34
24.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS ARAGON.

"CONSIDERACIONES PARA LA INSTALACION DE UN SISTEMA DE CONTROL DE ACCESO A UN EDIFICIO."

T E S I S P R O F E S I O N A L

Que para obtener el Título de:

INGENIERO EN COMPUTACION

P r e s e n t a n:

SANDRA LOPEZ FERNANDEZ.

MIGUEL ANGEL SANTILLAN RAMIREZ

México, D. F. 1997.

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

YO SANDRA DEDICO EL PRESENTE TRABAJO A:

MI MADRE Y MIS HERMANOS

A MI ESPOSO Y A MI HIJO

YO MIGUEL ANGEL DEDICO EL PRESENTE TRABAJO A:

MIS PADRES Y MIS HERMANAS

A MI ESPOSA Y A MI HIJO

CONSIDERACIONES PARA LA INSTALACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A UN EDIFICIO.

ÍNDICE

CONSIDERACIONES PARA LA INSTALACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A UN EDIFICIO.

Objetivo:

Definir los requerimientos, procedimientos y normas que se deben de tener en cuenta durante la planeación y posterior implementación de un sistema de control de acceso a un edificio.

INTRODUCCCIÓN

El rápido avance de las comunicaciones, hardware y software en los últimos años, nos brinda la oportunidad de aplicar tales desarrollos en áreas tan diversas como la imaginación nos lo permita, un caso específico ha sido la implementación de esta tecnología a la modernización de los edificios, con lo cual se les ha brindado de cierta autonomía e inteligencia en su funcionamiento, por esta razón se les ha denominado "EDIFICIOS INTELIGENTES". Algunas de las ventajas que esto implica, es brindar un mayor número de servicios a los usuarios, reducir los costos de mantenimiento del inmueble y ofrecer un alto grado de seguridad en cuanto a siniestros y accesos a los mismos.

En el presente trabajo se muestra un panorama de los sistemas de control de accesos para un edificio.

En el capítulo uno se describen brevemente los fundamentos y normas de la transmisión de datos, así como algunos conceptos básicos para una mayor comprensión de los capítulos posteriores.

El capítulo dos plantea la problemática existente en cuanto al control de acceso, se introduce al concepto de edificio inteligente y se muestran algunos de los servicios que estos contienen. Así mismo se describen una serie de dispositivos los cuales pueden ser interconectados a un diseño específico, para desarrollar una red de control de accesos.

En el capítulo tres, se plantean las consideraciones a tomar en cuenta para la implementación de un sistema de control de accesos por dispositivos

biométricos, interconectándolos a una red de control existente en un edificio. Se mencionan también las características técnicas que deben cumplir cada uno de los dispositivos que se vayan a seleccionar, ya que deben satisfacer las necesidades del diseño de la red en cuanto a hardware, software y canales de transmisión.

En el cuarto capítulo se describen las características de los dispositivos y el software seleccionados, junto con los requerimientos y procedimientos de instalación, también son mencionadas las pruebas preliminares para el funcionamiento de la red.

CAPITULO I. SISTEMAS DE COMUNICACIÓN DE DATOS.

Objetivo:

Describir los fundamentos y normas de la transmisión de datos en los sistemas de comunicación.

CAPITULO I. SISTEMAS DE COMUNICACIÓN DE DATOS.

En el presente capítulo se plantean los conceptos fundamentales sobre los sistemas de comunicación de datos. Se conocerán cada uno de sus componentes y los factores que influyen en la transmisión, se definirá lo que es una red de transmisión de datos, a la vez que se menciona el modelo de referencia OSI y la relación que existe con estas redes. También se habla de los organismos y comités más importantes en cuanto a la emisión de estándares de comunicación. De igual forma se describen los diferentes medios de transmisión y se tratan los distintos tipos de topologías. Por último se comentarán algunas de las aplicaciones y ventajas de las redes, así como sus tendencias a futuro.

1.1. TRANSMISIÓN DE DATOS.

Es el sistema de comunicación que interconecta a un conjunto de equipos electrónicos, que tienen como propósito procesar y almacenar grandes volúmenes. Este está constituido por equipos terminales de datos y un medio de comunicación eléctrico u óptico compatible a dichos equipos, que permite la transferencia de información en forma codificada, como se ve en la fig. 1.1

Fig. 1.1 Sistema básico de transmisión de datos puede ser alámbrico o inalámbrico en una red de datos.

De acuerdo a lo anterior, un medio conduce señales eléctricas u ópticas, las primeras representan información en relación a niveles de voltaje, y las señales ópticas refieren la información de acuerdo a la intensidad luminosa de un haz. Estas señales requieren de un medio de transmisión que puede ser alámbrico, el cual es aquel que utiliza un conductor de cobre y óptico, para transmitir señales eléctricas u ópticas respectivamente. Y un medio inalámbrico se define como el que utiliza la atmósfera y el espacio libre para la transmisión de información. Como ejemplos de las alámbricas se tienen el par trenzado, el cable coaxial, la fibra óptica, etc., y en los inalámbricos tenemos las microondas, los sistemas satélites, etc.

De acuerdo a lo anterior, un sistema de transmisión de datos se divide en subsistemas. Un subsistema de transmisión de datos es aquel que tiene como objetivo el procesamiento de señales analógicas y digitales, las cuales comprenden una serie de operaciones como son:

Modulación.- Es el proceso por el cual una propiedad o un parámetro de una señal se varía proporcionalmente a una segunda señal. En el caso de la modulación en fase y pulsos. Al equipo que realiza este proceso se le denomina MODEM (Modulador-Denominador).

Multiplexaje.- Es el proceso por el que la información proveniente de varios canales, comparten.

1.2. REDES DE TRANSMISIÓN DE DATOS.

La finalidad de una red de transmisión de datos es la necesidad de compartir recursos físicos y lógicos entre usuarios haciendo uso de las técnicas de transmisión existentes. Las formas geométricas que adquieren las conexiones en una red se denominan topologías. Existen diversas topologías las cuales se describen a continuación:

Estrella.- La topología estrella establece conexiones punto a punto entre un nodo central y todos los demás nodos de la red. Este nodo central especial, actúa como controlador de la red canalizando los datos hacia el destinatario tal como lo haría la operadora de un conmutador telefónico.

Algunas de las ventajas de esta topología es que el nodo aísla a una estación de trabajo de otra, resultando una red fiable frente a averías en la estación de trabajo (la avería de una estación de trabajo no afecta el funcionamiento de la red). En cuanto a la flexibilidad, permite incrementar o disminuir con sencillez el número de nodos, dado que las modificaciones son sencillas, ya que todas se localizan en el nodo central. Las desventajas son que no permite cursar grandes flujos de tráfico por congestionar el nodo central. Así también el costo por concepto de cableado o instalación es elevado, además no es adecuada para redes con gran cobertura geográfica.

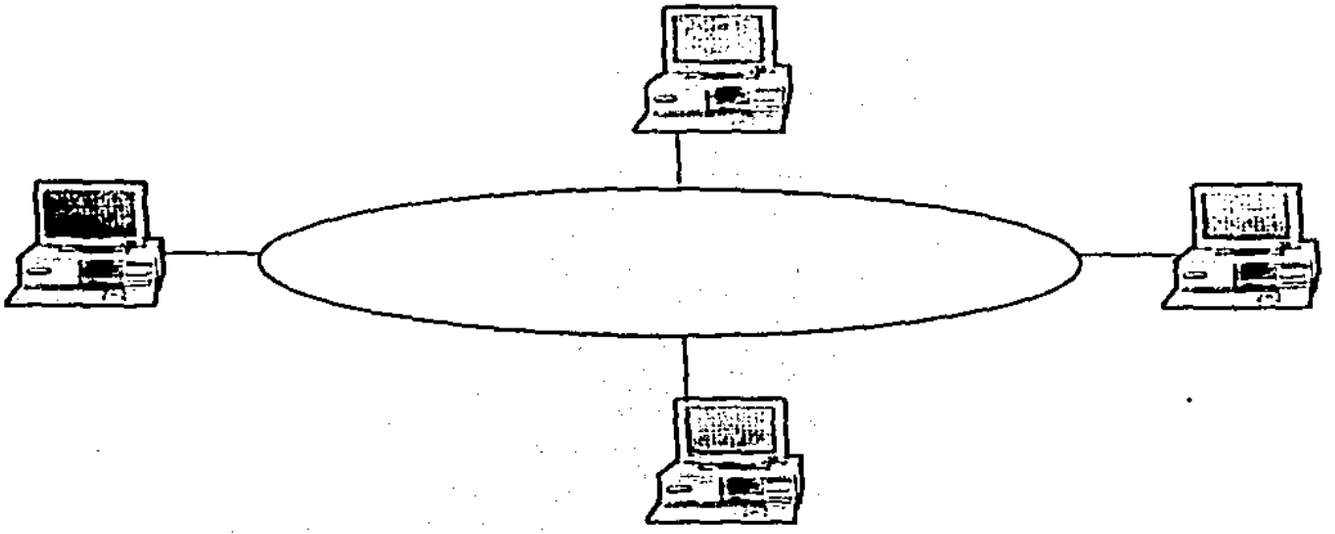

Fig. 1.2. Topología de anillo.

Bus.- En esta topología todos los equipos se conectan a un canal común, esto es, tiene un medio de comunicación. El enlace que conecta a un nodo de la red en un cable troncal se denomina derivación. En este tipo de red el medio de transmisión es pasivo, ya que son las interfaces las que proveen el acceso del nodo hacia la red.

Las ventajas que tiene son: Que si existe alguna avería en las estaciones de trabajo, no implica trastorno en la red, además presenta en su instalación y el retardo de propagación de información es reducido. También tiene un costo reducido y una gran flexibilidad para incrementar el número de estaciones de trabajo.

Sus desventajas son: Al encontrarse una avería en cualquier parte del bus, esta no puede reconfigurarse, dejando a los nodos posteriores a la avería fuera de la red.

Otra desventaja es la necesidad de retransmisión en caso de la detección de posibles colisiones de información en el bus. Lo anterior se soluciona mediante un procedimiento que corrija esta situación. La fig.1.3. ilustra el bus lineal.

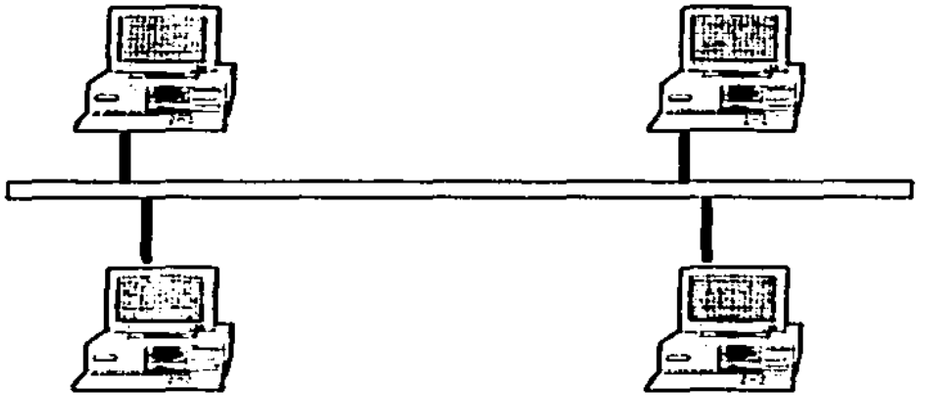

Fig. 1.3. Topología de bus.

Nota: Requiere impedancia de terminación de línea a fin de equilibrar la impedancia total, esto es, cuando el cable es coaxial.

Malla.- En este tipo de topología, cada nodo está conectado a todos (red completa) o a varios (red incompleta) nodos, formando una estructura que puede ser regular (simétrica) o irregular (asimétrica). Las conexiones son punto a punto e implican conexiones redundantes entre nodos.

Las ventajas son: Gran fiabilidad frente a fallas y posibilidades de reconfiguración además maneja tráfico de datos elevado con retardos aceptables. Las desventajas son: El costo en medios de comunicación e instalación es elevado, tiene poca flexibilidad para la incorporación de nuevas estaciones de trabajo, así mismo no

es recomendable para grandes dispersiones geográficas debido a su elevado costo y variedad de medios de comunicación. La fig. 1.4. ilustra esta topología.

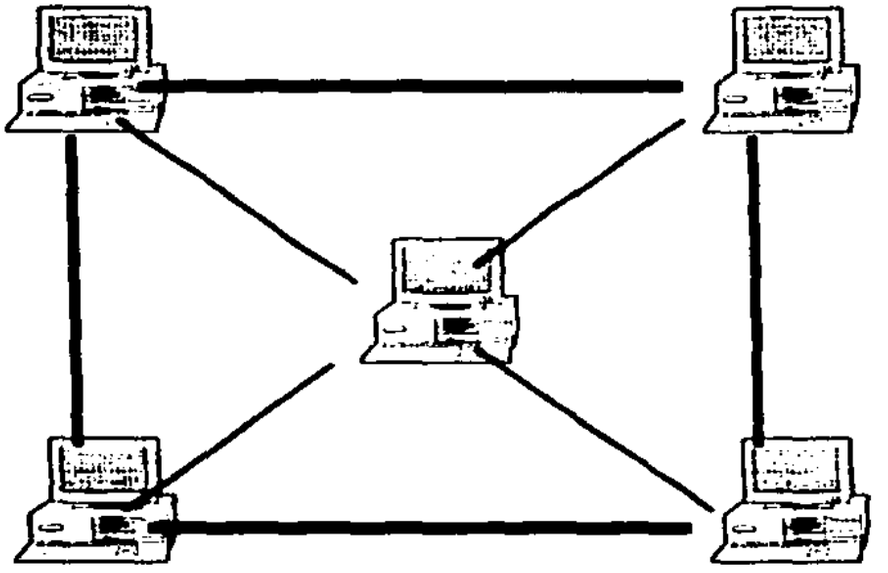

Fig. 1.4. Topología de malla.

Los procedimientos de comunicación de redes están soportados por la topología de las mismas. Éstos procedimientos definen su arquitectura, la cual esta sustentada en el nodo de referencia OSI, que promueve la ISO (International Standard Organization), que se describe a continuación.

En un esfuerzo por crear una normalización internacional de varios protocolos, la organización internacional de normas (ISO), crea un modelo de referencia basado en capas. A este modelo se le conoce como modelo de referencia OSI, por que precisamente se refiere a la conexión de sistemas heterogéneos, es decir sistemas dispuestos a establecer comunicación con otros distintos.

El modelo OSI esta constituido por siete capas. Los principios aplicados para el establecimiento de estas capas fueron las siguientes:

1. Una capa se creará en situaciones en donde se necesita un nivel diferente de abstracción.

2. Cada capa deberá efectuar una función bien definida.

3. La función que realizará cada capa deberá seleccionarse con la intensión de definir protocolos normalizados internacionalmente.

4. Los límites que realizará cada capa deberán seleccionarse tomando en cuenta el mínimo flujo de información a través de las interfaces.

5. El número de capas deberá ser los suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa, y por otra parte, también deberá ser lo suficientemente pequeña para que su arquitectura no llegue a ser difícil de manejar.

A continuación se explicarán las capas mostradas en la fig. 1.5.

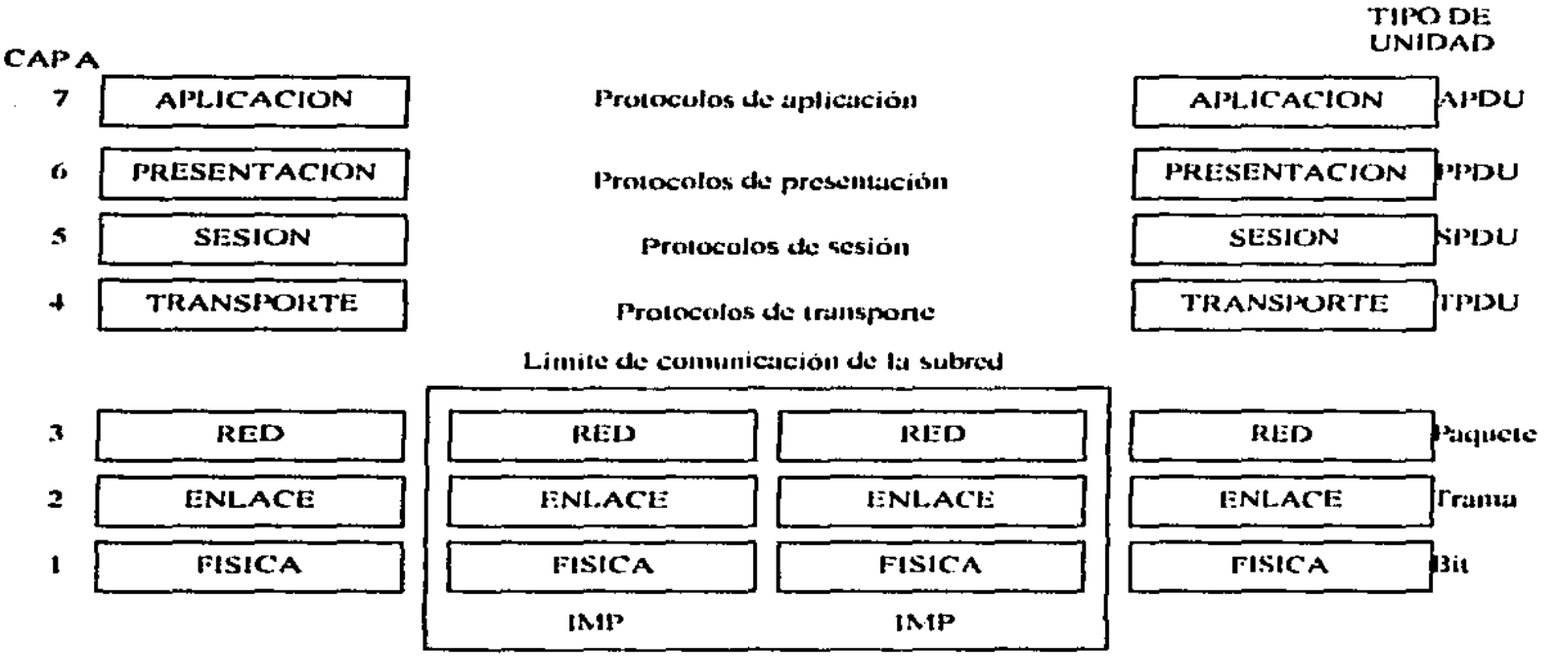

Fig. 1.5. Arquitectura de la red (basada en el modelo OSI)

Nivel físico.- Las funciones incluidas dentro de este estrato se encargan de activar, mantener y desactivar un circuito físico entre un ETD y un ECD. Dentro de este nivel se encuentran características como son: mecánicas. Eléctricas, ópticas, así como los medios de transmisión y el ancho de banda.

Nivel de enlace.- Es el responsable de la transferencia de datos por el canal. Proporciona a los datos la sincronización necesaria para delimitar el flujo de bits del nivel físico. Así mismo, garantiza la identidad de los bits encargándose de que los datos lleguen sin errores al ETD receptor. Evita que un transmisor muy rápido sature con datos a un receptor lento.

Nivel de red.- Define la interfase entre el ETF de usuario y la red de conmutación de paquetes, además de la interfase de un ETD con otro a través de

esta red. Encamina paquetes origen-destino. Selecciona las rutas de transmisión. Establece la interconexión con redes heterogéneas.

Nivel de transporte.- Proporciona la interfase entre la red de comunicación de datos y los tres niveles superiores. Acepta datos de la capa de sesión y los divide en unidades más pequeñas, si es necesario, para pasarlos a la capa de red y asegurar que lleguen correctamente al otro extremo.

Nivel de sesión.- Funciona como interfase del usuario con el nivel de transporte. Ofrece un mecanismo organizado de intercambio de datos entre usuarios puede seleccionar el tipo de control y de sincronización que desea de la red, por ejemplo:

1.- Diálogo bidireccional alternado o bidireccional simultáneo.
2.- Puntos de sincronización para comprobaciones intermedias y recuperaciones durante la transferencia de archivos.
3.- Abortos y arranques.
4.- Flujo de datos normal y acelerado.

Nivel de presentación.- Asigna una sintaxis a los datos, es decir, determina la forma de presentación de los datos según este modelo, que con los códigos (ASCII, EBCDIC; etc.) pueden representar caracteres alfanuméricos. Una de las funciones que efectúa es la compresión de datos, para reducir el número de bits a transmitir.

Nivel de aplicación.- Se encarga de atender el proceso de aplicación del usuario final. A diferencia del nivel de presentación, este nivel tiene en cuenta la

semántica de los datos. Tiene funciones de operación de edición, transferencia de archivos, correo electrónico, etc.

1.3. ESTANDARES DE COMUNICACIONES.

El IEEE (Institute of Engineer Electric and Electronic) es un organismo de estandarización que establece las normas bajo las cuales se rigen las técnicas de comunicación, equipos y control de calidad. La IEEE ha producido varias normas para las redes tipo LAN (red de área local). A las cuales se les conoce como IEEE 802, en las que se incluye la CSMA/CD. Las normas IEEE 802 han sido adaptadas por el ANSI (American Nacional Standars) como una norma gubernamental y por la ISO como una norma internacional (conocida como ISO 8802).

El comité 802 divide su estudio en el siguiente grupo de normas. Cada una de ellas es publicada en un manual separado, a continuación se enuncian:

802.1 Gestión y niveles superiores (HILI)
802.2 Control lógico de enlace (LLC)
802.3 CSMA/CD
802.4 Token Passing Bus (paso de testigo en bus)
802.5 Token Passing ring (paso de testigo en anillo)
802.6 Redes metropolitanas MAN

El CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía) tiene la tarea de promover las recomendaciones técnicas sobre aspectos telefónicos. De

este comité una de las normas más importantes es la 802.3 que por tener aplicación en este proyecto se explica a continuación.

1.3.1. CSMA/CD.

Este modelo se basa en un nivel y un subnivel, los cuales se mencionan en los siguientes párrafos.

Nivel físico.- Este nivel dependerá del medio. Su función es introducir las señales eléctricas en el canal y proporcionarles el sincronismo adecuado, así como codificar y decodificarlas. El nivel físico esta conformado por dos entidades principales. La entidad de codificación/decodificación de datos y la entidad de acceso al canal en recepción y transmisión. El canal al cual se hace referencia puede ser cable coaxial, par trenzado y fibra óptica (en el punto 1.4.4 se define el canal para CSMA/CD).

Subnivel de acceso al medio. Se encarga de transmitir la trama al nivel físico, además de almacenarla en buffers o memorias intermedias. Así mismo intenta evitar colisiones en el canal de comunicación y gestiona los medios para detectarlas.

En la fig. 1.6. se ilustra el modelo de este protocolo. A continuación se describe el procedimiento de acceso al medio.

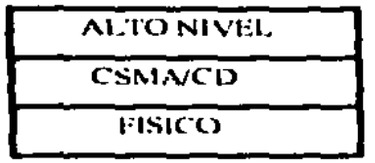

Fig.1.6. Modelo de referencia CSMA/CD.

1.3.2. NORMA 802.3 CSMA/CD.

Para el control de una red de área local con topología en bus el procedimiento más probado es el que se clasifica como un sistema sin prioridad y con detección de portadora (colisión). La versión más extendida es Ethernet, la cual tiene su historia basada en el sistema ALOHA. Desarrollado por Abramson en Hawaii. Fue XEROX Corporation quien investigo el tema del CSMA/CD y que puso en el mercado el primer producto comercial.

El protocolo CSMA/CD, se refiere a una estación que desea transmitir, esta escucha la información que fluye a través del cable. Si el cable se encuentra ocupado, la estación espera hasta que este en estado inactivo, en caso contrario transmite de inmediato. Si dos o más estaciones en forma simultánea transmiten a través de un cable inactivo generarán una colisión. Por lo cual esperarán entonces un tiempo aleatorio e intentarán transmitir nuevamente.

Los espacios o períodos de tiempo (tiempo de escucha entre intentos, etc.) se determinan según estudios de simulación, en donde se gráfica el rendimiento del sistema en función de la velocidad de transmisión. Algunos valores usados son: 18, 24, 32 y 51 microseg.

La velocidad de transmisión de este protocolo es de 10 Mbps para un canal metálico.

FUNCIONES DE CSMA/CD ETHERNET.

- Transmisión y recepción en formato de paquetes.
- Decodificación de paquetes y supervisión de direcciones antes de pasar a las capas superiores de software.
- Detección de errores dentro de los paquetes de datos o en la red.

Generalmente Ethernet funciona mejor para redes con pocos nodos, pero esto dependerá de las tarjetas de comunicaciones que tengamos en nuestros equipos. Al elegir una tarjeta de comunicaciones se deben de tomar en cuenta ciertas consideraciones, que se comentarán en capitulos posteriores.

Por su tipo de acceso (CSMA/CD), a pesar de la velocidad de transmisión, la curva de degradación es muy pronunciada cuando la carga de trabajo en la red es muy fuerte.

Ethernet tiene como ventaja la compatibilidad con cualquier otro tipo de protocolo y tiene como tendencia a futuro aumentar el ancho de banda a fin de asegurar la compatibilidad con protocolos de alta velocidad de transmisión como son ATM y SONET.

1.4. TOPOLOGIA DE UNA RED ETHERNET.

Una red Ethernet puede estar constituida por dos topologías que son: estrella y bus, para escoger alguno en especial, es necesario saber las necesidades que debe cubrir la red a diseñar, así como las cualidades que ofrece cada topología.

La topología de estrella para una LAN está conformada en nuestros días por un servidor central conectado a repetidores o concentradores, por medio de los cuales son conectadas las estaciones de trabajo a través de una tarjeta de comunicaciones Ethernet. El cable puede ser par trenzado, coaxial o fibra óptica.

En una red con topología de bus, las estaciones de trabajo (nodos) están también conectadas por medio de una tarjeta de comunicaciones Ethernet, a un cable coaxial, en el cual a su vez se conecta el servidor y las estaciones. En esta topología el cable debe estar terminado en sus extremos por medio de conectores terminadores que equilibran la línea.

Existen algunas consideraciones para la adquisición de tarjetas Ethernet. Como son, escoger adecuadamente el tipo de conector que se va a utilizar; esto dependerá del medio de transmisión que vayamos a utilizar en nuestra red. El tipo de bus (ISA, EISA, MCI, etc.), ya que esto estará determinado por los slots de expansión que existan en nuestro equipo de computo.

CONEXIONES ENTRE NODOS.

Los tipos de conexión que existe entre nodos son punto a punto, multipunto y punto a multipunto. A continuación se describen cada uno de ellos.

La conexión punto a punto es una conexión que nos permite tener una gran facilidad de operación debido a que solo intervienen dos equipos terminales de datos y un sólo canal de comunicación, esto permitirá que la comunicación sea bidireccional y además que no se permita el acceso a otro usuario.

En la conexión multipunto se nos permitirá que en un solo canal de comunicación están conectados una o varios equipos terminales de datos, sin que esto represente un problema de conmutación, esto se logrará utilizando un software de comunicación que ayude a la anulación de interferencias entre los equipos terminales de datos.

La conexión punto a multipunto nos permite tener un sólo canal de comunicación, el cual será compartido por varios equipos terminales de datos, esto implicará tener un equipo terminal de datos que tenga la función de controlar la transmisión en este único canal.

TRAMA DE LA NORMA 802.3.

La trama para el estándar de comunicación 802.3 comienza con un preámbulo de 7 octetos cada uno con un patrón de bits 10101010. La codificación Manchester para este patrón genera una onda cuadrada de 10 MHz, que dura 5.6s, para permitir que el reloj del receptor se sincronice con el transmisor. A continuación un octeto de inicio de trama que contiene el patrón 10101011, para denotar el inicio de los mismo.

La trama contiene dos direcciones, una es para el destinatario y la otra para la fuente. La norma permite tener el campo de 2 ó 6 octetos, pero los parámetros

definidos para la norma correspondiente a la banda base de 10 Mbps, por ser este un protocolo orientado a byte solamente utilizan direcciones de octetos. El bit de orden mayor en la dirección del destinatario, corresponde a un 0, en las direcciones ordinarias, y un 1 para las direcciones de grupo. Las direcciones de grupo autorizan a múltiples estaciones para escuchar en una sola dirección.

El campo de longitud indica cuantos octetos están presentes en el campo de datos, desde un mínimo de 0 hasta un máximo de 1500. Aunque un campo de datos de 0 octetos es legal, origina un problema para distinguir las tramas que son válidas y las que no lo son. El 802.3 establece que las tramas válidas deberán tener por lo menos una longitud de 64 octetos, desde la dirección destinataria hasta el código de redundancia. Si la parte de datos correspondiente a una trama es menor de 46 octetos, el campo de relleno se utilizará para completar la trama al tamaño mínimo requerido.

El campo final correspondiente al código de redundancia que es un código de 32 bits, que representa el conjunto de datos. Si algunos bits de datos se recibirán erróneamente (debido al ruido del cable),e s casi seguro que el código de redundancia será incorrecto y por lo tanto, el error será detectado. En la fig. 1.12 se ilustra la trama descrita.

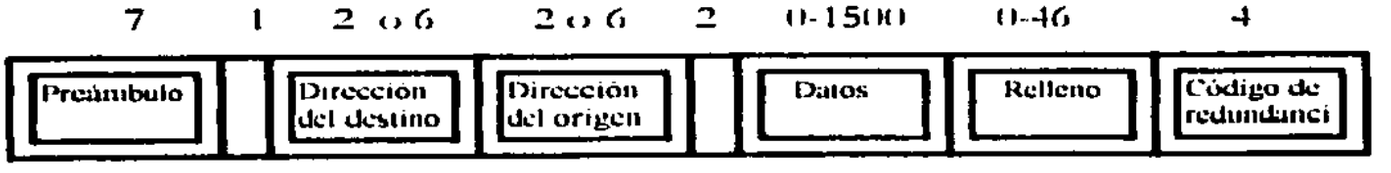

Fig. 1.10. Formato de la trama para el 802.3

1.4.1. CABLEADO PARA ETHERNET.

De acuerdo a las especificaciones de la IEEE cada tipo de cable tiene una longitud máxima permisible y un número máximo de dispositivos que pueden ser ligados a cada segmento. Así el número máximo de dispositivos y nodos en una red Ethernet simple no debe exceder 1024, operando a 10 Mbps sin importar el tipo de cableado que se este utilizando.

Ethernet es el más popular método de acceso en redes en el mercado mundial. Los productos Ethernet y los diseños de red son estandarizados de acuerdo a la regla IEEE 802.3 con la implementación de estándares para coaxial delgado (10BASE2), coaxial grueso (10BASE5), para trenzado sin blindar (10BASET) y cable de fibra óptica (10BASEFL). Lo anterior se muestra en la fig. 1.7.

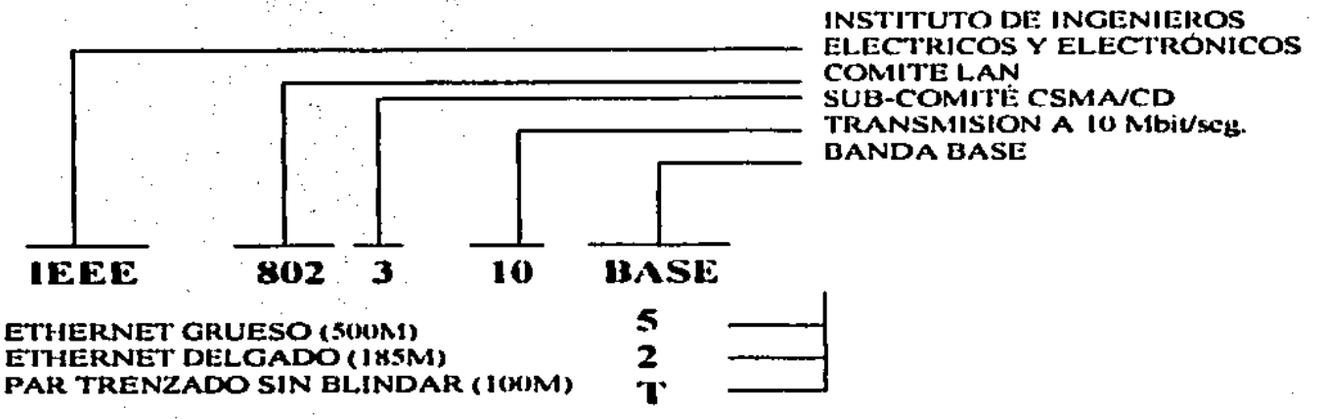

Fig.1.7. Norma IEEE 802.3

A continuación se describen los tipos de cableado para esta red.

Cable coaxial. Es el más utilizado en la transmisión de datos. Es ideal para redes, se caracteriza por su capacidad para el manejo de tráfico pesado a altas velocidades, su baja interferencia y el poder acarrear datos a largas distancias en comparación con el par trenzado. Existen dos tipos de cable: coaxial delgado y coaxial grueso, los cuales se describirán a continuación. La fig. 1.8. ilustra el cable coaxial.

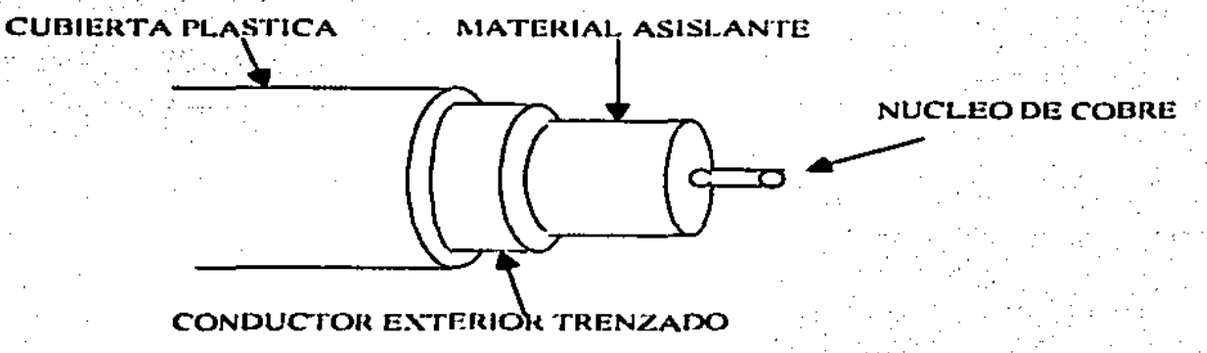

Fig. 1.8. Cable coaxial.

Coaxial grueso (10BASE5). Es un cable fuertemente blindado, inflexible (1/2" de diámetro). El cable coaxial de cobre RG-8 50 Ohms, tiene buena protección a las interferencias electromagnéticas, pero es relativamente caro y es difícil de instalar con un radio de curva de 25.4 cm y requiere transceptores, y un cable pendiente (drop cable) para conectar los dispositivos a la red. Por estas razones el cable coaxial grueso es más utilizado como columna vertebral (backbone) de una red.

Coaxial delgado (10BASE2). Este cable es más delgado y más flexible en su blindaje (1/4" de diámetro). El cable coaxial RG-58 presenta una impedancia de 50 Ohms, es extremadamente usado para redes pequeñas o grupos de trabajos locales. Este cable tiene baja protección a la interferencia electromagnética que el

coaxial grueso. Además de que es más fácil su instalación, es más versátil y es menor su costo.

Par trenzado (10BASET). El cable de par trenzado puede ser blindado (STP pos sus siglas en inglés) o sin blindar (UTP) a pesar de ser el más barato de los cables de comunicación para Ethernet no es el óptimo, ya que no tiene inmunidad a interferencias como el cable coaxial o la fibra óptica, y no soporta las grandes distancias de conexión de estos dos medios. El cable de par trenzado es ideal para redes que trabajan en lugares aislados a las interferencias electromagnéticas. La línea de par trenzado recomendado para enlazar segmentos es la línea blindada 24 AWG de 100 Ohms o sin blindar 26 AWG de 150 Ohms.

Cable de fibra óptica (10BASEFL). Posiblemente el propósito más común del cable de fibra óptica en una LAN, es aumentar las distancias que normalmente se manejan con cable coaxial. El cable de fibra óptica transmite datos vía pulsos de luz infrarroja. Es inmune a la interferencia eléctrica, haciéndolo un medio confiable para la transmisión de datos. Tiene un gran ancho de banda y puede transmitir datos a distancias extremadamente grandes. Además como no emite señales eléctricas es casi imposible interferir una transmisión.

Recientemente los precios para red de fibra óptica han venido bajando drásticamente, haciendo a la fibra óptica una opción más accesible. La fibra óptica puede ser utilizada en enlaces punto a punto en topología estrella. Un cable de fibra óptica, es mostrado en la fig. 1.9.

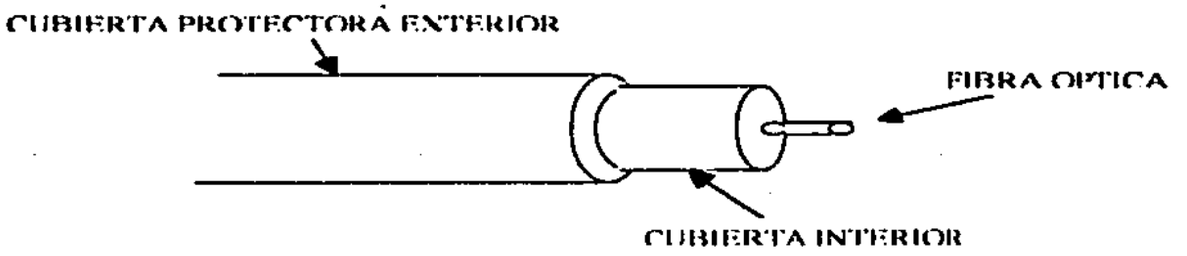

Fig. 1.9. Cable de fibra óptica.

1.4.2. APLICACIONES Y SERVICIOS DE ETHERNET.

ADMINISTRACIÓN.

En el área administrativa las redes de área local han tenido un gran auge, por su relativa facilidad de instalación, sus bajos costos de instalación y operación, y por las grandes ventajas que brindan a sus usuarios en el intercambio de información a grandes velocidades. Gracias a estas se observa una gran tendencia hacia la automatización en las oficinas, por lo que los trámites administrativas dentro de estas se han agilizado en gran medida. Ethernet soporta cantidades elevadas de tráfico originado por las bases de datos, esto, por su alta velocidad de comunicación, además de contar en la actualidad con microprocesadores, con velocidades de procesos muy elevadas, así mismo la tecnología de 32 y 64 bits en las tarjetas de comunicación permiten un rápido intercambio de información entre terminales en una red.

SECTOR EDUCATIVO.

En el área educacional, apoya a las técnicas de enseñanza, en el acceso a grandes volúmenes de información para grupos de estudio, en el mismo momento, por lo que la consulta a bases de datos en hipertexto de bibliotecas o centros de información es muy común en nuestros días.

Existen también programas de simulación de procesos en institutos de enseñanza, así como en institutos de investigación, en los cuales es posible que diferentes usuarios en el mismo instante, realicen la simulación de un proceso, cambiando únicamente ciertas variables.

LA BANCA.

Dentro del área bursátil sería, casi imposible imaginarse una sala bancaria, realizando los complejos trámites actuales de un usuario sin las redes internas, ya que estos pueden llegar a cientos diariamente en cada sucursal, esto permite mantener al instante actualizadas las bases de datos de los bancos. Así también estas redes simplifican indescriptiblemente el trabajo en las ajetreadas casas de bolsa, en donde el manejo de información exacto y en el momento preciso, es determinante en la negociación de las acciones. Para esta aplicación Ethernet ofrece tiempos de respuesta mínimos, alta capacidad de canal y confiabilidad de la transmisión.

EDIFICIOS INTELIGENTES.

Una aplicación que se les ha dado en los últimos años las redes de área local, es la de controlar y monitorear los sistemas de comunicación y confort dentro de un edificio, así como brindar servicios adicionales a los usuarios del mismo. Este tipo de sistema puede controlar y monitorear los siguientes sistemas:

- Sistema de aire acondicionado
- Sistema de iluminación
- Suministro de energía eléctrica
- Plantas de energía eléctrica
- Extractores
- Sistemas hidráulicos
- Sistemas de seguridad (protección contra incendio, control de accesos, protección contra intrusos, circuito cerrado de televisión, etc.), los cuales se centralizan en una red de área local.

Entre las ventajas que se tienen al contar con un sistema de control centralizado podemos citar:

a) Ahorros de energía eléctrica que pueden ir desde el 15 hasta el 40 %.
b) Incremento en el confort y en consecuencia en la productividad del personal, en el caso de ser un edificio de oficinas.
c) Reducción considerable en los gatos de operación del edificio, así como en la remodelación del interior del mismo.

Al brindar todas estas ventajas en la operación de un edificio por medio del sistema de control centralizado, se les otorga cierta inteligencia al mismo, por lo que se le denomina "EDIFICIO INTELIGENTE".

El objetivo de un edificio inteligente es, ser confortable, flexible, económico en su operación y controlable.

La red Ethernet puede ser la base para lograr este objetivo, ya que es altamente compatible con una diversidad de equipos de control, así también puede manejar un gran número de usuarios y puede extenderse a través de todo un edificio por medio de equipos que garantizan la calidad de la transmisión.

1.5. TENDENCIAS DE LAS REDES DE DATOS.

Durante los últimos años en nuestro país se ha destacado la llamada "fiebre" de la conectividad la cual ha provocado que la importancia de las redes de microcomputadoras en México cobra cada día mayor fuerza.

Con el surgimiento de los sistemas operativos de red que integran a las redes corporativas (como Novell Netware) se inició un proceso de avance gigantesco, ya que sin importar el protocolo que la tarjeta de red trabaje, podrá existir conectividad hacia otros ambientes de computo con diferentes arquitecturas.

Lo anterior establece que puede existir una conexión entre redes de distinta o igual estándar, lo cual implica amplias posibilidades de interconectividad entre redes de cualquier cobertura.

Con el surgimiento y comercialización de protocolos que proporcionan conectividad entre redes locales con microcomputadoras o mainframes, el futuro de las LAN se aclara cada día más; no es coincidencia que muchos de los fabricantes de productos de comunicaciones estén invirtiendo grandes cantidades de dinero en el desarrollo de utilerías para red y perfeccionando los existentes para hacerlos más competitivos en el mercado internacional.

Una de las tendencias más importantes es la integración de servicios vocales (voz) y no vocales, lo cual es posible obtener con una red LAN, que al interconectarse con distintos ambientes logra ser un sistema de transmisión integral que permita migrar hacia las tecnologías RDSI y RDSI-B.

Con el surgimiento del estándar TCP/IP, el campo de aplicación de redes locales se amplía aún más debido a que la conexión a otros ambientes heterogénicos (distintas topologías, protocolos, etc.) se realiza en forma transparente para el usuario permitiendo a la red LAN incorporar sus servicios a otros computadores y al mismo tiempo hacer uso de los servicios proporcionados por los demás computadores conectados.

Debemos esperar muchos cambios durante los siguientes años, incluyendo desde luego un mejor rendimiento del hardware con procesadores novedosos. El procesamiento paralelo con equipos duales de transmisión entre computadoras 20 veces más rápidas que las actuales, nuevos medios de transmisión basados en fibras ópticas, etc.

El futuro inmediato de la tecnología de las microcomputadoras es predecible: serán más rápidas, más funcionales y más interactivas. Muchos otros avances se

realizarán en éste último concepto que involucran a los servicios por medio de sofisticación del software y sobre todo, del soporte integrado a los sistemas.

CAPITULO II. SISTEMAS DE CONTROL DE ACCESOS.

Objetivo:

Enumerar la diversidad de sistemas de control de acceso existentes, así como las ventajas que estos representan.

CAPITULO II. SISTEMAS DE CONTROL DE ACCESO

Existen diversas técnicas automatizadas de control de acceso. Los sistemas automáticos controlan el acceso a un edificio sin la ayuda de un guardia; pueden permitir el acceso basándose en el reconocimiento de un código en memoria, el reconocimiento de huellas digitales, el reconocimiento de un patrón de voz, etc. que se da por medio de equipo detector o lector.

Un número importante de factores son considerados al seleccionar un sistema de control de acceso. El más importante es la resistencia a la falsificación. El grado de resistencia requerido está en función de la importancia y de que tan crítica es el área que se esta controlando. La resistencia a la falsificación es una medida de la dificultad para duplicar el código de acceso. Los sistemas de reconocimiento del habla, la retina y la firma son considerados los más resistentes debido a la interacción dinámica necesaria para la identificación personal.

Los sistemas de reconocimiento de geometría de la mano y huella digitales se consideran como de medios a alto, mientras que cuando el acceso es dado por tarjetas, códigos en memoria y teclado ofrecen baja resistencia a la falsificación.

Otro factor importante a considerar en el control de acceso es el tiempo que tarda una persona normal en entrar, ya que mientras la puerta permanezca abierta otra podría introducirse.

Algunos sistemas dan una señal de alarma cuando la puerta permanece demasiado tiempo abierta. Además, es necesario considerar el tipo de cerradura.

2.1. SISTEMAS CONTROLADORES DE ACCESO.

Existen diferentes dispositivos par controlar el acceso a un área, la selección de este dispositivo está en función del nivel de seguridad deseado y del costo. A continuación se describen algunos de los sistemas más comunes.

2.1.1. TECLADO Y CÓDIGO EN MEMORIA.

En ellos se debe dar un código que se encuentra en memoria con la secuencia adecuada usando un teclado. Cuando el código es correcto se otorga el acceso activando inmediatamente la cerradura que abre la puerta.

Un punto vulnerable que presenta este sistema, es que, una vez que se ha abierto la puerta, más de una persona puede entrar pudiendo ser alguna no autorizada. Algunas, ofrecen seguridad adicional, activando una alarma cuando la puerta permanece demasiado tiempo abierta.

Los sistemas con teclado y código en memoria proveen relativamente un nivel bajo de seguridad por lo que es importante darle una aplicación adecuada dependiendo de la necesidad que se requiera cubrir.

2.1.2. TARJETAS CODIFICADAS.

La mayoría de los sistemas de control de acceso usan tarjetas codificadas con sus respectivas lectoras. Para lograr el acceso la persona introduce o presenta su tarjeta a la lectora.

Dicha tarjeta en tamaño y apariencia se parece a una tarjeta de crédito. Aunque las técnicas de grabación del código varían en cada fabricante, se puede almacenar millones de combinaciones. La codificación puede ser magnética o electrónicamente con los datos necesarios para la completa identificación de la persona. Algunos, proporcionan una fotografía y las características propias del portador para una posible revisión complementaria.

Su aplicación requiere tener un procesador central con los datos de cada usuario, conectando a este, las lectoras de tarjetas remotas. Puede controlar el acceso y la salida de cientos de usuarios usando lectoras en varios lugares. Cuando una tarjeta se presenta a la lectora, esta censa la información codificada y la transmite al procesador, el cual recibe la información y la compara con los datos en memoria y en unos milisegundos decide si negar o acceder la entrada. Cuando el acceso es concebido el controlador manda una señal que abre inmediatamente la puerta.

La unidad central de control permite al operador realizar muchas funciones, una de las cuales es cancelar tarjetas perdidas o robada. Es necesario que la cancelación de tarjetas sea tan rápido y fácil como sea posible.

Una de las funciones adicionales en algunos sistemas es que no se permite el uso de la tarjeta para entrar hasta que ésta haya sido usada para salir del área de control. Con lo que se evita que la tarjeta pase de una persona que se encuentra adentro a otra que quiere entrar.

Las lectoras de tarjeta identifican a la tarjeta no al portador. La vulnerabilidad más común es la pérdida y que su propietario no se percate. Una combinación teclado y código en memoria robustece al sistema.

Las tarjetas pueden ser codificadas para dar información adicional, por ejemplo, el puesto del usuario, cuando y a que hora esta permitido el acceso.

A continuación se describen algunas formas más populares de control de acceso por tarjetas codificadas:

a) Tarjeta de identificación por foto. Este tipo puede ser la credencial de empleado con la fotografía del propietario, la cual puede ser inspeccionada por un guardia. Es difícil cuantificar la efectividad de este tipo de control de acceso, debido a que entra en juego el criterio del guardia cuando examina la credencial. Otro factor que interviene es el número de personas que estén entrando al mismo tiempo, además de que la credencial es fácil de falsificar.
b) Tarjetas con código magnético. Las tarjetas con código magnético tiene una hoja flexible de material magnético, entre dos hojas de material plástico, en la que graba un arreglo de marcas magnetizadas permanentemente. El código es determinado por la polaridad de las marcas.

Las desventajas que presentan estas tarjetas es que el código se puede borrar si es expuesta a una fuente campo magnético. Es posible falsificarlas, pero en general no presentan problemas.

c) Tarjetas con tira magnética. Una tarjeta de este tipo presenta una tira magnética a lo largo de uno de sus lados. La cual se codifica con los datos del portador. Algunos sistemas utilizan codificación alfanumérica permitiendo el nombre y datos adicionales.

Los sistemas que usan tarjetas con tira magnética tienen actualmente un amplio uso; pueden ser falsificadas y también existe el riesgo de un borrado accidental.

d) Tarjetas de código de barra. Éstas tarjetas son codificadas por un arreglo geométrico grabado en cintas, los espacios representan dos codificados. La ventana de estos códigos es que no requiere un lector sofisticado. Puede ser leído pasando un detector óptico sobre la tarjeta.

La desventaja es que el código es visible y puede ser fácilmente duplicado, aunque en las versiones recientes solo puede ser leído usando luz ultravioleta o infrarroja.

e) Tarjetas de proximidad. Las tarjetas de proximidad se codifican eléctricamente, un campo electromagnético es transmitido por una unidad estacionaria de interrogación ubicada junto a la entrada de acceso. Cuando la tarjeta esta expuesta al campo electromagnético se induce un voltaje en la tarjeta que activa un circuito eléctrico pasivo, entonces la unidad interrogadora censa la información y la envía a la unidad de control, si el dato es válido se

abre la puerta. La ventana de estos sistemas es que no es necesario insertar la tarjeta en la lectora.

2.1.3. COMPARACIÓN POR VÍDEO.

En la comparación por vídeo, se utiliza un circuito cerrado de televisión y en combinación con el personal de seguridad se realiza el control de acceso. Dicho control es manual, ello implica que sea más lento y además depende de la dedicación y concentración del operador para el buen desempeño del sistema.

Las áreas que requieren de alta seguridad, el sistema controlador de acceso, verifica la identidad del solicitante a través del reconocimiento de huellas digitales, geometría de la mano, patrón de voz y algunas otras características que hacen única a una persona.

Para esto, se requiere digitalizar previamente los datos que identifican al usuario. Es muy común, que la persona que desea el acceso se identifique con una tarjeta codificada, posteriormente, para confrontar sus datos se procede a la verificación.

La verificación de entrada es digitalizada y comparada a alta velocidad con los datos de referencia para que en pocos segundos el acceso pueda ser concebido dependiendo de el resultado de la comparación.

Desafortunadamente, las características físicas de la gente cambian en tiempos relativamente cortos. Por ejemplo, las huellas digitales pueden verse afectadas por

una herida, por el desgaste y pos estar en contacto con superficies abrasivas dependiendo de la actividad que el usuario realice. El patrón de voz y la firma pueden ser afectados por stress la fatiga. Por estas razones el sistema debe tolerar un porcentaje de errores.
A continuación se describen algunos de los sistemas más comunes de verificación.

2.1.4. RECONOCIMIENTO DE HUELLA DIGITAL.

En estos sistemas, la huella que se desea reconocer se encuentra entintada en una superficie determinada. El área de la huella digital es explorada por métodos ópticos, digitalizada y transmitida a la unidad de control, la cual guarda esta información junto con los datos de la persona que posteriormente solicitará el acceso.

La identificación se lleva a cabo por comparación, es decir, la unidad de control compara la huella leída con el patrón guardado en memoria. Se comparan con los datos de las pequeñas interrupciones, la terminación de arrugas y ramificaciones de un número de aproximadamente cien marcas impresas en una huella.

La terminal de este sistema cuenta con un "display", un teclado o lector de tarjeta, un dispositivo sobre el cual se pone el dedo del solicitante y un explorador óptico (scaner) para obtener la información de la imagen de la huella digital. El teclado o la lectora de tarjeta, son utilizados para identificar a la

persona, ya sea que introduzca su tarjeta o teclee un número asignado previamente. En el display se indican los pasos a seguir para lograr el acceso.

Es muy común, que el sistema guarde información de más de un dedo, debido a que pueden producirse heridas o daños que causarían un error en la comparación de huellas, si esto ocurre se tiene la opción de cambio de dedo.

2.1.5. RECONOCIMIENTO DE LA FIRMA.

El sistema de reconocimiento de la firma, se basa en la comparación de las características dinámicas del firmante. Estas características son la precisión ejercida al ejecutar la firma y la velocidad con que se realiza. Dos son las técnicas utilizadas para identificar la firma. Una usa un censor de presión especial puesto sobre el escritorio, el cual censa la fuerza aplicada al escritorio por firmante. Con ésta técnica no se requiere de una especial. La segunda técnica, utiliza una pluma especial que censa el movimiento de la punta y además la presión aplicada por el firmante.

El patrón de presión y movimiento de la pluma son diferentes en cada firmante lo que da un alto grado de certidumbre sobre la autenticidad de la firma. La falsificación de la firma original es muy difícil, debido a que la velocidad de escritura y la presión no están directamente relacionadas con la apariencia.

2.1.6. RECONOCIMIENTO DE LA GEOMETRÍA DE LA MANO.

Debido a que desde el momento en que se nace hasta que se muere, las manos cambian y aun así permanecen características en ellas como son: las dimensiones comparativas, la forma de los dedos, la posición exacta de las articulaciones, en fin, innumerables cianotipos complejos que hacen de la mano un elemento único para garantizar una identificación infalible.

El sistema cuenta con una cámara electrónica digital integrada, la cual toma una foto en tercera dimensión de la mano y un microprocesador extrae el patrón único de identidad de la persona en cuestión.

2.1.7. RECONOCIMIENTO DEL PATRÓN DE VOZ.

La persona que desea el acceso al área controlada, entra primero a una cabina para prueba de voz, en donde se identifica a través de un teclado o tarjeta codificada. Debe previamente recordar el mensaje individual que debe repetir frente a un micrófono, dicho mensaje generalmente está formado por cuatro palabras de dieciséis monosílabos aproximadamente. Éstas frases tiene una duración de alrededor de dos segundos. La repetición de la frase en el micrófono es procesada y comparada con los datos en memoria. El sistema compara la amplitud de la onda de voz, además de la frecuencia y el tiempo.

2.1.8. RECONOCIMIENTO DE LA RETINA.

Para un control individual de acceso, en estos sistemas, se analiza el patrón arterial de la retina del ojo. El ojo es expuesto a una cámara que explora el área circular de la retina con un haz de luz infrarrojo de extremadamente baja intensidad. La luz reflejada por el fondo del ojo, es enfocada a un fotosensor que mide la magnitud de la luz en varios puntos distintos a lo largo de 420°. El resultado describe una forma por los datos de los puntos.

En la siguiente tabla se describen los equipos de control de accesos.

EQUIPOS DE CONTROL DE ACCESO						
EQUIPO	DESCRIPCION	CONFIABILIDAD	VELOCIDAD DE RECONOCIMIENTO	PUERTOS DE COMUNICACIÓN	TASA DE ERRORES PERMISIBLES	PRECIO
TARJETAS CODIFICADAS	FOTO	BAJA	BAJA	NO	ALTA	BAJO
TARJETAS CODIFICADAS	CODIGO MAGNETICO	MEDIA	ALTA	SI	MEDIA	MEDIO
TARJETAS CODIFICADAS	CODIGO DE BARRAS	MEDIA	ALTA	SI	MEDIA	MEDIO
TARJETAS CODIFICADAS	DE PROXIMIDAD	MEDIA	MEDIA	NO	ALTA	MEDIO
TECLADO	CODIGO EN MEMORIA	BAJA	MEDIA	SI	ALTA	BAJO
COMPARACION DE VIDEO	CIRCUITO CERRADO DE TELEVISION	MEDIA	BAJA	SI	ALTA	ALTO
RECONOCIMIENTO	IDENTIFICACION DE FIRMA	MEDIA	MEDIA	SI	MEDIA	ALTO

RECONOCI-MIENTO	PATRON DE VOZ	MEDIA	MEDIA	SI		ALTO
BIOMETRICO	IDENTIFICA-CION DE HUELLA DACTILAR	ALTA	ALTA	SI	MUY BAJA	ALTO
BIOMETRICO	IDENTIFICA-CION DE LA MANO	ALTA	ALTA	SI	MUY BAJA	ALTO
BIOMETRICO	IDENTIFICA-CION DE LA RETINA ALTA	ALTA	ALTA	SI	MUY BAJA	MUY ALTO

TABLA I. DISPOSITIVOS DE CONTROL DE ACCESOS

De acuerdo a esta tabla observamos que las opciones más convenientes y recomendables para el control de acceso son los equipos de identificación biométrica.

2.2. SISTEMAS DE CABLEADO PARA REDES.

Para plantear la red soporte de este tipo de sistema se tiene como alternativa para el cableado las siguientes opciones: Par trenzado, cable coaxial delgado, cable coaxial grueso y fibra óptica. Como ya se ha mencionado en el capítulo I las ventajas de cada una de ellos.

En la tabla 2 se resumen las características de cableado propuesto para la instalación de la red.

SISTEMA DE CABLES PARA RED						
CARACTERISTICAS	COAXIAL GRUESO ETTHERNET	COAXIAL DELGADO ETTHERNET	PAR TRENZADO SIN BLINDAR	PAR TRENZADO BLINDADO	FIBRA OPTICA	FIBRA OPTICA
ESPECIFICACIONES DE LA IEEE	802.3 10BASE2	802.3 10BASE2	802.3 10BASET	N/A	FOIRL	802.3 10BASEFL
NUMERO MAXIMO DE NODOS POR SEGUNDO	100	30	2	2	2	2
MAXIMA LONGITUD DE CABLE POR SEGMENTO	500 METROS	185 METROS	100 METROS	150 METROS	1,000 METROS	2,000 METROS
MAXIMA LONGITUD DE CABLE ENTRE NODOS	2.5 METROS	0.5 METROS	0.3 METROS	0.45 METROS	2.5 METROS	2.5 METROS
TIPO DE CONECTOR	AUI (DB-15) N-SERIES	BNC	RJ-45 (ISO 8877)	RJ-45 (ISO 8877)	TIPO-ST II SOBRE BAYONETA o TIPA-SMA SOBRE TORNILLOS	TIPO-ST II SOBRE BAYONETA o TIPA-SMA SOBRE TORNILLOS
CABLE	CONEXIONES RJ-45: 100 OHM AWG 24 DIW PAR TRENZADO SIN BLINDAR 150 OHM AWG 26 DIW PAR TRENZADO BLINDADO CONEXIONES BNC: 50 OHM (RG-58). OPCIONAL 75 OHM (RG-59) 0 93 OHM (RG 62) COAXIAL CONEXIONES AUI: ESTANDAR 15 ALAMBRE AUI TRANSRECEPTOR CABLE PARA CONEXIÓN A 10BASE5 CONEXIONES ST II Y SMA: 50/125 m FIBRA, 62.5/125 m FIBRAS, 85/125 M FIBRAS, Y 100/140 m FIBRA					

TABLA 2. ESPECIFICACIONES DE CABLEADO PARA TRANSMISION DE DATOS.

2.3. SISTEMA DE COMPUTO.

En la red de control de accesos debe de existir un equipo que realice la función de controlador de equipos lectores o detectores. En el cual se almacenan y procesaran los registros y la información proveniente de los equipos de control de acceso. Este equipo bien puede ser una computadora personal (PC). Las computadoras pueden procesar y almacenar grandes volúmenes de información provenientes de sus distintos medios, por ello es que estos juegan un papel muy importante en el sistema de control de accesos.

Existe una gran variedad de computadoras personales por lo que la selección para este proyecto requiere de una vista general de las características de los microprocesadores más comerciales en que se basan dichos equipos. A continuación se muestra en la tabla 3 una comparación de estos. De la misma tabla observamos que debido a sus características de memoria y velocidad, la computadora que realizará la función de controlador es la que utiliza el procesador PENTIUM.

EQUIPOS DE COMPUTO					
MICROPROCESADOR	FABRICANTE	VELOCIDAD	BITS/PALABRAS (MHz)	MEMORIA RAM (Mb)	CACHE (Kb)
80286	INTEL	16	16	2-16	64
80386	INTEL	16-60	32	2-32	256
80486	INTEL	25-66	32	4-64	512
PENTIUM	INTEL	40-90	64	8-128	1 Mb

TABLA 3. EQUIPOS DE COMPUTO

2.4. SISTEMAS CONTROLADORES.

Existen en el mercado una amplia gama de equipos controladores diseñados para resolver de una manera fácil y confiable todas las necesidades de un edificio. Los controladores se dedican a la supervisión y control de los equipos que suministran servicios troncales al edificio, utilizando secuencias lógicas preprogramadas, enfocadas básicamente al ahorro de energía. También son de gran ayuda para disminuir el desgaste de los equipos, al secuenciar su funcionamiento exclusivamente cuando éste se requiere. Los controladores dentro de sus funciones tienen la de controlar el acceso utilizando equipos lectores o detectores conectados al mismo, lo cual nos permite incrementar la seguridad y el control del edificio. En la tabla 4 se describen algunos de los equipos controladores existentes en el mercado. De esta tabla obtuvimos que la mejor opción por sus características es el METASYS IACX-600.

CONTROLADORES						
EQUIPO	MARCA	MODELO	CONFIGURACION	EXPANSION	COMPATIBILIDAD CON OTROS SISTEMAS	PRECIO
CONTROLADOR	METASYS	IAC-600	MODULAR	SI	SI	ALTO
CONTROLADOR	INFINITY	ACX-700	MODULAR	SI	SI	ALTO
CONTROLADOR	JOHNSON	ZAC-9000	MODULAR	SI	SI	ALTO

TABLA 4. EQUIPOS CONTROLADORES.

MODEMS

Los equipos MODEMS (Modulador-Demodulador) son utilizados para transmitir información por medios alámbricos o inalámbricos a distancias tales, que las normas de comunicaciones entre equipos de cómputo, detectores, etc. no nos permitiría, como es el caso de la RS-232 (V.22). En la tabla 5 observamos que de acuerdo a sus atributos y mejoras, la mejor opción es el HAYES ACCURA 24.

MODEMS					
MARCA	MODELO	VELOCIDAD	TIPO DE INFORMACIÓN	NORMA DE COMUNICACION	SINCRONO/ ASINCRONO
HAYES	ACCURA 24	2400	D	V.21, V.22, V.22 BIS	A
HAYES	ACCURA 24BIC + FA	9600	D,F	V.21, V.22, V.22 BIS	A
HAYES	OPTIMA 24	9600	D	V.21, V.22, V.22 BIS	S
HAYES	OPTIMA 24	34800	D,F,V,S	V.21, V.22, V.22 BIS, V.32	S/A
BOCA	FDV 241	9600	D,F,V	V.21, V.22, V.22 BIS, V.29, V.42	A
BOCA	FDV241	9600	D,F,V	V.21, V.22, V.22 BIS, V.29, V.42	A
BOCA	SE1440	57600	D,F,V,S	V.21 V.22, V.22 BIS, V.29, V.42.	S

D= DATOS
F=FAX
V= CORREO DE VOZ
S= SONIDO

TABLA 5. EQUIPOS MODULADORES-DEMODULADORES.

TARJETAS DE COMUNICACIONES.

La tarjeta de red permite que una computadora se comunique con el servidor y las demás computadoras a través de la red general del edificio. Eso permite que la administración de la red llegue al nivel de cada computadora, por ejemplo, el administrador podrá monitorear y actualizar el contenido del disco duro de cada computadora sin necesidad de trabajar directamente con ella.

En la tabla 6 se muestra un comparativo de tarjetas de red, de la cual advertimos que la opción más viable es la 3COM Etherlink III 3C509B-COMBO, la cual nos permite utilizar diferentes medios de transmisión.

TARJETAS DE COMUNICACIÓN

TARJETA DE COMUNICACIÓN	BUFFER	CONECTOR	COMPATIBILIDAD	IRQ'S	SOFTWARE	FAB.	SLOT
AE 200 LC	16K	RJ45 BNC	IBM PC	2, 5,10, 12	NETWARE 286/386 LAN MANAGER FTP PC/TPC		
ELITE 16	16K	AUI BNC	IBM PC, NT, AT	2, 4, 7, 10, 11, 15	NETWARE 286/386 LAN MANAGER V20 LAN SERVER	SMC	
ELITE 16 T	16K	RJ45 AUI	IBM PC, NT, AT	2, 4, 7, 10, 11, 15	DOS, OS/2 UNIX, XENIX	SMC	
ELITE 16 COMBO	16K	RJ45 BNC AUI	IBM PC, NT, AT	2, 4, 7, 10, 11, 15	NETWARE LAN MANAGER	SMC	
ETHERLINK III 3C509	16K	AUI BNC	IBM PC, NT, AT	3, 5, 7, 9, 12, 15	NETWARE 286/386	3COM	ISA

					LAN MANAGER		
ETHERLINK III 3C509-TP	16K	AUI RJ45	IBM PC, NT, AT	3, 5, 7, 9, 12, 15	NETWARE 286/386 LAN MANAGER	3CO M	ISA
ETHERLINK III 3C579	16K	AUI BNC	IBM PC, NT, AT	3, 5, 7, 9, 12, 15	NETWARE 286/386 LAN MANAGER	3CO M	EISA
ETHERLINK III 3C579-TP	16K	AUIRJ45	IBM PC, NT, AT	3, 5, 7, 9, 12, 15	NETWARE 286/386 LAN MANAGER	3CO M	EISA
ETHERLINK III 3C509 COMBO	16K	AUI RJ45 BNC	IBM PC, NT, AT	3, 5, 7, 9, 12, 15	NETWARE 286/386 LAN MANAGER	3CO M	ISA

TABLA 6. TARJETAS DE COMUNICACIÓN ETHERNET.

CONVERTIDORES DE SEÑAL.

La necesidad de intercomunicación de los sistemas de control de acceso, se logra a través de este tipo de equipos, los cuales cambian el protocolo de comunicaciones. Esto con el fin de mantener la comunicación entre los equipos con diferentes medios como son los controladores y los equipos de control de accesos. En la tabla 7 podemos comparar las características de estos equipos, y así discernir de acuerdo a nuestras necesidades cual será el equipo que nos brinde mayores ventajas, en su utilización.

CONVERTIDOR DE SEÑAL							
						CONVERTIDOR DE SEÑAL	
CONVERTIDOR DE SEÑAL	MOD.	SINCRONA	ASINCRONA	MAXIMA VELOCIDAD	CONECTOR HEMBRA RS-232 PUERTO DB25	UNICAMENTE DATOS	TODAS LAS SEÑALES
RS-232 A RS-485/RS-422	HK-IC107AE		SI	64 Kbps	SI	SI	
RS-232 A RS-485/RS-422	HK-IC107C		SI	64 Kbps	SI	SI	
RS-232 A RS-485	HK-IC485AE-R2	SI	SI	64 Kbps	SI		SI
RS-232 A RS-485	HK-IC485C-R2	SI	SI	64 Kbps	SI		SI
RS-232 A RS-422	HK-IC456AE-R2	SI	SI	64 Kbps	SI		SI
RS-232 A RS-422	HK-IC456C-R2	SI	SI	64 Kbps	SI		SI

TABLA 7. DISPOSITIVOS CONVERTIDORES DE INTERFAZ

TRANSRECEPTORES (TRANSEIVERS).

La interconexión entre diferentes canales de comunicación como son cable coaxial, fibra óptica, etc. se logra a través de estos equipos, y estos son muy utilizados en la comunicación entre los sistemas de datos en un edificio por medio de una columna vertebral de comunicaciones (backbone). En la tabla 8 se muestran algunos de estos equipos.

TRANSRECEPTORES						
TRANSRE-CEPTOR	MODELO	CODI-GO	CONECTORES	INDICADORES	NUMERO DE PUERTOS AUI	ESTANDAR
COAXIAL GRUESO	ETTHERNET w/AUI MONITOR	HK-LE003	(1) VAMPIRO (1)AUI 15-PIN M	LEDs: PODER SQE, COLISION TRANS, RECEP	1	IEEE 802.3 ETTHERNET VER.2
COAXIAL GRUESO	ETTHERNET (2 o 4 PUERTOS)	HK-LE050A HK-LE052A	(1) VAMPIRO (2) AUI 15-PIN M (4) AUI 15-PIN M	LEDs: PODER SQE, COLISION TRANS, RECEP	2(LE050A) 4(LE052A)	IEEE 802.3 ETTHERNET VER.2
COAXIAL DELGADO	BNC w/AUI MONITOR	HK-LE004A	(1) BNC (1) AUI 15-PIN M	LEDs: PODER SQE, COLISION TRANS, RECEP	1	IEEE 802.3 ETTHERNET VER.2
COAXIAL DELGADO	BNC (2 o 4 PUERTOS)	HK-LE051A HK-LE053A	(1) BNC (2) AUI 15-PIN M (4) AUI 15-PIN M	LEDs: PODER SQE, COLISION TRANS, RECEP	2(LE051A) 4(LE053A)	IEEE 802.3 ETTHERNET VER.2
PAR TRENZA-DO	10 BASET MICRO LD	HK-LE210A	(1) AUI 15-PIN M (1) RJ-45 H	LEDs:TRANS RECEP, COLISION, ESTADO	1	IEEE 802.3 ETTHERNET VER.2

PAR TRENZADO	PAR TRENZADO	HK-LE111A	(1) AUI 15-PIN M (1) RJ-45 H	LEDs: PODER, SQE, COLISION, TRANS, RECEP, CONEXIÓN	1	IEEE 802.3 10 BASE T
FIBRA OPTICA	FIBRA OPTICA	HK-LE030A-ST HK-LE030A-SMA	(1) AUI 15-PIN M	LED	1	10 BASE FL
FIBRA OPTICA	FIBRA OPTICA (2 o 4 PUERTOS)	HK-LE023A-ST/SMA (2) HKL-E024-ST/SMA	(2)AUI 15-PIN M (4)AUI 15-PIN M	LEDs: PODER, SQE, COLISION, TRANS, RECEP, CONEXIÓN	2(LE023A) 4(LE024A)	10 BASE FL

TABLA 8. DISPOSITIVOS TRANSRECEPTORES (TRANSCEIVERS)

CAPITULO III. CONSIDERACIONES PARA EL DISEÑO DE UNA RED DE CONTROL DE ACCESO.

Objetivo:

Mencionar las principales consideraciones que se deben tomar en cuenta para el diseño e implementación de un sistema de control de acceso a un edificio.

CAPITULO III. CONSIDERACIONES PARA EL DISEÑO DE UNA RED DE CONTROL DE ACCESO.

Dentro del diseño de la red, deberán contemplar todos los aspectos de instalación, mantenimiento, operación, administración, etc., para que en algún instante de la vida de nuestro edificio, se nos vaya a presentar un imprevisto que no haya sido contemplado en el diseño del mismo, por lo que se dividirá este diseño en diferentes planos, los cuales se explicaran a continuación.

3.1. CONSIDERACIONES PARA UNA RED DE CONTROL DE ACCESOS.

Plan de instalación: para la instalación de la red de control de accesos, se deberán de tomar en cuenta ciertas consideraciones para una óptima instalación y una efectiva confiabilidad del sistema.

La protección que ofrece un sistema de seguridad, depende de la forma en que se instala, y de la confiabilidad del sistema.

La protección que ofrece un sistema de seguridad, depende de la forma en que se instala, y de la confiabilidad de sus componentes; si estos se conectan con alambres fácilmente accesibles para los intrusos y las interconexiones se realizan con empalmes de alambres descubiertos, el nivel de seguridad será bajo. Un elemento que se ha diseñado para funcionar en un local, no es seguro si se utiliza en el exterior. Al instalar un sistema, se puede caer en el error de comprar

componentes baratos, lo que puede llegar a tener problemas de falsas alarmas y costos elevados de mantenimiento. Así mismo, se deben considerar los lugares ideales donde estarán situados los cables de conexión, esto es, la canalización debe localizarse en un lugar donde sea susceptible a movimientos bruscos, a su vez debe ser sencillo su manejo en caso de mantenimiento. Los equipos controladores estarán situados en áreas restringidas, dentro del edificio inteligente, esto para brindarle una mayor confiabilidad al sistema. Todos estos aspectos, deben ser tomados en cuenta por el arquitecto y el ingeniero encargado del diseño e instalación de todos los sistemas de control del edificio.

Plan de operación: Dentro de este plan deberá tomarse en cuenta que cada controlador deberá ser capaz de ejercer control y monitorear sus variables independientemente de otro controlador en la red, y deberá contar con un procesador de control digital con contador de tiempo real, para así ejecutar lazos de control (loops).

Los equipos detectores y sensores operarán recibiendo información (codificada o sin codificar) y posteriormente transmitiéndola por la red (control de accesos) hasta el equipo controlador, el cual procesará y almacenará la información que servirá para poder determinar si se dará o no el acceso.

Para el sistema de control de accesos se definirán 5 niveles de accesos de seguridad, los cuales serán asignados de acuerdo a la actividad que realice cada empleado del edificio.

1) Nivel general (personal en general y visitantes).

2) Nivel de servicio (personal capacitado para trabajo en áreas críticas dentro del edificio).
3) Nivel de mantenimiento (personal de mantenimiento o equipos, personal de limpieza).
4) Nivel ejecutivo (personal ejecutivo).
5) Nivel de control y de seguridad (personal de seguridad y monitoreo del edificio).

Así, el personal que labora en el nivel 1, solo tendrá acceso al nivel 2 u superior, por medio de un permiso el cual será habilitado en el nivel 5, ya que estos son los encargados de monitorear la red de control de accesos. Este permiso, se brindará, si existe alguna persona como responsable del acceso al área en cuestión. Esta metodología se realizará cada vez que personal de cierto nivel, quiera acceder a otro superior. No teniendo que efectuar estos pasos si se requiere acceder a niveles inferiores al que se tiene.

Plan de administración; En este plan se deberán se basar los otros planes, además se tomarán en cuenta aspectos relacionados con la supervisión y control de las instalaciones y equipos que integren los servicios básicos del edificio, los cuales se llevaran acabo por medio de un centro de control, cuya localización se determinará de acuerdo al diseño del edificio.

En el cuarto de control central se instalarán los tableros del sistema de alarma, detección, voceo y protección contra incendio, además de conectividad entre la computadora central con el sistema de control de accesos y controles del sistema de circuito cerrado de televisión, debiendo de existir una comunicación bidireccional entre estos y la computadora central. Para el registro de eventos, el

apoyo en acciones de emergencia y la corrección de situaciones de funcionamiento anormales.

La computadora central deberá contar con programas suficientes para llevar a cabo automáticamente las funciones de control, respaldo de información, registro en las bases de datos y notificación impresa y visual de eventos al operador, a quien también le deberá permitir el acceso en tiempo real al conocimiento de estado de los parámetros de operación por medio de gráficos desplegados en pantalla. Así mismo, deberán incluirse programas para llevar a cabo protocolos de pruebas de los sistemas de seguridad y emergencia.

Plan de mantenimiento: Se desarrollarán gráficos para el desplegado de información y para la interacción del operador por pantalla, el nivel de detalle que lo exija cada instalación, permitiendo ubicar fácilmente donde sucedió el evento.

El software contendrá como mínimo las siguientes características:

- Algoritmos de control.
- Horarios para el funcionamiento de los equipos.
- Protección de los equipos de control en caso de falla de energía.

Todos los programas deberán ser efectuados automáticamente sin necesidad de la intervención del operador y deberán ser flexibles para permitir hacer modificaciones y ajustes. Así también ejecutará el manejo de alarmas, estas deberán ser monitoreadas, almacenadas y enviadas para generar reportes directos

a la computadora de control de accesos, sin importar la topología existente en nuestra red.

La red general se configurará en una topología que permita la total conectividad a lo largo de todo el edificio, y a su vez posibilitando una conectividad de máxima flexibilidad y eficacia con otros edificios o áreas colindantes si ello fuese necesario.

El papel que desempeñara nuestra red en un edificio es brindar seguridad y control en el acceso de personal tanto a áreas restringidas, como a las que no lo son. En la fig. 3.1 se muestra una distribución simple de una red de control de accesos.

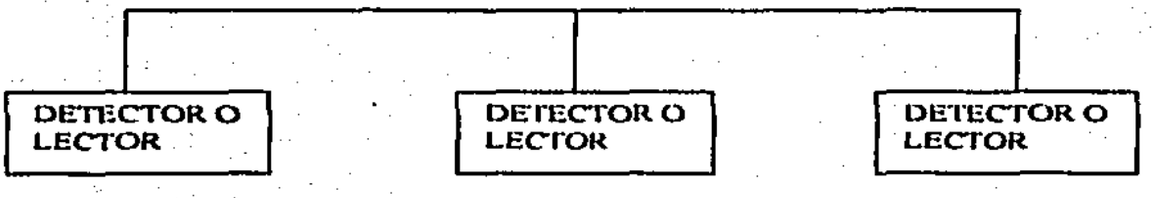

Fig. 3.1 Distribución de una red de control de accesos simple.

En la figura 3.2 se muestra la distribución que se propone, para el diseño de una red de control de accesos. El controlador general del edificio se refiere al CPU que servirá de controlador (administrador) de todos los servicios automatizados que tenga el inmueble. El controlador de la subred de control de accesos, será un equipo CPU de menor potencia y velocidad que el controlador general, esto con la finalidad de evitar el desperdicio de recursos. Y los equipos detectores podrán ser cualquiera de los mencionados en el capítulo anterior, el cual se decidirá de acuerdo a las necesidades específicas del edificio.

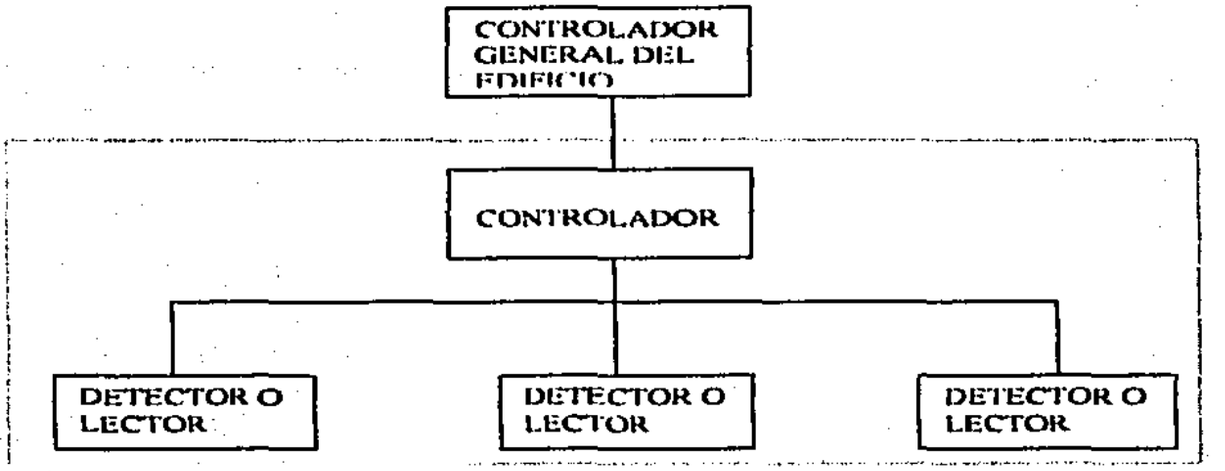

Fig. 3.2 Red de control de accesos.

A continuación se mencionarán características y consideraciones que deben de tomarse en cuenta para la realización de un sistema de control de accesos, tomando en cuenta los avances tecnológicos en el mercado en cuanto a hardware y software.

3.1.1. RED.

El diseño de una red de control de accesos, es brindar la mayor seguridad posible en cuanto al manejo del tráfico de personal en áreas restringidas, también el obtener un control instantáneo de la hora de entrada de usuarios en ciertas zonas. Éste sistema puede utilizarse como reloj verificador localizándolo en las zonas de entrada del inmueble. Con esto se ahorran costos a mediano plazo, ya que al implementar un equipo de detección biométrica se excluye el uso de consumibles como en el caso de los lectores de tarjeta; en los cuales después de determinado

tiempo es necesario reemplazar las tarjetas por el desgaste que sufren por el uso continuo, así mismo cuando se pierde esta por descuido.

Al implementar un detector de parámetros biométricos se inhibe la posibilidad de falsificación del medio de acceso, ya que las características fisiológicas de cada individuo son únicas y permanecen constantes, como es el caso de la huella digital, el iris del ojo y la forma y dimensiones de la mano. Por lo que la detección se basará en dispositivos biométricos capaces de reconocer la forma y dimensiones de la palma de la mano.

La red que soportará el servicio de control de accesos, manejará un tráfico bajo, debido a que la información transmitida por los detectores no será constante, además el tamaño de la palabra es pequeño, por lo que no necesita un gran ancho de banda. Esta red debe tener una alta confiabilidad en cuanto a la calidad de información, con lo que la presencia de errores se reducirá a un nivel casi nulo, también existirán procedimientos para evaluar la calidad de transmisión en cuanto a la detección de errores, debido a ello el sistema de transmisión se basará en la transmisión asíncrona.

El diseño de nuestra red se dividirá en tres áreas, las cuales se explican a continuación.

1) Detección de personas que acceden a cierta área. Esta sección involucra a los dispositivos de detección que cumplen con la función de accesar la información al sistema, la cual será comparada y procesada para obtener o no el acceso a cierta área. La conexión de estos con el (las) computador(as) se hará por medio de equipos MODEM cuando así lo requiera, esto será; si

sobrepase la distancia recomendada por la norma de transmisión que este siendo utilizada, a su vez estos equipos MODEM así como los detectores se conectarán a través de un canal, que podrá ser alámbrico o inalámbrico, esto dependerá de los equipos que se vayan a implementar, así como de los recursos con los que se cuenten para la implementación del sistemas, ya que los equipos con transmisión inalámbrica son más costosos en su mayoría que los alámbricos. Debido a que la información transmitida es escasa y aleatoria, un cableado de par trenzado satisfacerá ampliamente nuestros requerimientos de ancho de banda, velocidad y costo, ya que este tipo de cableado tiene un rango de velocidades de hasta 10Mbps y con una atenuación aceptable, esta área se muestra en la fig. 3.2.

2) Computador(as) de control: Son los equipos que controlan todos los dispositivos de detección que al conectarse a un CPU (computadora personal) lo hacen a través de sus puertos o tarjetas multipuertos, logrando una topología individual para cada computador en estrella; estas computadoras compartirán información y recursos entre si, por lo que al interconectarse logran una topología de bus a través de un cable coaxial delgado con velocidad de transmisión de 10 a 100 Mbps. Como se muestra en la fig. 3.2. Debido a que el tráfico en esta área es más abundante que en la primera, es por lo cual se penso en este medio de transmisión.

3) Backbone. Esta sección tiene el objetivo de conectar las redes locales ubicadas en los diferentes pisos, con lo cual establece un sistema de transmisión común reduciendo costos por concepto de interconexión como son los puentes.

Este sistema de transmisión logra una topología en bus de alta velocidad, los requerimientos del cableado son baja tasa de errores, alta inmunidad a interferencias electromagnéticas, tramos con longitudes elevadas sin la utilización de repetidores, un rango de velocidades de 100Mbps en adelante, un gran ancho de banda y una alta inmunidad al robo o interferencia de las señales.

3.1.2. TELECOMUNICACIONES.

El edificio inteligente debe contar con infraestructura necesaria para brindar servicios de telecomunicaciones, esto con el fin de que el control general del edificio pueda ser monitoreado desde el mismo inmueble o de otro que se encuentre a cientos de kilómetros de forma confiable, para este caso es necesario la utilización de líneas de comunicación que pueden ser:

- Líneas telefónicas.
- Enlaces de microondas.
- Enlaces satélitales.

Esto nos brinda eficiencia en cuanto a los servicios que se ejercen en el edificio inteligente. En el caso de la red de control de accesos existirá una interconexión con el controlador general del edificio. Esta interconectividad nos permitirá realizar envíos de mensajes o correo electrónico entre terminales de supervisión de la red.

Para la interconexión de la red de control de accesos con el controlador general del edificio, se llevará a cabo un proceso de conversión de protocolos, debido a que una red transmite en forma asíncrona y la otra forma síncrona.

3.1.3. SERVICIOS DE ADMINISTRACIÓN.

El control de esta red será distribuido con el fin de no saturar o bloquear los procesos que se llevan a cabo en el controlador de la red, brindándole con esto autonomía a cada uno de los puntos de detección, pudiendo realizar procesos específicos en cada uno de ellos. Esto nos permitirá que en caso de que falle el controlador de la red, no se afectarán los puntos de detección, ya que estos trabajarán independientemente.

Se asignarán claves por grupos o individuales para tener acceso a ciertas áreas.

Se tomarán en cuenta parámetros para futuras expansiones de la red, con la implementación de concentradores, repetidores, convertidores, multiplexores y tarjetas multipuertos de acuerdo a las necesidades requeridas, también se podrán realizar cambios en los medios de transmisión para mejorar los anchos de banda y la velocidad de transmisión.

3.1.4. MANTENIMIENTO Y OPERACIÓN.

Los dispositivos de la red de control de accesos serán supervisados por medio de software el cual monitorea constantemente con el fin de registrar los cambios de

estado que se presenten llevando un registro contínuo de la operación del sistema, con lo que se tiene la posibilidad de identificar fallas o intentos fallidos de acceso, por lo que deberá de contener rutinas para diagnóstico, para corrección de errores, así como envíos de parámetros de control.

Es necesario tener un registro estadístico de los cambios de los dispositivos de la red para detectar los horarios en los que son más necesarios los dispositivos lectores, ya que la posibilidad de presentarse una falla en estos es mayor que en un equipo que no tienen un uso muy frecuente.

El desarrollo de este software se obtendrá directamente de la compañía fabricante de los equipos detectores o en su defecto será realizado por un ingeniero de sistemas.

A continuación se mencionarán los requerimientos de transmisión por partes de la red de control de accesos propuesta.

3.1.5. REQUERIMIENTOS DE TRANSMISIÓN.

Para la implementación de un sistema de transmisión en la red de control de accesos deben de tomarse en cuenta ciertos aspectos para un funcionamiento óptimo, ya que si no existe un cableado que sea flexible para ser utilizado en cualquier tipo de transmisión (voz, datos y vídeo) demeritará en el funcionamiento a futuro de la misma, ya que es posible que en determinado tiempo se cambien los equipos que se utilizan en esta red por otros con una tecnología superior a la actual.

Debido a esto, es necesario utilizar el concepto de cableado estructurado, el cual se forma por medio de transmisión y puntos de conexión, que pueden ser utilizados indistintamente por redes de transmisión de datos, voz y vídeo, que funcionen con equipos de distintos proveedores. De esta forma se pueden tener los cableados para una red aún sin conocer el tipo de red o tecnología a utilizar.

La descripción de estos requerimientos se hará por partes para brindar una información más detallada.

La conexión entre los equipos detectores y el equipo controlador, como mencionamos anteriormente, se realizará por medio de par trenzado. Para esto, nuestro equipo detector contará con un puerto serial de comunicaciones RS-232. Así mismo nuestro equipo controlador contará con una o más tarjetas multipuertos en la(s) que se conectarán los detectores. Dependiendo de la distancia entre estos, se considerará la utilización de equipos MODEM. La transmisión en este punto será asíncrona por lo cual la velocidad de transmisión es baja y no sobrepasará los 96000bps. La detección y corrección de errores en esta parte de nuestra red se dará por medio del código Hamming. Debido a que en la transmisión asíncrona no existe protocolo se utiliza únicamente el medio Start-Stop.

La conexión entre los equipos controladores de la subred (en el caso de existir más de uno) , como con el controlador general del edificio, se hará por medio de tarjetas de comunicaciones , que funcionarán bajo el protocolo de comunicaciones Ethernet (CSMA/CD) y el medio de transmisión será cable coaxial delgado con conectores BNC. La velocidad de transmisión en esta sección rondará los 10Mbps, brindando con esto un perfecto intercambio de

información entre las bases de datos, además de ofrecer información en tiempo real del estado de todos los equipos de nuestra red de control de accesos. La corrección y detección de errores en esta sección de la red se hará por medio del código Manchester.

El controlador general del edificio podrá conectarse al backbone por medio de otra tarjeta de comunicaciones, esta dependerá del protocolo de comunicaciones (sistema operativo) bajo el que este funcionando. El medio de conexión dependerá del diseño del Backbone. Es decir del tipo de medio que se este utilizando como tal (cable coaxial grueso o fibra óptica), teniendo que utilizarse un transceiver para esto.

3.2. ALTERNATIVAS TECNOLÓGICAS.

3.2.1. HARDWARE.

Algunos dispositivos que se pueden implementar en el diseño de la red, son listados a continuación:

Equipos detectores o lectores para control de accesos.

- Tarjetas codificadas con fotografía.
- Tarjetas codificadas con código magnético.
- Tarjetas codificadas con código de barras.
- Tarjetas codificadas de proximidad.
- Teclado con código en memoria.

- Comparación de video.
- Reconocimiento de firma.
- Reconocimiento de patrón de voz.
- Reconocimiento biométrico de huella dactilar.
- Reconocimiento biométrico de la retina.
- Reconocimiento biométrico de la mano.

Cableado

- Par trenzado.
- Par trenzado blindado.
- Cable coaxial delgado.
- Cable coaxial grueso.
- Fibra óptica.

Equipos de computo

- Con microprocesador 80486
- Con microprocesador PENTIUM.
- BOCA FDV241.
- BOCA FDV24IE.
- BOCA SE1440.

3.2.2. SOFTWARE DE PROPÓSITO GENERAL.

A continuación se mencionarán los sistemas operativos bajo los cuales podrá trabajar la red de control de accesos, así como el software con el que puede ser monitoreada la misma.

SISTEMAS OPERATIVOS PARA REDES.

El sistema operativo de una red, es el conjunto de programas que regulan y distribuyen el funcionamiento de la misma, proporciona elementos para establecer la interfase con el usuario, controla y define los grupos y niveles de seguridad, es el encargado de la integridad y seguridad de la información contenida en ella; además controla la compartición de recursos. En general, optimiza los recursos del sistema para un mejor rendimiento y aprovechamiento de los mismos.

Algunas de las tareas que realiza el sistema operativo, para satisfacer las necesidades de los usuarios, y para administrar los recursos de las redes son:

- Manejadores de dispositivos de entrada y salida.
- Un sistema de archivos.
- Interprete de comandos.
- Utilerías.

NOVELL NETWARE.

El Advanced Netware es un sistema operativo de red independiente del hardware, por lo cual puede correr en una gran variedad de redes. Ha estado en el mercado desde 1983 y es el sistema operativo más ampliamente usado en redes de área local.

Novell desarrolló originalmente el NETWARE como el sistema operativo para el equipo NOVELL-S NET. Una red que utiliza una topología estrella y un servidor propietario basado en el microprocesador MOTOROLA 68000. Debido a que este microprocesador no tenía ningún sistema operativo estándar NOVELL decidió desarrollar el suyo partiendo de cero y lo optimizó para redes, diseñando de paso todas sus características alrededor de la funcionalidad de la red.

Cuando comenzó el éxito de las PC (computadoras personales), los autores de NETWARE vieron que, este software esta escrito en lenguaje C, podría fácilmente convertirse a la arquitectura de la familia INTEL 8088 y que podría soportar virtualmente cualquier red en el mercado.

Debido a que el ROM BIOS de la IBM PC XT fue diseñado para un sistema operativo (DOS) de un solo usuario, y como NETWARE es particularmente multiusuario, los programadores de NETWARE decidieron ignorar el ROM BIOS y así comunicarse directamente con el hardware, para eliminar efectivamente cualquier limitación. Lograron con ello, permitir a NETWARE procesar requerimientos de otra estación de trabajo. La única desventaja de esta forma de operar, es la imposibilidad de utilizar las interfaces (drivers) del DOS

para disco duro. NOVELL surte estas interfaces para discos compatibles con IBM y muchos fabricantes surten sus propios drivers para NETWARE.

A continuación se presenta una lista resumida de las principales características del NOVELL NETWARE en el cual se resaltan sus principales ventajas y desventajas.

VENTAJAS.

A) Rendimiento muy superior a los demás sistemas operativos para redes cuando se utilizan de 20 a 100 nodos.
B) Facilidades de conectividad para establecer comunicación hacia otros ambientes ya sea remotos o locales mediante PUENTES o RUTEADORES.
C) Sistema de seguridad completo y eficiente el cual asigna derechos a diferentes tipos de usuarios para la utilización de recursos.
D) Posibilidad de definición de menús mediante una utilería en el NETWARE para accesar a programas en la red o comandos de esta.

DESVENTAJAS.

A) Sistema de mensajes entre usuarios, deja mucho que desear.
B) Requiere de una mayor preparación técnica por parte de los usuarios, principalmente del supervisor de la red, lo cual implica conocimientos de controladores de disco, protocolos de comunicación, direcciones de nodos, etc.
C) Instalación tardada, ya que una adecuada instalación y configuración requiere de varias horas, esto dependiendo de la capacidad del servidor, tiempo en el

cual NETWARE sólo esta verificando partes del disco duro; este problema es posible aminorarlo, ya que el NETWARE solicita al usuario el intervalo de chequeo de pistas del disco duro, lo cual permite calcular el tiempo de formateo.

D) El costo de NETWARE es elevado, lo cual se justifica si la red es grande y/o se requiere alta seguridad en la información contenida. Esta desventaja la elimina NETWARE con su versión ELS diseñada para redes de 4 a 8 nodos.

UNIX.

UNIX, es un sistema operativo que ha evolucionado durante los últimos veinte años hasta convertirse en un entorno e influyente en el mundo. Entre sus características fundamentales se pueden enumerar que:

- Es una poderosa herramienta de software. UNIX introdujo una nueva idea en la computación; la creación de programas de aplicación y la resolución de problemas concernientes a comunicación, programación, etc. pueden ser resueltos mediante la interconexión de programas y procesos simples. Estos programas son diseñados para realizar bien una única tarea, con lo cual, pueden contribuirse grandes aplicaciones a partir de secuencias de orden simples, debido a esto, resulta ser muy productivo al elaborar aplicaciones complicadas con programas simples.

- Facilidad de ser transportado a otras computadoras. UNIX ha sido transportado a casi cualquier computadora construida, de trama; o moderado o grande. Solo unos cuantos cambios o adaptaciones mínimas han sido necesarios para hacer a UNIX utilizable sobre nuevas computadoras.

- Las versiones modernas de UNIX están organizadas para funcionar en un ambiente de red. Las herramientas de comunicación internas del sistema, la fácil aceptación de rutinas de dispositivos adicionales bajo nivel y la organización flexible del sistema de archivos, son naturales para el entorno de red. Usar computadoras en grupos de trabajo es posible gracias a las capacidades de conexión a recursos dispuestos en red que ofrece UNIX.

UNIX ofrece productos para construir redes y las características son las siguientes:

- Permite la ejecución de programas en forma asíncrona.
- Es portable por estar escrito en lenguaje de alto nivel.
- Es modular. Se compone de un conjunto de herramientas básicas que integradas forman estructuras complejas.
- Permite el procesamiento por lotes.
- Presentan una estructura de archivos jerarquía, que ha sido fundamento de muchos sistemas operativos, incluyendo DOS y OS/2.
- Permite la comunicación entre procesos, tienen entrada y salida compatibles, todos los dispositivos y archivos son vistos como archivos.
- Tiene un conjunto de utilerías, entre ellas las que permiten crear, modificar, escribir y desarrollar programas y archivos de texto.

Todas estas razones ayudan a la popularidad que UNIX ha gozado en años recientes, sus bondades están ligadas estrechamente a las del lenguaje C, por haber sido desarrollado con este.

3.2.3. SOFTWARE PARA CONTROL DE ACCESOS.

Existen diversas compañías dedicadas a la fabricación y a la implementación de dispositivos para el control de accesos, los cuales a su vez desarrollan el software necesario para el funcionamiento de los mismos. Como los que a continuación se mencionan.

3.2.3.1. HAND NET

Este software es utilizado para el control de los lectores biométricos, fue realizado en lenguaje C, sin embargo este se ofrece al cliente bajo la característica de programa ejecutable, ya que es un software de explotación y uso general. Las fuentes de este sistema, son propiedad de Recognition Systems, por lo cual podrá ser modificada la información contenida en los archivos de transacciones.

Algunas de sus características son:

- Soporta una red local de hasta 31 dispositivos biométricos lectores de la mano, basado en un sistema de control de accesos con base de datos distribuidos.
- Capacidad para enrolar usuarios.
- Definición de la clave de usuarios (hasta 10 dígitos).
- 62 tiempos de trabajo diferentes (horarios).
- 64 niveles de acceso (por tiempo y lugar).
- Definición de días festivos.
- Monitoreo de la red.

- Control de toda la red desde el concentrador (controlador) para actuar sobre indicaciones específicas (bloquear lectores, accionar puertas, alarmas, etc.).
- Emisión de reportes por:

- Usuario
- Fecha
- Hora
- Lector
- General
- Y combinaciones de los anteriores
- Horarios
- Días festivos

Niveles de acceso.

- Fijar la fecha y la hora de arranque de cada lector.
- Generación de archivos con la información de todas las transacciones en código ASCII. Esto hace que los archivos generados por el software sean 100% transportables a cualquier sistema para su explotación.

Además el software HAND NET brinda la alternativa de manejarlo por medio de menús, los cuales despliegan la siguiente información:

Actividad: Despliega en pantalla todas las transacciones o situaciones del sistema en tiempo real.

Log: Identificación y clave de acceso del operador.

Override: Operación remota de los dispositivos controlados por los handkeys.

Reportes: Emisión de reportes de transacciones, generación de archivos tipo ASCII y listado de los archivos de trabajo.

Uso: Mantenimiento al archivo de usuarios (altas, bajas y cambios).

Configuración: Mantenimiento a los archivos de programación, horarios, niveles de acceso y días festivos.

Download: Envío de parámetros de control de información de usuarios a los HANDKEYS de la red (selectivo o general).

3.2.3.2. SISTEMA DSX-1030

El software DSX-1030 de DSX Access System, Inc.; es líder mundial en el control de accesos, basado en una computadora personal. Este software cuenta con las siguientes características:

Debido a su gran flexibilidad, es posible controlar diferentes tecnologías, como lectoras de tarjetas, lectores biométricos, así como combinaciones de estos. El sistema DSX-1030 es eficiente ya que cuenta con un sistema lector único simple. La transición de un sistema lector único simple a uno con muchas locaciones a través de cientos de kilómetros y conteniendo cientos de lectores de tarjetas, está

logrando con el mismo software y añadiendo más modelos del mismo hardware. El DSX-1030 no depende del hardware, no hay módulos adicionales al software.

En DSX- 1030 los reportes están diseñados para apuntar a la dirección exacta que usted desea, se pueden especificar los rangos por fechas, tiempos, combinaciones de puertas, de división o de compañías, posesión individual de tarjeta o por tipo de evento o combinaciones de ambas. DSX también tiene la utilería de base de datos que permite 16 campos definidos por el usuario de hasta 50 caracteres cada uno por tarjeta. Los títulos de cada campo pueden estar por departamentos, antecedentes escolares, género, tipo de sangre, color de pelo, modelo de carro, o cualquier otro campo definido por el usuario. La búsqueda puede ser generada no solamente en cualquier campo definido por el usuario, sino por la combinación de uno a 16 campos.

La interfase de operador del DSX es fácil de usar, al abrir manualmente una puerta establece una conexión controlada por módem, cada paso es conducido por un menú. El operador cuenta también con una ayuda de contexto sensible. La tecla F1 de cualquier teclado de datos presenta una ayuda en pantalla, con información específica para ese punto en concreto. La seguridad del sistema es brindada por una contraseña única por cada operador, cada operador puede tener acceso a la porción del programa que esta autorizado únicamente.

El sistema DSX-1030 provee 1000 diferentes niveles de acceso, cada nivel describe un grupo separado de puertos, que con la tarjeta pueden entrar. Los niveles de acceso de puertas pueden también programarse con la hora y la fecha del día o días festivos. Este número de nivel de acceso le permite al sistema mejorar a las necesidades que se requieren.

Este sistema puede monitorear hasta 30,000 puntos separados, cada punto puede tener un mensaje único de definición y de acción. Los puntos de alarma pueden ser programados, armados y desarmados por ellos mismos en planes individuales que pueden variar con la hora, los días de la semana y días festivos. Si la alarma es activada, el operador es avisado con una alerta audible. Una descripción del punto de alarma y un mensaje de alerta se despliega, mediante el teclado el operador obtiene el lugar exacto de alarma en la pantalla, así como un alejamiento o acercamiento de ella. Sobre la decisión de la alarma, el operador mediante el teclado especifica la acción tomada y cualquier otro comentario que pueda aclarar el evento. El DSX acomoda hasta 10,000 pantallas gráficas individuales, ambos controles de alarma de entrada y salida son exhibidos en el momento mismo que se requieren, son monitoreados automáticamente tanto local como remota.

Además este sistema cuenta con control de elevadores, para casos locales y de control con módem.

3.2.3.3. SLM.

SLM es el primer programa de administración de tiempo y asistencia, desarrollando en ambiente Windows para las necesidades de las empresas mexicanas. El sistema le permite al usuario interactuar con su nómina, realizar un análisis de las causas que provocan las horas no trabajadas y elaborar la prenómina de manera automática.

SLM le permite identificar de manera inmediata, en un ambiente de ventajas y en forma amigable, las excepciones que se presentaron en cada día de trabajo o por un periodo de tiempo específico.

SLM hace interfase con su programa de nómina y prácticamente con cualquier equipo de control de accesos, lo que le da a las empresas un nivel superior de administración de personal y evita el tradicional verificador de tarjetas. Así mismo, permite fuera de línea, obtener estadísticas sobre la información de las transacciones generadas por los dispositivos de control de accesos. Los principales reportes son:

- Número de eventos por día (por tipo de evento o general).
- Número de eventos por persona.
- Número de eventos por fecha.
- Reporte de ausentismos.
- Integrador de horas trabajadas.
- Número de alarmas por tipo.
- Horas extras autorizadas.
- Permisos, comisiones u otros.
- Vacaciones y/o incapacidades.

El SLM incorpora catálogos de personal que hacen interfase con la nómina, de esta forma no es necesario actualizar dos bases de datos para la administración del sistema.

Gracias a la flexibilidad del sistema y su facilidad de manejo, es posible diseñar reportes de acuerdo a las necesidades específicas de cada empresa, estos pueden

ser, reportes diarios de la asistencia del personal, o del rango de fechas solicitado por el usuario. De la misma manera se pueden elaborar reportes por cada una de las excepciones que se presentaran en el periodo de tiempo que seleccione el usuario. Los reportes son tabulares o gráficos y pueden ser presentados en pantalla o impresos.

Después de haber hecho un estudio a fondo sobre las diferentes alternativas en el diseño de una red de control de accesos, se llegó a la conclusión de que un sistema basado en lectores biométricos Handkey, es el más conveniente para la seguridad y el control de un edificio.

CAPITULO IV. REQUERIMIENTOS PARA LA IMPLEMENTACIÓN DE UNA RED DE CONTROL DE ACCESO.

Objetivo:

Enumerar los requerimientos y procedimientos para la implementación de una red de control de acceso a un edificio.

CAPITULO IV. REQUERIMIENTOS PARA LA IMPLEMENTACION DE UNA RED DE CONTROL DE ACCESO.

En el presente capítulo se plantearán los requerimientos para la instalación y puesta en marcha de los detectores biométricos, con los cuales se supervise y se controle el tráfico de personas; así como los procesos involucrados con la seguridad de los usuarios del inmueble, el manejo de esta información será por medio de la red de control de accesos.

Básicamente los detectores biométricos permitirán implementar un sistema de "Seguridad", Control de accesos y Alarmas" además registrarán los códigos de las personas que quieran pasar de una área de nivel inferior a una superior. Dicho código será cortejado con la información en la memoria del sistema, para verificar el horario, nivel de acceso y secuencia de lectura del mismo. En caso de que estos parámetros sean positivos, el detector desactivará los sistemas de bloqueo para permitir el paso.

Durante el desarrollo de este capítulo, se observarán características que deben tomarse en cuenta para la implementación óptima de cualquier sistema, como son los requerimientos del sistema, procedimientos de instalación y pruebas preliminares. Ya que toda esta información es indispensable para obtener un buen resultado del diseño propuesto.

La protección que ofrece un sistema de seguridad, en control de accesos, depende de la forma en que se instala y de la confiabilidad de sus componentes.

Al instalar una red o sistema, se puede caer en el error de adquirir componentes baratos, lo que puede llevar a tener problemas y costos elevados de mantenimiento, por esta razón es indispensable el saber elegir adecuadamente los equipos que se vayan a utilizar en el diseño de cualquier sistema o red.

Los elementos que se requieren para diseñar la red de control de accesos, son los siguientes:

4.1. HARDWARE.

En cuanto a HARDWARE es necesario:

- Equipos de identificación biométrica (ID3D HANDKEY) sin exceder la cantidad de 31, junto con sus accesorios.
- Un equipo de computo PC o compatible con sus periféricos.
- Tarjeta de comunicación Ethernet 3 COM 3C509.
- Impresora.

HANDKEY.

Como Se ha mencionado anteriormente, este dispositivo es un equipo lector biométrico, cuyos requerimientos de instalación son:

- Voltaje de operación: 12-14 V C.D., corriente de operación: 0.5 A máximo, potencia máxima: 7 Watts, todos estos serán suministrados por una fuente regulada, que cumpla con las características requeridas por el equipo.

- Temperatura de operación: 32 a 110° F (0 a 70° C), para la mejor respuesta de los equipos lectores.

- Humedad de operación: 95% no condensado, para evitar la formación de cortocircuitos por presencia de agua dentro del equipo.

Así mismo existen unos equipos y accesorios indispensables en la instalación de los HANDKEYS, como son:

- Fuente de poder para handkey 13.8 V, 3 A a 60 Hz, la cual alimentará de energía eléctrica a cada uno de los equipos lectores.

- Batería de respaldo de operación 7.0 A/Hr, esta nos ofrecerá la seguridad de no perder información, por falta de energía.

- Driver controlador y alarma audible, los cuales servirán para controlar los lectores desde el equipo de computo.

- Accesorios para fijar el handkey en pared. Este accesorio nos brinda la ventaja de tener el lector HANDKEY totalmente fijo en alguna pared, con lo cual se evitaran problemas de falsos contactos debidos al movimiento de los dispositivos ocasionados al introducir la mano.
- Teclado numérico de salida. El cual servirá para introducir el código numérico, con el cual el software HANDNET podrá buscar en la base de datos el registro solicitado para ser comparado con el registro de la persona que quiera accesar a determinada área en ese preciso momento.

- Semáforo de control (Rojo-Verde). Nos servirá para saber si la comparación del patrón de nuestra mano con el registro efectuado inicialmente ha sido correcto, obteniendo de esta forma la apertura o no de una puerta.

- Botón de liberación de emergencia. Este Botón, nos servirá para liberar una puerta de su cerrojo, sin que sea necesaria la utilización de un dispositivo lector, este estará localizado junto a la puerta, pero en el lado opuesto de donde se encuentre el equipo HANDKEY.

- Botón de liberación de escritorio. Al igual que el anterior, nos servirá para liberar una puerta, nada más que a diferencia del otro este se localizará en un escritorio, el cual deberá ser de la persona a cargo del área restringida.

- Chapa magnética de control de tráfico. Este dispositivo sirve para abrir o cerrar una puerta a distancia, y se controla por medio de una señal eléctrica.

- Monitor de estado de puerta. Como su nombre lo dice, monitorea la posición en la cual se encuentra la puerta, la cual puede ser abierta o cerrada.

- Otro punto que debe ser tomado en cuenta a la hora de diseñar un sistema de seguridad como este, es la canalización por la cual vamos a interconectar nuestros equipos, ya que debe de localizarse en zonas que sean inmunes a ser violadas por algún transgresor. Así mismo deben de encontrarse fijas para evitar movimientos que vayan a ocasionar daño a los conductores, y de esta forma asegurar que no existan falsos contactos ni cortos circuitos.

EQUIPO DE COMPUTO.

Este equipo de computo, realizará la función de controlador central de todos los equipos HANDKEY, de tal manera que trabajará como servidor de los equipos de control de accesos.

Los requerimientos para este equipo son:

- Una unidad de potencia en caso de falta de energía, para asegurar que no se pierda la información.

- 16 Mb en RAM, con lo cual se optimiza el software.

- Microprocesador PENIUM a 133 MHz.

- Monitor a color SVGA. Con el cual se pueden obtener los gráficos y tablas necesarios para una buena administración de la red de control de accesos.

- Disco duro con 1 Gb, para asegurar que quepa el software tanto de control de accesos, puntualidad y asistencia. Así como las bases de datos de los usuarios.

- Mouse para un manejo rápido y simple del software.

- Otro requerimiento en la instalación, es una óptima conexión con la red general del edificio, la cual se logrará por medio de una tarjeta de comunicaciones, que necesariamente requiere un bus de expansión para su instalación.

TARJETA DE COMUNICACIONES ETHERNET 3COM 3C509.

Esta tarjeta nos permitirá enlazar la red de control de accesos, con la red general del edificio, es compatible con IBM, PC, XT y AT, utiliza conectores AUI y BNC.

- El requerimiento indispensable para esta tarjeta, es un bus de expansión ISA o EISA para la instalación de la misma en el equipo controlador.

- Que exista un canal de comunicaciones, para interconectar las dos redes anteriormente descritas.

- Temperatura de operación de 0 a 70° C. Así como humedad de 10 a 90% no condensada, para un óptimo funcionamiento.

IMPRESORA.

Al tener este dispositivo conectado al equipo de computo, nos permitirá obtener reportes impresos de todos los eventos, transacciones y alarmas que se registran en el sistema, por lo que debe cumplir con las siguientes características:

- Del tipo de inyección de tinta, con velocidad de impresión de 240 caracteres por segundo, 2 páginas por minuto.

- Dirección de impresión bidireccional en modo texto y unidireccional para el modo imágenes.

ESTA TESIS NO DEBE SALIR DE LA BIBLIOTECA

- Resolución hasta 720 x 720 ppp. Para la perfecta impresión de los gráficos.

- Cartuchos de tinta, múltiples a color, para una mejor presentación y definición de los reportes y gráficos.

4.2. SOFTWARE.

El SOFTWARE indispensable, es:

- Sistema operativo para redes (UNIX).
- Sistema para control de accesos HANDNET.
- Sistema de tiempo y asistencia (SLM).

Así mismo existirán dos medios de comunicación, los cuales están conformados por:

- Cableado de par trenzado y coaxial delgado.
- Convertidor de interfase RS-232/RS-485.
- Un transreceptor.

SISTEMA OPERATIVO UNIX.

Como hemos mencionado en el capítulo anterior existen algunas ventajas que nos brinda UNIX para el control del edificio, ya que tanto las aplicaciones como los programas de comunicaciones están entrelazadas al sistema operativo, lo cual redunda en una conexión ágil y abierta entre sus aplicaciones y sus comandos.

Además de estar perfectamente documentado y de existir una amplia bibliografía sobre el sistema.

Al ser un sistema multiusuarios y multitareas ofrece un potencial amplio para realizar diversas funciones al mismo tiempo, con lo cual se vuelve más versátil el control del sistema, en este caso el edificio.

HANDNET.

Todos los paquetes de software necesitan determinadas características en cuanto a hardware e incluso software, para poder ejecutarse de una forma óptima, para el HANDNET, en especifico, requerimos:

- En cuanto a Hardware; una computadora personal o 100%compatible con IBM, con microprocesador 486 o superior, 4Mb en RAM mínimo, 30Mb en disco duro como mínimo para cargar el paquete junto con sus librerías, un puerto paralelo para impresora. Así como un puerto serial para interconectarse con los lectores HANDKEYS y un ratón (mouse) para el mejor manejo del software.

- Los requerimientos en cuanto a software para que el HANDNET pueda trabajar sin ningún problema son: sistema operativo MS-DOS 6.0 o superior y Windows 3.1 o superior.

SLM.

Los requerimientos indispensables para la instalación de este software de tiempo y asistencia son:

- Equipo de computo PC o compatible con microprocesador 486 o superior, 4 Mb en RAM, 40 Mb en disco duro y un ratón

- En cuanto a software es necesario que el equipo tenga un sistema operativo MS-DOS 6.0 o superior y la interfaz gráfica windows 3.1 o superior.

4.3. SISTEMAS DE COMUNICACIÓN.

En este punto describiremos las características de los dos sistemas de comunicación existentes en este diseño.

CABLEADO.

Para la comunicación entre los equipos HANDKEYS, se utilizará cable de par trenzado (cable telefónico), al menos dos pares calibre 20 o 22 AWG. Se sugiere utilizar par trenzado blindado para protección del ruido eléctrico ambiental.

La interconexión entre la red de control de accesos con el backbone, se hará por medio de cable coaxial delgado, tipo Thin Ethernet Plenum.

CONVERTIDOR DE INTERFASE RS-232 A RS-485.

El convertidor IK107AE de Black Box, nos permite conectar uno de los equipos HANDKEY al equipo controlador (PC), teniendo una velocidad de transmisión de 64Kbps, una potencia de 8 Watts y 230 VAC a 50-60 Hz. Este tipo de convertidor opera de forma bidireccional,, transmite y recibe señales de datos.

TARJETA DE COMUNICACIONES 3COM ETHERLINK 3C509.

Inicialmente se instalará la tarjeta de comunicaciones (o se dará de alta si ésta ya existe), para lo cual tendremos que mover la cubierta de la computadora y escogeremos un slot de expansión que se encuentre libre para instalarla, para el caso de esta deberá ser un slot ISA o EISA.

Al instalar la tarjeta es preciso tener cuidado en su manejo, ya que esta puede sufrir daño debido a corriente estática, por está razón es necesario eliminar esta corriente de nuestro cuerpo, esto se consigue tocando el chasis metálico de la computadora con nuestra mano. A continuación de esto podemos agarrar e insertar la tarjeta en el slot designado, tendiendo cuidado de que esta quede perfectamente insertada, entonces podemos fijarla por medio de tornillos al chasis, de esta manera esta lista para iniciar su configuración la cual consiste en los siguientes pasos:

- Cargar los manejadores de la tarjeta en el disco duro de la computadora.
- Configurar por medio del software del fabricante.

4.4. PROCEDIMIENTOS DE INSTALACION.

INSTALACIÓN DEL HANDKEY.

El HANDKEY es un equipo electrónico el cual contiene dispositivos de lectura de datos para el control de accesos como son: el teclado y el dispositivo biométrico (lectura geométrica de la mano). Este equipo tiene la tarea de activar o desactivar un acceso de acuerdo a la información que recibe de los dispositivos lectores. Es por esta razón que los HANDKEYS se instalarán cerca de los dispositivos de acceso y no podrán estar expuestos a fenómenos meteorológicos ni a rayos solares. Se instalarán sobre una base, o empotrados en la pared, dependiendo del lugar donde se vayan a localizar.

La instalación sobre una base, se llevará a cabo con un pedestal, el cual deberá estar anclado al piso. Se recomienda que se tenga un metro de altura con respecto al piso; Así como usar las bases de goma del lector para proporcionar mayor adherencia a la superficie. Para fijar el lector se recomienda realizare cuatro perforaciones ¼" en la superficie de montaje. Usar abrazaderas 6-32 de 3/8" de largo, para sujetar el HANDKEY en la superficie, así como usar arandelas planas en cada una de las abrazaderas.

Las conexiones eléctricas pueden realizarse a través de agujeros de 7/8" que se encuentran en la parte trasera del panel, las cuales permiten un conducto de ½" apropiado para el cableado del lector, cabe mencionar que cuando se usa cable blindado el conducto más apropiado es el de ½".

Para una instalación más fácil y segura del cableado externo se recomienda destapar la parte trasera del lector. Para destaparlo, es necesario seguir las instrucciones que se indican en el instructivo. Una vez que se ha realizado las conexiones necesarias tapar el lector nuevamente.

Para fijación en la pared o empotrado, se usara un accesorio especial, el cual deberá localizarse a 1.05 mt. Sobre el nivel del suelo. Cuando el montaje es de este tipo la puerta trasera no se utiliza, la ejemplificación de esta fijación se muestra en la fig. 4.1.

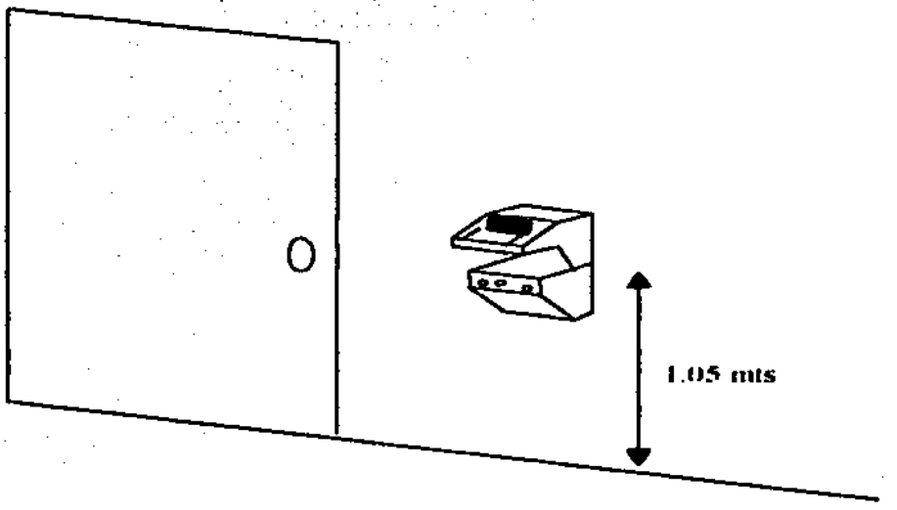

Fig. 4.1 Fijación del Handkey en la pared.

Cuando el montaje del lector sea empotrado en la pared, se sugiere que aproximadamente 3.5" del lector queden dentro de la misma, sobresaliendo solo la parte del display y el teclado del HANDKEY. Las conexiones eléctricas pueden estar dentro del montaje en la pared usando el conducto localizado en la parte trasera hasta una terminal de conexión. Es ampliamente recomendable que la instalación cuente con tierra física.

En la tabla 9 se enlistan las terminales de conexión del equipo HANDKEY. Así como una breve descripción de las mismas.

1	+13.8 VCD	POWER
2	-13.8 VCD	INPUT
3	RXD	
4	GROUND	CH-1 RS 232
5	TXD	
6	-RT	
7	+RT	CH-0
8	-NT	RS422/485
9	+NT	
10	DO/DATA/A-X	
11	GROUND	
12	DI/CLK/LOCK	OUTPUT
13	DOOR SWITCH	
14	GROUND	
17	REX SWITCH	
18	+5 VOLTS OUT	
19	DO/DATA	CARD
20	CARD PRESENT	READER
21	DI/CLOCK	INPUT
22	GROUND	

Tabla 9. Terminales del lector Handkey

Las conexiones de potencia son las siguientes:

- Voltaje de entrada: 12-14 VCD
- Voltaje de carga fluctuante: 13.5-13.8 VCD
- Corriente de entrada: 0.5 A
- Potencia de entrada: 7 Watts

Se recomienda usar la fuente de poder IS-400 de Recognition Systems, la cual proporciona tales requerimientos. La fuente de potencia debe ser conectada directamente a las terminales de potencia +13.8 VCD (1) y la tierra (2). La distancia del lector de mano a la fuente de poder o la Batería debe ser razonablemente corta. Se recomienda el uso de cable mínimo del calibre 16.

La parte negativa de la fuente de poder debe ser conectada a tierra. Esta conexión es en la fuente de poder no en el lector. En caso de falla puede ser que la tierra elegida no sea la correcta.

El alambrado del interruptor de estado de puertas es requerido para señalar los accesos autorizados. El interruptor debe ser del tipo normalmente cerrado, cuando la puerta se encuentre cerrada. Deberá operar con 0.5 mA y 5 VCD. El interruptor debe ser conectado a la terminal No. 22 para su cableado.

La cerradura de la puerta también es controlada por el lector HANDKEY, este debe ser programado para una salida lock/aux y se debe desactivar el jumper W4 del lector.

El cableado para circuito de control auxiliar puede ser usado para un control local de luces y alarmas, o señales remotas para dispositivos de monitoreo de alarma. Esta salida proporciona 15 VCD a 0.1 A máximo. La carga debe conectarse directamente a las terminales No. 10 (aux. out) y No. 1 (+13.8 VCD) se recomienda usar cable del número 18.

CONEXIÓN ENTRE HANDKEYS.

Los HANDKEYS son interconectados en forma de red (LAN) para proporcionar una mayor eficiencia. Cuando se usa este tipo de configuración los HANDKEYS se interconectan a través del puerto de comunicación serial RS-485.

La topología de la red, es de tipo bus, debido a que presenta simplicidad en su instalación y flexibilidad para incrementar el número de HANDKEYS, el número máximo de equipos en red será de 31 FIG. 4.2.

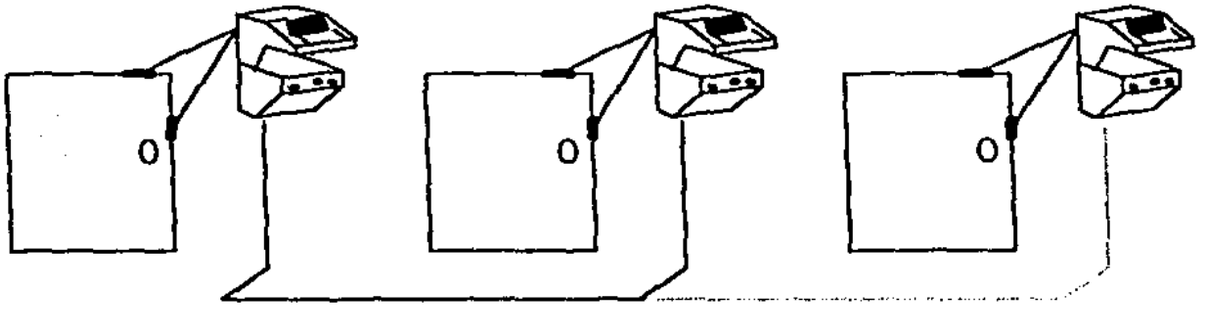

Fig. 4.2 Conexión entre HANDKEYS.

El medio de transmisión y conexión que se usara para los HANDKEYS es cable telefónico, o sea par trenzado del tipo blindado, 22 AWG. El blindaje debe romperse para la conexión de los lectores, se debe conectar un lado del blindaje a la terminal No. 4 de tierra del lector y el otro lado la siguiente lector. En caso de no tener tierra entre dos lectores, estos deben ser interconectados por el blindaje. No se debe olvidar que la distancia entre HANDKEYS no debe exceder los 1,200 mts.

Conectar un par trenzado a las terminales (7) + RT y (6) – RT del lector de mano. Todos los lectores deben tener activado el jumper W5. Se recomienda respetar el código de colores en el sistema (ver sección técnica del apéndice A), tal que todas las terminales +RT y –RT sean conectadas correctamente unas con otras. Los lectores de los extremos finales del par trenzado deben estar interconectados a la tarjeta OEL y el jumper W7 activado.

CONEXIÓN ENTRE HANDKEY Y EL CONTROLADOR DE LA RED.

Al tener interconectados los handkeys en red, es necesario tener un equipo controlador central para el registro y control de eventos, para nuestro caso en particular, será una computadora personal, la cual registrará todos los eventos que se realicen en la red y a su vez permitirá la comunicación con la red del edificio. FIG. 4.3.

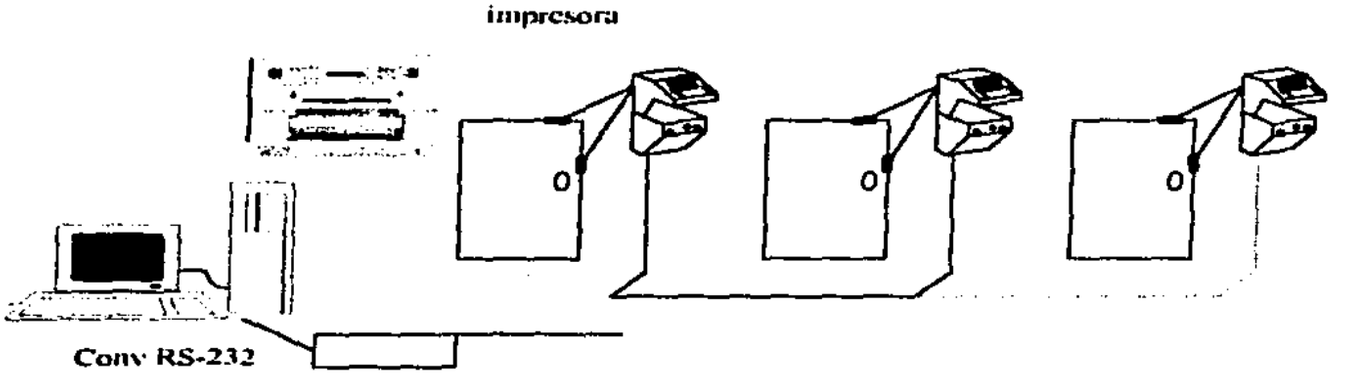

Fig. 4.3 Conexión entre HANDKEYS y el controlador de la red.

La conexión entre el controlador (PC) y los handkeys, se realizará por medio del puerto de comunicaciones RS-232 de la PC y el RS-485 de los equipos hadkeys, por lo cual es necesario implementar un convertidor de interfase RS-232 – RS-485. Ya que la transmisión es baja y el volumen de datos reducido, se utilizará par trenzado blindado como medio de transmisión.

Para tener un control óptimo de las operaciones realizadas en nuestra red, tendremos conectada una impresora a nuestra computadora personal, lo cual permitirá obtener reportes impresos de los eventos, transacciones y alarmas que se registren en el sistema en tiempo real.

CONEXIÓN ENTRE LA RED DE CONTROL DE ACCESOS Y AL RED GENERAL DEL EDIFICIO.

Para la conexión entre la PC y el backbone del edificio, se hará uso de una tarjeta de comunicaciones 3COM ETHERLINK 3C509, un transreceptor y cable coaxial delgado. La tarjeta de comunicaciones nos permitirá establecer la comunicación entre la red general del edificio y la red de control de accesos, ya que cada una de las redes tienen características diferentes, en cuanto a velocidad, tipo y canal de transmisión; esta interconexión se hará al nivel de la capa física del modelo de referencia OSI.

La red de control de accesos tiene una velocidad de transmisión de 9600 Kbps, la transmisión es asíncrona sin un gran ancho de banda, el canal es cable de par trenzado. En cambio en la red general del edificio la velocidad de transmisión es de 10 Mbps, la transmisión es síncrona con un ancho de banda mayor, debido a

que los volúmenes de información que se transmiten son mayores y el medio de transmisión es un cable coaxial delgado.

El procedimiento que se debe llevar a cabo para hacer esta interconexión, se describe a continuación.

- Inicialmente se instalará o se dará de alta la tarjeta de comunicaciones (si esta ya existe), para lo cual tendremos que mover la cubierta de la computadora y escogeremos un slot de expansión que se encuentre libre para instalarla, para el caso de esta deberá ser un slot ISA.

- Ya habiendo conectado y dado de alta tarjeta, conectaremos esta con el transreceptor. El último paso en cuanto a hardware, será conectar el transreceptor con el backbone del edificio.

4.5. PRUEBAS PRELIMINARES DE OPERACIÓN.

PRUEBAS INICIALES A LOS EQUIPOS HANDKEYS.

Las pruebas que se pueden efectuar, se realizarán por medio del software Handnet, y estas consisten en comprobar que todos los nodos de la red estén activos y que pueda efectuarse la comunicación entre ellos.

Antes de realizar estas pruebas es necesario revisar que el canal serial cero este seleccionado para operar como un enlace de datos RS-422 o RS-485. Para operar como RS-422 el jumper W5 debe ser desactivado y el W7 estar activo.

Para aplicaciones de red estándar, el canal cero debe operar como RS-485. En este caso, el jumper W5 debe estar activado en todos los lectores de red y el W7 activado sólo en el lector de cada extremo final del par trenzado RS-485. Los lectores por defecto tienen el jumper W5 activado y desactivado el W7.

En cada prueba del lector se debe verificar que opere como se describe en la sección de operación. Cada uno de los lectores tiene salidas de chequeo individual, para ellos se debe conectar la unidad registradora hacia la red para completar las conexiones de las terminales 6 y 7 de cada lector. Se debe asegurar de que el lector este configurado como lector de registro.

Entonces se debe de entrar al Modo Comando y seleccionar Network Status (Estado de Red). En el display de la unidad de registro se debe observar el estado de la red así como que los lectores estén en línea.

Colocar el control de accesos en línea y en tiempo. Direccionar los lectores en un rango de 0 a 31. Conectar el lector hacia la red a través de las terminales 6 y 7 para completar las conexiones.

PRECAUCION

Recordar que todos los lectores deben tener direcciones en la red. Usando el display de la unidad de registro en Network Status, verificar que se tenga las comunicaciones de red establecidas entre la unidad de registro y los lectores de control de accesos.

Una vez que todos los lectores estén conectados, probar la red registrando patrones individuales usando el lector de registro y verificar que estén registrados sobre las estaciones de control de acceso. En seguida checar completamente las salidas del sistema y familiarizarse con su operación para probar todos los comandos del sistema.

PRUEBAS PRELIMINARES A LA TARJETA DE COMUNICACIONES 3COM ETHERLINK 3C509.

Es necesario estar seguro de que los manejadores (drivers) de red o administradores de memoria han sido instalados antes de correr el programa de configuración y diagnóstico.

Existen diferentes tipos de pruebas para diagnósticos de la tarjeta como son, a los componentes físicos y a la configuración de la misma.

Si alguna de estas pruebas falla, esto no quiere decir necesariamente que el adaptador este defectuoso. El problema puede ser la elección incorrecta de los parámetros, esto es, que existan conflictos entre los parámetros del adaptador y los de otras tarjetas, o de una instalación impropia.

Para asegurar una buena instalación es necesario seguir los siguientes pasos:

a) Asegúrese de que la tarjeta está bien conectada en el slot de expansión.

b) Inspeccione todos los cables y conexiones.

c) Asegúrese de que su computadora haya arrancado bajo el sistema operativo correcto para el cual se están instalando los controladores.

d) Si se esta corriendo el grupo de pruebas para los adaptadores 3C509 coax., 3C579 coax. o 3C509-COMBO coax., asegúrese de que el conector de ciclo (loopback) este perfectamente conectado al adaptador, o que el adaptador este conectado a un cableado conveniente y la red este inactiva.

e) Asegúrese de que los parámetros para el adaptador no son los mismos usando en otra tarjeta instalada en la computadora.

4.6. RECOMENDACIONES.

Una vez que los lectores son instalados y conectados como se describe, la potencia puede ser aplicada y la instalación probada.

Antes de aplicar potencia, se debe asegura que el voltaje de la fuente de poder sea el correcto así como la polaridad, de lo contrario podría causarse daños al equipo.

Cuando se inicia la operación del lector, la cámara de exposición automáticamente se activa, antes de cualquier operación se debe asegurar que la placa y los espejos estén limpios y libres de obstrucciones.

PROCEDIMIENTO PARA VERIFICACIÓN DE IDENTIDAD.

1. Si se lleva un anillo gírelo hasta que la piedra este cara arriba.

2. Introducir el ID a través del teclado.
3. Deslizar la mano firmemente con la membrana entre los pins.
4. Cerrar los dedos entre los pins hasta que las luces sobre el panel salgan.
5. Mantener los dedos y la palma de la mano contra la plataforma.
6. Remover la mano cuando en el display se indique "remove hand" (quitar la mano) o "ID verified" (identidad verificada).

NOTA. Si se registra un usuario con anillos grandes, este debe traerlos puestos siempre que quiera una verificación de lo contrario no será reconocido. Se recomienda tener una copia del procedimiento cerca del lector de mano.

REGLAS PARA COLOCAR CORRECTAMENTE LA MANO.

a) Deslizar la mano hacia delante sobre la placa, de tal forma que los dedos toquen el pin respectivo.

b) Todos los pins deben estar en posición normal, en caso de romperse uno se sugiere cambiarlo por uno nuevo.

c) Puede usarse la mano izquierda con la palma hacia arriba. Si se usa este método, el registro debe ser con la palma hacia arriba.

CONCLUSIONES

Uno de los resultados más fascinantes y notables obtenidos a partir de los avances tecnológicos, en el área de seguridad son los apartados de identificación biométrica; los cuales brindan un alto grado de inmunidad a falsificaciones, ya que esta tecnología se basa en el reconocimiento de un rasgo corporal único, por lo que reconoce a las personas y no a objetos. La llegada de estos dispositivos al mercado electrónico, permite integrarlos en diseños que brinden un alto grado de seguridad. Debido a esto, se decidió implementar estos dispositivos en el diseño de una red de control de accesos.

La implementación de estos dispositivos biométricos en este tipo de red no solo nos permite el control de la seguridad en cuanto accesos, sino que también sirve para llevar un registro de puntualidad y asistencia al software SLM.

Gracias a la ventaja que nos brinda el utilizar a una computadora personal como controlador de la red, tenemos comunicación con la red general del edificio inteligente por medio de una tarjeta de comunicación Ethernet. Esto nos da la opción de accesar a la información de la red desde cualquier terminal autorizada en el edificio, para obtener información estadística, reportes en pantalla y escritos por medio de una impresora, lo cual facilita la administración de la red.

Al trabajar de esta forma, los costos de administración del inmueble se reducen y le brindan mayor funcionalidad y seguridad, además de obtener un mejor control del personal que accesa a zonas restringidas.

GLOSARIO

Ancho de banda. Rango de frecuencias asignadas a un canal el sistema. La diferencia expresada en Hertz entre las frecuencias más alta y más baja.

Archivo de datos. Conjunto de registros relacionados organizados de una forma específica . En sistemas grandes, los archivos de datos están siendo remplazados gradualmente por bases de datos a fin de limitar la redundancia y mejorar la confiabilidad y la puntualidad.

ASCII (American National Standar Code for Information Interchange, X-4-1986). Es un código de paridad de 7 bits establecido por el American National Standars Institute para lograr compatibilidad entre datos y consta de 96 caracteres mayúsculos y minúsculos visibles en la pantalla y 32 caracteres de control no visibles.

Base de datos. Conjunto no redundante de elementos de datos interrelacionados procesables por una o más aplicaciones. Juego de archivos con conexión lógica entre sí tiene un acceso común.

Backbone. Red de distribución Vertical.

Bit. Es un dígito binario.

Bps (bit por segundo). Unidad básica para medir la velocidad de comunicación de datos. Unidad de velocidad de transmisión igual al número de condiciones discretas o eventos de señales por segundo.

Bus. Organización de vías de acceso eléctricas en un circuito.

Byte. Un grupo de bits al que se le conoce como carácter, puede ser de 8,16,32 o 64 dependiendo la tecnología que se use.

Canal de comunicación	Sinónimo de línea o enlace. Trayectoria para comunicación de datos.
CCITT.	Comité Consultivo Internacional para Telefonía y telegrafía. Organización establecida por estados unidos para desarrollar estándares mundiales de tecnología de comunicaciones.
Codificación Manchester.	Medio a través del cual se pueden combinar señales de datos y reloj independientes en un caudal de datos autosincronizable, adecuado para la transmisión en un canal serial.
Colisión.	Múltiples transmisiones concurrentes en el cable, generando datos desorganizados.
Computadora personal (PC).	Nombre alternativo de microcomputadora, que sugiere que la computadora será utilizada para realizar trabajo personal e individual o para mantenimiento.
Comunicaciones.	Transmisión de inteligencia entre puntos de origen y recepción sin alteración de la secuencia o estructura del contenido de la información.
Comunicación de datos.	Transmisión y recepción de datos, a menudo incluyendo operaciones como codificación, decodificación y validación.
Conectividad.	En una LAN, posibilidad de cualquier dispositivo conectado al sistema de distribución de establecer una sesión con cualquier otro dispositivo.
Conector BNC.	Conector de cable coaxial de la serie BNC de 50 Ohms de 50 del tipo que se encuentra comúnmente en equipo RF.
Conexión.	Punto de acceso, con un conector adecuado, a un medio de comunicación.

Confiabilidad. En comunicaciones de datos o equipo de computación, es el grado en el que el hardware o el software opera en forma receptible, a menudo caracterizado (en el caso del hardware) como un tiempo medio entre fallas (MTBF) bajo.

Controlador de la red. Es una computadora personal (PC) que se encarga de realizar las funciones centralizadas básicas, para las que se diseño la red.

Control de acceso al medio. (MAC). Porción de la estación de datos 802 del IEEE que controla y media el acceso al medio.

CPU. (Central Processing Unit). Unidad Central de procesamiento. "Cerebro" de la computadora de uso general que controla la interpretación y ejecución de instrucciones. La CPU no incluye interfaces, memoria principal o periféricos.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Acceso múltiple con sensibilidad de portadora, con detección de colisiones. Método de acceso a redes para manejar colisiones de paquetes de datos.

DB-25. Designación de un juego de clavija y enchufe normalizado que se utiliza en el alambrado RS-232C; tiene un conector de 25 espigas (pines).

Detección de la portadora. Señal generada por la capa física para la subcapa de acceso con el fin de indicar que una o más estaciones transmiten en ese momento en el cable troncal.

DOS. (Disk Operating System o Sistema operativo de disco). Termino general empleado para definir el sistema operativo que se utiliza en computadoras con unidades de disco.

Enlaces de datos. Montaje de dos o más instalaciones de terminales e interconexión de canales de comunicaciones que operan de acuerdo con un método particular que permite el

	intercambio de información.
Estación.	Dispositivo físico que se puede alcanzar con una LAN con medio compartido con el fin de transmitir y recibir información en ese medio compartido.
Estación de trabajo.	Equipo de entrada/salida en el cual trabaja el operador.
Estación de trabajo del administrador.	Microcomputadora que contiene un paquete integrado de software diseñado para elevar la productividad de los ejecutivos o administradores. En general, aunque no exclusivamente, una estación de trabajo incluirá un procesador de palabras, una hoja de cálculo, un programa de comunicaciones y un manejador de datos.
ETD.	Equipo terminal de datos.
ETCD.	Equipo terminal de circuito de datos.
Ethernet.	LAN y su protocolo asociado producido por (pero no limitado) Xerox, Digital Equipement Corporation e Intel. Ethernet es un sistema de banda base.
Hand key.	Lector de geometría de la mano registrado por System Recognition Inc.
ID.	Identificación de identidad.
IEEE	(The Institute of Electrical and Electronics Enginners, Inc.) Instituto de Ingenieros Eléctricos y electrónicos.
Interfase.	Frontera compartida entre elementos del sistema; definida por interconexiones físicas comunes, señales y significados de señales intercambiadas.
Interfase de la unidad de enlace (AUI).	El cable, conectores y circuitos de transmisión que se utilizan para interconectar el subcapa de señalización física y la MAU.

ISO/OSI (International Standards Organization Open Systems Interfase). Organización Internacional para Normalización. A este cuerpo de normalización internacional se le conoce mejor en el ambiente de comunicación de datos por el desarrollo del modelo de red de siete capas, con reconocimiento internacional, que se denomina "modelo de referencia para interconexión de sistemas abiertos" (OSI en inglés).

Jumper. Puente de conexión.

MAU. Unidad de conexión al medio.

Microprocesador. CPU de una computadora que contiene los elementos lógicos para manipular datos y realizar operaciones aritméticas o lógicas con ellos. Es un C.I. que usualmente realiza todas las funciones de unidad central de proceso de una computadora.

Módem (MODulador/DEModulador). Dispositivo que modula y demodula (o desmodula) señales transmitidas a través de instalaciones de comunicación. A menudo, un módem se conoce como conjunto de datos.

Netbios. Sistema básico de entrada-salida para red.

Nodo. Cualquiera estación terminal, computadora u otro dispositivo en una red de computadoras.

Octeto. Elemento orientado a bits que consta de ocho bits binarios contiguos.

Ordenador. Computadora.

Password. Palabra de pase o palabra clave.

PIN (Personal Identification Number). Número de identificación personal. El cual permite asignar un conjunto de números, los cuales tienen la función de operar como clave para obtener acceso en algún

	dispositivo de seguridad.
Periférico.	Equipo de cómputo externo a la CPU que realiza diversas funciones de entrada y salida.
Procesamiento de transacciones.	Estilo de procesamiento de datos en el que se actualizan archivos y se generan resultados de inmediato como consecuencia de la entrada de datos.
Programa.	Conjunto de instrucciones escritas en un lenguaje de programación que se utiliza para definir una operación o conjunto de operaciones para una computadora.
Protocolo.	Conjunto formal de convecciones que rigen el formato y la sincronización relativa de intercambio de mensajes en una red de comunicaciones.
Puente.	Dispositivo de conectividad que trabaja en la capa de enlace (2) del modelo de referencia OSI.
RAM	(Random Access Memory). Memoria de acceso aleatorio. Dispositivos de memoria semiconductora que se utilizan en la construcción de computadoras. El tiempo que se requiere para obtener datos es independiente de la ubicación.
Red centralizada.	Red de computadoras con un nodo de procesamiento central a través del cual circulan los datos y comunicaciones.
Red de área local (LAN).	Red de computadoras y comunicaciones que cubre una área geográfica limitada, que permite que todos los nodos se comunique con todos los otros nodos, y no requiere un nodo o procesador central.
Red de computadoras	Un o más computadoras enlazadas con usuarios o entre si vía una red de comunicaciones.
Red de comunicacion	Red total de dispositivos y medios de transmisión (radios, cables, etc.) necesarios para transmitir y recibir

es.	inteligencia.
Repetidor.	Dispositivo que se utiliza para extender la longitud, topología o interconectividad del medio físico más allá de las especificaciones impuestas por un solo segmento, hasta la máxima longitud aceptable de la línea de transmisión troncal en una sesión de comunicación.
ROM	(Read Only Memory). Memoria sólo de lectura. Dispositivo de memoria que se utiliza en computadoras y que no puede ser alterado durante el uso normal de la computadora. Normalmente es un dispositivo semiconductor.
RS-232C.	Estándar de comunicación publicada por la Electronic Industries Asociation (EIA), que corresponde a la tercera versión revisada de la norma original RS-232. Compatible con la recomendación V.24 de la CCITT. Es la interfase localizada entre el ordenador, o terminal, y el módem es un ejemplo de protocolo de la capa física, en el que debe especificarse en forma detallada los aspectos mecánico, eléctrico, funcional y procedual de dicha interfase .
RS-422.	Norma que se utiliza en conjunto con la RS-449 para especificar las características eléctricas de circuitos balanceados.
RS-499.	Norma de la Electronic Industries Association para conectar el equipo terminal de datos y el equipo de circuito con mayores velocidades de transmisión, longitudes de cable más grandes y diez funciones adicionales. Se han añadido varios circuitos que no estaban presentes en la RS-232C.
RS-485.	Norma de la Electronic Industries Association, sucesora de RS-232C y RS-449. Interfase entre equipos terminales de datos y equipos de control de acceso o seguridad.

Ruteador.	Dispositivo de conectividad que trabaja en la capa de red (3) del modelo de referencia OSI.
Señal (codificada).	Símbolo de autoridad que se transmite entre estaciones mediante el uso de un método de acceso de señales para indicare qué estación tiene el control del medio en un momento dado.
Sistema de manejo de datos.	Sistema que proporciona los procedimientos y programas necesarios para colectar, organizar y conservar archivos de datos o base de datos.
Sistema operativo.	Programa que maneja el entorno de Hardware de un sistema de computación.
Software.	Término que se utiliza para diferenciar programas de computadora de los "fierros" o hardware de un sistema de computación.
Terminal.	Dispositivo que hace posible la entrada y la salida de datos de una computadora. El término se utiliza con mayor frecuencia asociado con un dispositivo que tiene un teclado para entrada de datos y una impresora o un monitor de vídeo para presentar datos.
Topología.	Descripción del arreglo geométrico físico de los nodos y enlaces que forman una red, conforme a su conexión física.
Transmisión asincrónica.	Modo de transmisión de comunicaciones de datos en la que los intervalos de tiempo entre caracteres transmitidos pueden ser de longitud desigual. La transmisión es controlada por elementos de inicio y suspensión al inicio al final de cada carácter de aquí que se el llame transmisión de inicio y suspensión.
Transmisión de señales (codificadas).	Técnica de evasión de colisiones en la que se escudriña a cada estación y debe pasar el resultado de esta revisión por línea.

Vía de acceso. Hardware y software necesarios para hacer que dos redes tecnológicamente diferentes se comuniquen entre si; una vía de acceso ofrece conversión de protocolo de una arquitectura de red a otra y puede, por lo tanto, utilizar las siete capas de referencia OSI.

Wiegand. Estándar de transmisión de datos.

BIBLIOGRAFIA

Andrew S. Tanenbaum
Redes de ordenadores
Prentice-Hall Hispanoamérica, S.A.
México, 1991

Uyless Black
Redes de computadores
Protocolos, normas e interfaces
Macrobit Editores S.A de C.V.
México, 1990.

AT&T
Manual del SYSTEMAX PDS
México, Marzo, 1994.

BESCO Sistemas de seguridad
Control de accesos
México, 1994.

Recognition System, Inc.
ID3D-R Handkey Han Reader Operating and Installation Manual.
Cabell, U.S.A.,1990.

IMC Networks
Repeaters: What are they? And Why do I need them?
Invine CA, U.S.A., 1993.

ERICSSON S.A. DE C.V.
Redes inteligentes
Sistema de gestión de voz y datos Manual
México, 1990.

Northern computer, Inc. (Atapco Security and comunications group)
Acceses Control Solution Manual
Milwakee, WI. U.S.A., 1991

Northem Telecom (Cala) Corp.
Red de distribución integrada para edificio Manual
Miami Lakes, Fl. U.S.A 1993

Jhonson Controls Inc.
Metasys netware sales resource Manual
Inteligent Access Control
Milwakee, WI. U.S.A., 1992

PEI COBB FREED AND PARTNERS
"Anatomía de un edificio inteligente"
Arq. Sergio Zepeda
México, 1991

SAINCOMEX S.A DE C.V.
Edificios Inteligentes
México, 1993

Black Box Catalogue
The source for connectivity
LAN, WAN Y DATACOMM
México, 1994

Northem Telecom Inc.
LAN MAXIMER
Soluciones para redes de alta capacidad Manual
Morton Grove, Illinois U.S.A., 1993

IMEI
Productos y soluciones
Edificios Inteligentes
México, 1993

3COM
Tarjetas de comunicación para red
Etherlink
U.S.A., 1994