema debe periódicamente examinar el estado de las colas dadas de alta en su sistema, para detectar fallas como el que una impresora esté en mal estado, que un trabajo en BATCH haya entrado en un ciclo (LOOP), etc. El Sistema Operativo VMS proporciona un comando para poder verificar el estado de las impresoras y de las colas de trabajos en lotes (BATCH), dicho comando es SHOW QUEUE (muestra colas).

SHOW QUEUE despliega el estado de las colas del sistema así como todos los trabajos en cada una de dichas colas de trabajo, la información se muestra en orden alfabético. Este comando tiene varios calificadores, los cuales nos permiten obtener información adicional de cada cola:

- **/BY_STATUS=ESTADO**

  Despliega el tipo estado en que se encuentran los trabajos, Los tipos son ejecución (EXECUTING), contenidos (HOLDING), pendientes (PENDING), retenidos (RETAINED) y de actualización de tiempo (TIMED_RELEASE).

- **/BATCH**

  Despliega el estado de las colas BATCH.

- **/GENERIC**

  Muestra el estado de las colas genéricas del sistema de cómputo VAX.

- **/SUMMARY**

  Despliega el total de trabajos, indicando el estado de cada uno de ellos.

- **/FULL**

  Muestra toda la información relacionada con las colas tanto de impresión como BATCH.

Los códigos de estado más comunes de las colas en un sistema VAX son:

- **Dispositivo no válido.** Indica que el dispositivo al cual ha sido asignado el trabajo no responde.

- **Pausa.** El comando STOP/QUEUE (detener cola) ha sido ejecutado desde una terminal.

- **Detenida.** La cola de impresión o BATCH no está trabajando. Se aplicó el comando STOP/QUEUE a la cola en este estado.

- **Ocupada.** La cola no puede procesar trabajos adicionales porque uno o más trabajos están en proceso.

- **Cerrada.** La cola no aceptará trabajos hasta que se abra de nuevo.

- **Idle.** La cola está esperando por trabajos para su procesamiento.

- **Remota.** La cola está asignada a un dispositivo que no está conectado al sistema local.

- **Stalled.** El procesamiento de la impresión se ha detenido por causa de que haya ocurrido un problema en el dispositivo de salida.

3.3.7 Monitoreo del estado de los trabajos en cola

El Administrador del Sistema puede monitorear el estado de los trabajos en cola. El Sistema Operativo VMS cuenta con el comando SHOW ENTRY (muestra entrada) para checar dicho estado. El formato es :

$SHOW ENTRY [número de trabajo]

Con número de trabajo nos referimos al número que el sistema asigna a un trabajo cuando este entra para su procesamiento a una cola. Por ejemplo si se especifica SHOW ENTRY 200, se obtienen las características del trabajo número 200.

Los trabajos en cola presentan entre otros, cualquiera de los siguientes estados :

- **Abortado.** La ejecución de un trabajo está terminando.
- **Ejecución.** El trabajo se está ejecutando desde una cola BATCH.
- **Almacenado (holding).** El trabajo está contenido en el sistema hasta que se libera para su ejecución.
- **Almacenado hasta (holding until).** El sistema contiene el trabajo en cola hasta que se cumpla determinada cantidad de tiempo.
- **Pendiente.** El estado del trabajo es de espera.
- **Imprimiendo.** El trabajo de impresión se está ejecutando en una impresora o terminal.
- **Stalled.** Se tiene un problema en el dispositivo donde se estaba ejecutando el trabajo en cola.

Debido al uso frecuente de las impresoras en el ACSE, el monitorear los trabajos es importante para obtener el estado de ellos. En ocasiones las colas de impresión están detenidas por alguna falla en la impresora o por el atascado de papel, esto provoca que los trabajos en cola queden pendientes o en algún otro estado de los antes mencionados, si por alguna razón el Administrador del Sistema no se percata de ello a través de un monitoreo general, se tienen situaciones conflictivas a nivel de usuarios por la obtención de cada uno de sus trabajos o por la posible pérdida de estos. En la figura 3.7 se tiene la salida del comando SHOW ENTRY.

```
Batch queve EXE1, idle, on MEBAPB:

Generic batch queve GENERICA
Terminal queve REPORT$PRINTER, stalled, on MEBAPB::LTA:, mounted form DEFAULT

Entry       Jobname         Username        Blocks      Status

47          VAX1            BAPSYS              3       Aborting
49          VAX1            BAPSYS              3       Pending

Batch queve SYSBASE$BATCH, idle, on MEBAPB::

Batch queve SYS$BATCH, idle, on MEBAPB::
```

Figura 3.7 Comando show entry

3.3.8 Atributos de las colas de impresión

VMS asigna atributos (características) a cada cola de trabajo cuando es creada, tales atributos son :

- **Dueño.** Toma por defecto como dueño al usuario que crea el proceso de la cola.

- **Prioridad Base.** Se refiere al papel que ocupará el trabajo cuando está con otros para poder ejecutarse primero o después.

- **Definición de la forma de impresión.** Son la características de presentación de la impresión en papel.

- **Código de protección.** Permisos para que usuarios del sistema tengan o no acceso a la cola de trabajo.

Se pueden anular los atributos que una cola de impresión toma por defecto y definir así una configuración personal cuando el Administrador del Sistema lo prefiera. El comando SET QUEUE/[calificador] [nombre de la cola] permite hacer modificaciones, por ejemplo para especificar el tamaño mínimo y máximo de los archivos a procesar en una cola de impresión se utiliza el calificador /BLOCK_LIMIT=(tamaño mínimo, tamaño máximo). También se pueden definir nuevos atributos tales como :

- Separación de las páginas en los trabajos de impresión.
- El número mínimo y máximo de trabajos en una cola de impresión.
- Características de la impresora.

3.3.9 Borrado de una cola de impresión

Borrar una cola de impresión significa eliminarla del sistema de cómputo VAX en el cual esté definida. Antes de borrar una cola de impresión se debe de parar su uso, para ello se utiliza el comando STOP/QUEUE/NEXT, después de esto se procede al borrado de dicha cola.

En el siguiente ejemplo se elimina la cola de impresión llamada IMP_1, se puede observar como se detiene su uso :

```
$STOP/QUEUE/NEXT IMP_1
$DELETE/QUEUE IMP_1
```

Si lo que se desea borrar es solamente un trabajo que esté en la cola de impresión VMS cuenta con el comando DELETE/ENTRY (borra entrada) para efectuar tal operación, no importa que dicha cola esté procesando información o esté en alto total. Para entender este comando consideremos el ejemplo siguiente, en el cual se elimina el trabajo número 715 :

```
$DELETE/ENTRY= 715
```

3.3.10 Problemas asociados con impresoras

En un sistema de cómputo los problemas relacionados con el equipo de impresión son muy comunes, ejemplos de ellos son :

- Papel atascado en el periférico.
- Cintas atoradas o densidad de impresión pobre.

Cuando se presentan problemas como los anteriores las impresiones se detienen cuando aún no se han concluido, pero existe un comando de VMS que permite la recuperación de impresiones después de alguna falla, la instrucción es START/QUEUE/BACKWARD (empezar desde atrás), en el siguiente ejemplo se indica al sistema que reinicialice la impresión dos páginas atrás, inmediatamente después se inicializa la cola de impresión IMP_1:

```
$START/QUEUE/BACKWARD = 2 IMP_1
$START/QUEUE
```

3.3.11 Manejo de los trabajos BATCH en VMS

Cuando se ejecuta un trabajo en una consola de modo interactivo, no se pueden introducir más comandos a menos que dicho trabajo se haya terminado o de que se tengan suficientes consolas para seguir operando. Para esto las colas BATCH optimizan el uso de terminales, consolas y otros dispositivos manteniendo en ellas procedimientos a ejecutarse.

El comando SUBMIT se encarga de colocar en las colas BATCH los trabajos destinados a ellas. Las operaciones que se pueden realizar sobre una cola BATCH son similares a las de una cola de impresión, excepto en las de creación y parado.

Para crear una cola BATCH VMS proporciona el siguiente comando, en este se inicializa una cola llamada BATCH_1.

```
$INITIALIZE/QUEUE/BATCH/START BATCH_1
$SUBMIT LOGIN.COM
```

La instrucción SUBMIT LOGIN.COM pone en la cola creada para el sistema, el procedimiento (es un programa con determinadas funciones) LOGIN.COM, el cual se ejecutará según se haya definido en el mismo programa.

Para detener la ejecución de una cola BATCH se aplica el comando STOP/QUEUE (detener cola) y para detener la ejecución de un trabajo se utiliza STOP/ENTRY (para entrada).

3.4 Monitoreo del Sistema Computacional del ACSE

El monitoreo de un sistema de cómputo es una de las principales responsabilidades del Administrador del Sistema. Monitoreo de un sistema significa observar y obtener el estado de actividad de dicho sistema, desde el punto de vista de sus recursos como lo pueden ser la memoria, el CPU, los accesos a disco, las líneas de comunicación en red, etc.

El Sistema Operativo VMS cuenta con una utilería llamada MONITOR, la cual permite realizar al Administrador del Sistema la tarea de monitorear el sistema de cómputo, además desde el comando SHOW se puede obtener información para que al igual que la utilería anterior el Administrador interprete o analice varios de los estados de desempeño del sistema de cómputo, contenidos en reportes y gráficas.

3.4.1 Utilería MONITOR

Para desplegar información acerca del uso de los recursos del sistema de cómputo del ACSE, el Sistema Operativo VMS provee una herramienta de trabajo llamada MONITOR (monitoreo). Para accesar a ella se introduce el siguiente comando:

```
$MONITOR
MONITOR>
```

Estando en el PROMPT MONITOR, el usuario puede introducir distintos comandos para realizar cualquiera de las tareas siguientes:

- Despliegue de determinada información
- Ejecutar procedimientos
- Estadísticas del uso de recursos en determinado período de tiempo
- Obtener ayuda de la utilería
- Salir de la utilería

3.4.2 Monitoreo del sistema del ACSE

El monitoreo del sistema de cómputo del ACSE se realiza ocupando la utilería MONITOR, también se utiliza el comando SHOW proporcionado por VMS. Es importante para el desempeño de los procesadores principales del ACSE (BAPs), verificar el estado del CPU, de la memoria y de las entradas y salidas de dispositivos, para ello desde el PROMPT de MONITOR se introduce el comando MONITOR SYSTEM (Monitoreo del Sistema) el cual nos despliega informacón relacionada con los recursos antes mencionados. En la figura 3.8 se muestre una salida típica del monitoreo de los recursos del ACSE de una de las VAX principales.

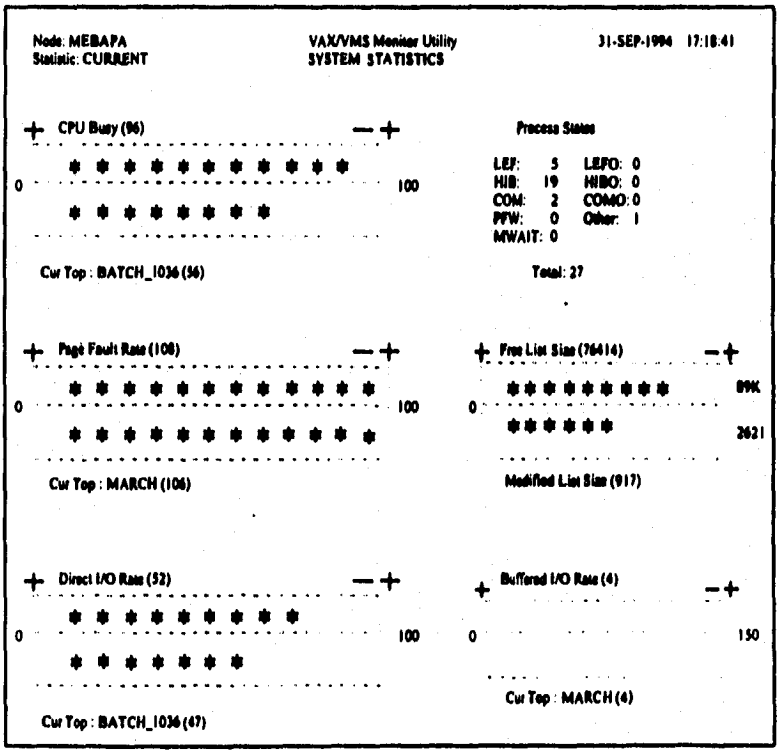

Figura 3.8 Monitoreo del sistema VAX del ACSE

El monitoreo del sistema es regular, esto significa que se realiza cada determinada cantidad de tiempo (cada 3 segundos por defecto, a partir de que se introduce el comando). El Administrador del Sistema tiene la responsabilidad de estar verificando constantemente a través de MONITOR o SHOW el estado de las computadoras de ACSE, la salida la puede tener en una terminal o bien se puede direccionar a un archivo para después mandarlo a impresión. Se pueden automatizar este tipo de procedimientos utilizando para ello programas que se ejecuten cada determinada cantidad de tiempo (en una cola BATCH).

3.4.3 Monitoreo de procesos

Para observar el comportamiento de los procesos de la VAX, el Administrador del Sistema ejecuta el comando MONITOR PROCESSES (Monitoreo de Procesos). La salida que se obtiene se actualiza cada 3 segundos, un ejemplo de ella es la obtenida en la figura 3.9 que se muestra a continuación :

```
$ MONITOR PROCESSES/TOPCPU

                        VAX/VMS Monitor Utility
                    TOP CPU TIME PROCESSES
                          on node MEBAPB
                      03-SEP-1996 19:13:54

                      0        25        50        75        100

21200524 BATCH_1036   78  ********************
21200646 J_WARTEN     9   ***
2120083F WATTEWS_I    3   *
```

Figura 3.9 Monitoreo de procesos

3.4.4 Monitoreo de un sistema VAXCLUSTER

Con el comando MONITOR CLUSTER, el administrador del sistema obtiene estadísticas de los recursos del VAXCLUSTER (CPU, memoria y disco). En la figura 3.10 presentamos la información relacionada con uno de los BAPs del ACSE.

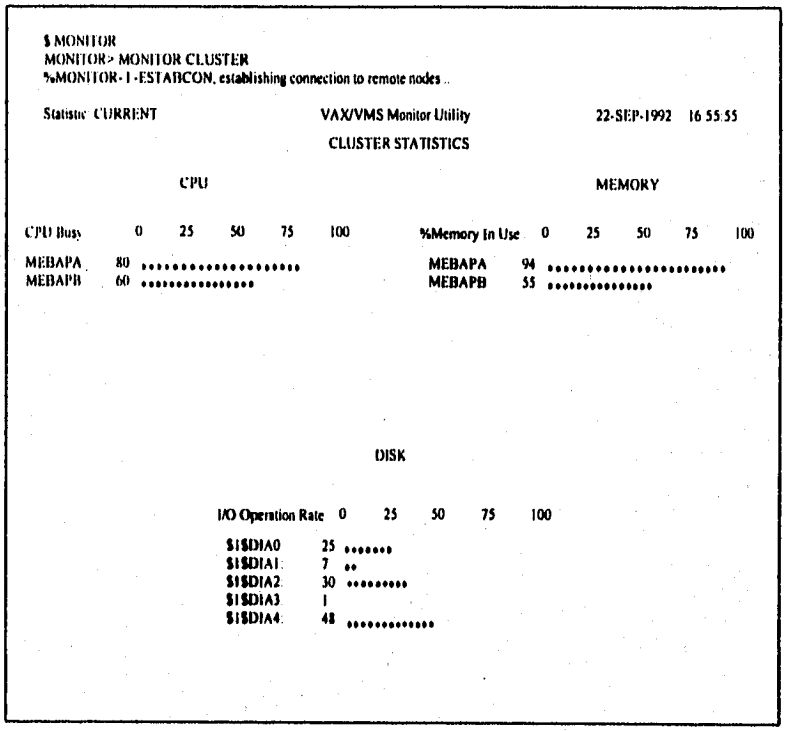

Figura 3.10 Monitoreo de un sistema VAXCLUSTER

3.4.5 Monitoreo de DECnet

El comando MONITOR DECNET se utiliza para obtener la información relativa al desempeño de la red. Obtenemos características tales como el arivo y recepción de paquetes de información.

3.4.6 Monitoreo de los discos del ACSE

El monitoreo de los Discos del ACSE se lleva a cabo con el comando MONITOR DISK, con el obtenemos estadísticas como la que se muestra en la figura 3.11

```
$SHOW DEVICE D

Device                  Device            Error  Volume          Free  Trans
Name                    Status            Count  Label           Blocks  Count
DSA1:                   Mounted               0  USER01          232644      1
$1$DIA0:        R5X2FI  Mounted               0  MEBAPA_SYS      327360      1
$1$DIA1:        R1WBEI  ShadowSetMember       0  (member of DSA1:)
$1$DIA2:        R1CTQI  Mounted               0  QUORUM          176874      4
$1$DIA3:        R1VBAH  ShadowSetMember       0  (member of DSA1:)
$1$DIA4:        R5WI2I  Mounted               0  MEBAPB_SYS      332349    316
$1$DKA400:      MEBAPB  Online                0
```

Figura 3.11 Monitoreo de los discos del ACSE

3.4.7 Procedimientos de VMS para Monitoreo

El Sistema Operativo VMS tiene 3 archivos ejecutables que permiten mejorar la tarea de Monitoreo para el Administrador del Sistema. Dichos archivos son tres, los cuales son descritos a continuación:

- **SUBMON.COM**

  Ejecuta un procedimiento de comandos llamado MONITOR.COM y es automáticamente instalada cuando se arranca el Sistema Operativo.

- **MONITOR.COM**

  Es una colección de datos y envía un reporte en cada petición de monitoreo que se le haga.

- **MONSUM.COM**

  Envía 2 diferentes tipos de reportes, uno por un período de 24 horas, y otro por el tiempo principal de uso del Sistema. Para ejecutar este programa se tiene que realizar de forma manual.

3.4.8 Monitoreo del ACSE con el comando SHOW

El Sistema Operativo VMS permite a través del comando SHOW (mostrar) monitorear el estado del sistema de cómputo desde la línea de comandos de VMS, para ello este comando, tiene distintos calificadores los cuales se analizan a continuación:

- SHOW SYSTEM (Mostrar Sistema)
- SHOW MEMORY (Mostrar memoria)

SHOW MEMORY (Mostrar memoria)

El buen desempeño de un equipo de cómputo radica en el hecho de cuánta memoria física contiene. El Sistema Operativo VMS provee un comando llamado SHOW MEMORY, el cual despliega información acerca de la memoria física de la VAX en cuestión (en el caso del ACSE, de los BAPs). Es muy importante correr este comando varias veces al día para verificar y asegurar que por cuestiones de memoria no fallará el sistema o al menos para tomar las acciones correspondiente para poder evitarlo (eliminar los procesos que estén provocando alguna situación de este tipo).

Con el comando SHOW MEMORY se presenta información relacionada con:

- Memoria Física Libre
- Entrada para Procesos (entry slots)
- Balance Set Slots
- Fixed-size Pool Areas
- Memoria para Paginación

Memoria Física Libre

Se tiene el tamaño de memoria sin uso en el sistema y que está disponible para que sea ocupada por los procesos que la requieran. Si esta memoria fuera menor a cien bloques entraría a actuar un proceso llamado SWAPING, el cual consiste en ejecutar la tareas destinadas a la memoria física en un medio de almacenamiento destinado para ello (disco duro de la VAX), con la característica de que toda la aplicación se realizará sobre el disco.

Entrada para procesos (entry slots)

Indica con la opción FREE (libre) el número adicional de procesos que pueden ser creados en la VAX. Si se presentara un cero, ya no puede entrar al sistema otro usuario y por lo tanto no pueden ser creados procesos nuevos (ni por los usuarios que ya estén trabajando en el sistema).

Balance set slots

En esta categoría se tiene el número de procesos adicionales que pueden entrar en un proceso de SWAP. Si se tiene un cero en procesos libres, en el balance set slots manda a SWAP si es que hay disco disponible.

Fixed-size pool areas

Este tipo de memoria es utilizada por los dispositivos de entrada y salida. Si llegara a ser cero cualquier valor de esta opción, el sistema la incrementa.

Memoria para paginación

Punto muy importante ya que si faltara este tipo de memoria el sistema puede dejar de efectuar tareas relacionadas con el procesamiento de la información del ACSE (baja totalmente el desempeño del equipo de cómputo), lo cual implicaría que el sistema de cómputo se alentara y por consiguiente este podría llegar a fallar totalmente sin responder a ningún comando. Se tienen un archivo para el manejo de la paginación llamado PAGEFILE.SYS, el cual puede estar almacenado en un disco duro de la VAX.

En el ACSE se tenían problemas relacionados con el archivo de PAGEFILE.SYS, porque se agotaba cada determinado tiempo, el sistema se tenía que parar totalmente para eliminar todos los procesos que se hubieran estado ejecutando en ese momento. La solución fue incrementar el tamaño de dicho archivo para que fuera ocupado por los procesos que lo requirieran. En la figura 3.12 se presenta una corrida de este comando relacionada con uno de los equipos del ACSE.

```
$ SHOW MEMORY

System Memory Resources on 31-SEP-1993 11:07:03.
Physical Memory Usage (pages):      Total     Free     In Use      Modified
    Main Memory (16.00Mb)           32768     23954    8516        298

Slot Usage (slots):                 Total     Free     Resident    Swapped
    Process Entry Slots             30        11       19          0
    Balance Set Slots               27        10       17          0

Fixed-Size Pool Areas (packets):    Total     Free     In Use      Size
    Small Packet (SRP) List         640       102      538         96
    I/O Request Packet (IRP) List   328       96       232         176
    Large Packet (LRP) List         39        19       20          1648

Dynamic Memory Usage (bytes):       Total     Free     In Use      Largest
    Nonpaged Dynamic Memory         643584    36512    607072      30272
    Paged Dynamic Memory            205312    75600    129712      74480

Paging File Usage (pages):                                Free      Reservables   Total
    DISK$CDCDA_SYS:[SYSD.SYSEXE]SWAPFILE.SYS              15000     15000         15000

    DISK$CDCDA_SYS:[SYSD.SYSEXE]PAGEFILE.SYS              23636     -6941         30000

0 of the physical pages in use, 3976 pages are permanently allocated to VMS
```

Figura 3.12 Monitoreo de la memoria de la VAX con SHOW MEMORY

SHOW SYSTEM (Mostrar Sistema)

El comando SHOW SYSTEM muestra todos los procesos que están en el momento de ejecutarse, en el sistema VAX. El monitorear los procesos ayuda al Administrador del Sistema a detectar algún proceso que esté en algún estado que no sea conveniente para el ACSE, por lo tanto el Administrador tomará la decisión a realizar con dicho proceso (eliminarlo por ejemplo).

La información que se despliega con este comando es el identificador del proceso (el cual sirve para hacer referencia de un proceso, como para eliminarlo o suspender su ejecución), el nombre del proceso, el estado del proceso, la prioridad del proceso, tiempo de CPU, etc.

3.4.9 Monitoreo del VAXCLUSTER del ACSE

Para la revisión de un VAXCLUSTER el Sistema Operativo VMS proporciona el comando SHOW CLUSTER para desplegar información relacionada con este ambiente de trabajo VAX. Se tienen dos tipos de presentación de la información relacionada con un VAXCLUSTER:

- Despliegue estático (SHOW CLUSTER, mostrar cluster), con este comando se presenta en la pantalla el estado del VAXCLUSTER al momento de ejecutar el comando.

- Despliegue dinámico (SHOW CLUSTER/CONTINUOUS, mostrar información continua del cluster), la información presentada se lleva a cabo cada determinada cantidad de tiempo.

En la figura 3.13 se tiene la salida estática del comando SHOW CLUSTER, en ella se tiene el estado de los BAPs del ACSE, si se llegara a presentar que alguno de ellos no es miembro del VAXCLUSTER se tendrían problemas de redundancia ya que el ACSE ejecuta una alarma auditiva cuando sucede algún problema relacionado con los procesadores principales.

```
$ SHOW CLUSTER

        View of Cluster from system ID 1025    node: MEPAPB    23-SEP-1990  15:08:33

SYSTEM                          MEMBERS
NODE        SOFTWARE
MEBAPA      VMS V5.4            MEMBER
MEBAPB      VMS V5.5            MEMBER
```

Figura 3.13 Comando SHOW CLUSTER

CAPITULO 4

Rendimiento del Sistema de Cómputo del ACSE

CAPITULO 4

Rendimiento del Sistema de Cómputo del ACSE

El Administrador del Sistema VAX del ACSE debe de procurar que el rendimiento o desempeño del equipo sea lo más óptimo posible, esto es, que el control de los recursos con que se cuenta sea eficiente, eficaz y suficiente para efectos de operación de los servicios de comunicación móvil satelital, en términos de computación nos referimos específicamente a la memoria, CPU y a los dispositivos de entrada/salida (impresoras, discos, terminales, etc.).

4.1 Factores que afectan el rendimiento de un sistema

Los principales factores que afectan el rendimiento de un sistema de cómputo VAX son los siguientes, en orden decreciente de importancia:

- Diseño del Sistema
- Configuración del Sistema
- Diseño de la Aplicación

Diseño del sistema

El Diseño del Sistema se refiere a cómo fue implantado el sistema desde el punto de vista del ambiente de procesamiento de la información, ya que puede estar totalmente automatizado o bien puede ser operado por el personal de la organización, esto es, existiría un proceso manual de operación. En el caso del ACSE se pueden presentar ambas opciones, ya que el sistema puede quedar trabajando sin ayuda humana (estado automático), pero en caso de que existan algunas alarmas importantes el personal adecuado tiene que actuar de manera inmediata para solucionar el problema presentado.

Es importante mencionar que aunque un sistema sea altamente confiable, como lo es el caso del equipo de cómputo VAX del ACSE, es indispensable contar con personal que supervise dicho sistema, porque a partir de esto se puede obtener la experiencia necesaria para conocer el comportamiento de dicho sistema.

Configuración del sistema

La configuración del sistema se basa fundamentalmente en el tipo de componentes y características que se tengan de hardware, esto es, la velocidad del CPU, tamaño de la memoria, medio de comunicaciones, controladores de entrada/salida inteligentes, espacios para futuras expansiones, etc.

El equipo VAX 4000 modelo 105-A del ACSE (recordar que se trata de equipo redundante, esto es, existen dos máquinas principales) presenta las características siguientes :

- La Unidad Central de Proceso (CPU) de la VAX 4000 es modelo KA53, la cual trabaja con un reloj de 333 MegaHertz.
- Contiene controladores para memoria, discos, puertos y ethernet.
- Soporta comunicaciones síncronas y asíncronas a través de puertos especiales.
- La memoria con que se cuenta es de 128 Megabytes (Mb).
- Soporta discos con capacidad de almacenamiento de 381Mb, 852Mb, 1.6Gb (Gigabytes), 95Mb, 320Mb y hasta 4.0Gb. En el ACSE se cuenta con las dos primeras capacidades de almacenamiento.

Diseño de la aplicación

El diseño de la aplicación se refiere al tipo de software que va a ejecutarse sobre la VAX para realizar una tarea determinada, intervienen aspectos tales como el diseño de archivos, manejo de las estructuras de datos, algoritmos de procesamiento, etc.

El tipo de aplicación del ACSE es un software para monitoreo y control de todo el procesamiento de la información que interviene en el manejo de las comunicaciones móviles de MOVISAT, se consideran aspectos como los siguientes : administración de los usuarios del sistema (bases de datos), almacenamiento de los mensajes (para fines de entrega a un usuario final y para su facturación), sistema operativo, software de red, etc.

4.1.1 Administración del rendimiento del sistema

Para comenzar a administrar el desempeño de un sistema de cómputo se pueden elaborar diseños de pruebas de los recursos del sistema (como por ejemplo simular cargas de trabajo sobre el CPU, la memoria y los dispositivos de entrada/salida), las cuales serán implementadas y monitoreadas por el Administrador del Sistema y así se obtendrá un análisis confiable para tomar decisiones de afinación o mejora.

La afinación se refiere a las modificaciones que se le efectúen al sistema de cómputo y que afecten el rendimiento de este (no se consideran cambios a la configuración del hardware, sino a los parámetros del sistema). La afinación es un proceso que se va realizando conforme al uso del sistema de cómputo, ya que no se realiza de un momento a otro. La mejora que se puede obtener de una afinación realizada, va de un cinco a un diez por ciento.

El sistema operativo VMS provee un programa llamado AUTOGEN que ayuda al Administrador a realizar cambios en los parámetros del sistema (el programa AUTOGEN se localiza en el directorio SYS$UPDATE), entre sus funciones está la determinación de los recursos de hardware, el manejo de los parámetros del sistema, creación de listas con las imágenes a instalar, calcula el tamaño de las páginas y áreas de swap (memoria en disco).

Los parámetros del sistema controlan funciones del mismo tales como la administración de la memoria y de los dispositivos de entrada/salida y del control de la ejecución de procesos (tiempos de CPU). Los parámetros que pueden ser ajustados son:

- Colas BATCH
- Sistema de Archivos (su tamaños y su localización)
- El Archivo de Autorización de Usuarios (UAF)
- Los tamaños de los archivos y sus localidades

4.1.2 Medidas del desempeño

Una medida del desempeño es un aspecto simple que permite la comparación del rendimiento del sistema de cómputo entre dos eventos en el tiempo. El Administrador del Sistema debe de utilizar las medidas de desempeño para evaluar el rendimiento de las computadoras (hardware) y de las entidades de datos (software) de los cuales se encarga. Existen tres categorías dentro de las medidas del desempeño computacional:

- Suficiencia
- Eficiencia
- Eficacia

Cada una de las características anteriores se detallan a continuación:

Suficiencia

Relaciona la carga de trabajo que se presenta en un sistema con la capacidad de los recursos de cómputo (memoria, CPU y dispositivos de entrada/salida) del mismo. En este sentido se plantean dos preguntas:

- ¿Son adecuados los recursos de cómputo para la carga de trabajo que existe sobre ellos?

- ¿Están los recursos con capacidad para el exceso de trabajo?

Son dos cuestiones muy importantes porque si los recursos con que se cuentan son escasos o bien limitados en capacidad de respuesta para realizar el trabajo, no podremos desarrollar más de lo que nuestro sistema de cómputo ofrece, esto es, es peligroso aumentar la carga de trabajo a un sistema si este no cuenta con lo necesario para efectuar dicho trabajo.

Por ejemplo en el ACSE la capacidad de disco, la memoria y la velocidad en procesamiento son de vital importancia porque de no contar con lo suficiente de cada uno el procesamiento de información (mensajes) podría tener problemas en cuanto al uso de recursos, un caso de esto, considerando a los discos de almacenamiento, es el siguiente: a los usuarios de comunicaciones móviles vía satélite se les proporciona un espacio en disco para el almacenamiento de sus mensajes, únicamente se reparte el disco entre determinado número de usuarios y con un espacio específico, en caso de que hubiera demanda de este servicio se optaría por la adquisición de un nuevo disco. En caso de no hacerlo de la manera anterior los discos sufrirían un sobre-almacenamiento y por tanto se perdería información valiosa tanto para el ACSE como para el usuario.

Dentro de este contexto, en el ACSE cuenta con los recursos de cómputo necesarios para soportar todo el procesamiento generado por MOVISAT, está diseñado para expansiones futuras desde el punto de vista de comunicaciones y cómputo.

Eficiencia

La eficiencia se define como la facultad para lograr un efecto determinado. En cómputo se considera sobre el cómo los recursos serán utilizados para realizar su trabajo. Esta medida incluye:

- La utilización del recurso, el cual se está consumiendo. Por ejemplo el uso de una impresora, con el tiempo pierde poder de trabajo y su desempeño empieza a decrecer.

- Costo del procesamiento, se refleja en dinero el poder procesar más rápidamente los datos en un sistema de cómputo.

Consideramos Importante que a los recursos de cómputo del ACSE (computadoras y periféricos) se les debe de proporcionar un mantenimiento preventivo, para evitar en lo mayor posible fallas posteriores. Se propusieron dos mantenimientos anuales a todo el equipo, el resultado ha sido satisfactorio. En caso de que se presenten equipos dañados se cambian total o parcialmente, por ejemplo si el CPU de una VAX se daña, el cambio que se realiza es parcial ya que sólo se cambia la tarjeta madre, lo contrario sucede con una unidad de disco la cual se cambiaría totalmente.

Eficacia

La eficacia se define como la fuerza y poder para realizar un trabajo determinado, para ello hay que conocer la demanda de trabajo que se tiene para el sistema de cómputo. La medida de la eficacia está integrada por:

- Tiempo de respuesta, es el intervalo de tiempo que se tiene entre la ejecución de un comando (una instrucción a realizar por el sistema) y la respuesta que ofrece el sistema cuando se ha completado la tarea.

- Cantidad de trabajo por unidad de tiempo, por ejemplo un programa corriendo o transacciones procesadas.

- Turnaround (vuelta), es el intervalo de tiempo entre la ejecución de un trabajo en BATCH y su puesta en la cola.

Dependiendo del lugar de la organización o empresa se le dan a las medidas de desempeño ciertas prioridades:

- En un centro de datos (banco de información) la suficiencia y la eficiencia representan dinero, por tanto la prioridad de estas medidas es alta, tal es el caso de MOVISAT ya que se cuidan estas características para obtener ganancias sobre el servicio que se presta.

- El personal de un lugar en donde se efectúen operaciones (control de datos), cuidará de la eficacia y la eficiencia de los recursos con que se cuenta.

- Para usuarios finales de un sistema de cómputo es muy importante la eficacia de sus recursos.

4.1.3 Recursos del sistema

Cada componente de un sistema puede ser considerado como un recurso, básicamente los recursos de un sistema de cómputo son:

- Memoria
- CPU (Unidad Central de Proceso)
- I/O (Dispositivos de Entrada/Salida)

El desempeño o rendimiento de un recurso está determinado por:

- **Capacidad.** Velocidad a la cual un recurso puede desempeñar un trabajo.

- **Demanda.** Cantidad de trabajo solicitada por el recurso, incluyendo la velocidad a la cual el recurso responde al trabajo y la distribución del trabajo en el tiempo.

Un recurso que ha alcanzado su capacidad de trabajo entra en un estado de saturación. Para comprender esta idea ponemos el ejemplo de lo que sucede cuando se tienen varios procesos ejecutándose en la memoria del sistema de cómputo y se cuenta con el espacio en disco de almacenamiento que está destinado para ser ocupado como una extensión de la memoria física puede llegarse a saturar este espacio por la ocupación del mismo (mucha carga de trabajo).

En la gráfica de la figura 4.1 se muestra la relación entre la demanda y el tiempo de respuesta en un sistema de cómputo. En las computadoras del ACSE se ha comenzado a obtener este tipo de gráficas desde el punto de vista de la computadora como tal (hardware) y del software (bases de datos y programas de usuarios). Hasta ahora el comportamiento que se ha tenido es muy estable, ya que la demanda de procesamiento no ha sido muy alta por características mismas del sistema.

Conforme a la demanda que se tenga, en nuestro caso A (demanda baja), B (demanda media) y C (demanda alta) el tiempo de respuesta será menor para una demanda baja y mayor para una demanda alta, en este último caso la capacidad del recurso puede llegar a su límite.

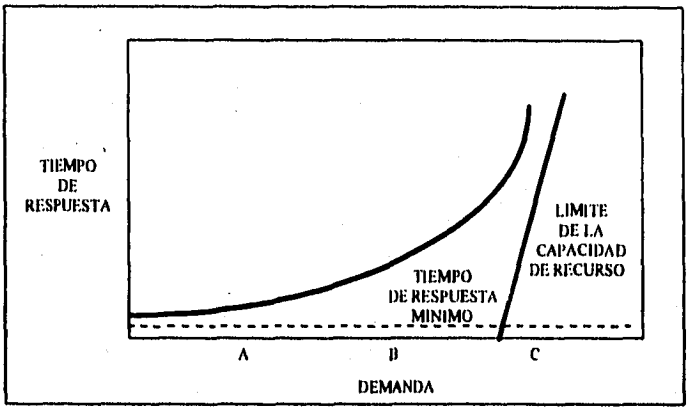

Figura 4.1 Relación entre el tiempo de respuesta y la demanda en un sistema de cómputo

Analizaremos el comportamiento de un sistema de cómputo con múltiples recursos. La limitación de un recurso llega a la saturación si la demanda de trabajo hacia éste aumenta. Observemos la gráfica de la figura 4.2 en ella se muestran los tres recursos básicos de un sistema de cómputo: memoria. CPU y dispositivos de E/S (entrada/salida). El tiempo de respuesta de la memoria es alta en comparación con los otros dos recursos cuando se tiene demanda de trabajo.

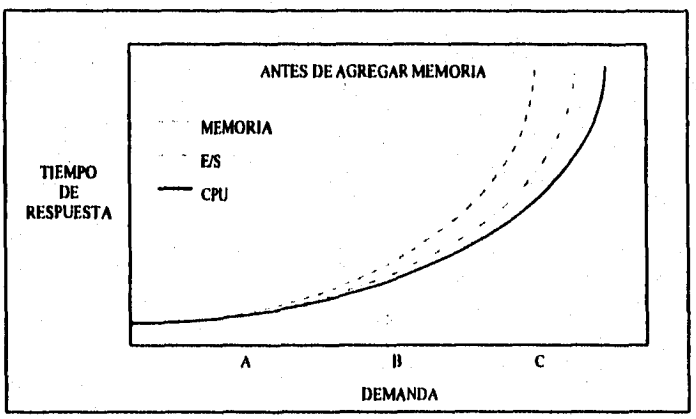

Figura 4.2 Relación demanda/tiempo de respuesta con recursos limitados de memoria

Ahora consideremos que la memoria fue aumentada debido a la situación presentada en el caso anterior, dado que se tiene más recurso de memoria el tiempo de respuesta será menor cuando la demanda de trabajo vaya siendo cada vez más alta, en la figura 4.3 se observa este comportamiento con más detalle.

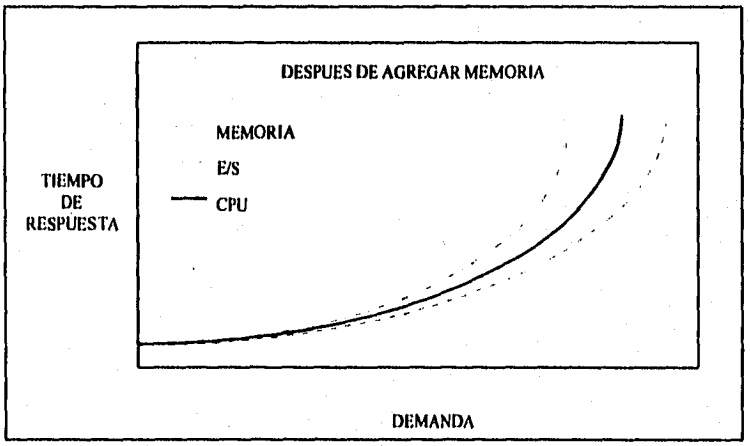

Figura 4.3 Relación demanda/tiempo de respuesta después de agregar memoria al sistema

Con relación a la cantidad de trabajos corriendo (programas o transacciones) en un sistema de cómputo por unidad de tiempo, con memoria limitada y con aumento de memoria se presentan las situaciones siguientes:

Cuando la memoria está limitada se llega a un estado en el cual aunque la demanda sea grande no se entregarán resultados de los trabajos (figura 4.4), aunque como lo muestra la gráfica se tienen recursos de CPU y de dispositivos de E/S.

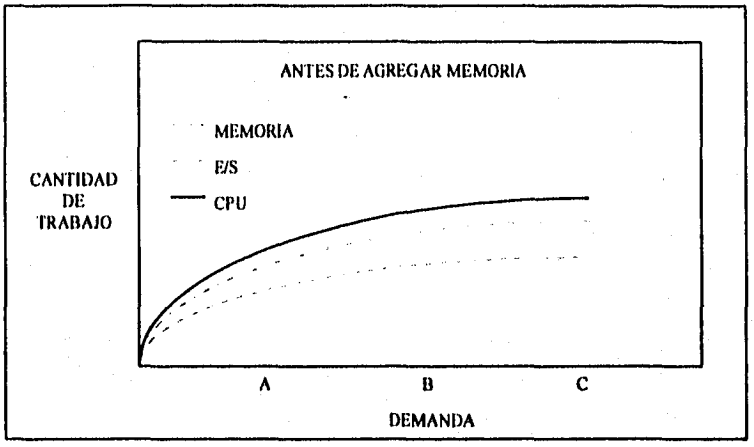

Figura 4.4 Relación demanda/cantidad de trabajo con memoria limitada

Si la memoria se expande (caso anterior) el sistema responderá positivamente, esto se observa claramente en la gráfica de la figura 4.5, en donde ahora los recursos de CPU y dispositivos de E/S quedan limitados, se dispone de memoria para satisfacer la demanda.

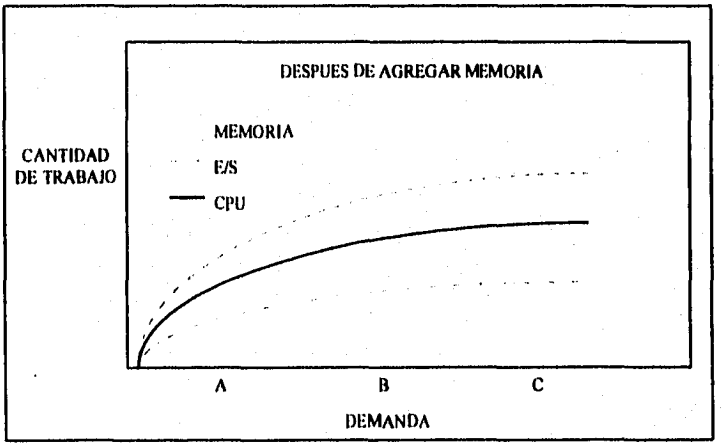

Figura 4.5 Relación demanda/cantidad de trabajo con memoria expandida

.4.1.4 Mejora del desempeño de un sistema saturado

Existen tres caminos para enfrentarse con un sistema que está saturado (estado de embotellamiento):

- Incrementar la capacidad los recursos que están limitados.

- Reducir la demanda del recurso limitado, esto es, correr lo menos posible trabajos o usuarios del sistema y también se podría considerar un rediseño de la aplicación que estemos utilizando.

- Pasar la demanda de un recurso limitado a otro recurso, a este proceso se le conoce con el nombre de descarga de trabajo.

Se ha implementado dentro del esquema de administración del ACSE, tener un registro confiable del estado de los recursos como memoria, CPU, discos, unidades de cinta, impresoras, etc. Se lleva a cabo mediante listados de texto (en los cuales se muestran los resultados obtenidos a partir de los comandos de monitoreo del sistema) generados desde una consola de administración (terminal VT420) durante dos veces al día, además se realiza de manera personal una revisión constante.

4.1.5 Controlando recursos de entrada/salida

El desempeño de un disco depende principalmente de la configuración del hardware que se tenga y del tipo de disco. Existe un concepto en VAX llamado fragmentación del disco, el cual se explica a continuación.

- **Fragmentación del disco**: El espacio libre en disco se dividé en muchas áreas pequeñas en lugar de una sola área contigua, esto no ocasiona problemas de desempeño y permite la fragmentación de archivos.

- **Fragmentación de archivos:** Se tiene cuando a un archivo se le divide en múltiples extensiones pequeñas en lugar de que ocupe un espacio largo, puede ocasionar muchas operaciones de Entrada/Salida.

4.1.6 Controlando recursos de memoria

El sistema operativo VMS es un sistema multiusuario y utiliza el concepto de Memoria Virtual. El SO es el responsable de calendarizar el uso de los recursos del sistema tales como la memoria y el CPU.

4.1.6.1 Memoria física y memoria virtual

La memoria física es aquella que reside en la computadora en un dispositivo electrónico, y es ocupada para almacenar la información que será procesada por la máquina.

La memoria virtual permite la ejecución de procesos cuando sólo algunas partes de sus espacios de direcciones están residentes en memoria principal, esto es, permite la ejecución de programas o imágenes que no residen completamente en memoria física. La parte del programa que no está en memoria es almacenada sobre un disco, esta acción es transparente para el usuario.

4.1.6.2 Espacio de direcciones virtuales

El Espacio de Direcciones Virtuales bajo VMS tiene las siguientes características:

- Cada octeto (byte) de memoria es individualmente direccionable
- El primer byte es localizado con la dirección cero
- La memoria virtual está dividida en páginas de 512 octetos
- Las páginas virtuales son numeradas comenzando con el VPN 0 (Virtual Page Number)
- Las páginas virtuales son almacenadas sobre disco

El espacio de direcciones virtuales del sistema operativo VMS está dividido en:

- Espacio del sistema
- Espacio de procesos
- Espacio de direcciones físicas

Espacio del sistema

En esta parte se encuentran los servicios que el sistema operativo VMS ofrece, el registro de administración del sistema (RMS, Record Management System), así como el código y datos de VMS.

Espacio de procesos

En este espacio se tienen los programas de ejecución, librerías, procesos para el control de la información y el lenguaje intérprete de comandos.

Espacio de direcciones físicas

El espacio de direcciones físicas es el conjunto de direcciones sobre memoria física y varia de una arquitectura a otra, presenta las características siguientes:

- La memoria física está dividida en páginas de 512 octetos
- Las páginas son numeradas con el PFN 0 (Page Frame Number)
- Un programa puede tener más páginas virtuales que páginas físicas
- Cada proceso tiene una porción de páginas virtuales de memoria física

4.1.7 Paginación y swapping

Existen dos métodos usados por el sistema operativo VMS para administrar los recursos de memoria, ambos métodos ocupan uno o más discos para la extensión de la memoria física.

Paginación

La paginación es un esquema de control de memoria que suprime el requisito de asignación contigua de memoria física. La correspondencia de direcciones se emplea para mantener la ilusión de continuidad del espacio de direcciones virtuales de un proceso a pesar de su ubicación discontigua en memoria física.

Básicamente, la memoria física se divide conceptualmente en una serie de porciones de tamaño fijo, llamados marcos de página. El espacio de direcciones virtuales de un proceso se divide además en bloques de tamaño fijo del mismo tamaño llamados páginas. La asignación de memoria consiste en hallar un número suficiente de marcos de página sin utilizar para cargar en ellos las páginas del proceso solicitante. Para hacer corresponder las páginas virtuales con sus marcos de páginas físicos asociados se utiliza un mecanismo de traducción de direcciones. Puesto que cada página se hace corresponder separadamente, los diferentes marcos de página asignados a un solo proceso no necesitan ocupar áreas contiguas de memoria física. En la figura 4.6 se muestra el proceso de paginación.

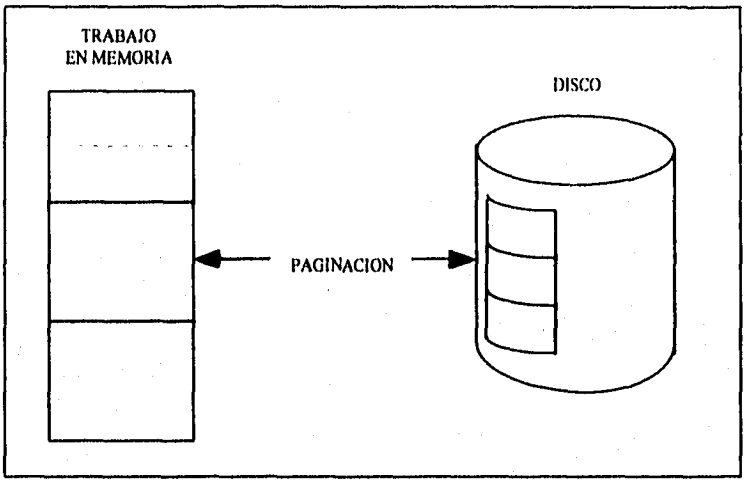

Figura 4.6 Proceso de paginación

Swapping

La palabra swapping literalmente significa cambiando, en el sistema operativo VMS se conoce así a la técnica usada para mover procesos que están trabajando desde la memoria física hasta un medio auxiliar de almacenamiento, como lo es un disco.

El swapping es requerido para permitir a un número grande de procesos compartir el sistema de cómputo cuando no todos ellos quepan en la memoria física.

Existe un proceso conocido como SWAPPER que se encarga de manejar el swapping. La diferencia entre paginación y swapping está en que la primera trabaja con páginas y el segundo con procesos.

En los sistemas VAX y por tanto en las computadoras principales del ACSE existe un archivo conocido con el nombre de SWAPFILE.SYS, el cual es un archivo especial almacenado en un disco y sirve para realizar el swapping entre la memoria física principal y el medio de almacenamiento, es controlado por el SWAPPER y creado bajo la dirección del Administrador del Sistema.

En la figura 4.7 se tiene un esquema de relación entre la memoria física con un determinado número de procesos y el medio de almacenamiento (disco) disponible para aceptar tales procesos.

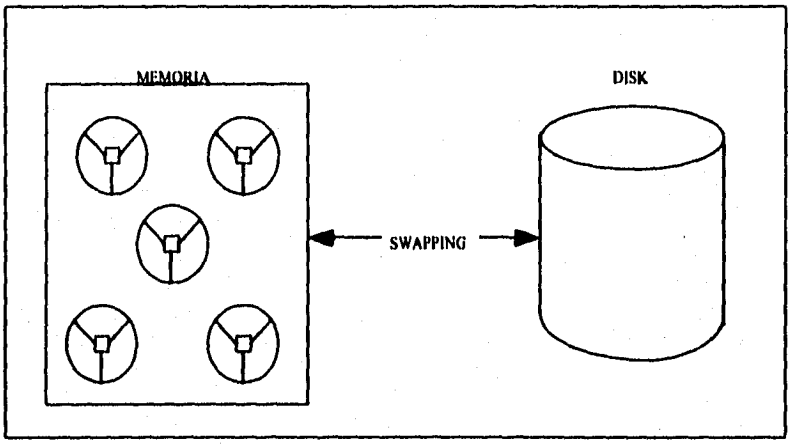

Figura 4.7 SWAPPING

4.1.8 Instalación de imágenes

El sistema operativo VMS cuenta con una utilería llamada INSTALL, la cual permite la instalación de elementos de software a un sistema de cómputo. Dicha utilería puede mejorar el desempeño de las imágenes (programas) cuando van a ser instaladas, especialmente cuando esas imágenes:

- Son ejecutadas frecuentemente
- Son accesadas de forma concurrente por varios usuarios
- Cuando requieran aumentar de privilegios para su uso

De cualquier modo, las imágenes instaladas consumen recursos de memoria y ellas también necesitan ser reinstaladas cuando el sistema se inicializa (cuando se da de baja al sistema de cómputo, lo que está almacenado en memoria se borra).

Los comandos para que las imágenes se instalen al momento de levantar el sistema (REBOOT) se localizan en un programa de inicio en el sistema operativo VMS que tiene por nombre SYS$MANAGER:SYSTARTUP_V5.COM, para poder instalar las imágenes con el comando INSTALL se utilizan los comandos CREATE (o bien ADD), por ejemplo:

$INSTALL CREATE [nombre de la imagen]

La instalación de una imagen crea un archivo de entrada conocido (KFE, known file entry) este se encuentra en una base de datos y ocupa arriba de 52 octetos (bytes) por imagen. Otro archivo conocido como RMS busca en esa base de datos y abre la imagen guardada en el KFE. Se cuenta con un calificador para el comando de instalación, llamado /HEADER_RESIDENT, el cual conserva la cabecera de la imagen residente en memoria (ocupa al menos 204 octetos (bytes) por cada cabecera de una imagen.

Para el equipo del ACSE es importante el monitoreo constante de las imágenes que están instaladas, para ello se usa el comando INSTALL, con el se presentará el prompt de la utilería, desde el cual se introduce el comando LIST/FULL (lista completa) y así se obtiene una lista de los programas instalados. Los comandos antes mencionados se dan de la manera siguiente:

```
$INSTALL
INSTALL> LIST/FULL
```

En la figura 4.8 se tiene una salida después de la ejecución del comando LIST/FULL desde INSTALL, se puede observar el directorio por defecto en donde se localizan los programas .EXE, la línea que dice conteo de entradas (Entry access count) indica que desde que el sistema fue iniciado (se realizó un BOOT), la imagen en cuestión ha tenido el número indicado de corridas. La parte que dice actual/compartición máxima nos muestra si el programa está siendo ocupado actualmente y también el número de veces que ha corrido simultáneamente. Con esta herramienta se puede detectar alguna imagen que esté en un ciclo infinito y que además está ocupando recursos de manera innecesaria.

```
$ INSTALL
INSTALL> LIST/FULL

DISK$VMSRL5:<SSO.SYSCOMMON.SYSEXE>.EXE

      .
      .
      .
        BACKUP;2          Open          Shar
        Entry access count                =21
        Current / Maximum shared          =0 / 21
        Global section count              =2

COPY;2  Open Hdr  Shar
        Entry access count                =1126
        Current / Maximum shared          =0 / 3
        Global section count              =2

DCL;2                     Open Hrd Shar          Lnk
        Entry access count                =950
        Current / Maximum shared          =0 / 7
        Global section count              =1

DECALC;1                  Open          Shar
        Entry access count                =5
        Current / Maximum shared          =0 / 4
        Global section count              =3

DECGRAPH;1                Open Hrd Shar
        Entry access count                =406
        Current / Maximum shared          =0 / 2
        Global section count              =1

EDT;1                     Open Hdr Shar
        Entry access count                =1469
        Current / Maximum shared          =0 / 13
        Global section count              =1

FORTRAN;2                 Open Hdr Shar
        Entry access count                =396
        Current / Maximum shared          =0 / 4
        Global section count              =2
      .
      .
      .
```

Figura 4.8 Comando LIST/FULL para el monitoreo de imágenes

Existen otros comandos dentro del sistema operativo VMS para obtener las imágenes que se procesan en la computadora.

Otra lista que puede ser obtenida desde el prompt de INSTALL es la que se puede observar en la figura 4.9, para ello se utiliza el comando LIST/GLOBAL (lista global), en orden de columnas se muestra la información siguiente:

- Nombre de la imagen (sección en este caso)
- Número de versión (en hexadecimal) y es un valor único
- Sección global permanente (PRM) creada por el comando INSTALL
- Número de páginas para esta sección
- Páginas utilizadas en el sistema global de imágenes

En la parte final se tiene el número global de secciones usadas (imágenes actuales) y el número global de páginas utilizadas junto con las páginas en uso en la memoria local del sistema.

```
INSTALL>LIST/GLOBAL
                        System Global Sections

BASICMSG_001    (63E2CDE4)  PRM     SYS     Pagcnt/Refcnt=61/0
PASCAL_001      (46F4425D)  PRM     SYS     Pagcnt/Refcnt=255/0
MONITOR_001     (12E48723)  PRM     SYS     Pagcnt/Refcnt=10/0
DECALC_001      (15B11F78)  PRM     SYS     Pagcnt/Refcnt=495/0
EDT_001         (12E3441E)  PRM     SYS     Pagcnt/Refcnt=41/0
DIRECTORY_001   (12E2A803)  PRM     SYS     Pagcnt/Refcnt=3/0
COPY_001        (12E31DDC)  PRM     SYS     Pagcnt/Refcnt=48/0
MAIL_001        (12E43548)  PRM     SYS     Pagcnt/Refcnt=133/266
```

Figura 4.9 Comando LIST/GLOBAL para el monitoreo de imágenes

El borrado de una imagen es conveniente cuando se han observado que existen programas instalados y que realmente no se están ocupando. Para eliminar una imagen se corre el comando siguiente:

$INSTALL DELETE [nombre de la imagen]

4.1.9 Controlando recursos de CPU

El controlador de trabajos (JOB CONTROL) permite el balanceo de los trabajos en lotes (BATCH) cuando una cola genérica está asociada con una o más colas de ejecución. Algunas de sus principales características son:

- Especialmente útil para sistemas VAXCLUSTERS y sistemas con diferentes nodos en los que se tengan colas genéricas.

- Cuando un trabajo sobre una cola genérica es calendarizado para su ejecución, el controlador de trabajos lo asigna a una cola de ejecución.

- Si las colas de ejecución existentes tienen la misma carga de trabajo, el controlador asigna el trabajo a realizarse a la primera cola de ejecución asignada por la cola genérica.

El manejo de los procesos en el sistema operativo VMS cae en 32 niveles de prioridad (figura 4.10), divididos en dos categorías:

- Procesos con tiempo compartido, los cuales abarcan prioridades con niveles que van desde 0 hasta 15.

- Procesos en tiempo real, con las prioridades restantes, esto es, de 15 a 31.

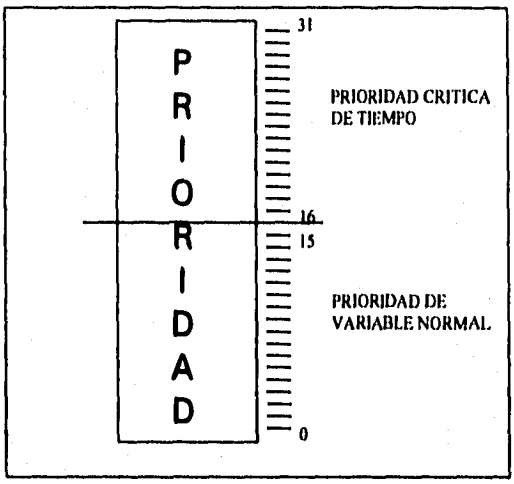

Figura 4.10 Prioridad de los procesos

4.1.10 Conceptos de calendarización

Desde que el procesador puede ejecutar instrucciones para un proceso en cualquier momento, el sistema operativo VMS calendariza (da cierto tiempo) a los procesos para su ejecución en el procesador. Esta actividad de calendarización tiene las siguientes características:

- Es llevada a cabo por el SCHEDULER (proceso de VMS).
- Los procesos son calendarizados utilizando la combinación de dos técnicas: por prioridades y por una parte de tiempo para cada proceso.

4.1.10.1 El Scheduler

El Scheduler es un proceso del sistema operativo VMS que tiene las siguientes características:

- Determina a qué proceso se le permitirá el uso de procesador (CPU) después de la ocurrencia de algún evento.

- Está basado en prioridades. El proceso con la prioridad más alta es el siguiente en ejecutarse, si el proceso que actualmente está en ejecución tiene prioridad más baja.

Se pueden tener procesos ejecutables residentes o no residentes (en el CPU). Como se menciona anteriormente existen 32 niveles de prioridades, la mitad de esas prioridades es asignada para procesos de tiempo crítico (tiempo real) y la otra parte para los procesos normales.

Los procesos en tiempo real ocupan del nivel 16 al 31, son aplicaciones muy delicadas que no pueden esperar tiempo extra, ya que pueden perjudicar algún proceso en el sistema de cómputo.

Los niveles de prioridad asignados a procesos normales, esto es, de 0 a 15 son usados para aplicaciones que pueden esperar cierta cantidad de tiempo (por ejemplo aplicaciones en BATCH).

4.1.10.2 Lógica de Calendarización

Para que un proceso se pueda ejecutar se cumple lo siguiente:

- Cada proceso tiene una prioridad actual y se fundamenta en una prioridad base.

- El sistema operativo VMS ejecuta dinámicamente los cambios en prioridad en respuesta a ciertos eventos que pueden ocurrir en el proceso.

- Los niveles actuales de prioridad nunca pueden ser menores a una prioridad base.

- El proceso con la prioridad más alta es el próximo a ejecutarse.

- Si un proceso se está ejecutando y llega otro con prioridad más alta, el primero se va al final de la cola para que después continúe ejecutándose.

- Un proceso puede ser sacado del CPU varias veces incluso hasta que alcance su objetivo final.

- Los procesos no residentes en memoria y los de alta prioridad pueden ser forzados para que tengan prioridades más bajas. Y los procesos residentes en memoria pueden dejar de serlo.

4.1.11 Ajustando límites de CPU

Si se presentaran problemas de CPU en un sistema de cómputo se pueden tomar decisiones como las siguientes:

- Añadir otro CPU del mismo tamaño o bien agregar alguno con características mejoradas para así evitar embotellamientos (estado de saturación).

- Si lo anterior no es posible, quizá por cuestiones tecnológicas o meramente económicas, existen otros caminos para poder resolver la situación de demanda de CPU.

- Con la herramienta AUTHORIZE se pueden modificar o instalar los límites para el uso del CPU, con el comando MODIFY/CPUTIME=[tiempo], con el cual se le especifica a un usuario determinado el máximo de tiempo en CPU que puede ocupar, si se le especifica un tiempo igual a cero indicará al sistema que el tiempo de uso de CPU para el usuario será infinito.

- Restringir horas de acceso a los usuarios al sistema de cómputo. Para realizar esta actividad se utiliza el comando de la herramienta AUTHORIZE llamado MODIFY/NOACCESS. Por ejemplo: MODIFY/NOACCESS=(PRIMARY, 18-8, SECONDARY, 9-17), permite el acceso de 9 AM hasta las 6 PM en los días primarios (días definidos por el Administrador del Sistema) y después de las 6 PM hasta las 9 AM en días secundarios.

4.1.12 Modos usados dentro del sistema operativo VMS

Los modos usados en la arquitectura del sistema operativo VMS son los siguientes:

- Modo kernel
- Modo de ejecución
- Modo de supervisor
- Modo usuario

Modo kernel

Es el modo con más privilegios sobre el sistema y en el se localizan las funciones del sistema operativo, como pueden ser una pila de tiempo de interrupciones, se lleva a cabo la sincronización para efectos de multiprocesamiento, actividades de manejo de memoria y dispositivos de entrada/salida, etc.

Modo de ejecución

Se encuentra el código del VAX RMS, el cual se encarga de ejecutar comandos y emitir posibles errores.

Modo de supervisor

En esta parte se encuentra el lenguaje de comandos de DIGITAL en un nivel primario, para así llegar al modo de usuario.

Modo usuario

Se tienen más comandos (DCL), aplicaciones de software y utilerías para ser utilizadas por un usuario. Es el modo por defecto.

En la figura 4.11 se muestra un diagrama con los componentes y modos de acceso del sistema operativo VMS.

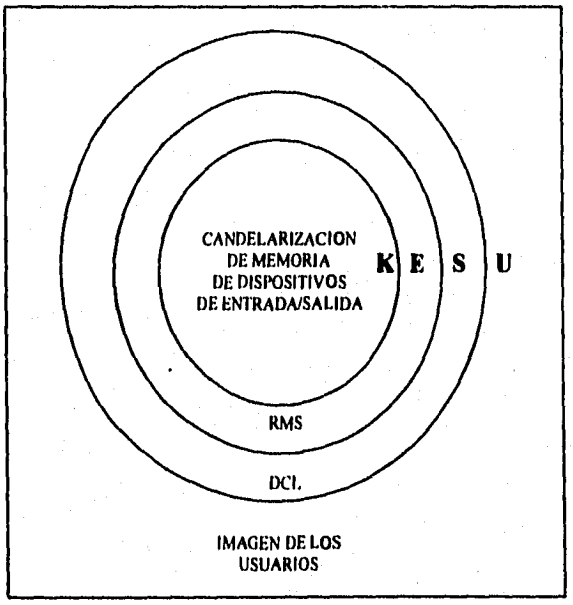

Figura 4.11 Componentes y modos de acceso de VMS

Con el comando MONITOR MODES se puede obtener una estadística en donde se muestra el estado de los modos de VMS, en la figura 4.12 se tiene una gráfica en la cual se presenta el uso de los modos de un sistema de cómputo (en nuestro caso los BAPs del ACSE).

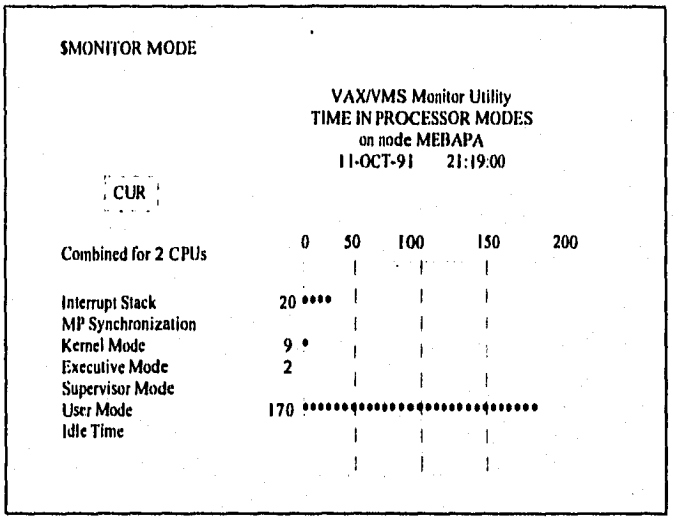

Figura 4.12 Comando MONITOR MODES

CAPITULO 5

Seguridad del Sistema Computacional del ACSE

CAPITULO 5

Seguridad del Sistema Computacional del ACSE

La seguridad es el conjunto de medidas tomadas para protegerse contra robos, ataques, crímenes y espionajes o sabotajes. Por lo tanto la seguridad es contar con medidas de protección para quedar cubierto frente a contingencias adversas.

El uso creciente y la confianza en las computadoras en todo el mundo ha echo surgir una preocupación legítima con respecto a la seguridad informática. El uso de las computadoras se ha extendido en ambientes comerciales, telecomunicaciones, educacionales, gubernamentales, militares e incluso en los hogares. Grandes cantidades de datos son almacenados cada vez más en computadoras. Entre ellos se incluyen registros sobre individuos (médicos, financieros, bancarios), negocios (activos, inventarios, contabilidades, nóminas, personal, datos de fabricación) y diferentes registros públicos y secretos gubernamentales y militares. Grandes transacciones monetarias tienen lugar diariamente en forma de transferencias electrónicas de fondos ; así mismo como notificaciones de propiedad intelectual y datos comerciales estratégicos son también almacenados, procesados y diseminados mediante computadoras. Entre ellos se incluyen diseños de nuevos productos, planes y estrategias comerciales, listas de clientes y datos de ventas, contratos legales y muchos otros.

El acceso, revelación o destrucción no autorizada de datos puede violar la privacidad individual. La corrupción de datos comerciales puede provocar pérdidas significativas y potencialmente catastróficas a las empresas. El problema potencial con las computadoras radica en que los recursos empleados para almacenar datos valiosos no suele venir acompañado de las medidas de gestión necesarias para prevenir la exposición a perder la información almacenada.

Por tanto, el uso de prácticas y políticas de seguridad adecuadas con frecuencia suele adaptarse después y no antes de confiar datos y activos a las computadoras. Esto tiende a crear ventanas de vulnerabilidad de las cuales pueden tomar provecho los salteadores. Además, algunos de los muchos beneficios de la computación pueden representar importantes debilidades de seguridad y posibles puntos de penetración en sistemas inadecuadamente diseñados.

Los sistemas informáticos y los diseñadores de software deberían preocuparse de los temas de seguridad e incorporar salvaguardias y mecanismos adecuados para reforzar las políticas de seguridad. Por otra parte, el uso de extensas medidas de seguridad puede aumentar el coste y restringir la utilidad, facilidad de uso y rendimiento de los sistemas informáticos.

5.1 Amenazas y objetivos de seguridad

Las principales amenazas a la seguridad percibidas por los usuarios y los proveedores de sistemas basados en computadoras incluyen:

- **Revelación no autorizada de la información**

  La revelación de información a entidades no autorizadas puede dar lugar a brechas en la privacidad y a pérdidas tangibles o intangibles para el propietario de la información. La revelación del número de tarjeta de crédito, del diseño de un producto patentado, de una lista de clientes, de una oferta de contrato o de datos militares estratégicos pueden ser utilizados por adversarios de muchos modos diferentes. Dependiendo de la naturaleza de la información en cuestión, las consecuencias del abuso pueden ir desde la simple inconveniencia hasta pérdidas catastróficas.

- **Alteración y destrucción no autorizada de la información**

  La alteración o destrucción no autorizadas de información que no pueda ser recuperada es potencialmente igual de peligrosa. Incluso sin fugas externas, la pérdida de datos vitales pueden afectar gravemente a una empresa.

- **Uso no autorizado de servicios**

  El uso no autorizado de un servicio puede dar lugar a pérdida de beneficios para el proveedor del servicio. Al igual que la mayoría de las otras formas de penetración en el sistema, pueden ser explotada para obtener acceso ilegal a la información. Incluso una penetración sin malas intenciones puede generar mala publicidad y disuadir a clientes potenciales.

- **Denegación de servicios a usuarios legítimos**

  La denegación de servicio implícita generalmente alguna forma de daño al sistema informático que da lugar a la pérdida parcial o completa del servicio prestado a los clientes legítimos. Una forma de denegación de servicio viene representada por programas que se autorreproducen y propagan, llamados gusanos informáticos. Aunque los gusanos no realizan directamente actos hostiles cuando invaden una computadora, tienden a consumir recursos hasta el punto de ahogar al sistema y dejarle inútil para proporcionar servicios normales a los usuarios legítimos. En varios casos de conocimientos público, los gusanos informáticos han sobrecargado y llevado a una parada virtual importantes redes informáticas. Incluso una pérdida temporal de servicio puede ser nociva si afecta a un sistema que de otro modo sería funcional en un momento crítico de operación. El daño de cualquier sistema de transacciones en línea, produce generalmente pérdidas ya que al menos temporalmente deja de rendir para el proveedor del servicio y posiblemente para sus clientes.

En principio el objetivo de la seguridad informática es prevenir y eliminar amenazas potenciales. En particular, un sistema seguro debería mantener la integridad, disponibilidad y privacidad de los datos. Es decir, los datos mantenidos por el sistema deberían ser correctos, disponibles y privados. Por lo que se refiere a la seguridad, la integridad de datos significa generalmente:

- Protección frente a modificaciones no autorizadas
- Resistencia a la penetración
- Protección frente a la modificación no detectada de datos

La corrección de datos es una noción más general que la seguridad, ya que suele implicar provisiones adicionales tales como fiabilidad de la entrada de datos y ausencia de errores en la manipulación. En relación con la seguridad, la disponibilidad de datos se interpreta generalmente en el sentido estricto de impedir denegación de servicio debido a influencias externas. La seguridad es una medida de la confianza en la obtención de los objetos establecidos.

5.2 Intentos de penetración

Existen numerosos modos y puntos de entrada por los cuales se puede intentar la penetración de un sistema informático. Algunos de los rnás conocidos son:

- **Terminal con sesión abierta**

  El terminal queda desatendido por el usuario. Un intruso puede acceder al sistema con acceso completo a todos los datos disponibles para el usuario legítimo cuya identidad asume

- **Contraseñas**

  Las contraseñas utilizadas para autorizar a los usuarios pueden ser obtenidas por intrusos con propósitos de acceso ilegal de varios modos, incluyendo la adivinación, el robo, la prueba y error y el conocimiento de contraseñas suministradas por vendedores para generación y mantenimiento de sistemas

- **Inspección**

  Con frecuencia, los usuarios pueden ser capaces de descubrir información a la que no tienen autorización para acceder simplemente inspeccionando los archivos del sistema. En muchos sistemas existen archivos que disponen de controles de acceso inadecuados o demasiado permisivos

- **Puertas cepo**

  Se trata de puntos secretos de entrada sin autorización de acceso. Los diseñadores de software las prepara a veces, presumiblemente para permitirles a ellos acceder y posiblemente modificar sus programas después de la instalación y puesta en uso. Las puertas cepo pueden ser objeto de abusos por alguien que conozca su existencia y el procedimiento de entrada.

- **Escucha electrónica**

  Puede conseguirse mediante conexiones de intercepción pasiva o activa o mediante captura electromagnética de la radiación de pantalla

- **Mutua confianza**

Una programación demasiado confiada o poco cuidadosa puede llevar a dejar de comprobar la validez de los parámetros transferidos. En consecuencia, un invocado puede obtener acceso no autorizado a información protegida. Otros descuidos incluyen el paso de parámetros por frecuencia en vez de por vales. En este caso, un programa de usuario puede invocar al sistema operativos con punteros a parámetros que residen en el espacio del usuario. Tras pasar la verificación efectuada por el sistema operativo, el usuario puede sustituir rápidamente los valores originales por otros no autorizados. La ejecución consiguiente de la rutina del sistema puede entonces ser aprovechada para obtener acceso no autorizado a información que debería estar protegida.

- **Caballos de Troya**

Una programación puede ocultar intencionadamente parte de su funcionalidad, con frecuencia dañina, con el fin de pasar datos o los derechos de acceso del usuario de alguien más. Es posible escribir un sencillo programa caballo de Troya para robar contraseñas de usuario imitado el programa legítimo de apertura de sesión (log-in) y reproduciendo fielmente la secuencia y diálogos de presentación normal. Un programa caballo de Troya es especialmente fácil de implantar en sistemas en donde los terminales se hallan en recintos públicos, dejando una copia activa en una terminal y haciendo que simule la pantalla de presentación/despedida.

- **Gusanos informáticos**

Estos programas pueden invadir las computadoras, generalmente a través de una red, y denegar servicio a los usuarios legítimos utilizando cantidades desproporcionadas de recursos de procesamiento y comunicación para su autopropagación.

- **Virus informáticos**

  Los virus son trozos de códigos que infectan a otros programas y con frecuencia realizan actividades dañinas, tales como eliminar archivo o corromper el bloque de arranque de un disco.

- **Prueba y error**

  La potencia de procesamiento de una computadora puede ser utilizada por un intruso que pretenda entrar al sistema para automatizar repetitivamente la apertura de sesión y descifrar de la contraseña, o tratar de descubrir las claves de mensajes o contraseñas mediante prueba y error.

- **Búsqueda de basura**

  La búsqueda en la basura puede ser utilizada para descubrir contraseñas o escudriñar los archivos, volúmenes y cintas suprimidos. En muchos sistemas, el borrado de los archivos se efectúa actualizando las entradas de los directorios y devolviendo los bloques de datos al espacio de bloques libres. Es posible reconstruir información útil revisando los bloques libres.

5.3 Políticas y mecanismos de seguridad

Las políticas de seguridad especifican qué es lo que se desea en términos de protección y seguridad. Los mecanismos de seguridad especifican cómo llevar a la práctica las políticas de seguridad y cómo hacerlas cumplir en un sistema determinado.

El objetivo principal de los sistemas operativos y del software de sistemas es proporcionar un conjunto de mecanismos de seguridad flexibles y funcionalmente completos con el fin de posibilitar a los usuarios y propietarios de la información a hacer cumplir políticas de seguridad como mejor les convenga

5.3.1 Políticas de seguridad

Las políticas de seguridad han estado presentes desde que la acumulación de los primeros datos de valor necesitaron protección. Generalmente engloban procedimientos y procesos que especifican:

- Cómo se puede introducir y sacar información del sistema
- Quién está autorizado a acceder a qué información y bajo qué condiciones
- Cuáles son los flujos permisibles de información dentro del sistema

Pueden imponerse limitaciones adicionales, tales como restringir consultas de base de datos que afecten a conjuntos demasiado largos o demasiado pequeños, para reducir el peligro de deducir datos por interferencia estadística. Las políticas de seguridad suelen estar guiadas por los antiguos principios de:

- Mínimo privilegio
- Separación de deberes
- Rotación en roles

Mínimo privilegio

Cada sujeto debería tener permitido acceso únicamente a la información esencial necesaria para completar las tareas que el sujeto esta autorizado a realizar.

Separación de deberes

Si hay un conjunto de operaciones que pueden poner en riesgo una organización, debería exigirse que dos o más personas con intereses contrapuestos estuviesen implícitas en ellas. Expresando sencillamente, deberían ser necesarias dos personas con dos llaves diferentes para abrir la caja de caudales.

Rotación en roles

Las operaciones delicadas no deberían ser confiadas permanentemente al mismo personal; una cierta rotación en las responsabilidades es mas probable que descubra incorrecciones.

La elección de una política de seguridad adecuada para una instalación dada y para datos específicos dentro de ella conlleva generalmente a un compromiso entre el riesgo percibido de exposición, la perdida potencial debida a la perdida o exposición de la información y el coste de proporcionar un nivel especifico de seguridad. El proceso consiste en la evaluación del riesgo y la valoración del costo, el cual incluye el costo adicional del equipo y personal y la reducción del rendimiento debido a la implementación de medidas de seguridad.

Una vez cubierto el análisis, se definen las políticas de seguridad apropiadas. La mayoría de las políticas de seguridad relativas a computadoras pertenecen a una de las categorías básicas:

- **Control de acceso discrecional (CAD)**

  Estas políticas son generalmente definidas por el propietario de los datos, quien puede transferir derechos de acceso a ortos usuarios.

- **Control de acceso obligatorio (CAO)**

  Las restricciones de acceso obligatorio no están sujetas a la discreción del usuario y por lo tanto limitan al daño que un caballo de Troya puede causar. En este esquema, los usuarios se clasifican de acuerdo con niveles de autoridad o autorización. Los datos se clasifican en clases de seguridad según el nivel de confidencialidad, y se definen reglas estrictas respecto a que nivel de autorización se requiere para acceder a los datos de una clase de seguridad especifica.

Las políticas de seguridad que tienen en cuenta amenazas tanto externas como internas son muy importantes en tornos que gestionan datos críticos, ya que la mayoría de las incorrecciones las originan los usuarios internos.

5.3.2 Mecanismos de seguridad y principios de diseño

Las medidas de seguridad incluyen el control y la monitorización de los accesos físicos a las instalaciones físicas de las computadoras además de la seguridad interna del sistema informático. La seguridad física o externa incluyen técnicas estándar de vallados, vigilancia, validación y monitorización de presencia. En áreas especiales se pueden imponer restricciones adicionales de acceso. El administrador del sistema tiene el control sobre el nivel de seguridad que se haya implementado en el sistema a su cargo.

La seguridad física también puede incluir medidas para recuperación frente a desastres, que con frecuencia suponen la replicaron de datos críticos y/o equipos en localizaciones geográficamente dispersas para minimizar la exposición a las consecuencias de desastres tales como el fuego o la inundación.

Los temas de principal preocupación para los diseñadores de sistemas operativos, es decir, en los mecanismos de seguridad interna que proporcionan la base para la implementaron de políticas de seguridad. Los principios generales de diseño para mecanismos de protección son:

- Mínimo privilegio
- Separación de privilegios
- Mínimo mecanismo común
- Economía de mecanismo
- Mediación completa
- Valores predeterminados seguros
- Diseño abierto
- Aceptabilidad del usuario

Mínimo privilegio

Cada sujeto debería utilizar el mínimo grupo de privilegios necesarios para completar su tarea. Este principio limita el daño ocasionado por los ataques de caballos de Troya. Aboga efectivamente por el soporte de pequeños dominios de protección y la conmutación de dominios cuando haya que modificar el acceso.

Separación de privilegios

Cuando sea posible, el acceso a objetivos debería depender de la satisfacción de mas de una condición.

Mínimo mecanismo común

Esta estrategia aboga por la minimización de la cantidad de mecanismos comunes a y dependientes de múltiples usuarios. Las implicaciones sobre el diseño incluyen la incorporación de técnicas para mantener separados a los usuarios, tales como la separación física en maquinas diferentes dentro de sistemas distribuidos.

Economía de mecanismo

Mantener el diseño tan sencillo como sea posible facilita la verificación y la corrección de las implementaciones.

Mediación completa

Cada petición de acceso para cada objeto debería conllevar la comprobación de autorización. El mecanismo de comprobación debería ser eficiente ya que tiene una gran influencia sobre el rendimiento del sistema.

Valores predeterminados seguros

Los derechos de acceso deberían ser adquiridos solo con permiso explícito, y el valor por defecto debería ser la falta de acceso.

Diseño abierto

El diseño del mecanismo de seguridad no debería de ser secreto y no debería depender de la ignorancia de los atacantes.

Aceptabilidad del usuario

El mecanismo debería ser fácil de usar de modo que sea aplicado correctamente y no rehuido por los usuarios.

Los mecanismos de seguridad de sistemas informáticos incluyen la validación, el control de acceso, el control de flujo, las auditorias y la criptografía.

5.4 Validación

El objetivo principal de la validación es permitir acceso a los usuarios legítimos del sistema y denegarlo a los no autorizados. Las dos principales medidas de efectividad de la validación son: la tasa de falsas aceptaciones, es decir, el porcentaje de usuarios ilegítimos erróneamente admitidos, y la tasa de falsos rechazos, es decir, el porcentaje de usuarios legítimos a los que se deniega acceso debido a un fallo en el mecanismo de validación.

La validación unidireccional se basa generalmente en:

- **Posesión de un secreto (contraseña)**

  La contraseña es el mecanismo de validación más común basado en la compartición de un secreto. En sistemas basados en contraseña, cada usuario tiene una contraseña, que puede ser inicialmente asignada por el sistema o por un administrador; muchos sistemas permiten a los usuarios cambiar posteriormente sus contraseñas. El sistema almacena todas las contraseñas de usuario y las utiliza para validarlos. Cuando un usuario inicia su sesión, el sistema solicita y el usuario suministra una contraseña presumiblemente secreta y especifica.

- **Posesión de un artefacto**

  Los artefactos comúnmente utilizados para la validación de usuarios incluyen bandas legibles por máquina (generalmente con bandas magnéticas) y varios tipos de tarjetas electrónicas inteligentes.

- **Características fisiológicas o de compartimiento específicas del usuario**

  En este grupo se consideran características fisiológicas del usuario, tales como huellas, patrones capilares en la retina, geometría de la mano, características faciales, dinámica de firma, patrón de voz y temporización de pulsación de tecla.

5.5 Protección de sistemas informáticos

El motivo original de los mecanismos de protección surgió con la aparición de la multiprogramación. La intención era confinar el programa de cada usuario en su área asignada de memoria y así impedir que los programas traspasaran y dañaran otras área. Dado el creciente deseo de compartir objetos en memoria principal y secundaria, se idearon mecanismos más complejos para el control de acceso.

La protección en memoria principal va unida generalmente a la traducción de direcciones. Su objetivo es permitir que procesos residentes concurrentes y potencialmente sospechosos compartan el espacio común de direcciones físicas en la memoria principal. En sistemas con asignación contigua de memoria, la protección se obtiene generalmente con ayuda de algún tipo de registros límite. Cuando se carga el programa, se preparan los registros límite para que especifiquen la extensión de su espacio de direcciones legítimo. En tiempo de ejecución, cada referencia a memoria es preexaminada para verificar que se encuentre dentro de los límites. En caso contrario, se deniega el acceso a memoria y se genera una excepción que activa el mecanismo de protección. La protección se asegura haciendo que la modificación de los registros límite sea una operación privilegiada que solo puede ser ejecutada cuando la maquina esta operando en el estado supervisor privilegiado.

5.6 Seguridad de software en VAX

Para cubrir las necesidades básicas de seguridad de software, el administrador del Sistema debe de conservar los archivos SYSUAF.DAT, RIGHTSLIST.DAT y NETPROXY.DAT actualizados, usar banderas y restricciones de horario con la utilería AUTHORIZE, insistir en claves de acceso (passwords) no triviales, no publicar los números de las computadoras de la red, no dar acceso al archivo SYSUAF.DAT, utilizar códigos de protección en los archivos, restringir el uso del sistema con cuentas cautivas, restringir los privilegios de usuarios, crear reportes de las cuentas para checar el uso del sistema, etiquetar discos y cintas de una manera sistemática (ordenada).

Otros conceptos adicionales de seguridad que el administrador puede incluir son: claves de acceso secundarias, archivos de seguridad de entrada (LOGIN), auditorías de seguridad y alarmas en los archivos.

5.6.1 Seguridad en un sistema VAXCLUSTER

Un Sistema VAXCLUSTER debe ser tratado con un simple dominio de administración. Este debe ser administrado como un sistema simple, por un administrador o cooperando en un equipo de administración. Si un sistema VAXCLUSTER tiene diferentes ambientes de trabajo, los diferentes sistemas tienen accesos en común, comparten recursos y pueden ser guiados por una sola política de administración. Es importante considerar:

- Los privilegios de los usuarios de un nodo VAX pueden afectar a otros nodos.

- No existe una protección por defecto en los archivos de un nodo. El administrador del sistema puede implementar la protección adecuada, utilizando para ello las herramientas necesarias.

- Una red puede proveer gran seguridad aislada entre sus nodos, lo cual no sucede en un VAXCLUSTER.

- Un sistema implica nombres de usuarios, códigos de identificación de usuarios (UIC, User Identification Code) y permisos de acceso al Sistema.

5.6.2 Seguridad de archivos

A cada usuario es normalmente asignado un nombre de usuario y una clave de acceso en el archivo de autorización llamado SYSUAFT.DAT el cual es una Base de Datos que el Sistema Operativo VMS utiliza junto con la herramienta AUTHORIZE para la administración de los usuarios. El usuario cuando entra al sistema tiene que dar su nombre de usuario y su clave de acceso (password). Es posible que el password sea nulo y por lo tanto solo se debe introducir el nombre de usuario. Con la utilería AUTHORIZE se pueden dar de alta en la cuenta de un usuario las características siguientes:

- Una fecha de expiración de los registros del UAF
- La longitud mínima de la clave de acceso (contraseña)
- Fecha de expiración del password
- Se pueden definir claves de acceso secundarias sobre las cuentas

Cuando en el sistema VAX se da de alta una nueva clave de acceso se realiza automáticamente (si el administrador así lo desea) un proceso de verificación para que el Sistema Operativo acepte o no la nueva clave de acceso. Este proceso consiste en la búsqueda de la palabra correspondiente a la nueva clave de acceso en un Diccionario almacenado en el Sistema Operativo VMS, si la palabra ya existe, VMS no permitirá su inserción en el Sistema.

El proceso de búsqueda no indica que el Sistema Operativo pueda generar claves de acceso, esto solamente se puede llevar a cabo con la utilería AUTHORIZE.

5.6.3 Diccionario de claves de acceso en VMS

Como se mencionó anteriormente las claves de acceso son automáticamente checadas en un diccionario de claves de acceso del sistema operativo, para estar seguros de que la palabra no esta presente en dicho diccionario, el cual consiste de una lista (almacenada en un archivo que se encuentra en el directorio SYS$SYSTEM y se llama VMS$PASSWORD_HISTORY.DATA), formada por 100 claves de acceso que ya han sido utilizadas por cada cuenta de usuario, el diccionario está almacenado en un archivo sobre el Sistema Operativo VMS llamado SYS$LIBRARY.

Se puede deshabilitar el proceso de búsqueda con un bandera llamada DISPWDDDIC (Disenable Password Dictionary), la cual se enciende en la cuenta respectiva, con la herramienta AUTHORIZE.

5.6.4 Administración de claves de acceso

Si el sistema de cómputo necesita de protección de acceso, se requiere del uso de las claves de acceso (passwords). En algunas Organizaciones se llegan a implementar accesos con un esquema doble, esto es, con dos contraseñas se puede entrar al sistema.

Cuando se da de alta una nueva cuenta de usuario con la utilería AUTHORIZE , se especifica el nombre del usuario así como una clave de acceso inicial. Cuando se asignan claves de acceso iniciales de manera temporal, es recomendable hacer uso del Generador Automático de Claves de Acceso desde AUTHORIZE, se indica al sistema con el calificador /GENERATE_PASSWORD del comando ADD, al momento de dar de alta la cuenta. El sistema responde con una lista de las posibles claves, el administrador selecciona una de ellas y después se continúa con el proceso de alta de usuario.

Cuando se añade un nuevo usuario en el UAF, se puede definir que cuando el usuario entre por primera vez a su cuenta tenga que cambiar su clave de acceso, esto es, que la clave de acceso definida por el administrador del sistema expire (con el calificador /PWDEXPIRED en AUTHORIZE).

5.6.5 Claves de acceso del sistema operativo

Las Claves de Acceso del Sistema Operativo son usadas para controlar el acceso a terminales, considerando :

- Terminales usando líneas de comunicación o que interactúen con redes de computadoras que sean públicamente accesadas.
- Terminales que no sean inspeccionadas frecuentemente.
- Terminales dedicadas.

5.6.6 Protección de las claves de acceso

Es importante dar un mantenimiento continuo a las claves de acceso de un sistema de cómputo. Se recomienda :

- Mantener segura la clave de acceso de la cuenta SYSTEM, la cual es estándar en todos los sistemas VAX, es importante que sea modificada regularmente. En las computadoras del ACSE (BAP A y BAP B) es modificada cada mes por el Administrador del Sistema. Es de uso exclusivo y no se transmite la clave, solamente a gente estratégica como lo puede ser el encargado de las comunicaciones.

- Deshabilitar cuentas que no sean usadas, para evitar su mal uso. Se hace a través de una bandera llamada DIDUSER (desuso) con la herramienta AUTHORIZE.

- No permitir que gente del exterior, por ejemplo personal de mantenimientos preventivos, tenga cuentas exclusivas para sus servicios. Es recomendable dar de alta una e inmediatamente darla de baja del sistema.

- Mantener la protección de los archivos de autorización de usuarios. El archivo UAF debe de pertenecer a la cuenta SYSTEM.

5.6.7 Protección de archivos y directorios

El Sistema Operativo VMS ofrece dos mecanismos de protección de archivos para restringir el acceso a los archivos de determinado usuario y para prever el borrado de archivos y directorios.

El primero es el estándar y se basa en el Código de Identificación del Usuario (UIC, User Identification Code) y es aplicado a todos los usuarios de los archivos. El formato del UIC está definido entre paréntesis cuadrados de la siguiente forma : [GRUPO,MIEMBRO]. El grupo está dentro de un rango de 0 a 37777 en octal y pueden existir en un grupo miembros que van desde 0 hasta 177777, también en octal.

El sistema utiliza el UIC para determinar quien puede leer, escribir, ejecutar o borrar un archivo. Los usuarios están definidos de acuerdo a las categorías siguientes: SYSTEM, OWNER, GROUP y WORDL.

El segundo método que se utiliza para la protección de archivos es el de Listas de Control de Acceso (ACL, Access Control Lists), con este se da un nivel más refinado de protección de archivos. Pueden ser usadas independientemente del UIC.

Las ACLs son importantes herramientas de protección para los usuarios de VMS y generalmente son usadas donde se tienen sistemas de cómputo donde los requerimientos de seguridad son de niveles medio y alto. Predomina este esquema donde el nivel de compartición de recursos es muy amplio.

Una ACL consiste en controlar el acceso a las entradas (ACE, Access Control Entries) al sistema en cuestión para dar o negar el uso de objetos del sistema, archivos o dispositivos. En cada ACE se especifica a un usuario o a un grupo de usuarios con sus respectivos tipos de accesos permitidos. La ACL define el acceso de un usuario al sistema más precisamente que cuando se utiliza el tipo de protección UIC, debido a que con las ACLs se pueden formar grupos que contienen distintos códigos de identificación.

El sistema operativo VMS contiene un archivo llamado RIGHS DATABASE que contiene una lista de nombres especiales llamados identificadores, dicho archivo es la Base de Datos del Sistema. Al entrar al sistema se crea un proceso que se va a encargar de buscar en dicho archivo el identificador del usuario que desea entrar, si se encuentra, el acceso al sistema se le permite, en caso contrario se le niega.

5.6.7.1 Creación y mantenimiento de ACLs

Se utiliza el editor en VMS para crear y mantener una lista de control de acceso (ACL) para determinado objeto dentro del sistema de cómputo. Se utiliza el comando SET ACL para manipular una lista de control de acceso, esto es, se puede efectuar las operaciones de agregado, borrado o copiado de ACLs.

5.6.7.2 Identificadores

Los identificadores en una ACL especifican a los usuarios que tendrán el permiso (acceso) a un objeto del sistema de cómputo. Con objeto nos referimos a un archivo en directorio o un dispositivo. Cuando algún usuario entra al sistema el identificador que le pertenece está almacenado en la Base de Datos del Sistema, son copiados a un archivo (lista) que es una estructura que el Sistema Operativo utiliza para verificar la existencia de dicho usuario.

Existen tres tipos de identificadores :

- Identificadores de código de usuario
- Identificadores generales
- Identificadores generados por el sistema

Identificadores de código de usuario

Dependen del Código de Identificación del Usuario (UIC), el cual identifica únicamente a un usuario dentro del sistema de cómputo. Típicamente este tipo de identificadores son presentados en formato numérico, hexadecimal o bien en alfanumérico, de esta manera se tiene :

[INGENIERIA,ESTRADA]	Alfanumérico
[300,200]	Numérico
%X08001006	Hexadecimal

El Sistema Operativo VMS automáticamente agrega un identificador (UIC) a la base de datos del Sistema cuando una nueva cuenta es creada.

Identificadores generales

Un identificador General es definido por el Administrador del Sistema en la Base de Datos del Sistema para identificar a grupos de usuarios con una actividad en común, por ejemplo : FINANZAS, COMUNICACIONES, SISTEMAS, etc.

El identificador general se construye con una cadena alfanumérica de 1 a 31 caracteres. Puede estar constituida por un solo carácter (no es conveniente para cuestiones de administración), además se puede incluir el signo de pesos ($) y guiones bajos. Se utiliza AUTHORIZE para crear los identificadores generales.

Identificadores generados por el sistema

Los Identificadores Generados por el Sistema describen a ciertos tipos de usuarios del sistema de cómputo VAX, están basados en el uso del sistema. Por ejemplo :

Usuario	Actividad
BATCH	Trabajos en cola (archivos para ejecución o impresión).
NETWORK	Accesos hechos en el sistema por DECnet (protocolo de comunicaciones de DIGITAL).
INTERACTIVE	Accesos interactivos (terminales).
LOCAL	Accesos hechos por la terminal de un usuario local.
REMOTE	Todos los accesos realizados por usuarios a través de la red.

Para sumarizar, las ACLs pueden ser creadas por defecto por el sistema operativo para proteger objetos específicos y también por los usuarios para la seguridad de sus archivos o directorios. Un ACL consiste de ACEs para otorgar o negar el acceso a un objeto en particular que pertenece al sistema de cómputo.

5.6.8 Auditoría de seguridad

Con Auditoría de Seguridad nos referimos a la revisión de la protección del sistema de cómputo VAX. Las alarmas de seguridad son mensajes que se envían al operador de una terminal indicándole eventos específicos del sistema. Las alarmas pueden ayudar a detectar entradas fallidas al sistema, esto es, que algún usuario haya intentado entrar al sistema, sin tener los requisitos como lo es la clave de acceso.

Además las alarmas de seguridad ayudan a monitorear la actividad general del sistema; son configurables como por ejemplo se le puede indicar al sistema que mande una alarma cuando el Archivo de Autorización de Usuarios (UAF) ha sido modificado.

Antes de habilitar las alarmas de seguridad sobre plataforma VAX (un VAXCLUSTER por ejemplo), el Administrador del Sistema tiene que asegurarse de que el proceso llamado Comunicaciones del Operador (OPCOM, Operator Communications) esté corriendo, este proceso tiene la finalidad de presentar en pantalla un mensaje de que algo ha ocurrido en el sistema, de igual forma el evento se registra en un archivo en la VAX. Existe un proceso llamado AUDIT_SERVER (servidor de auditoría) que es el usado para escribir todas las alarmas de seguridad en el sistema.

Para habilitar la generación de alarmas, se utiliza el comando DCL llamado SET AUDIT (instala auditoría) con el siguiente formato :

SET AUDIT /ALARM /ENABLE = [OPCION]

En la parte opcional se puede especificar la palabra AUTHORIZATION, con esto se logra un monitoreo al archivo UAF, a la Base de Datos del Sistema y a las claves de acceso. Otra opción es BREAKIN la cual monitorea operaciones de entrada al sistema exitosas.

5.6.8.1 Utilería para análisis de auditoría (ANALIZE/AUDIT)

Con la utilería para Análisis de Auditoría de VMS se puede extraer y desplegar información desde los archivos de registro de alarmas. El Administrador del Sistema puede obtener reportes distintos para que a partir de ellos se evalué la seguridad del sistema VAX.

Las distintas formas de reportes son :

- **Listado breve**

  Provee una línea por cada registro en el archivo de alarmas (evento), la salida siempre muestra fecha, hora, tipo de registro (LOGIN, acceso, etc.), nombre de la máquina VAX, nombre de usuario, identificador del proceso y terminal.

- **Listado completo**

  El reporte con el formato de Listado Completo presenta todos los datos de cada registro procesado en el archivo de alarmas, muestra las mismas características que el de listado breve, agrega el estado del registro.

- **Listado resumido**

  El Listado Resumido es un compendio de los eventos de alarmas en determinada fecha, en esta lista se consideran al total de registros leídos en el periodo indicado, fallas de entrada, cambios al UAF, entradas exitosas, cambios a la Base de Datos del Sistema, volúmenes montados o desmontados, objetos accesados, etc.

Para mantener un ambiente seguro en la red de cómputo del ACSE en donde las VAX 4000-105A son los procesadores principales, como Administrador del Sistema se tiene que checar lo siguiente :

Determinar a qué horas del día se tiene un mayor uso de los recursos del sistema. Para nuestro caso existen cuentas que se necesitan durante gran parte del tiempo, para el control de aspectos de comunicaciones y operación del ACSE, por tal motivo :

- Es importante conocer los programas que normalmente se ejecutan (imagen), para así percibir cualquier anomalía en caso de que otra imagen este presente en el sistema.

- Identificar si es necesario que existan usuarios con altos privilegios, en el ACSE solo la cuenta SYSTEM tiene todos los privilegios.

- Un control de los trabajos en cola de impresión y en espera para ejecución para saber qué tan regulares son.

Es recomendable obtener diariamente reportes de auditoría (listados) para que el Administrador del Sistema pueda verificar que es lo que está sucediendo con los accesos al sistema y así tomar decisiones relacionadas con la seguridad del ACSE (en nuestro caso), se puede automatizar esta tarea para que no falte el reporte diario.

5.6.9 Claves de acceso primarias y secundarias

Cuando en una cuenta se tiene doble clave de acceso se dice que tenemos una clave primaria y otra secundaria, esto es, clave uno y clave dos respectivamente.

El uso de claves de acceso dobles es en algunas ocasiones algo problemático y principalmente se necesitan en sistemas de cómputo con altos niveles de seguridad. Las claves dobles ofrecen tres ventajas, tales como: cuando son usados sobre bases generales, ellas facilitan la verificación de la identidad física de cada usuario al momento de entrar al sistema, esto es, a través de un contacto visual por parte del Administrador, o bien cuando se trata de entrar al sistema vía una red (DECnet).

Sistemas con niveles medios de seguridad podrían utilizar las claves dobles como una herramienta para cuando la primera clave ha sido cambiada o cuando el generador de claves ha sido forzado, se presenten inexplicables rompimientos de entrada.

Para la implementación de las claves dobles se utiliza AUTHORIZE con el calificador /PASSWORD, la notación es la siguiente:

UAF> ADD nombre_de_usuario /PASSWORD = (primario,secundario)

Si se tuviera una cuenta con solo la clave primaria de acceso, a dicha cuenta se le podría dar de alta una clave secundaria, utilizando para ello el comando MODIFY desde AUTHORIZE:

UAF> MODIFY nombre_de_usuario /PASSWORD = (primario,secundario)

La clave primaria no se afectará y hereda sus características a la nueva clave (su tiempo de vida y su longitud mínima).

5.6.9.1 Expiración de las Claves de Acceso

El administrador del sistema puede utilizar AUTHORIZE para imponer algunas características importantes relacionadas con la utilización de las claves de acceso para los usuarios del sistema de cómputo, como por ejemplo la longitud mínima de la clave de acceso, cada cuánto tiempo la clave expira (tiempo en el cual la clave deja de funcionar), etc.

Con el calificador /PWDLIFETIME (tiempo de vida de la clave de acceso) en AUTHORIZE, se puede establecer el máximo tiempo que puede transcurrir entre el cambio de la clave antes de que al usuario se le deshabilite la entrada al sistema. Por defecto el valor dicho calificador es de 180 días, dependiendo de las necesidades de cambio de claves, se puede indicar la cantidad de tiempo que se requiera.

La importancia de utilizar en la administración del sistema el tiempo de vida de las claves de acceso, radica en que se obliga a los usuarios a cambiar su clave de manera regular. El tiempo puede ser diferente para cada usuario.

5.6.9.2 Longitud de la clave de acceso

Con AUTHORIZE y el calificador /PWDMINIMUM (clave de acceso mínima), se puede indicar al sistema cuál será la mínima cantidad de caracteres que formarán a la palabra que representa a la clave de acceso. Los usuarios pueden especificar claves de acceso arriba de la máxima longitud aceptada, esto es, arriba de 31 caracteres.

Conclusiones

Durante el desarrollo de este trabajo se observó que el Administrador de un Sistema de Cómputo es el responsable de la puesta en marcha y mantenimiento de dicho sistema. Es importante recalcar que no solamente el Administrador entiende asuntos relacionados con el Hardware y Software, sino que comprende las necesidades de toda una comunidad de usuarios, para así determinar en lo que sea posible qué es lo que un usuario requiere para desarrollar su trabajo en buenas condiciones.

Se llevo a cabo un análisis de las principales tareas que un Administrador de un Sistema debe de realizar para obtener el más óptimo desempeño del mismo.

El estudio realizado ofrece los conocimietos necesarios para poder manejar y controlar a los usuarios del ACSE, llevar a cabo aspectos de seguridad como lo es el control de acceso a las computadoras principales, el respaldo de información, el monitoreo uniforme de todo el sistema en sus diferentes aspectos, esto es, desde el punto de vista físico y lógico (hardware y software), y así tomar desiciones para el mejoramiento del sistema de cómputo del ACSE entre las que podemos mencionar futuras expansiones computacionales en caso de que haya mayor demanda del servicio de MOVISAT.

Hacemos mención que el esquema de administración presentado ha comenzado a aplicarse en todos sus aspectos dentro del ACSE, obteniendo resultados muy satisfactorios para el Organismo, ya que se han logrado ventajas en la operación, control y mantenimiento de los procesadores principales, que en nuestro caso son las computadoras VAX.

Otra aplicación a futuro en la cual nuestro trabajo va a ser una herramienta de apoyo la constituye otro sistema de comunicaciones móviles, en el cual se cuenta con una VAX de mayor tamaño siguiendo el mismo patrón de administración.

Consideramos que este trabajo tendra repercusiones importantes en cuestiones laborales para el Administrador de un Sistema en las diferentes áreas de cómputo de nuestra empresa, no importando la plataforma y ambiente de trabajo, ya que son una serie de conocimientos y experencias que se obtuvieron durante la relización de este.

Bibliografía

Libros

Akkoyunlu, E; A. Bernestein; and R. Schantz.
Interprocess Communication Facilities for Network Operating System

Denning, P. J.
Operating Systems: Principles and Theory
In Encyclopedia of Computer Science and Engineering, 1983

Goodenough, J.B.
Exception Handling: Issues and Proposed Notation
Communications of the ACM, 1975

Lamport, L.
Concurrent Reading and Writing
Communications of the ACM, 1974

Milan Milenkovic
Sistemas Operativos
McGRAW-HILL, 1995

Manuales

DECnet 105 Routing Overview Manual
Digital Equipment Corporation
Maynard, Massachusetts, 1989

DEC Network Integration Server
Digital Equipment Corporation
Maynard, Massachusetts, 1994

Domestic Mobile Data Service for Telecomunicaciones de México
Technical Description of the Acces, Control and Signaling Equipment
Hugnes Network System Limited
Saxon Street
Milton Keynes MK146LD
United Kingdomm, 1994

VMS Handbook
Digital Equipment Corporation
Maynard, Massachusetts, 1990

VMS System Manager's Manual
Digital Equipment Corporation
Maynard, Massachusetts, 1989

VMS System and Network Managment I:
Servivol Skils
Digital Equipment Corporation
Maynard, Massachusetts, 1991

VMS System and Network Managment II:
Managing Established System
Digital Equipment Corporation
Maynard, Massachusetts, 1991

VMS System and Network Managment III:
Managing Change and Complexity
Digital Equipment Corporation
Maynard, Massachusetts, 1991

VMS User's Manual
Digital Equipment Corporation
Maynard, Massachusetts, 1989

VAX 4000 Model 105A
Operator Information
Digital Equipment Corporation
Maynard, Massachusetts, April 1994

VAX 4000 Model 105A
Customer Technical Information
Digital Equipment Corporation
Maynard, Massachusetts, April 1994

VAX 4000 Model 105A
Troubleshooting Diagnostics Information
Digital Equipment Corporation
Maynard, Massachusetts, April 1994

Seminarios

Acceso a Redes Mundiales de Información
Telecomunicación Corporativa TELCOR SA. de CV.1996

Introducción a las Redes Digitales de Servicios
Escuela Nacional de Telecomunicaciones
TELECOMM, febrero 1996