UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

ACCESO A UNA SUBESTACION ELECTRICA VIA REMOTA

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICISTA
P R E S E N T A:

HORACIO ALBERTO RODRIGUEZ TORAL

DIRECTOR DE TESIS: ING. ELEAZAR MARGARITO PINEDA DIAZ

MEXICO 2006

CONTENIDO

INTRODUCCIÓN

El presente trabajo aborda el funcionamiento de un sistema de adquisición e intercambio de información enfocado a la industria eléctrica. Esto se justifica dado que la interdependencia de casi toda actividad humana con el mundo de la informática es cada vez más amplia, y el desempeño de la ingeniería eléctrica por supuesto no le es ajeno y menos cuando esta rama del conocimiento es una de las que más desarrollo en la materia ha alcanzado.

Los objetivos de esta tesis son: servir como medio de consulta para estudiantes cuyas asignaturas tengan que ver con sistemas de redes computacionales, comunicaciones digitales, con las nuevas subestaciones que están compuestas por dispositivos electrónicos inteligentes, que no son otra cosa que pequeñas computadoras organizadas de manera tal que hacen muy eficiente la operación de protección de un sistema eléctrico, quien este interesado en saber los fundamentos de lo que en la actualidad esta tan presente en la vida cotidiana, me refiero al la internet, así como la caracterización de un ruteador comercial.

El tema uno contiene temas que en principio explican que es un sistema de control y adquisición de datos ya que los esquemas de distribución de energía eléctrica de la actualidad funcionan en base a ellos. Esto nos ayuda a entender el desarrollo de la comunicación entre computadoras, que comienza con sistemas realmente sencillos de adquisición de datos y de baja capacidad de procesamiento, hasta llegar a configuraciones que permiten un intercambio masivo de información.

Se definen los protocolos de acceso a redes más representativos, es decir la manera en que las computadoras se comunican entre si, esto para observar como el crecimiento del volumen de información provoca que los protocolos de comunicación se vayan tornando ineficaces dando lugar a otros que sean capaces de gestionar ya no solo datos sino también la capacidad de procesar imágenes y audio en grandes cantidades. Dentro de este tema se hace mención, a la seguridad de nuestras transmisiones que cada vez más se ve amenazada por virus informáticos y en algunos casos por la llamada fuga de información. Para finalizar este apartado hago mención de la tarea que desarrolla un dispositivo llamado ruteador, que finalmente es al que estudiaremos con más detalle en el segundo tema.

En el tema dos se describen las características generales de funcionamiento del ruteador, es decir, sus especificaciones, modos de interactuar en un sistema de comunicaciones y por supuesto su configuración para nuestro estudio. Este apartado es importante ya que siempre es oportuno tener en cuenta todos los

datos técnicos posibles con el fin de minimizar errores, y de encontrarlos, contar con las soluciones propuestas por el fabricante y ahora con la facilidad que se ofrece en internet de encontrar foros de discusión que pueden ayudarnos a enfrentar una gran cantidad de problemas que puedan surgir.

El tercer tema explica la importancia de mantener comunicación con determinado sistema eléctrico vía remota, esto con la finalidad, que toda empresa tiene de abatir costos y mejorar el servicio. Asimismo, para predecir fenómenos que provoquen falla o bajo nivel de productividad. Y ahora más cuando la mayoría de las subestaciones y otras instalaciones de suministro eléctrico son no habitadas, es decir que son completamente automáticas. Además se describen algunos equipos que nos permiten la adquisición de datos como son los dispositivos electrónicos inteligentes, en este caso relevadores microprocesados, que han desplazando a los antiguos sistemas de protección que únicamente abrían tal o cual circuito sin aportar datos adicionales que permitieran hacer estadísticas de comportamiento y programas de mantenimiento mas puntuales. También se mencionan las tarjetas de adquisición de datos como parte fundamental, así como algunos equipos que nos permiten la interconexión, sin olvidar claro, el tema de las interfaces.

En el último tema explico lo que habremos de observar una vez que establecemos comunicación con la computadora dedicada a monitorear una subestación eléctrica. Para ello nos valemos de un programa desarrollado ex profeso en el que se muestra mediante diagramas unifilares y ventanas de lectura en tiempo real, el estado que guarda la subestación, es decir, si está operando normalmente, hay una línea con falla, un relevador que ya no acciona, la temperatura del aceite en un transformador esta alcanzado niveles potencialmente peligrosos, un interruptor esta llegando a su limite de aperturas y por lo tanto necesita ser cambiado; o simplemente para verificar que la subestación esta marchando conforme a las normas. Y recabar información en las bases de datos con la cual se haga una evaluación de su funcionamiento para determinar si se esta trabajando sin perdidas o también para poder prevenir posibles anomalías.

TEMA 1. GENERALIDADES

1.1 Introducción.

En la actualidad es imprescindible tener en forma organizada, actualizada y con un costo razonable la información de un proceso cualquiera, que sin el apoyo de un sistema de medición y/o procesamiento de datos basado en sistemas electrónicos no seria posible dada la enorme cantidad de variables que se toman en cuenta. Los equipos de medición han pasado de simples sistemas de registro a complejos sistemas de almacenamiento y análisis de la información. Se dispone de bases de datos que se pueden consultar en tiempo real y complejos métodos de análisis para detectar cambios no previstos en el funcionamiento de un sistema y/o alcanzar el desempeño deseado del mismo, para satisfacer las cada día más estrictas condiciones de funcionamiento y al mismo tiempo obtener datos que nos lleven a la mejora continua de su desempeño.

Los sistemas de información se pueden clasificar en función de la forma en que procesan la información: tiempo real y lote. En el primer tipo, tiempo real, la información registrada es procesada inmediatamente, presentado los resultados para se tomen acciones inmediatas. Este tipo de sistemas son usados en la operación de procesos y se conocen como Sistemas de Control y Adquisición de Datos o por sus siglas en ingles “SCADA” (“Supervisory Control and Data Acquisition”). En general, el segundo tipo de sistemas almacena la información obtenida en campo para su posterior procesamiento. Este tipo de sistemas son usados en el pronóstico y estimación de necesidades.

Con la presencia cada vez más acentuada de sistemas informáticos en los ámbitos mas diversos de la actividad humana, y en particular de la microelectrónica, a niveles económicamente accesibles en la década de los 80´s, el uso de equipos electrónicos para la captura y procesado de información se ha vuelto una tarea común en variadas disciplinas del quehacer humano. Desde hace algunos años, el cambio que ha generado la microelectrónica hace que en muchos de los sistemas con el cual el hombre interactúa se disponga de equipos electrónicos para el manejo de la información y la operación de sistemas. El factor económico continúa siendo un limitante para el uso de la nueva tecnología para el manejo de la información. Sin embargo, este fenómeno es común en las nuevas tecnologías, pero tiende a estrecharse con lo que se va haciendo más accesible para un mayor número de aplicaciones.

En los países con gran desarrollo tecnológico, los sistemas electrónicos de manejo de información son más económicos que la mano de obra y equipos requeridos para procesar y capturar la información con los métodos manuales de procesamiento.
Según la aplicación que se pretenda automatizar será el tipo de sistema de información usado y el costo involucrado en su instalación, operación y mantenimiento.
Es necesario determinar claramente las características del sistema de información requeridos para un sistema de distribución eléctrica por ejemplo, al hacer una mejor predicción del crecimiento de demanda de energía que viene en función generalmente del crecimiento poblacional. Las ventajas y desventajas de un sistema, y sus características técnicas deseadas, tendrán un costo inicial y otro de operación y conservación. Es imperativo analizar ambos desde la etapa de concepción del sistema de información, el no solicitar alguna características técnicas puede traer un sobre costo de operación y conservación mayor a los ahorros logrados en la instalación del sistema.

Sistemas SCADA

Ya se menciono que los sistemas de operación y/o supervisión en tiempo real de procesos asistidos por computadora son conocidos con el nombre de SCADA. Estos sistemas están constituidos por tres componentes: estación central o maestra, sistema de comunicación y estación remota de medición y operación (ERMO) de los cuales se da una breve descripción.

1.- La estación maestra esta formada por el equipo de cómputo y programas que almacenan, organizan, presentan y analizan la información recabada en campo. Según el sistema, la estación maestra se encarga también de administrar los recursos de comunicación como puede ser radios, cable, teléfono, microondas, satélite, etc. La estación maestra informa a las ERMO sobre las tareas asignadas.
2.- El sistema de comunicación permite diferentes alternativas para recabar la información del proceso obtenida por las ERMO o informar a éstas sobre las actividades por realizar. Las alternativas van desde la transmisión manual de datos, el uso de radios, fibra óptica, microondas, satélite, etc. En función de la aplicación e infraestructura disponible, buscando siempre la solución más confiable segura y económica, se determina el medio de comunicación por usar. Hoy día, la mayoría de estas alternativas de comunicación presentan costos similares si se considera su duración a largo plazo.

3.- La estación remota de medición y operación esta compuesta por los equipos ubicados en campo que están en contacto directo con el proceso a medir y/o controlar. La ERMO está formada por tres componentes: la Unidad Terminal Remota (UTR), sensores y actuadores. Según la aplicación es posible encontrar en la ERMO un equipo de comunicación.

a) La UTR se encarga de manejar los equipos ubicados en la ERMO y presenta tres componentes: entradas-salidas analógicas y digitales, unidad central de proceso y puertos de comunicación:

1. La unidad central de proceso de una ERMO esta formada un microcontrolador. Que se encarga de administrar los recursos del sistema para realizar las tareas encomendadas de acuerdo con la programación introducida. Tiene diferentes alternativas de programación, y entre las más usadas están la lógica de escalera y, en fecha más reciente, el lenguaje ¨C++¨.

2.- Las entradas-salidas digitales y analógicas son los medios de comunicación entre el proceso a medir y controlar y la ERMO. Estas le permiten recibir (entradas) la información recabada por los sensores y enviar (salidas) a los actuadores además de información sobre las tareas a realizar. La información puede ser de dos tipos digital y analógica. La información digital solo puede tomar valores de verdadero (1) o falso (0). Las salidas analógicas toman valores continuos en el tiempo, dentro de un rango establecido previamente. Por lo general el rango es de 0 a 10 volts C.D. y a una corriente de 20 mA . Los rangos usados son estándares industriales ampliamente usados por los fabricantes de UTR, sensores y actuadores.

3.- Por último, los puertos de comunicación tiene como finalidad permitir el intercambio de datos con otros equipos digitales. Hoy día se cuenta con puertos de comunicación serial RS-232 o RS-485 así como puertos de comunicación del tipo Ethernet, como los usados en redes de computadoras.

b) Los sensores son los equipos que a partir de diferentes principios físicos y químicos miden el funcionamiento de un proceso. Estos sensores presentan una salida que es proporcional a la variable medible. Generalmente los sensores usan alguno de los formatos mencionados anteriormente para dar a conocer el valor de la variable medida. Existen sensores que se comunican en forma digital con la UTR mediante el puerto serial o Ethernet.

c). Los actuadores son los equipos que modifican el funcionamiento del proceso. Estos pueden recibir tanto señales analógicas como digitales que determinan su funcionamiento. Al igual que los sensores, existen actuadores que disponen de puertos de comunicación digital con el cual se comunican con la UTR.

El contar con sensores y actuadores que disponen de sistema de comunicación digital permite aumentar la velocidad y cantidad de información disponible. Lo cual se traduce en un mejor y más seguro intercambio de información y por consecuencia una mejor supervisión y operación del proceso.

1.2 Protocolos de acceso al medio.

El protocolo IEEE 802,3 original, proviene de la estandarización de un producto comercial: la red Ethernet, patentada por Intel, DEC y Xerox. La diferencia entre ambas redes estriba en que el protocolo de acceso Ethernet se integra a un protocolo de enlace de datos, mientras que IEEE 802.3 requiere el servicio de enlace LLC. En cualquier caso, ambas redes son compatibles.
El protocolo de acceso definido por la norma IEEE 802.3, se trata de un protocolo CSMA/CD con características además persistentes. Por tanto, se pueden producir colisiones en la operación del protocolo en las siguientes dos situaciones:

- Cuando una estación detecta el canal como libre pero en realidad, debido al tiempo de propagación de las señales en el mismo, otra estación ya había empezado a transmitir.

- Cuando más de una estación intenta transmitir durante el tiempo de transmisión de una trama en curso, una de ellas se “espera” a que acabe la primera, y después del llamado tiempo entre tramas colisionan en el acceso al canal.
La interfaz entre el MAC y el nivel físico se realiza a través de la denominada Capa Física de Señal ó PLS (Phisical Layer Signaling), que es independiente del medio de transmisión y que se comunica con el MAC mediante:

- Una señal de detección de actividad en el canal.
- Una señal de detección de colisiones.
- Un puerto de transmisión de datos.
- Un puerto de recepción de datos.

La característica de detección de colisiones permite a una estación abortar la transmisión de la trama en curso en cuanto se detecta la colisión. La ventana de detección de colisiones es igual a dos veces el tiempo máximo de propagación de la señal en el canal y, por tanto, depende únicamente de la longitud del mismo y de los recargos introducidos por los elementos repetidores entre segmentos.

Cuando la estación detecta una colisión deja de transmitir la trama y genera una secuencia especial de bits, denominada de JAM, para que todas las estaciones se den por enteradas de la colisión y no haya confusión con algún espurio en el canal, y entra en lo que se denomina una ventana de resguardo, definida así por el llamado algoritmo de resguardo ó back-off que consiste en lo siguiente:

- Cada una de las estaciones implicadas en la colisión realiza un cálculo de tiempo denominado de resguardo dependiente del número de intentos de transmisión con colisión.
- El tiempo de resguardo se calcula de forma pseudo aleatoria eligiendo entre 0 y 2↑i-1 slots de tiempo, donde i es un contador de intentos de retransmisión.
- Cada estación espera el número de slots de tiempo elegidos antes de reintentar la transmisión.
- Si las estaciones eligen el mismo número de slots volverán a colisionar, y cada una de ellas incrementa su contrador i.
- Antes de transmitir, la estación comprueba si canal está libre y si no es así, espera a que quede libre al finalizar la trama en curso y el denominado tiempo entre tramas.

Si la carga de información en el canal es considerable, la posibilidad de transmitir sin colisiones es muy baja, por ejemplo, para cargas del orden del 30%, los tiempos de acceso al canal pueden ser del orden de segundos, inaceptables para muchas aplicaciones. Todo ello se debe el carácter absolutamente estadístico y aleatorio en el que se basan los cálculos para sistemas de comunicaciones.
El nivel físico realiza la codificación de línea de las señales en código Manchester de tiene como principal ventaja su carácter autorreloj, lo que permite la sincronización de bit a los receptores a partir de un preámbulo de 10101010 repetido ocho veces en la cabecera de la trama. En recepción, el nivel físico realiza la codificación inversa de Manchester a NRZ.
En cuanto al formato de la trama hay que destacar el carácter lineal de las direcciones de MAC o físicas, compartido por las demás normas IEEE y los tamaños mínimos y máximos del campo de datos. Los campos son:

- Preámbulo: 7 bytes, para sincronización de la lógica de recepción.
- Delimitador de comienzo: 1 byte, idéntico a los del preámbulo pero con el último bit a 1.

- Dirección de destino y dirección de origen: 2 o 6 bytes, direcciones físicas la más que identifican a la placa de red.
- Tamaño del campo de datos: 2 bytes
- Datos: entre 0 y 1500 bytes, contiene la trama de LLC.
- Relleno: entre 0 y 46 bytes se utiliza para garantizar que el tamaño de la trama sea mayor o igual que 64 bytes.
- Prueba ó Cheksum: 4 bytes, calculado a partir de un polinomio generador de grado 32 se recalcula en recepción, se compara, y si no coincide el codificado con el calculado la trama es descartada.
- La norma fija un tamaño mínimo de trama en 64 bytes y un tamaño máximo en 1526 bytes por las razones siguientes:
- Según la definición original de la norma, en la que se define un canal de longitud máxima de 2500 metros, formado por cinco segmentos de 500 metros y 4 repetidores, para una velocidad de transmisión de 10 Mbps, el tiempo de slot (dos veces el tiempo máximo de propagación) durante el cual se puede producir una colisión, coincide con el tiempo de transmisión de 64 bytes por lo que al fijar un tamaño mínimo se permite distinguir tramas de colisiones.
- Se fija un tamaño máximo para reducir en lo posible las colisiones producidas al final de la transmisión de cada trama, y obtener al mismo tiempo una utilización razonable del canal sin que ninguna estación lo monopolice.

Una trama se considera inválida si se dan algunas de estas circunstancias:

- El tamaño es inconsistente con el codificado en el campo de datos.
- El cálculo de la comprobación ó cheksum no coincide con el codificado.
- El número de bytes no es exacto (trama desalineada).
- La trama es más corta que el valor mínimo (error runt).
- La trama es más larga que el valor máximo (error jabber).

Se define como colisión cuando dos estaciones accesan al medio simultáneamente, sin tener necesariamente carácter de error.
Básicamente existen dos tipos de protocolos de acceso al medio:

- Con colisiones

- Libres de colisiones

En los protocolos con colisiones el que éstas se produzcan forma parte del protocolo de acceso, donde por medios generalmente estadísticos o aleatorios la desahoga y, en definitiva, permite el acceso multiplexado de las estaciones al canal compartido. Las dos características principales de estos protocolos son:

- bajas prestaciones frente a cargas moderadas.
- bajo costo por su sencillez.

Algunos ejemplos genéricos de estos protocolos son:

- ALOHA
- ALOHA ranurado
- CSMA 1 persistente
- CSMA no persistente.
- CSMA p-persistente
- CSMA con detección de colisiones (CD).

Por otra parte, los protocolos de acceso al medio libres de colisiones, básicamente establecen un orden en la generación de tramas por parte de las estaciones que impide que dos estaciones accedan simultáneamente al canal. Se caracterizan por:

- buenas prestaciones incluso con cargas altas.
- mayor complicación y costo.

Estos protocolos se basan generalmente en algún mecanismo de paso de mensaje de permisos de tal forma que la estación sólo está habilitada para transmitir en posesión del testigo. Este mecanismo puede incrementarse tanto topologías de bus como de anillo.
Por lo anterior un protocolo destinado a una estación maestra de SCADA determina el intercambio de información con las Unidades de Transmisión Remota (UTR´s); estableciendo las convenciones necesarias, la trayectoria normal de comunicaciones y un elemento de datos estándar. Un protocolo es un concepto lógico, no una conexión física. A una conexión física se le llama interfaz. Al correr del tiempo, los fabricantes de UTR y las plantas de servicio han desarrollado

protocolos sin buscarle estandarización, es decir, la UTR de la compañía no puede comunicarse con la estación maestra de la compañía si no utilizan el mismo protocolo. La mayoría de los fabricantes de SCADA desarrollan emuladores de los protocolos de cada uno, mientras que algunas compañías mantienen protección de derechos de autor de sus protocolos.

1.3 IEEE 802.3u 100Base-T Fast Ethernet.

1.3.1. Introducción.

Esta tecnología es un estándar abierto internacional (IEEE 802.3u), no ha sido desarrollado ni es propiedad de ninguna compañía. Este tipo de estándar abierto protege la inversión de una compañía en tecnología por asegurar un nicho de mercado flexible y competitivo. Los derechos para desarrollar, fabricar y vender productos Fast Ethernet no tienen que ser comprados o licenciados. Cualquier compañía puede desarrollar productos Fast Ethernet, favoreciendo la competitividad y la bajada de precios.
Estos factores hace que esta tecnología sea dominante en muchos entornos, pues son los mismos factores que hicieron líder en su ámbito a su predecesor Ethernet en los años 80 y principios de los 90.

1.3.2. Área de uso.

Fast Ethernet es una tecnología de Red para Área Local (Local Area Network) y esta diseñada para conectar computadoras sobre un área pequeña, como pueden ser oficinas, edificios o pequeñas instituciones como un campus universitario de tamaño pequeño, por ejemplo. Esta tecnología no esta pensada para ser utilizada sobre áreas extensas, como campus de gran tamaño o ciudades enteras, para estos entornos se usaran tecnologías de Red para Área Extensa (Wide Area Network), que son sistemas diseñados para conectar elementos de una red o una red completa de Área Local a otros elementos o Redes de Área local sobre un área extensa.
Una posible definición de LAN puede ser: "Un sistema de conexión directa entre varias computadoras".

- Sistema: Las Redes de Área Local se estructuran con diferentes componentes, como cables, repetidores (comúnmente llamados hubs), interfaces de red (también conocidas como tarjetas de red ó NIC (Network Interface Card), nodos, y protocolos. Todos estos elementos juntos forman una red, si alguno de estos elementos falla, no tendremos una red.
- Conexión: Las redes proveen conectividad, un camino para que las computadoras intercambien distintos tipos de información, como pueden ser archivos de texto, vídeo, voz, etc.
- Directa: Todos los elementos se comunican entre si a través del mismo medio (cable y aparatos conectados a él), sin mas elementos intermedios en su comunicación.
- Varias: Computadoras: Es una red de computadoras, no seria tal si no hay por lo menos dos computadoras conectadas entre si.

Como ejemplo de uso de una Red de Área Local tenemos la compartición de archivos y el uso de impresoras comunes, además se tiene la oportunidad de que los discos duros de cada ordenador de la red sean accesibles por los otros miembros firmados en la red, realizándose las operaciones sobre los discos de otros equipos de la misma manera que se utiliza el propio, y esto sin mencionar al administrador de la red que tiene la posibilidad de gestionar según sus propósitos, los recursos de red que estén disponibles o incluso implementar nuevos recursos.

1.3.3 Características

a) Prestaciones.

Fast Ethernet es una red de comunicación de datos en serie, a través de pares de cobre o fibra óptica. Su velocidad es de 100 Mbits por segundo, siendo posible la comunicación en ambos sentidos (full-dúplex). Esto permite tasas de transferencia de hasta 12.1 Mbps.

b) Topología.

Fast Ethernet usa una topología lógica de bus, y físicamente tiene forma de estrella (ver figura 1.3.1, con los nodos conectados a un repetidor (hub)) central. Este repetidor actúa como el bus de la red, además se encarga de limpiar eléctricamente la señal y permiten que, si una conexión falla, las demás sigan funcionando.

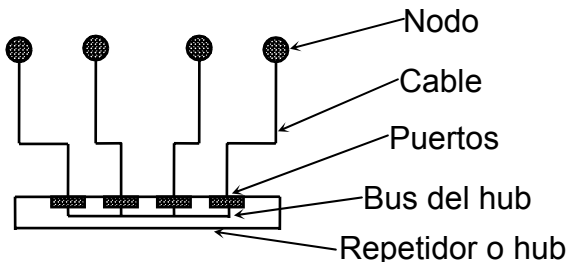


Figura 1.3.1 Topología Fast Ethernet.

c) Forma de Comunicación.

Los nodos (Computadoras, impresoras, dispositivos electrónicos inteligentes, etc.) se comunican entre ellos por medio de marcos (frames), que es su unidad básica de comunicación, como se puede ver en la figura 1.3.2, es una estructura o manera de organizar los datos, sabiendo a quien debe llegar y de quién procede. Para lograr este objetivo, a cada nodo se le asigna una dirección única, diferente de la del resto de los nodos (MAC address), sin entrar en demasiados detalles, esta dirección se aloja en la interfaz de red de cada nodo, teniendo cada tarjeta que hay en el mercado una dirección diferente. Así, un marco se estructura en tres campos de datos, uno para la dirección de destino, otro para la dirección fuente, y un tercero donde se envían los datos que sí mismos queremos enviar, llamados datos del mensaje o payload.

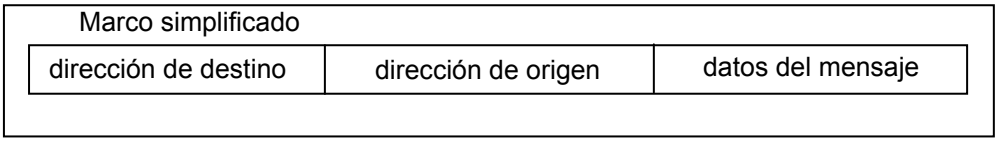


Figura 1.3.2 Estructura de un marco unidad básica de información.

d) Marco simplificado.

La manera en la que se gestionan los marcos es la siguiente, (ver figura 1.3.3): en una red compuesta por 4 nodos, A, B, C y D, si A genera un marco con destino a D, este marco es escuchado por B, C y D, pero solo lo acepta D, ya que B y C lo descartan porque la dirección destino del marco no es la suya (lo "filtran"), y D al ver que tiene como destino a él lo recibe.

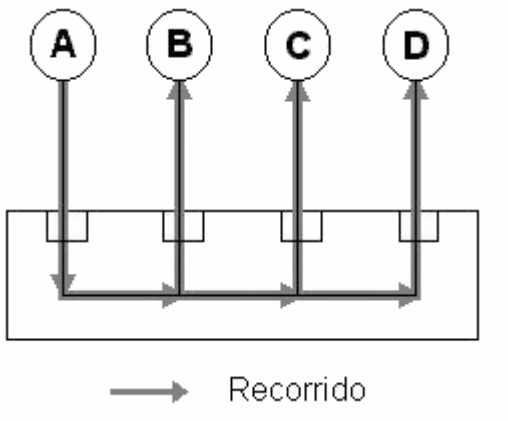


Figura 1.3-3 Gestión del marco en los nodos.

Esto tiene una consecuencia importante: solo un nodo puede transmitir a la vez en la red, ya que si otro lo hace al mismo tiempo se generan problemas, para resarcirlos existen mecanismos que implementan una serie de reglas para el acceso al medio.

e) Los accesos a la transmisión.

- MA - Acceso múltiple (Multiple Access). Cuando hablan más de dos.
- CD – Detección de colisión (Collision Detection). Cuando desean hablar más de dos nodos a la vez.

Así sería su funcionamiento:
1. Si el medio esta desocupado puede transmitir.
2. Si el medio está ocupado debe esperar.
3. Si ocurre una colisión, esperar un tiempo que se genera aleatoriamente e ir al paso 1.

También existe una dirección especial, llamada amplia o broadcast, los marcos con esta dirección de destino son escuchados por todos los miembros y procesados por todos ellos. Un uso típico de esta técnica es hacer desde un nodo una petición a todos los nodos para saber que servicios provee cada uno de ellos a la red y que sean accesibles desde el nodo que realizó la petición. Otro caso particular es que un nodo procese todos los marcos que encuentra, aunque no sean para él, aunque esto tiene una utilidad como diagnóstico de la red.

f) Protocolos.

El sistema de comunicación por marcos proporciona un nivel básico de comunicación (correspondiente a las capas 1 y 2 del modelo OSI, esto se explica

más adelante), para que el intercambio de datos entre nodos sea útil y eficiente se utilizan una serie de reglas, llamadas protocolos.

Ejemplo: Tenemos una red formada por dos nodos (ver figura 1.3.4), A y B, A quiere obtener un pequeño fichero de texto de B, para ello, utilizan unos tipos de marcos con una estructura muy concreta para saber en todo momento que se quiere hacer:
Como se observa, se trata de una manera simple de intercambiar datos, y en realidad mecanismos semejantes se usan para transferir páginas web desde sitios de Internet al navegador (TCP/IP y HTTP).
Los protocolos están a otro nivel lógico que los marcos, éstos están relacionados con el medio físico, mientras que las órdenes 1-4 son independientes del medio por el que se transmitan, esta jerarquía de protocolos y/o de funcionamiento y su abstracción entre ellas es la base de las comunicaciones (ver modelo OSI).

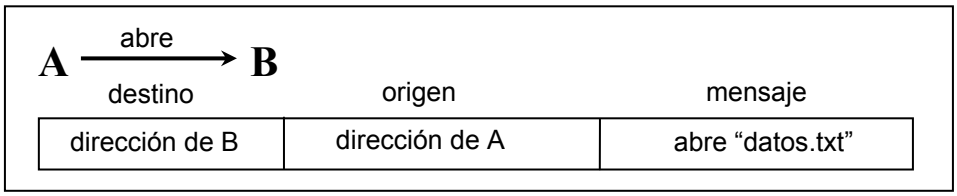
g) Elementos físicos de una red Fast Ethernet.
Los indispensables son:

- Nodos
- Repetidores (hub)
- El interfaz de Red (NIC)

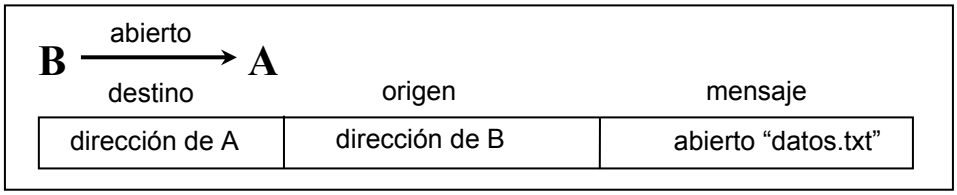
Otros elementos que no son en principio necesarios pero en la práctica resultan ser útiles:

- Conmutadores (Switch)
- Encaminadores (Router)

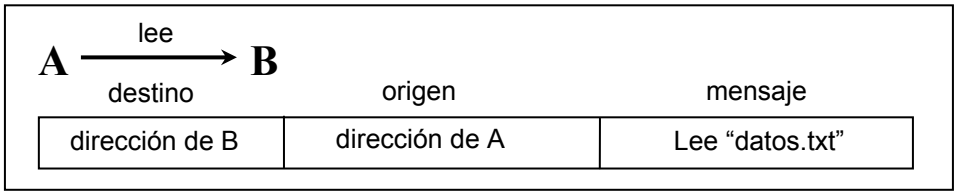
A continuación se dará una breve descripción de cada uno:
Los nodos pueden ser computadoras, impresoras, conmutadores, encaminadores, etc.
El interfaz de red (tarjeta de red o NIC), es el elemento que conecta un nodo a un repetidor a través del cable. Los nodos pueden tener mas de un NIC, pero un NIC solo alcanza a un nodo (dos nodos no pueden compartir el mismo NIC).
El cable que del que existen distintos tipos, según su calidad y ámbito de actuación entre los que existe el 100BaseTX ó cable de cobre blindado, relativamente barato, unos 100 metros de alcance antes de necesitar un repetidor.



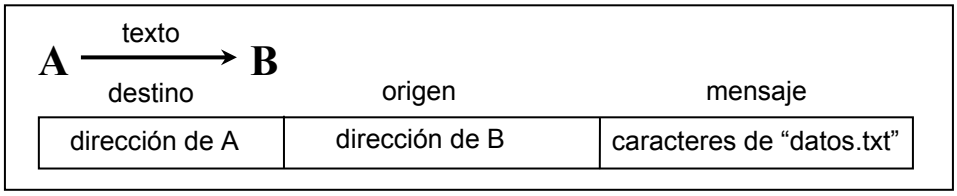
a) Abrir fichero



b) Respuesta a la apertura del fichero



c) Leer el fichero



d) Respuesta a la lectura del fichero

Figura 1.3.4 Ejemplo de intercambio de datos.

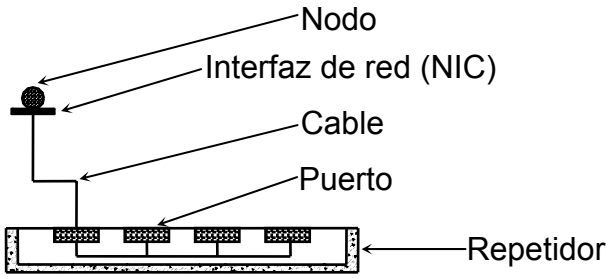


Figura 1.3.5 Elementos físicos básicos de una red Fast Ethernet

El 100BaseFX ó fibra óptica, cara con largo alcance, 2/5 Km. Y el 100BaseT4 ó cable de cobre de baja calidad

Los conmutadores trabajan a nivel de marcos, permiten interconectar redes de área local (LAN) simples entre ellas, formando SLAN´s (Switched LAN), proporcionan un gran rendimiento, se consiguen redes de mayor extensión (sobre todo si se utiliza fibra óptica), y también aumenta su complejidad.

Los encaminadores: realizan una función similar a los conmutadores, pero trabajando a nivel de protocolo y permiten conectar diferentes tipos de LAN, como una Fast Ethernet con otra que no lo sea. Son de uso extendido para proporcionar acceso a Internet funcionando como puerta de acceso (gateway). De hecho, cuando se descarga una página de Internet la información atraviesa múltiples ruteadores hasta llegar a su destino y de vuelta.

1.4 Ethernet a 1 Gbps.

1.4.1. Generalidades.

También conocida como Gigabit Ethernet, se trata de un tipo de red de área local que fue estandarizada en junio de 1998 la identificación recibida por el estándar ha sido la de IEEE 802.3z. Básicamente supone una evolución de 100 base-T, pero con velocidad de transmisión en línea de 1 Gbps. Aunque existen productos de este tipo, más que nada podemos hablar de perspectivas de uso, aunque la mayoría de fabricantes han estado durante los últimos años lanzando productos al mercado basándose en el borrador de la norma.

La red mantendría el protocolo CSMA/CD, pero como sucede en 100 base-T, las distancias de los canales deberían reducirse en proporción al aumento de la velocidad, si se quiere mantener el tamaño mínimo de trama en 64 bytes, con el fin de poder detectar las colisiones. En este caso, la longitud de un canal a 1 Gbps, no podría superar los 20 m, lo que ciertamente no es muy operativo.

La solución adoptada es incrementar el tamaño de trama mínimo a 512 bytes, mediante la inclusión de relleno en las tramas de tamaño menor, aunque con la consiguiente pérdida de eficacia. No obstante, un aspecto por otro (aumento de la velocidad y aumento del tamaño de las tramas) se estima en 70% la eficiencia de este tipo de red. El problema que podría aparecer con el envío de paquetes pequeños se resuelve mediante la implementación de una característica

denominada ráfagas de paquetes (packet bursting) que permite a los servidores, conmutadores y otros dispositivos a entregar ráfagas de paquetes pequeños.
El uso previsto de este tipo de red será principalmente la colección de conmutadores, a modo de troncal. Incluso la conexión de servidores carece de sentido dada la capacidad de los procesadores y arquitecturas actuales que no serían capaces de aprovechar tan gran ancho banda. Los usos mas comunes de la norma le harán convivir con otras especificaciones IETF y de IEEE, tales como 802.3X para control de flujo, 802,1Q para LAN virtuales, 802.1 Para priorización de tráfico y RSVP para reservas de ancho de banda.
En un futuro cercano se plantea la posibilidad de realizar emigraciones los protocolos Ethernet actuales a Gigabit Ehernet, cuatro de los posibles escenarios son:

- Actualización de enlaces entre conmutadores y servidores para obtener enlaces de alta velocidad entre ellos.
- Actualización enlaces entre conmutadores 10/1000, para conseguir enlaces a 1 Gbps entre ellos.
- Actualización de troncales Fast Ethernet conmutadas agregando un conmutador Gigabit Ethernet.
- Actualización de una red troncal FDI conectando hubs FDI con conmutadores Gigabit Ethernet.

1.4.2 Arquitectura de Gigabit Ethernet.

Para acelerar la velocidad de Fast Ethernet de 100 Mbps a 1Gbps, se necesitaron grandes cambios en la Interface Física. Se decidió que Gigabit Ethernet pareciera idéntico a Ethernet en el nivel de enlace de datos.
El reto de superar la aceleración a 1 Gbps, fue resuelto al mezclar dos tecnologías: IEEE 802.3 y ANSI X3 T11, la figura 1.4-1 muestra los diversos protocolos que se tomaron en cuenta para elaborar el Gigabit.
Con estas dos tecnologías juntas, el estándar puede aprovechar la alta velocidad de la tecnología basada en fibra óptica manteniendo el formato de trama de IEEE 802.3 de Ethernet, la compatibilidad con los medios instalados, y el uso de transmisión bidireccional o full-duplex ó unidireccional (half duplex) vía CSMA/CD.

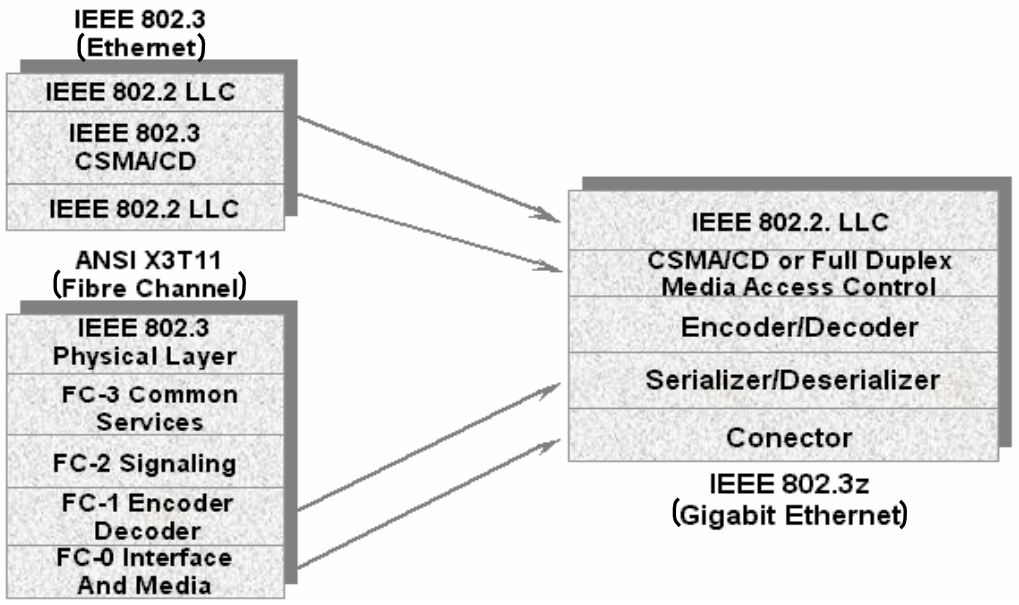


Figura 1.2.4 Pila del protocolo Gigabit Ethernet

1.4.3 Interfaz Físico.

La especificación del medio físico ó PMD (physical medium dependent) para canales de fibra óptica permiten la transmisión bidireccional de 1,062 baudios en. Gigabit Ethernet incrementará esta tasa de transmisión a 1,25 Gbps.
Las especificaciones del medio físico definidas en IEEE 802.3z son para fibra óptica y cable de cobre apantallado de 150 ohms.
La fibra óptica es un medio de transmisión que ofrece varias ventajas respecto al cable de cobre. Las principales son su gran ancho de banda (32 THz·km) y sus bajas pérdidas (0.17 dB/km) prácticamente constantes con la frecuencia. Además la fibra no es afectada por ruido ni interferencias de alta frecuencia, por lo que la hace muy segura para la transmisión de datos.
La desventaja de la fibra es que es más cara que el cable de cobre. Por estas razones, las versiones Ethernet con fibra son usadas cuando las distancias largas, la inmunidad frente al ruido y la seguridad sean lo principal y el coste sea secundario.
Debido a la necesidad de cursar un tráfico elevado, las redes de fibra óptica están empezando a aparecer. Estas redes están diseñadas a partir de enlaces ópticos punto a punto ya desarrollados. En el caso de Gigabit Ethernet, se utiliza como

técnica de multiplexación densa DWDM. Los sistemas WDM utilizan longitudes de onda muy distantes entre sí, desaprovechando la capacidad de la fibra, por lo que se llega a DWDM, donde se utiliza una gran cantidad de canales ópticos separados apenas 1 nm entre sí.
Se abordará ahora la transmisión sobre fibra y sobre cable de cobre.

Transmisión sobre fibra óptica.
Gigabit Ethernet soportará dos tipos de fibra multimodo: fibra de 50 mm (diámetro del núcleo) y fibra de 62.5 mm.La fibra de 62.5 mm tiene en general un ancho de banda menor que la de 50 mm, especialmente para láseres de onda corta. En otras palabras, la distancia atravesada por la luz en una fibra de 62.5 es menor que en una de 50mm, especialmente con láseres de onda corta. Las fibras de 50 mm tienen características muy superiores de ancho de banda y serán capaces de atravesar distancias más largas en comparación a las fibras de 62,5 mm.

Especificaciones para el transmisor óptico.
Para Gigabit se requiere un transmisor tipo diodo láser, ya que proporciona un gran ancho de banda, permiten velocidades de modulación muy superiores a la de los LEDs (hasta 30 Gb/s) y su anchura de línea en ausencia de modulación es muy inferior a la de los LEDs (desde 3 a 3 nm hasta 100 KHz).
En Gigabit Ethernet se soportarán dos estándares de láser sobre fibra: 1000 Base Sx (láser de onda corta) y 1000 Base Lx (onda larga). La diferencia clave en el uso de tecnologías de onda larga y onda corta está en el coste y la distancia. Los láseres de onda larga son más caros, pero cubren mayores distancias. Los de onda corta, en cambio, son más baratos pero cubren menores distancias.
Los parámetros que caracterizan un transmisor óptico son:

- Longitud de onda: La frecuencia (y por ello la longitud de onda) de la luz depende del transmisor usado. Es deseable seleccionar longitudes de onda para la emisión en las que las pérdidas en la fibra sean bajas. Las pérdidas son mínimas en las ventanas de transmisión de 850, 1300 y 1550 nm.
- Potencia: El transmisor debe tener la suficiente potencia para conducir la señal óptica por la fibra. Igualmente, el receptor debe tener la suficiente sensibilidad para detectar la señal óptica recibida. En general, cuanto mayor potencia se transmite, se pueden sostener mayores pérdidas por atenuación, conectores y penalizaciones del enlace. La limitación en la transmisión es el coste. La potencia transmitida menos las pérdidas en

transmisión debe ser mayor o igual que la mínima potencia aceptable recibida.

- Tiempo de subida / tiempo de caída (Rise time/Fall time): El primero se define como el tiempo que tarda la potencia de salida del transmisor en subir desde el 20% al 80% de su valor final cuando la entrada es un pulso de corriente. Mientras que el segundo sería lo contrario: el tiempo que tarda en bajar la potencia del 80% al 20%.
- Ruido: La existencia de ruido en un láser de semiconductor se manifiesta porque, incluso en estado estacionario, la potencia y la salida de su campo eléctrico no permanecen constantes en el tiempo, sino que sufren fluctuaciones, debidas principalmente a la emisión espontánea. Las fluctuaciones en la intensidad del láser vienen descritas por el denominado ruido de intensidad relativo (RIN), mientras que las fluctuaciones en la fase emitida por el láser se denominan ruido de fase.
- Ancho espectral o anchura de línea: Las variaciones en la fase del campo de salida provocan que la frecuencia de emisión de cada modo longitudinal del láser fluctúe y por consiguiente que el espectro del láser tenga una cierta anchura espectral no nula, aun en ausencia de modulación.
- Relación de extinción (extinction ratio): La relación de extinción se define como el margen entre la potencia óptica media para valor lógico ‘1’ y la potencia óptica media para valor lógico ‘0’.

Especificaciones para el receptor óptico.

El receptor está compuesto por un fotodetector de alta velocidad, un amplificador y un circuito de polarización. Su salida es un par complementario positivo de puertas lógicas ECL que produce pulsos de una frecuencia de hasta 1250 MHz.

Además, el receptor incluye un circuito detector de señal que indica si un cable está enviando un código 8B/10B. Su funcionamiento se basa en el hecho de que el código 8B/10B tiene su potencia concentrada a frecuencias como 650 Mhz. De este modo, el detector ignora fuentes de luz ajenas como la luz del sol.

Una de las características de Gigabit es usar los cables de fibra ya instalados para transmitir a velocidades de Gigabit, por lo que lo anterior al principio fué inaceptable. La corporación del estándar IEE 802.3z decidió desarrollar una solución que permitiera trabajar con Gigabit sin reducir la distancia de los enlaces ni incrementar el costo sustancialmente. El resultado fue el uso de la llamada emisión condicionada. Su funcionamiento es simple: según el tipo de cable, el láser difunde la luz como si fuera un LED, lanzando la potencia a través del núcleo

más o menos igual para todos los modos, con esto, la dispersión intermodal puede ser minimizada.
La mayoría de los proveedores proporcionan un acondicionador para láseres de onda corta dentro del transmisor. Para láseres de onda larga se proporciona un acondicionador externo.

Balance de potencia.
Como el enlace de fibra tiene pérdidas, es necesario calcularlas cuando se diseña un sistema de fibra óptica. El balance de potencias es una guía de estimación para las pérdidas de potencia desde el transmisor hasta el receptor. El peor caso se estima como la diferencia entre la potencia media mínima transmitida y la potencia media mínima recibida. El balance de potencias establece el máximo rango óptico de longitud de un enlace de fibra óptica flexible. Las pérdidas totales del medio óptico se desglosan en: pérdidas de la fibra, pérdidas por conectores o empalmes, pérdidas por elementos intermedios de distribución de la señal y caídas significativas de potencia.

El conector óptico.
El conector óptico sirve para acoplar el medio físico dependiente (PMD) al medio físico de transmisión (fibra). Para un acoplo eficiente se necesitan muy bajas tolerancias en el conector, por eso los conectores son caros y difíciles de diseñar.
Un buen conector debería tener los siguientes requerimientos:

- Las pérdidas del conector deben ser mínimas. Esto es especialmente crítico en un sistema que tiene varios conectores intermedios.
- El conector debe resistir los cambios de temperatura, humedad y otros cambios del medio ambiente.
- El conector debe de ser fácil de usar.
- El conector debe ser duradero.
- Los conectores más utilizados actualmente son del tipo SC y ST.
- El conector especificado para 1000 BASE-SX y 1000 BASE-LX es un conector SC dúplex, cuyas dimensiones y interface se encuentran en IEC 617544 y ISO/IEC 11801. Este conector usa un mecanismo de push-pull para el acoplamiento

1.4.4 Esquemas de codificación.

Gigabit Ethernet utiliza la codificación 8B/10B, que es más eficiente (necesita menos ancho de banda) que la codificación Manchester usada por Ethernet.
La codificación 8B/10B funciona de la siguiente forma:
Se transmite en línea símbolos de 10 bits, que dan lugar a un alfabeto formado por 2^{10} palabras de 10 bits. De todas esas palabras se eligen las mejores palabras (en total 2^{8}), es decir, las que al transmitirlas ocupen menos ancho de banda. El criterio que se sigue es que no haya muchos ceros seguidos (para no perder el sincronismo) y tampoco muchos unos seguidos (para no recalentar la electrónica). Las palabras elegidas constituyen el código de línea y son asignadas a las palabras que puede generar el usuario.
Así, para transmitir con una velocidad de 1Gps, si usamos Manchester necesitaríamos 2GHz de ancho de banda, en cambio si usamos 8B/10B necesitamos 1.25GHz.
Las ventajas de usar codificación son básicamente tres: la codificación ayuda a diferenciar los bits de datos de los de control, limita los errores en la transmisión y aumenta la posibilidad de que la estación receptora pueda detectar y corregir errores de la transmisión.
Un elemento muy importante que posibilita la compatibilidad entre los distintos esquemas de codificación usados por las LAN (Ethernet usa codificaión Manchester, Fast Ethernet usa 8B/6T, Gigabit Ethhernet usa 8B/10B,...) es el serializador/deserializador, que es el responsable de dar soporte a múltiples esquemas de codificación, permitiendo la presentación de estos esquemas a los niveles superiores.

Nivel de Enlace Lógico.

El protocolo de enlace de datos utilizado es el 802.2 LLC y es común para todas las redes de área local. La definición de un protocolo de enlace de datos común aporta una ventaja considerable, la interoperabilidad entre todas las LAN. Por tanto, la trama de Gigabit Ethernet es compatible con la de Ethernet y la de Fast Ethernet.
El nivel de enlace lógico define los servicios de acceso para los protocolos que siguen el modelo de referencia OSI, pero como no todos los protocolos siguen este modelo, hace falta información adicional, de eso se encarga el protocolo SNAP.

1.5 Interconexión de redes locales instaladas en ubicaciones remotas.

1.5.1 Generalidades.

En este caso el objetivo es interconectar dos o más redes locales, mediante un servicio de red pública o mediante algún enlace propietario. Lo primero que hay que decidir es a qué nivel se interconectan las redes con dos alternativas:

- Conexión a nivel de enlace de datos mediante puentes remotos.
- Conexión a nivel de red mediante ruteadores.

Ambas alternativas tienen ventajas e inconvenientes. Veámoslas en primer lugar para la interconexión mediante puentes:
ventajas: mejores prestaciones menor costo, facilidad de instalación y gestión.
Inconvenientes: no se aíslan las llamadas tormentas de transmisión, en el caso de conexión de varias redes puede no aprovecharse de forma óptima el servicio de red pública.
Y para la interconexión mediante ruteadores:

- Ventajas: facilidad para gestionar redes heterogéneas a nivel software (TCP/IP, Novell Netware, etc.), facilidad para la administración de direcciones en redes con el mismo protocolo de red (IP o IPX).
- Inconvenientes: pocas prestaciones, problemas de gestión cuando un segmento tiene varias salidas con posibilidad de formación de bucles, mayor costo.

Lógicamente, la otra decisión a tomar es que tipo de servicio de red pública es el más adecuado. Para ello, en cada caso hay que hacer una análisis de costes en función del tráfico previsto, tratando de optimizar la relación prestaciones/precio.

Como normas de interconexión se pueden mencionar a:

- RTB: transferencias esporádicas, colecciones locales, disponibilidad de uso de horas de tarifa reducida.
- RDSI: transmisiones masivas punto a punto, conexiones locales, utilización de puentes autoconfigurables, integración de voz y datos.

- RPCP X.25: transferencias de volumen medio, ponderación de la capacidad del enlace físico contratado, cuando existe necesidad de conexiones conmutadas con distintos puntos.
- Frame Relay: transferencias de volumen medio, conexiones punto a punto y permanentes, interconexión de redes locales.
- JDS: sólo apta para redes privadas virtuales, un contrato específico con el proveedor del servicio y desde luego incluyendo comunicaciones vocales.
- Líneas alquiladas: trasferencias masivas, conexiones punto apunto o permanentes.

También se pueden utilizar medios punto a punto privados como:

- Radioenlaces digitales.
- Enlaces ópticos.

Los radioenlaces digitales son una alternativa muy interesante para formar redes privadas virtuales en entornos regionales. Sus características, velocidades y precios varían mucho de unos a otros en función de la tecnología. Si embargo en los últimos años sus precios han bajado y los interfaces disponibles van desde velocidades de 2 Mbps compatibles con la JDP (RDSI), hasta enlaces Mbps de 34 y 155 Mbps compatibles JDS. La principal desventaja que presentan es la necesidad de trámites burocráticos para la asignación de frecuencias y la saturación del espectro en entornos urbanos.
En cuanto a los enlaces ópticos, han de ser de los tipos: infrarrojo y láser
Ambos tipo requieren visión directa, aunque los enlaces láser pueden cubrir distancias mayores (hasta varios kilómetros) y son más robustos frente a elementos meteorológicos adversos (lluvia y niebla). Las velocidades típicas de los enlaces de van e 64Kbps hasta 2 Mbps, siempre dentro de la JDP.
La principal ventaja de este tipo de enlaces es que no requiere ningún trámite administrativo para su instalación. La desventaja fundamental por otra parte es su mayor o menor dependencia de las circunstancias meteorológicas, por lo que en cualquier caso requieren un medio alternativo de respaldo (back-up).

1.5.2 Monitoreo en sistemas de distribución eléctrica.

Hasta hace poco tiempo, los ingenieros instrumentistas estaban demasiado preocupados en incrementar la funcionalidad de sus equipos, como para prestar atención a la operación remota de los mismos, y mucho menos a su integración. Más adelante, cuando las prestaciones de la mayoría de los equipos se fueron unificando, los fabricantes de instrumentos de sistemas eléctricos de potencia más aventajados buscaron nuevas fórmulas para incrementar sus prestaciones. Dado que la mayoría de los equipos hacían ya uso intensivo de los microprocesadores, se generalizó rápidamente la utilización del puerto paralelo para conexión a dispositivos de impresión y del puerto serie con interfaz RS-232, para la realización de comunicaciones más universales, tal y como se verá más adelante. Parece correcto pensar que los principales impulsores de este afán de comunicación con el exterior fueron las compañías eléctricas, que demandaban la posibilidad de poder registrar los resultados de las medidas, no sólo en papel, sino también sobre soporte magnético. Fue más adelante cuando los responsables de los departamentos de telecomunicaciones vieron la posibilidad de integrar la instrumentación dentro de sus sistemas SCADA.

Inicialmente, la operación remota sobre los equipos de medida se establecía mediante un enlace punto a punto, utilizando como infraestructura básica de telecomunicaciones la Red Telefónica Conmutada (RTC). Esta topología tiene como ventaja su sencillez de implementación, y como principal inconveniente, que no utiliza los recursos disponibles de forma óptima. Además, cada fabricante tiene su propio conjunto de protocolos. En la figura 1.5.1 se muestra la estructura de este tipo de operación remota de la instrumentación.

La topología anterior es poco práctica cuando se pretende monitorizar varios equipos de medida desde un único punto; en ese caso es necesario disponer de una línea telefónica por cada uno de los enlaces a realizar. Dado que las infraestructuras de telecomunicación constituyen recursos relativamente caros, y siempre que no sea necesario un acceso continuo a los equipos de media, puede optarse por compartir una o varias líneas entre varios equipos, llegando así a topologías que virtualmente pueden considerarse de tipo punto-multipunto. Sin embargo, esta opción no es siempre posible, ya que como se ha comentado anteriormente, los fabricantes suelen utilizar protocolos y configuraciones de modem específicas que dificultan la reducción de recursos en la cabecera de medida. La figura 1.5.2 muestra la estructura de operación descrita.

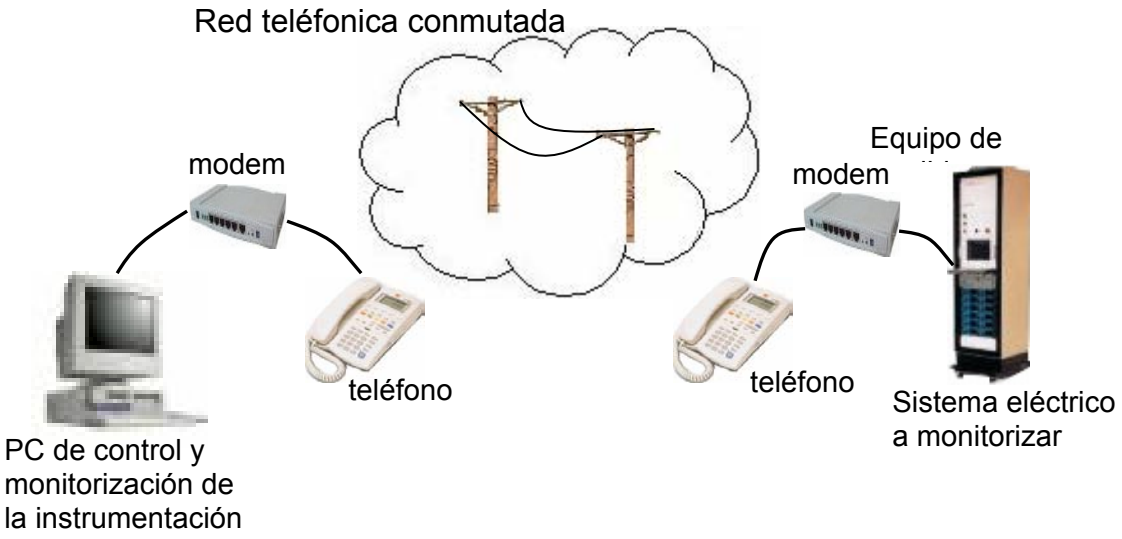


Figura 1.5.1 Topología telemática para la operación remota de instrumentación punto a punto.

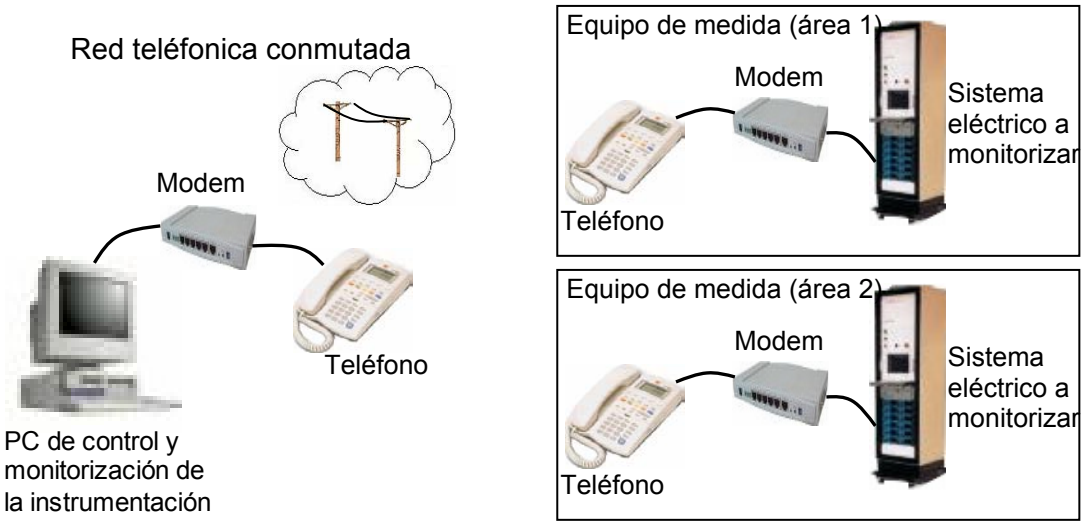


Figura 1.5.2 Topología telemática para la operación remota virtual de instrumentación con topología punto multipunto.

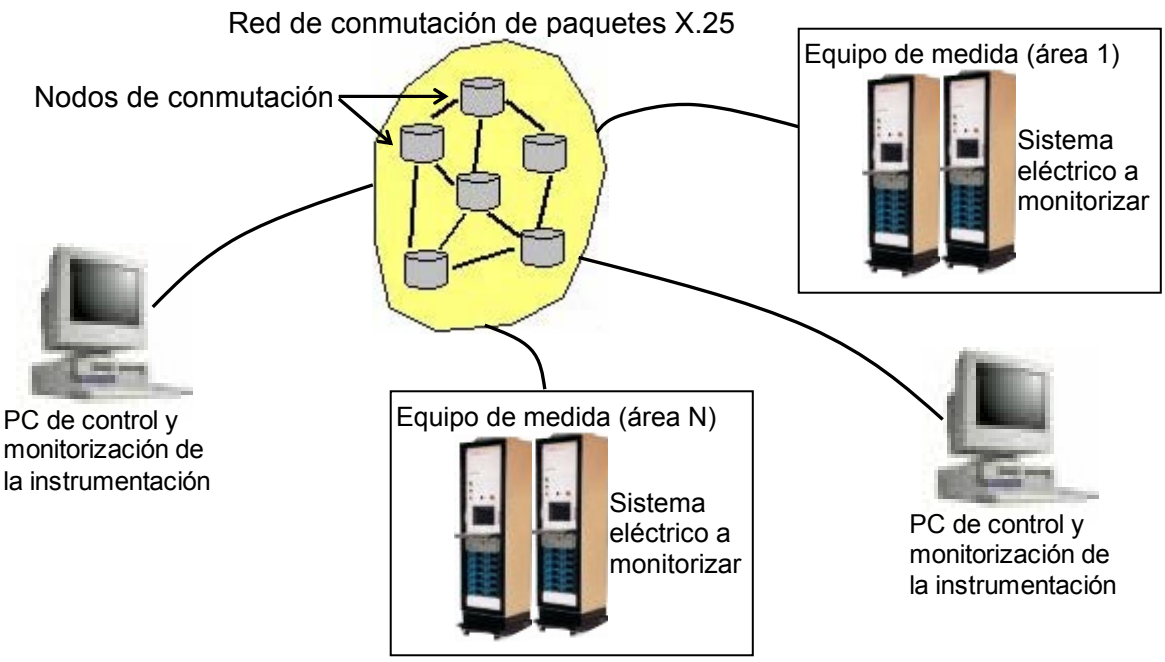


Figura 1.5.3 Topología de un sistema de medida basado en una red de conmutación de paquetes.

El desarrollo actual de las telecomunicaciones, tanto en su aspecto técnico como en su marco legal, permite que empresas con infraestructuras continuas como pueden ser: eléctricas, gas, ferrocarriles, etc., tengan sus propias redes de telecomunicación. Esta situación ha dado lugar al desarrollo de redes privadas de datos con protocolos estándares como X.25, que están orientadas a la transmisión y conmutación de datos, y que por tanto, permiten maximizar la utilización de recursos, reduciendo costes. La figura 1.5.3 muestra la estructura de una red de este tipo.

Actualmente la estructura se va complicando cada vez más, debido a la incorporación de nuevos elementos de transmisión de datos como son las fibras ópticas en los núcleos de los cables de tierra de alta tensión, y sobre todo, a la utilización de nuevos sistemas de transmisión y conmutación vía radio como el WUXQNLQJ.

Como recomendación podemos decir, que la adquisición de un equipo de medida debe estar condicionada por algo más que por sus prestaciones, ya que su integración en un sistema global de medida es un aspecto cada vez más importante.

La creciente liberalización del sector de la energía eléctrica, obliga a las compañías eléctricas a tomar medidas para afrontar el nuevo marco competitivo.

Aunque en nuestro país la competencia es solamente relativa a la producción autónoma de energía por parte de las compañías que producen su propia electricidad, ya que esta para su distribución solo esta permitida para el estado.
Para ello, se ha de mejorar la calidad del servicio así como reducir los costes de compra y mantenimiento.
Para incrementar la calidad del servicio, se requiere información continua del estado de la instalación, que permita prevenir posibles problemas que puedan afectar al funcionamiento óptimo del sistema. Por tanto, es necesario emplear los cada vez más complejos dispositivos electrónicos inteligentes (DEI) que cumplen todos los requerimientos y que a la larga no obstante su elevado costo permitan la recuperación de la inversión realizada en ellos través de la automatización de la operación de las instalaciones eléctricas de MT y AT.
Por esto, numerosas empresas han desarrollado sistemas integrados de protección y control (SIPC), así como una amplia gama de productos especializados pensados para la automatización de las subestaciones.
Los SIPC han sido concebidos para servir de solución óptima a las necesidades económicas, funcionales y de explotación del sector eléctrico. El SIPC mejora la seguridad de operación de la subestación y reduce su mantenimiento, detectando automáticamente cualquier anomalía que se produzca en la subestación y reduciendo al mínimo los tiempos de indisponibilidad de la instalación.
El SIPC proporciona una solución global para el control y la protección tanto de nuevas subestaciones como de aquellas que necesitan ser modernizadas.
Los componentes del sistema hardware del SIPC son controlados por potentes herramientas de software consiguiendo un mayor potencial y una mayor flexibilidad del sistema.
El eficaz funcionamiento de un sistema integral como es el SIPC, que incluye la gestión centralizada de numerosos procesos, no sería posible sin un soporte de software que agilice y facilite el control y la supervisión total sobre el sistema.
En este sentido, los sistemas deben disponer de un paquetes software bajo entorno Windows 3.x/95/98/NT o cualquier plataforma que se deseé manejar como la misma MAC de Machintosh, totalmente modular y adaptable a las distintos tipos de instalaciones eléctricas y que se encarga de realizar las siguientes funciones.

- Presentación gráfica del estado de la Subestación, incluyendo estados, alarmas, medidas y contajes, en diferentes niveles de páginas
- Mando local de la Subestación, con indicación de causas de bloqueo
- Listado cronológico de eventos y alarmas

- Acceso directo al software de protecciones sin abandonar el módulo
- de supervisión
- Creación de datos históricos con funciones estadísticas y presentaciones gráficas y en formato de base de datos.

1.6 Acceso remoto a redes.

Este es una de las variantes de interconexión que más se ha desarrollado en los últimos años, con aparición de productos hardware y software específico integrados dentro de sistemas operativos de red (Windows NT por ejemplo). Hasta hace poco, los únicos medios de acceso remoto disponibles eran los denominados servidores de terminales o concentradores, a los que se conectaban baterías de modems y las estaciones remotas se conectaban como terminales de un servidor, como se aprecia en la figura 1.6.1.
El interés del servicio de acceso remoto, es ofrecer al puesto de trabajo remoto todos los servicios de la red corporativa como si estuviera conectado físicamente a un segmento de red local. Para ello, el servidor de acceso remoto, además de incorporar el hardware adecuado de conexión para varios usuarios remotos simultáneamente, debe ser capaz de enrutar distintos protocolos (IP,IPX,Netbios).

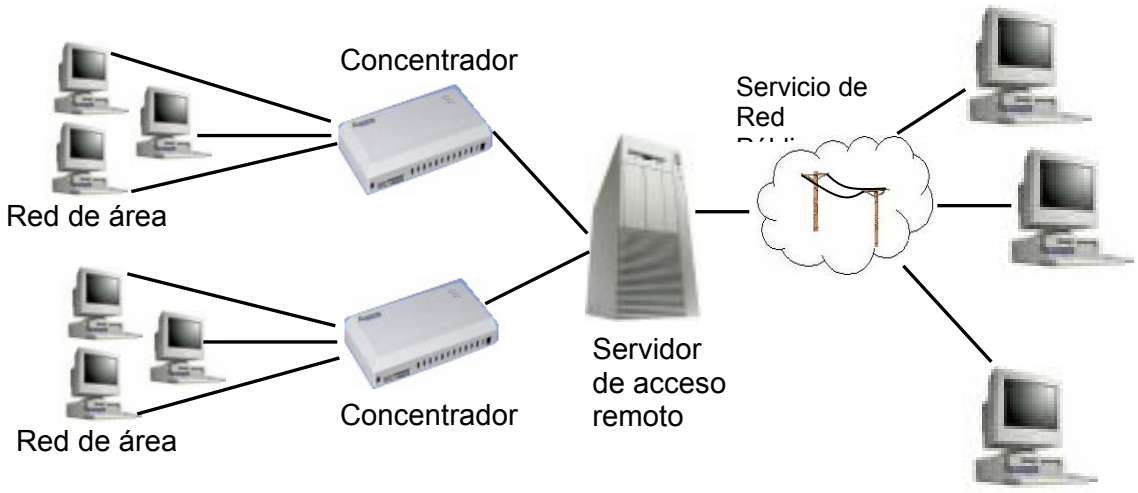


Figura 1.6.1 Acceso remoto.

Un aspecto fundamental en los servicios de acceso remoto es la seguridad. La seguridad se fundamenta en la identificación y autentificación de los usuarios

remotos, así como en la gestión de permisos de los citados usuarios dentro de la red corporativa.
Una importante decisión es el medio de comunicación o servicio de red pública elegido para la conexión remota. Las alternativas prácticas son las siguientes:

- RTB: es el medio más sencillo y universal, aunque resulta costoso para trasferencias masivas y en el caso de llamadas no locales.

- RDSI: sin duda es una de las mejores alternativas para este tipo de servicio por su buena relación prestaciones/coste en un entorno con tráfico masivo pero esporádico, como es típico en estos servicios.

Desde luego, existen otros métodos de acceso remoto una red como lo es la propia Internet u otros que en ese momento se hallen disponibles.. El acceso a través de Internet a una red corporativa completa es absolutamente desaconsejable por razones de seguridad, y el segmento de red conectado a Internet deberá estar aislado del resto de la red corporativa.

1.7 Definición y características del servicio de acceso remoto.

Con el desarrollo de las técnicas de teletrabajo, ya sea de puestos fijos de usuario en el domicilio del trabajador, o bien mediante las denominadas oficinas móviles, formadas por un computador portátil y en ocasiones teléfono móvil de ubicación geográfica, aparece la necesidad de ofrecer conectividad a estos usuarios para que hagan uso de los recursos de la red corporativa a que pertenecen.
Es interesante destacar, que los usuarios remotos deben poder acceder a los recursos de la red, como si estuvieran conectados en local a alguno los segmentos de la misma. Aunque a veces, lógicamente, con menores prestaciones en cuanto velocidad.
El servicio de acceso remoto será proporcionado por un dispositivo especial, denominado servidor de acceso remoto, puede ser de dos tipos:

- Hardware: dispositivo dedicado, con conexión múltiple a alguna red pública y a algún segmento de la red corporativa.
- Software: habitualmente incluido como parte del sistema operativo de red (ejemplos: MS Windows NT, Novell Netware).

Los servidores para acceso remoto o para concentración de terminales serie sobre segmentos de red local, en la práctica se comportan como ruteadores, pero con muchas tomas de red pública. Sus características y configuración depende mucho del fabricante. No obstante, en general, sus puntos fuertes y débiles son similares a los servidores software: la seguridad (identificación de usuarios, autentificación y registro de accesos) y capacidad de en enrutamiento de protocolos de red local (IP, IPX, NETBIOS, etc.) sobre protocolos punto a punto (PPP, SLIP).
Los servidores de tipo software son los mas socorridos por ser más flexibles, y disponerse de más información sobre ellos. Sin embargo, como ya se indico, la problemática de ambos es muy similar y las conclusiones generales que se pueden observar son comunes a ambos tipos. No obstante cabe citar que en general los hardware pueden soportar más accesos simultáneos (mas de 30) que los software, aunque en principio la limitación de los software sólo viene dada por la potencia del computador que hace de servidor.
El servidor de acceso remoto (Remote Access Server) es una combinación de dos componentes:

- Un servidor de una red de área local.
- Un cliente que se encuentra en una ubicación remota.

Las estaciones de trabajo conectadas a la red mediante RAS aparecen como si estuvieran conectadas directamente a la red. Participan plenamente en la red, compartiendo archivos e impresoras, accesando a bases de datos, conectándose a una computadora central, y comunicándose con otras estaciones de trabajo mediante correo electrónico.
Los servidores de acceso remoto pueden estar conectados a la RTB, RDSI o a una RPCP X.25, y permiten a los usuarios remotos tener acceso a un servidor a través de estas redes.
La transparencia del acceso a red que proporciona RAS la convierte en una herramienta útil para administradores de sistemas y profesionales que viajan con frecuencia. Por ejemplo, una configuración RAS de Windows NT consta de los siguientes componentes:

- Clientes de servicio de acceso telefónico a redes: los clientes de servidores de acceso remoto de Windows NT, Windows 95, Windows para trabajo en grupo, MS-DOS (que tenían instalado software de cliente de red Microsoft)

y LAN Manager, pueden conectarse un servidor Windows NT RAS. Los clientes también pueden ser cualquier cliente del PPP de Microsoft.

- Servidores de acceso remoto: el RAS de Windows NT Server permite que hasta 256 clientes remotos realicen llamadas. Windows NT Workstation permite un cliente remoto realizar una llamada. El servidor RAS puede configurarse para ofrecer acceso a toda una red o bien para restringir el acceso al servidor RAS únicamente.
- Protocolos LAN: los protocolos LAN transportan paquetes por redes de área local (Local Area Network), mientras que los protocolos de acceso remoto controlan la transmisión de datos a una red de área amplia (Wide Area Network). Windows NT reconoce protocolos LAN como TCP/IP, IPX, y NetBEUI, que permiten el acceso servidores Internet, Netware y UNIX. También reconoce las aplicaciones de Windows Sockets sobre TCP o IPX , llamadas canalizaciones, las llamadas de procedimiento remoto (RPC), y la API de LAN Manager.
- Protocolos de acceso remoto: Windows NT reconoce protocolos de acceso remoto como PPP, SLIP en clientes RAS y el protocolo RAS de Microsoft.
- Opciones WAN: los clientes pueden marcar utilizando líneas telefónicas estándar y un modelo o un grupo de ellos. Para obtener vínculos más rápidos se recomienda utilizar RDSI. También se pueden conectar clientes RAS con servidores RAS utilizando X.25, un falso módem RS-232C, un mediante el protocolo de túnel Punto-a-punto (PPTP).
- Características de seguridad: la seguridad de inicio de sección y de dominio de Windows NT, soporte para host de seguridad, servicio de datos cifrados, llamada de respuesta proporcionan, a los clientes remotos, un acceso seguro a la red.
- Soporte Internet: De servidores de acceso remoto permite a Windows NT proporcionar servicios completos a Internet. Un equipo Windows NT Server puede configurarse como un proveedor de servicios Internet, que ofrezca conexiones de marcado a un cliente PPP. Un equipo con Windows NT Workstation o Windows 95 puede llamar a un equipo conectado a Internet con Windows NT Server 3.5 o posterior, o a cualquiera de los servidores Internet basados en SLIP o en PPP estándar industrial.

1.8 Protocolos de acceso remoto.

1.8.1 Generalidades

Los protocolos de acceso remoto controlan la transmisión de datos a través de la red de área amplia. El sistema operativo y el protocolo o protocolos de red local de sus clientes y servidores de acceso remoto son los principales factores que afectan al protocolo de acceso remoto que usaran sus clientes. Los protocolos de acceso remoto son de cuatro tipos: protocolo Punto a punto (PPP), protocolo Internet de línea en serie (SLIP), protocolo RAS de Microsoft, y puerta de enlace NetBIOS. A continuación se hablara de los protocolos en cuanto a la tasa de transmisión en bits, para continuar con los protocolos de enlace y a continuación los protocolos de control de red.

Protocolos bit. Antes de 1980, la mayoría de los protocolos eran orientados a bit (no a bytes). los programas para la mayoría de ellos eran hechos a la medida, lentos y costosos. Algunos ejemplos de los llamados protocolos bit patentados son el ACS, el L&N Conitel, los sistemas Moore, el Westinghouse REDAC, el BBI/CSI, el TELEGYR 7500, el TRW y Rockwell. Un cambio de 1 bit significa un cambio de control en un protocolo bit.

Protocolos byte.

Un protocolo byte toma generalmente 10 bits (uno de iniciación, 8 de datos y 1 bit de paro o detección), lo cual representa un carácter del estandar ASCII (American Standar Code for Information Interchange); todos los comandos y datos pueden representarse por 136 caracteres ASCII que incluyen todas las teclas de un teclado estándar de computadora compatible PC, asi como caracteres de control que no se imprimen, que incluyen los Esc, Ctrl, Del, Shift, Backspace y Alt. Los protocolos byte son compatibles con los microprocesadores estándar de 8 bits que se emplean en las UTR. Relación precio/desempeño de las computadoras a mejorado por muchos órdenes de magnitud desde que los protocolos bit fueron la norma en la industria. Los lenguajes de alto nivel para computadora y las tarjetas de interfaz seriales que se vende como productos estándar son compatibles con el ASCII. Los analizadores de comunicaciones por redes comerciales sólo funcionan con protocolos estándar de comunicaciones; los fabricantes de UTR que no se sujetan las normas ASCII de byte abiertas deben proporcionar analizadores de comunicaciones hechos a la medida. Algunos ejemplos de protocolos orientados a bytes son el PG&E, el Harris 5000, el Ferranti 5000 y el Duke Power SDLC.

Un protocolo mas empleado es el Protocolo Punto a Punto (Point to Point Protocol) y en segundo plano el Protocolo de Interconexión de Líneas Serie (Serial Line Interface Protocol). Por supuesto, hay variaciones de ambos, fundamentalmente orientadas a lograr una compresión de los datos transmitidos.
Ello requiere, en el caso del equipo remoto, la instalación de un software de comunicaciones o conjunto de utilidades del sistema operativo que incorporen dicho protocolo. Así por ejemplo, Windows 98 incorpora de base ambos protocolos.
Por supuesto, como complemento para dichos protocolos, existirá otro u otros, como pueden ser TCP/IP, IPX, LAT, NetBEUI, en función del sistema operativo o aplicaciones.

1.8.2 Protocolo Punto a punto.

Este es un conjunto de protocolos de autentificación y de tramas que facilita soluciones de acceso remoto para trabajar en una red de múltiples proveedores. Se recomienda su uso dada su flexibilidad, por ser un protocolo estándar de la industria y porque así se facilitara una mayor flexibilidad futura con el hardware y software de cliente y servidor.
Es capaz de detectar errores y ofrece compresión de datos , que se negocian automáticamente cuando se realza la conexión a la red.
Permite características avanzadas, no disponibles con estándares más antiguos que con frecuencia proporcionaban poca seguridad y necesitaban inicios de sesión en modo de terminal.
También admite múltiples protocolos de red de área local. Con acceso telefónico a redes puede utilizar TCP/IP, IPX o NetBEUI como protocolo de red tanto para clientes remotos como para el servidor RAS.
Es previsible que se convierta en el principal estándar para la mayor parte de la informática de acceso remoto ya que muchos desarrolladores de sistemas se han decantado hacia él.
Las conexiones punto a punto deben cumplir los estándares establecidos de manera que la comunicación se lleve a cabo sin contratiempos. Tras la petición de acceso a un servidor, se producen las siguientes negociaciones para establecer la conexión:

- Negociar Protocolos de control de vínculo (LCP), el LCP se utiliza para establecer y configurar parámetros de vínculos y tramas tales como el tamaño máximo de trama.
- Negociar Protocolos de autentificación. Los protocolos de autentificación se utilizan para determinar la validación de nivel de seguridad que puede llevar a cabo el servidor de acceso remoto y la que requiere el servidor. El nivel de seguridad que se puede negociar varia desde autentificación de contraseña de texto simple hasta autentificación cifrada, pasando por la seguridad de devolución de llamada.
- Negociar Protocolos de control de red (NCP). Los NCP se utilizan para establecer y configurar distintos parámetros de protocolo de red para IP, IPX y NetBEUI. Esta negociación incluye la compresión de la cabecera del protocolo y el protocolo de control de compresión.

La conexión resultante permanece activa hasta que se desconecte la línea por cualquiera de las siguientes razones: el usuario cuelga explícitamente la línea, la línea se desconecta debido a un tiempo de espera inactivo, el administrador cuelga la línea o surge un error irrecuperable en el vínculo.

Las tramas de punto a punto definen la forma en que se encapsulan los datos antes de la transmisión en la red de área amplia. Mientras que el formato de área estándar de punto a punto garantiza que el software de acceso remoto de cualquier proveedor se pueda comunicar y sea capaz de reconocer paquetes de datos de cualquier software de acceso remoto que cumpla las normas. Utiliza tramas HDLC para la transferencia de datos serie, RDSI y X.25.

1.8.3 IP para líneas serie.

El protocolo de línea serie Internet SLIP (Serial Line Internet Protocol) es un antiguo estándar de acceso remoto que solían utilizar los servidores UNIX de acceso remoto para la conexión de terminales remotos vía RTB.
Es similar en cuanto a concepto al metodo de punto a punto, pero varía en que se trata de un estándar que sólo direccional las conexiones TCP/IP a través de líneas serie a., no ofrecen negociación automática de la configuración de red sin intervención del usuario, ni tampoco detección de errores. Además no permite la autentificación cifrada.

Los clientes con acceso telefónico a redes Windows NT que son compatibles pueden conectarse a cualquier servidor de acceso remoto mediante el estándar SLIP. Esto permite a los clientes de distintas versiones de Windows NT conectarse con la gran base instalada de servidores UNIX. Sin embargo, el servidor de acceso remoto de Windows NT no es compatible con clientes SLIP.

1.8.4 Protocolo RAS de Microsoft.

El protocolo RAS de Microsoft es un protocolo patentado de acceso remoto compatible con estándar NetBIOS. Este protocolo es compatible con todas las versiones anteriores RAS de Microsoft, así como con los clientes de la versión 3.1 de Windows NT, Windows para trabajo en grupo, de MS-DOS y de LAN Manager.
Con un cliente en RAS marque un número de teléfono en una versión más antigua de Windows tendrá que utilizar el protocolo NetBEUI. En este caso , el servidor RAS actuará como puerta de enlace o gateway para el cliente remoto, ofreciendo acceso a los servidores que utilizan los protocolos NetBEUI, TCP/IP o IPX.
En Windows NT, en cada equipo remoto que se conecta a un servidor RAS mediante PPP en una red TCP/IP, recibe automáticamente una dirección IP entre un rango estático asignado al servidor RAS por el administrador durante el proceso de instalación.

1.8.5 protocolos de control de red.

Los protocolos de control de red establecen y configuran distintos parámetros de protocolos de red para IP, IPX y NetBEUI.

- Protocolo de control del protocolo Internet (IPCP): se emplea para configurar y desactivar módulos de protocolo IP en ambos extremos del vínculo.
- Protocolo de control de intercambio de paquetes Internet (IPXCP): se emplea para configurar, activar y desactivar módulos de protocolo NetBEUI en ambos extremos de la conexión. NBF CP es un protocolo propuesto por Microsoft para la configuración NetBEUI.
- Protocolo de autentificación.

- La negociación de los protocolos de autentificación se produce inmediatamente después de determinar la calidad del vínculo y antes de la negociación de la capa de red.
- Protocolo de autentificación de contraseña (PAP): utiliza contraseñas de texto simple y el protocolo de autentificación menos sofisticados. Normalmente se negocian sin estación de trabajo remota y el servidor no pueden negociar una forma de validación asegura. El servidor Windows NT RAS se puede, en lugar para evitar contraseña de texto simple activando un nivel de seguridad elevado.
- Protocolo de autentificación o repuesta a desafió (Challenge-Handshake): utiliza una respuesta-desafío con una respuesta cifrada. Permite utilizar diversos tipos de algoritmos de cifrado. Microsoft RAS utiliza el cifrado DES cuando tanto el cliente como el servidor emplean Windows NT RAS. El cliente RAS también puede negociar un cifrado MD5 cuando se conecta a servidores de acceso remoto de otros proveedores. El servidor Windows NT RAS solamente proporciona cifrado DES y no negociara MD5 con el software de cliente de acceso remoto de otros fabricantes. MD5 es un esquema de cifrado utilizado por diversos proveedores PPP para la autentificación cifrada. Windows NT siempre negociará la autentificación cifrada cuando se comunique con otros equipos Windows NT . Al conectarse con servidores los software cliente de acceso remoto de otros proveedores, RAS puede negociar la autentificación con texto simple si el producto del tercer proveedor no admite la autentificación cifrada.

1.8.6 El modelo OSI.

Desarrollado en 1977 por la ISO (International Organization for Standardization), el modelo OSI para sistemas abiertos establece un marco de trabajo definiendo como deben de interactuar los sistemas de red en sus comunicaciones.
Las pilas de protocolos no son mas que una jerarquía de pequeños protocolos que trabajan juntos para llevar a cabo la transmisión de los datos de un nodo a otro de la red. Las pilas de protocolos se asemejan mucho a las carreras de relevos, pero en lugar de pasarse un testigo, se transmiten paquetes de datos de un protocolo a otro hasta que estos revisten la forma adecuada (una secuencia única de bits) para transmitirse por el entorno físico de la red.

El modelo OSI abarca una serie de eventos importantes que se producen durante la comunicación entre sistemas. Proporciona las normas básicas empíricas para una serie de modos distintos de conexión en red. Dichos modos pueden ser los siguientes:

- El modo en que los datos se traducen a un formato apropiado para la arquitectura de red que se está utilizando. Cuando se envía un mensaje de correo electrónico o un archivo a otra computadora, se esta trabajando, en realidad, con una determinada aplicación, como un cliente de correo electrónico o un cliente FTP. Los datos que se transmiten utilizando dicha aplicación tienen que convertirse a un formato más genérico si van a viajar por la red hasta llegar a su destino.
- El modo en que una PC u otro tipo de dispositivos de la red se comunican. Cuando se envían datos desde una PC, tiene que existir algún tipo de mecanismo que proporcione un canal de comunicación entre el remitente y el destinatario. Lo mismo que cuando se desea hablar por teléfono, para lo cual hay que descolgar el teléfono y marcar el número.
- El modo en que los datos se transmiten entre los distintos dispositivos y la forma en que se resuelve la secuenciación y la comprobación de errores. Una vez establecida la sesión de comunicación entre dos computadoras, tiene que existir un conjunto de reglas que controlen la forma en que los datos se transportan de una a otra.
- El modo en que el direccionamiento lógico de los paquetes pasa a convertirse en el direccionamiento físico que proporciona la red. Las redes informáticas utilizan esquemas de direccionamiento lógico, como direcciones IP. Por tanto, dichas direcciones lógicas tienen que convertirse en las direcciones reales de hardware que determinan las NIC instaladas en las distintas computadoras.

El modelo OSI se trata de una estructura jerárquica de 7 niveles o capas, cada capa o nivel se define en base a las funciones que realiza en la comunicación, su estructura se observa en la figura 1.8.1. Cada capa realiza una realiza sus funciones específicas, provee al nivel más elevado una abstracción sobre el desarrollo de las comunicaciones y al nivel más bajo le encarga tareas, que según se va bajando capas, se encuentran más cercanas al nivel físico de la comunicación.

Las capas del modelo OSI describen el proceso de transmisión de los datos dentro de una red. Las dos únicas capas del modelo con las que, de hecho, interactúa el usuario son la primera capa, la capa física y la última capa, la capa de aplicación.
La capa física abarca los aspectos físicos de la red, es decir, los cables, hubs y demás dispositivos que conforman el entorno físico de la red. Al ajustar un cable mal conectado a un nodo estamos interactuando con la capa Física.

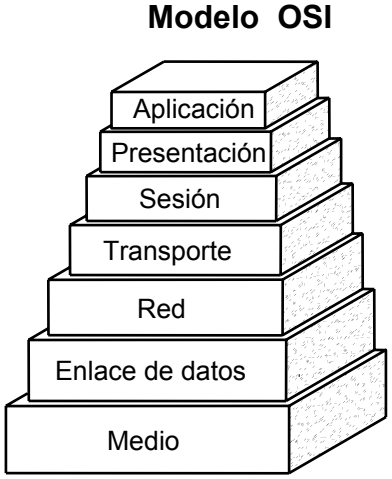
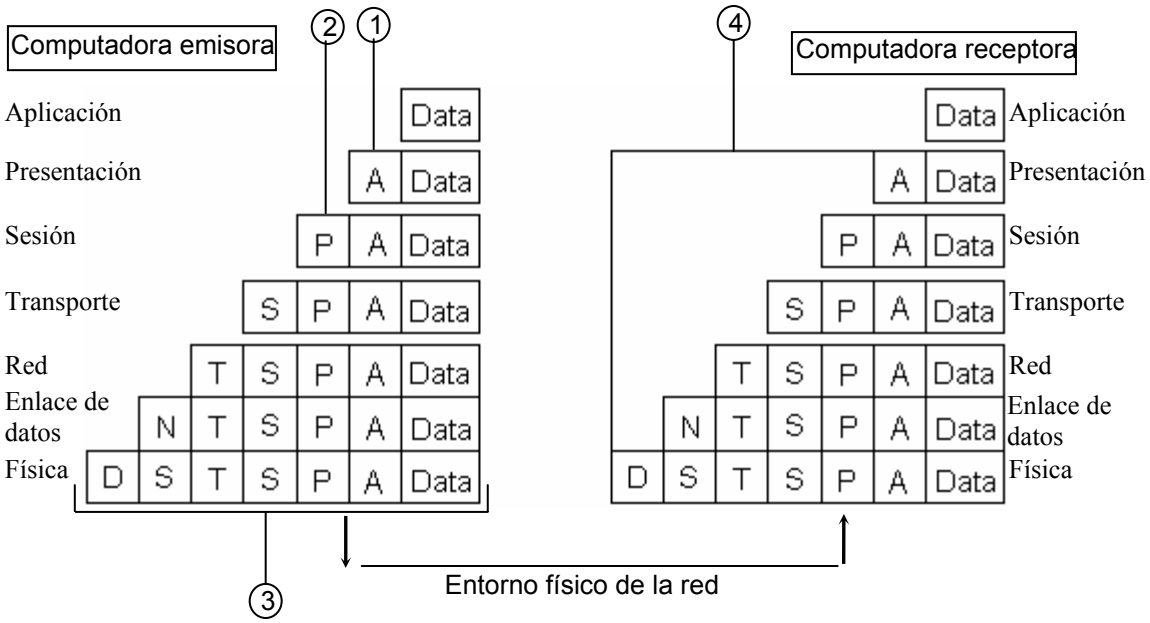


Figura 1.8.1 El modelo OSI ofrece un esquema teórico que explica el modo en que se desplazan los datos desde una computadora emisora a otra computadora receptora.

La capa de aplicación proporciona la interfaz que utiliza el usuario en su computadora para enviar mensajes de correo electrónico o ubicar un archivo en la red.
Antes de el explicar cada una de las capas que compone la pila, conviene hacerse una idea general de lo que ocurre cuando los datos se mueve en por el modelo OSI. Supongamos que un usuario decide enviar un mensaje de correo electrónico a otro usuario de la red. El usuario que envía el mensaje utilizará un cliente o programa de correo (como Outlook) como herramienta de interfaz para escribir y enviar el mensaje. Efectividad del usuario se produce en la capa de aplicación.
Cuando los datos abandonan la capa de aplicación (la capa insertara un encabezado de capa de aplicación en el paquete de datos), que éstos pasan por las restantes capas del modelo OSI. Para capa proporcionará servicios específicos relacionados con el enlace de comunicación que debe establecerse, o bien formateará los datos de una determinada forma.

Al margen de la función específica que tenga asignada una capa, todas adjuntan un encabezado (los encabezados vienen representados por cuadriláteros en la figura 1.8.2) a los datos. Puesto que la capa física está integrada por dispositivos de hardware (un cable, por ejemplo) nunca añade un encabezado a los datos.



1. Encabezado de la capa de aplicación.
2. Encabezado de la capa de presentación.
3. Paquete con todos los encabezados de las capas OSI.
4. Los encabezados se van suprimiendo a medida que los datos van subiendo por la capa OSI.

Figura 1.8.2 Los datos bajan por la pila OSI de la computadora emisora y suben por la pila OSI de la computadora receptora.

Los datos llegan así a la capa física (el entorno tangible de la red, como los cables de par trenzado y hubs que conectan las computadoras entre sí) de la computadora del destinatario, desplazándose por el entorno físico de la red hasta alcanzar su destino final, el usuario al que iba dirigido el mensaje de correo electrónico.

Los datos se reciben en la capa física de la computadora del destinatario y pasan a subir por la pila OSI. A medida que los datos van pasando por cada una de las capas, el encabezado pertinente se va suprimiendo de los datos. Cuando los datos y finalmente alcanzan la capa de aplicación, el destinatario puede utilizar su

cliente de correo electrónico para leer el mensaje que ha recibido. Continuación se explicará cada una de las capas que componen el modelo OSI, en orden descendente, es decir, partiendo de la capa de aplicación.

La capa de aplicación.

La capa de aplicación proporciona la interfaz y servicios que soportan las aplicaciones de usuario. Se encarga de ofrecer acceso general a la red.

También ofrece los servicios de red relacionados con estas aplicaciones de usuario, como la gestión de mensajes, la transferencia de archivos y las consultas a bases de datos. La capa de aplicación suministra cada uno de estos servicios a los distintos programas de aplicación con los que cuenta el usuario en su computadora. Entre los servicios de intercambio de información que gestiona la capa de aplicación se encuentran la Web, los servicios de correo electrónico como el protocolo simple de transferencia de correo, comúnmente conocido como SMTP (Simple Mail Transfer Protocol) incluido en el protocolo TCP/IP), así como aplicaciones especiales de bases de datos cliente/servidor.

La capa de presentación.

La capa de presentación puede considerarse el traductor del modelo OSI. Está capa toma los paquetes (la creación del paquete para la transmisión de los datos por la red empiezan realidad en la capa de aplicación) de la capa de aplicación y los convierte a un formato genérico que pueden leer todas las computadoras. Por ejemplo, los datos escritos en caracteres ASCII se traducirán a un formato más básico y genérico.

La capa de presentación también se encarga de cifrar los datos(que así lo requiere la aplicación utilizada en la capa de aplicación) así como de comprimirlos para reducir su tamaño. El paquete que crea la capa de presentación contiene los datos prácticamente con el formato con el que viajarán por las restantes capas de la pila OSI (aunque las capas siguientes irán añadiendo elementos al paquete, lo cual puede dividir los datos en paquetes más pequeños).

La capa de sesión.

La capa de sesión es la encargada de establecer el enlace de comunicación o sesión entre las computadoras emisora receptora. Esta capa también gestiona la sesión que se establece entre ambos nodos. Como se ve en la figura 1.8.3.

Una vez establecida la sesión entre los nodos participantes, la capa de sesión pasa a encargarse de ubicar puntos de control en la secuencia de datos. De esta

forma, se proporciona cierta tolerancia a fallos dentro de la sección de comunicación. Si una sesión falla y se pierde la comunicación entre los nodos, cuando después se restablezca la sesión sólo tendrán que volver a enviarse los datos situados detrás del último punto de control recibido. Así se evita el tener que enviar de nuevo todos los paquetes que incluía la sesión.

Protocolos que operan en la capa de sesión pueden proporcionar los tipos distintos enfoques para que los datos vayan del emisor al receptor: a comunicación orientada a la conexión y la comunicación sin conexión.

Los protocolos orientados a la conexión que operan en la capa de sesión proporcionan un entorno donde las computadoras conectadas se ponen de acuerdo sobre los parámetros relativos a la creación de los puntos de control en los datos, mantienen un diálogo durante la transferencia de los mismos, y después terminal de forma simultánea la sesión de transferencia.

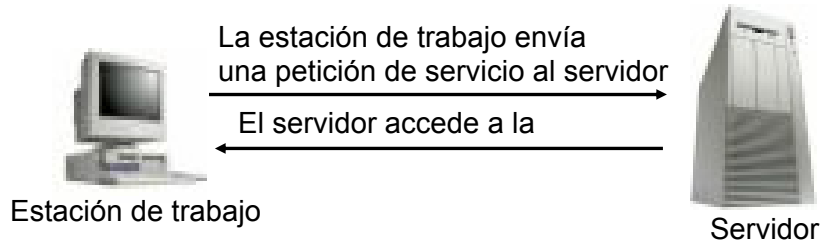


Figura 1.8.3 La capa de sesión proporciona el enlace de comunicación entre dos computadoras que se están comunicando.

Los protocolos orientados a la conexión operan de forma parecida a una llamada telefónica: en este caso, la sesión se establece llamando a la persona con la que se desea hablar. La persona que llama y la que se encuentra al otro lado del teléfono mantienen una conexión directa. Y cuando la conversación termina, ambos se ponen de acuerdo para dar por terminada la sesión y cuelgan el teléfono a la par.

El funcionamiento de los protocolos sin conexión se parece más bien a un sistema de correo regular. Proporciona las direcciones pertinente para el envío de los paquetes y esto pasan a enviarse como si se echaran a un buzón de correos. Se supone que la dirección que incluyen permitirá que los paquetes llegan a su destino, sin necesidad de un permiso previo de la computadora que va a recibirlos.

La capa de transporte.

La capa de transporte es la encargada de controlar el lujo de datos entre los nodos que establecer una comunicación; los datos no sólo deben entregarse sin errores, sino además en la secuencia que proceda. La capa de transporte se ocupa también de evaluar el tamaño de los paquetes con el fin de que éstos vengan el tamaño requerido por las capas inferiores del conjunto de protocolos. El tamaño de los paquetes lo dicta la arquitectura de red que se utilice.

La comunicación también se establece entre computadoras del mismo nivel (el emisor y el receptor); la aceptación por parte del nodo receptor se recibe cuando el nodo emisor ha enviado el número ha acordado de paquetes. Por ejemplo, el nodo emisor puede enviar de un solo golpe tres paquetes al nodo receptor y después recibir la aceptación por parte del nodo receptor. El emisor puede entonces volver a enviar otros tres paquetes de datos de una sola vez.

Está comunicación en la capa de transporte resulta muy útil cuando la computadora emisora manda demasiados datos a la computadora receptora. En este caso, el nodo receptor tomará todos los datos que pueda aceptar de una sola vez y pasara a enviar una señal de ocupado si se envían más datos. Una vez que la computadora receptora haya procesado los datos y este lista para recibir más paquetes, enviará a la computadora emisora un mensaje de luz verde para que envié los restantes.

La capa de red.

La capa de red encamina a los paquetes además de ocuparse de entregarlos. La determinación de la ruta que deben seguir los datos se produce en esta capa, lo mismo que el intercambio efectivo de los mismos dentro de la misma. La capa 3 que es donde las direcciones lógicas (como las direcciones IP de una computadora de red) pasan a convertirse en direcciones físicas (las direcciones de hardware de la NIC, la tarjeta de interfaz para la red, para esa computadora específica).

Los ruteadores operan precisamente en la capa 3 y utilizan los protocolos de encaminamiento de esta capa 3 para determinar la ruta que deben seguir los paquetes de datos.

La capa de enlace de datos.

Cuando los paquetes de datos llegan a la capa de enlace de datos, éstos pasan a ubicarse en tramas (unidades de datos), que vienen definidas por la arquitectura

de red que se está utilizando (como Ethernet). La capa de enlace de datos se encarga de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor, e identifica cada computadora incluida en la red de acuerdo con su dirección de hardware, la cual viene codificada en la NIC.

Los protocolos reales utilizan ambos métodos de comunicación: sin conexión y orientados a la conexión.

En los conjuntos de protocolos de red, como TCP/IP e IPX/SPX, se utilizan ambas estrategias de comunicación, la que precisa de una conexión y la que no, para desplazar los datos por la red. Por lo general, en la capa de sesión opera más de un protocolo para gestionar estas estrategias distintas de comunicación.

La información de encabezamiento se añade a cada trama que contenga las direcciones de envío y recepción. La capa de enlace de datos también se asegura de que las tramas enviadas por el enlace físico se reciben sin error alguno. Por ello, los protocolos que operan en esta capa adjuntarán un Chequeo de Redundancia Cíclica o CRC) al final de cada trama. El CRC es básicamente un valor que se calcula tanto en la computadora emisora como en la receptora. Si los dos valores CRC coinciden, significa que la trama se recibió correcta en íntegramente, y no sufrió error alguno durante su transferencia.

La capa física.

En la capa física las tramas procedentes de la capa de enlace de datos se convierten en una secuencia única de bits que pueden transmitirse por el entorno físico de la red. La capa física también determina los aspectos físicos sobre la forma en que el cableado está enganchado a la NIC de la computadora. En la computadora receptora de datos, la capa física es la encargada de recibir la secuencia única de bits.

1.9 Seguridad en el acceso remoto

La necesidad básica que estimula el crecimiento de la redes de área local es el incremento de la productividad, que en gran medida se logra al facilitar el acceso a un cúmulo de información. Siendo necesario por una parte, procurar un fácil acceso a gran cantidad de datos a usuarios en continuo crecimiento, mientras que por otro, se debe impedir a personas no autorizadas acceder a información disponible solo para ciertas personas. El permitir accesos remotos a la red exige un control exhaustivo de la seguridad.

La seguridad y la autorización empiezan con los conceptos de usuarios y contraseñas de paso. El administrador de la red define a todos los nuevos usuarios del sistema, les abre un registro y asigna a estos usuarios sus derechos sobre componentes de software y hardware de la red. Para obtener el acceso al sistema, los usuarios deberán hacer una conexión de entrada, especificando tanto su nombre de usuario como su contraseña de paso.
La autorización define los derechos de acceso de los usuarios en las redes y determina a que recursos tiene acceso un usuario y que operaciones puede realizar dicho usuario con esos recursos.
Un entorno operativo seguro, diseñado para cumplir los requisitos del nivel C-2 (Departamento de Defensa de EE.UU) de seguridad, como por ejemplo Windows NT, debe verificar:

- Acceso a recursos del sistema pueden ser controlados discretamente.
- Todos los accesos al sistema pueden ser grabados y auditados.
- El acceso al sistema será siempre mediante una contraseña y dejara unas pistas de auditoria.

Funcionamiento de la seguridad en el momento de la conexión.

A continuación se describe lo que sucede cuando un cliente llama a un servidor RAS para su conexión:

1. Un cliente llama el servidor de Acceso remoto a través de la acceso telefónico redes.
2. El servidor solicita una identificación al cliente (login y password).
3. El cliente envía una respuesta cifrada al servidor.
4. El servidor contrasta la respuesta con la base de datos de usuarios.
5. Si la cuenta es válida, el servidor verificará el permiso para acceso remoto.
6. Si se ha concedido el permiso para acceso remoto, el servidor se conectará con el cliente.

Activada la devolución de llamada, el servidor devolverá la llamada al cliente y repetirá los pasos 2 a 6.
Configuración de devolución de llamada
Como medida adicional de seguridad, RAS ofrece una característica de llamada de respuesta, que le permite asegurarse de que sólo los usuarios de determinadas

ubicaciones puedan acceder al servidor RAS. También ahorra dinero en teléfono al usuario.

Cuando un usuario establece una conexión con un servidor desde un cliente configurado para devolver la llamada, el servidor llama al usuario a un número de establecido o a un número proporcionado por el usuario en el momento de la conexión. En este método de seguridad frustrará la mayoría de los intentos de suplantación.

El privilegio de devolución de llamada se puede configurar para cada usuario al conceder los permisos para acceso remoto. La devolución de llamada puede realizarse a una dirección de destino fijada por el usuario al solicitar la colección, o a una dirección previamente establecida.

No se transferirán datos desde el cliente remoto o desde el servidor de acceso remoto hasta que el usuario no haya sido autentificado y se le haya devuelto la llamada (si activado la devolución de llamada).

El host de seguridad es un dispositivo de autentificación de otro fabricante que comprueba si la persona que llama desde un cliente remoto está autorizada para conectarse al servidor RAS. Está verificación complementa la seguridad ya suministrada por el servicio de acceso remoto.

Generalmente se encuentra entre el usuario remoto y el servidor RAS. Ofrece una capa de seguridad más al solicitar una clave determinada de hardware para proveer autentificación. La verificación de que el usuario está en posesión de la clave tiene lugar antes de que se conceda el acceso al servidor RAS. Está arquitectura abierta permite a los usuarios escoger entre diversas posibilidades de host de seguridad para aumentar la seguridad en el servicio de acceso remoto.

Por ejemplo, un tipo de sistema de seguridad consiste en dos dispositivos de hardware: el host de seguridad que se instala entre el servidor de acceso remoto (RAS) y su MODEM. La tarjeta de seguridad en sonoridad pequeña del tamaño de una tarjeta de crédito, recuerda a una calculadora de bolsillo sin teclas. La tarjeta de seguridad muestra un número de acceso diferente cada minuto. Este número se sincroniza con el mismo número calculado en el host de seguridad cada minuto. El usuario remoto, al conectarse, envía el número que está en la tarjeta de seguridad al host. Si el número es correcto, el host de seguridad conectará al usuario remoto con el servidor de acceso remoto.

Otro tipo de host de seguridad requiere que el usuario remoto escriba un nombre de usuario (que puede o no ser el mismo que el nombre de usuario de acceso remoto) y una contraseña (distinta de la contraseña de acceso remoto).

El host de seguridad debe configurarse de manera que permita al servidor RAS inicializar el módem antes de que surtan efecto las funciones de seguridad. El servidor RAS debe ser capaz también de inicializar directamente el módem conectado al host de seguridad sin que dicho host verifique la seguridad. El host de seguridad puede interpretar el intento de servidor para inicializar el módem como un intento de llamar.

1.10 Ruteadores

Los ruteadores son elementos de interconexión de nivel de red, trabajan de forma similar a los conmutadores y puentes ya que filtran el tráfico de la red. Es decir, cuando reciben un paquete por una conexión o puerto es el protocolo de red, en función de la dirección de destino y del correspondiente algoritmo de encaminamiento, quien decide porque puerto se transmiten los datos, en pocas palabras en lugar de transmitir según las direcciones de los paquetes de información, lo hacen en función del protocolo de red.
Son dispositivos de interconexión de redes incluso de distinta arquitectura. Capaces de direccionar la información a su destino utilizando para ello el camino apropiado.
Su función más habitual es enlazar dos redes que usen el mismo protocolo a través de una línea de datos como gráficamente se ve en la figura 1.10.1.
Los algoritmos de encaminamiento soportados por los routers pueden ser:

- No adaptativos: en los que las rutas de programan en los routers por configuración.
- Adaptativos: en los que los routers ejecutan entre sí un protocolo de intercambio de informaciones de estado que les permite definir rutas óptimas y reconfigurar sus tablas (por ejemplo el protocolo GGP de Internet).

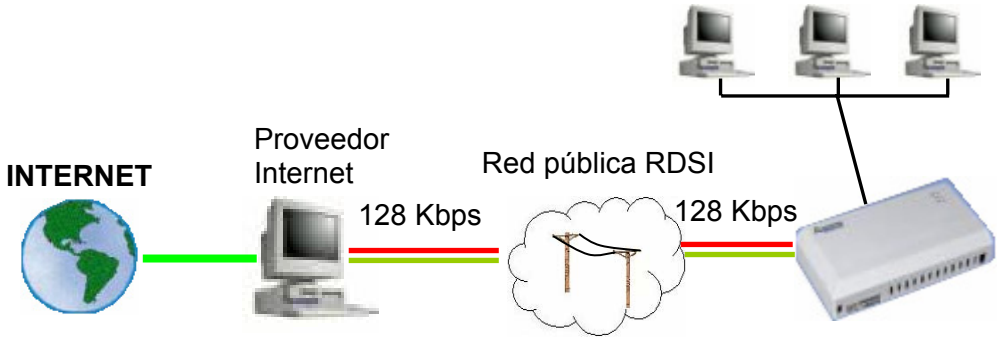


Figura 1.10.1 Ejemplo de aplicación del ruteador.

En teoría, la función que el modelo de referencia ISO asigna a los ruteadores es el de interconexión de redes incluso con distintos protocolos de red, mediante la

conversión de formatos de paquetes, además de la realización del puro encaminamiento.

Sin embargo, en la práctica, los ruteadores sólo implementan la función de encaminamiento. En el caso de que un paquete de un protocolo tenga que atravesar una red con distinto protocolo de red, el ruteador encapsula el paquete de la primera red en un paquete de la segunda, que se encaminara según el protocolo propio de dicha red, se extrae el paquete original. A esta técnica se le denomina tunneling.

El ejemplo más claro es la conexión de dos o más redes IP mediante una red X.25 cuyo ejemplo ilustrativo se presenta en la figura 1.10.2.

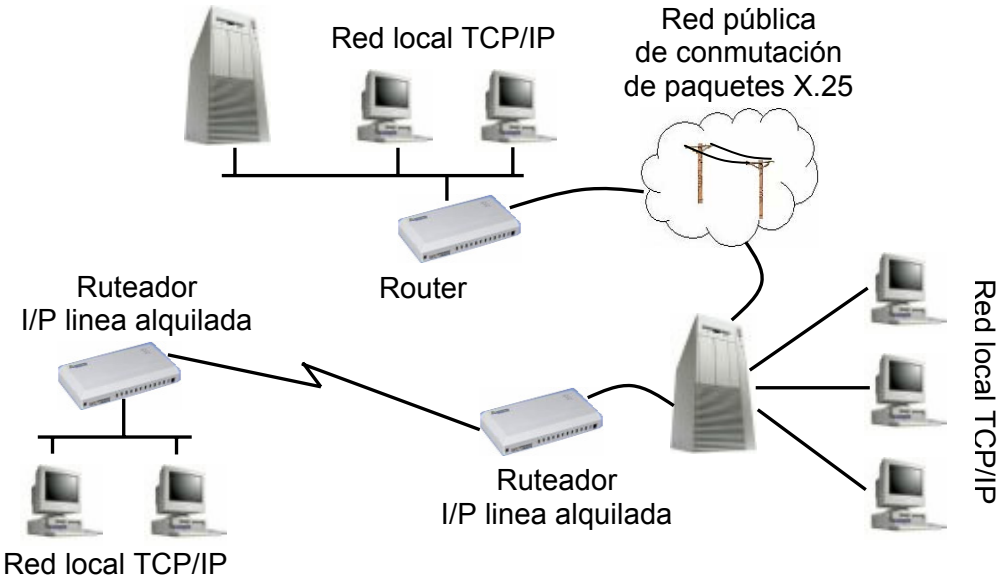


Figura 1.10-2 Interconexión de redes locales IP mediante X.25 tunneling.

Los ruteadores pueden encaminar paquetes pertenecientes a protocolos datagrama o protocolos de circuito virtual. Por ello, tradicionalmente se ha distinguido entre dos tipos de routers:

- Ruteadores datagrama: encaminan paquetes de protocolos datagrama, de tal forma que distintos paquetes de un mensaje pueden salir de la red incluso por conexiones distintas en función de lo que marque el algoritmo de encaminamiento en cada instante.

- Ruteadores de circuito virtual: los routers de este tipo son nodos de conmutación de paquetes que crean y mantienen circuitos virtuales entre entidades de red externas.

En cuanto a los routers de circuito virtual, su uso en la práctica se restringe a las conexiones X.25 y desde el punto de vista del usuario o del administrador de una red local interconectada por X.25, el ruteador hace las veces de ETD. Los nodos internos de una RPCP sí podrían realizar las veces de enrutador de circuito virtual, pero lógicamente su gestión e incluso implementación son responsabilidad del proveedor del servicio y transparente al usuario.
De igual manera, para interconectar redes X.25 entre si, se establecen conexiones de circuito virtual entre ruteadores de distinta redes, según la norma X.75, pero de forma transparente el usuario particular.
Un ruter puede encaminar un solo protocolo de red o puede ser capaz de encaminar distintos protocolos (IP, IPX, etc.). En este caso, se denomina router multiprotocolo y cuenta con el software necesario para el encaminamiento de cada protocolo, y debe ser configurado para ello.
Los ruteadores también pueden ser de tipo local, para interconectar segmentos de una red en una misma ubicación, o remotos, para la interconexión de segmentos de la red a través de un servicio de red pública. En este segundo caso, el router deberá tener al menos una interface de red local y una interface de red pública.
La decisión de conectar segmentos de red en local mediante ruteadores es muy discutible y puede acarrear más inconvenientes que ventajas. En primer lugar, el ruteador al igual que los puentes son elementos del tipo store and forward , es decir, que almacenan el paquete de red, decodifican los campos de control del mismo, y en función de ellos, toman la decisión de encaminamiento, y por fin realizan el entramado del paquete y lo retransmiten. En definitiva, su procesamiento es complejo, y los recargos que se introducen son apreciables y muy superiores a los de los puentes, sobre todo si el tamaño de los paquetes es pequeño.
La principal ventaja que aportan el es la no propagación de los paquetes broadcast (como por ejemplo en el caso denominado de tormentas ARP). Y en teoría facilitan la división administrativa de la red al poder de segmentarse a nivel de direcciones de red. Sin embargo, a cambio se pueden inducir bucles de encaminamiento en el caso de topologías redundantes de seguridad.

La configuración que debe evitarse siempre es la llamada red colapsada en el ruteador, ya que no aporta ninguna ventaja y perjudica muy grandemente las prestaciones.
Una arquitectura típica de ruteador queda detallada en la figura 1.10.3. Donde se observa su configuración normalizada, que se compone de un microprocesador, sus memorias y por su puesto, sus vías de conexión con las redes.

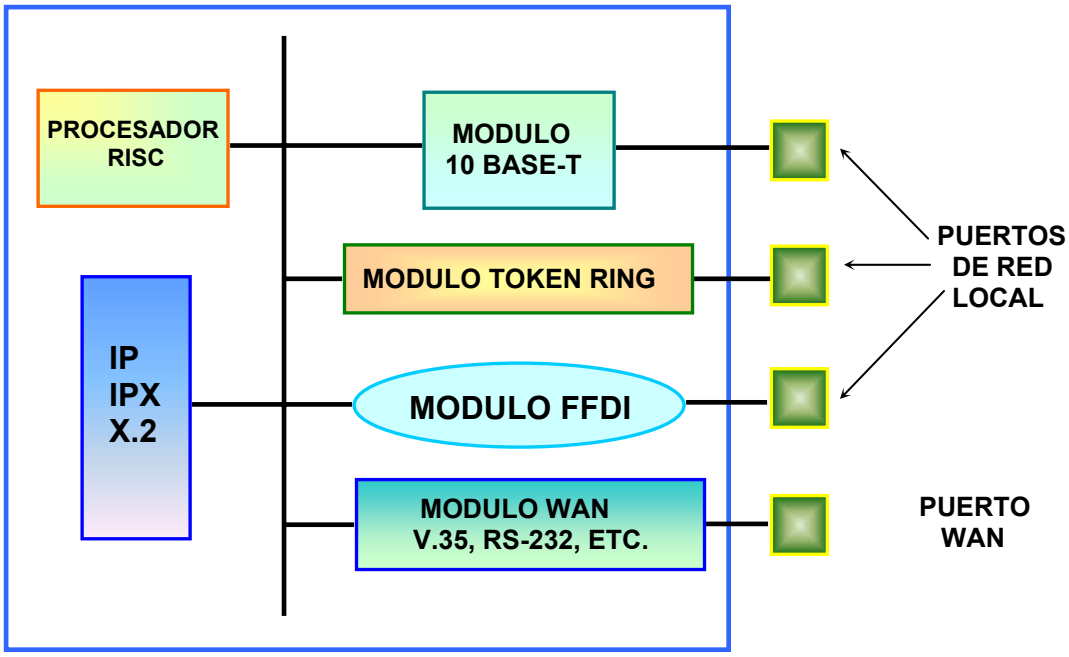


Figura 1.10.3 Arquitectura típica del ruteador.

Las características que definen la calidad del ruteador son:

- Velocidad de reenvio: parámetro análogo al caso de los puentes.
- Capacidad de manejo de paquetes por unidad de tiempo: teniendo en cuenta paquetes de tamaño mínimo.
- Capacidad multiprotocolo: fundamental cuando existen distintos protocolos trabajando en la red.
- Empleo del protocolo simple de gestión de red (Simple Network Management Protocol) que permita la configuración remota de los puertos incluyendo su activación y desactivación.
- Facilidad de instalación y configuración.
- Tolerancia a falla. Dado que el ruteador es un elemento crucial en la red, su capacidad para tolerar fallos es fundamental, por lo que al menos deberá

tener fuentes de alimentación redundantes y construcción modular, que permita cambiar fácilmente los módulos que presenten de errores, sobre todo la CPU, la memoria y las placas de cada puerto.

TEMA 2. DESCRIPCIÓN DEL RUTEADOR LANTRONIX

2.1 Descripción.

Los ruteadores permiten el tráfico de información entre una red local y redes remotas o computadoras aisladas. Los servidores se interconectan con módems para gestionar las peticiones de dispositivos e información definidos como servicios para los usuarios de red, y además, pueden proporcionar conexiones para incluir otros dispositivos en la infraestructura de la misma.
En el panel frontal del ruteador LRS1 viene un puerto serie hembra DB25 como el que se observa en la figura 2.1.1.

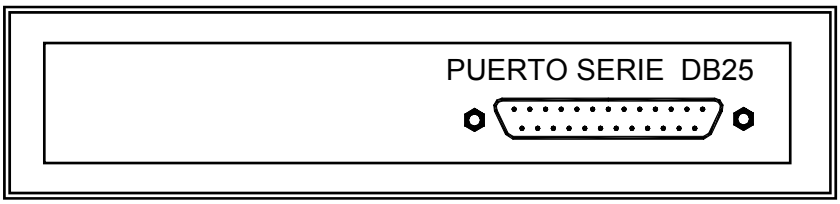


Figura 2.1.1 Puerto serie en el panel frontal.

En el panel posterior se encuentra un conector RJ45 para Ethernet, un botón de reset y un conector para la fuente de voltaje, cuyo aspecto es como el de la figura 2.1.2.

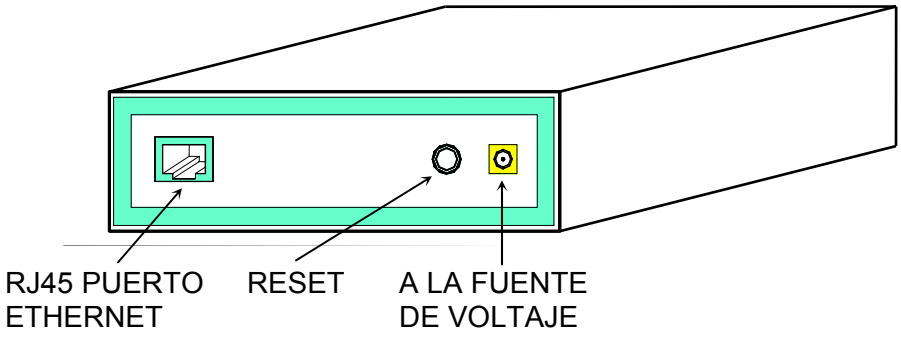


Figura 2.1.2 Panel trasero del LRS1

Nota: Si se presiona el botón de reset durante el periodo de arranque, se forza al LRS1 a tomar los valores de configuración básica programados por el fabricante.

Tiene cuatro LEDS indicadores en su parte superior como se observa en la figura 2.1.3.

Figura 2.1.3 Vista superior del LRS1 mostrando los LEDs.

Estos LED´s tienen las siguientes funciones:

El primero es un indicador de encendido, y se ilumina en color verde cuando el ruteador esta conectado a su fuente de voltaje.
El segundo es un indicador de enlace de red, enciende en color verde cuando el aparato está bien conectado y operando en la red.
Los otros dos indican la actividad de la red y el puerto serie. Estos pueden parpadear en amarillo, verde o rojo dependiendo de los procesos que esten llevando a cabo.

2.2 Especificaciones.

Requisitos de energía:
Voltaje de 110 V AC , 220 V AC
Frecuencia de 47-63 Hz
Corriente nominal de 700 mA @ 6 V
Consumo de energía de 4.2 Watts máximo.

Protección de 1.6A, 250 Volts

Cable de corriente:
Cable de 3 conductores de 1.0 mm2 mínimo por conductor (18 AWG).
Capacidad de 250 Volts AC, 10 Amps
Longitud de 3.0 metros

Limitaciones en el medio ambiente:
Rango de temperatura: 5° a 50° C (41° a 122° F)
Temperatura de almacenaje: -40° a 66° C (-40° a 151° F)
Cambio de temperatura máximo por hora: 20° C (36° F)
Un cambio brusco de temperatura provoca un mal funcionamiento del equipo por lo que se debe mantener alejado tanto de fuentes de calor como de dispositivos de enfriamiento, ventanas grandes o puertas que sean salidas al exterior.

Altitud:
Altura máxima de operacion: 2.4 km (8,000 ft)
Altura máxima de almacenaje 9.1 km (30,000 ft)
Si se emplaza el LRS por arriba de 2.4 km (8000 ft.), se debe de reducir la temperatura de operación en una relación de 1° F por cada 1000 ft.

Humedad:
Humedad relativa en operación de 10% a 90% no condensada y una recomendada de 40% a 60%.
Humedad en el almacenamiento de 10% a 90% no condensada.

El LRS1 cuenta con un puerto serie y conector DB25, un conector AUI, un puerto UTP (10/100BASE-T) y una salida BNC (10BASE2) como puerto para las conexiones de Ethernet.
Soporta los protocolos AppleTalk, IP, e IPX y es capaz de interconectar una red de computadoras u otros dispositivos que incluyan microprocesadores. Soporta velocidades de transmisión de entre 300 y 230400 bits por segundo.

2.3 Funcionamiento.

Cuando la información tiene que pasar de una red a otra, el dispositivo de conexión entre redes que se encarga de mover los datos es el ruteador. Para encaminar datos en una interconexión de redes es preciso que se produzcan dos eventos distintos: por un lado, que se determine la ruta apropiada para los paquetes y, por otro, que los paquetes se desplacen hasta su destino final.
Tanto la determinación de la ruta como el encaminamiento de los paquetes (o su conmutación, como también suele denominarse, ya que los paquetes son de hecho conmutados desde la interfaz saliente del ruteador) se producen en la capa 3 (capa de red) del modelo OSI. Otro evento importante que ocurre en la capa 3 es la resolución o conversión de las direcciones lógicas (como número IP cuando TCP/IP es el protocolo encaminado) en direcciones de hardware. Para comprender, mejor el proceso, se hace lo siguiente:

Determinación de la ruta.
Los ruteadores permiten dividir una red amplia en subredes lógicas: con ello, se consigue aislar el tráfico local en cada subred ,permitiendo así sacar el máximo partido a la ancho de banda disponible. Estos pasan entonces a encargarse de transmitir los paquetes de datos entre las subredes. Asimismo, pueden servir de dispositivo de conexión entre la red (las restantes redes corporativas consideran el conjunto de subredes como una sola red, incluso si ésta está dividida en partes lógicas), y como dispositivo de conexión entre el resto de redes a las que está conectada la propia red. El mejor ejemplo de conexión entre un gran número de redes distintas por motivos de intercambio de información es, sin duda alguna, Internet.
Las direcciones lógicas que se asignan a los nodos y a las interfaces del ruteador servirán para explicar el modo en que el aparato determina cuando debe y cuando no reexpedir tramas a una red. En ningún caso se trata de direcciones lógicas reales. Las direcciones lógicas reales, como las direcciones IP, son las que se utilizan en las redes del mundo real.
Crear subredes es la parte fundamental en la implementación del encaminamiento de datos en una red. Por ahora, basta comprender que las subredes son divisiones lógicas de una gran red corporativa.

La figura 2.3.1 muestra un red que se ha dividido en dos subredes distintas por medio de un ruteador. El tipo de conexiones (cable utilizado) entre ambas subredes (Ethernet, Token Ring, etc) y el ruteador no están ilustrados.
En este ejemplo el ruteador tiene dos interfaces de red, la interfaz 1 y la interfaz 2, que están conectadas a la subred 1 y a la subred 2, respectivamente. El sistema de direccionamiento lógico que se utiliza para asignar direcciones a los distintos nodos de la red (también se tienen que asignar direcciones lógicas a cada interfaz del ruteador) es aplicar el número de subred seguido de la letra que designa a dicha subred. Por tanto, al Nodo A de la subred 1 se le asigna la dirección lógica 1A (primero la designación de la subred y después la del nodo).

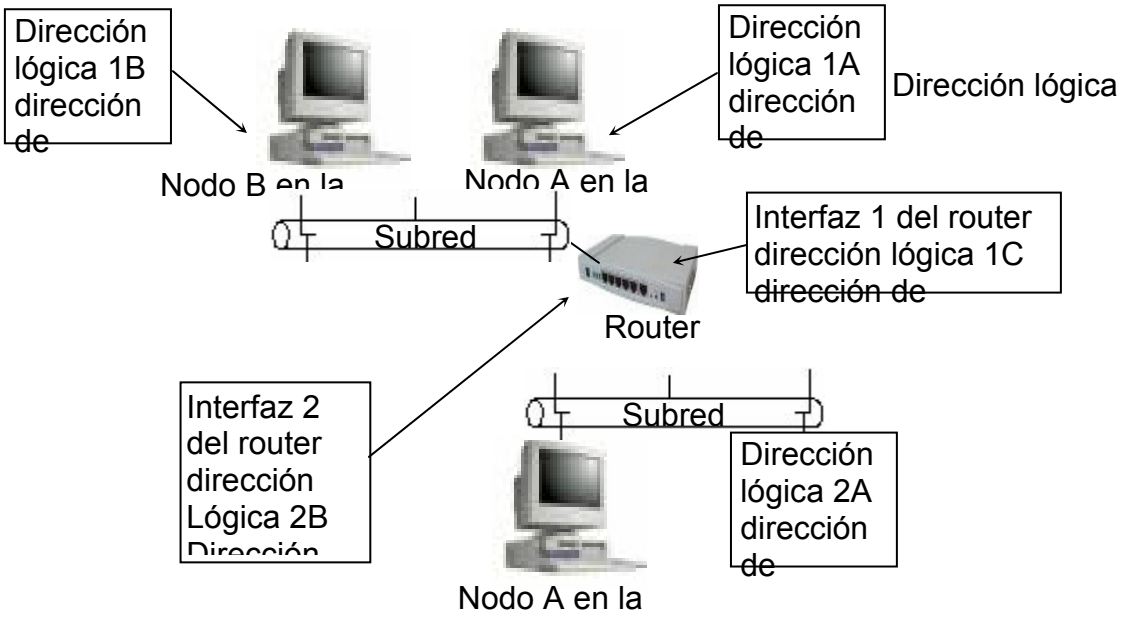


Figura 2.3.1 Red dividida en dos subredes lógicas.

Cada nodo de la red también tendrá asignada una dirección de hardware (recordando que las direcciones de hardware vienen ya asignadas de fabrica en las NIC, a las interfaces de ruteador también se les asigna direcciones de hardware en el momento de su fabricación). Para mayor claridad, las direcciones de hardware asignadas a cada uno de los nodos de la red se componen de una X seguida de un número. Por ejemplo, la dirección de hardware para el Nodo A de la

Subred 2 es X4, recordando que todas las direcciones de hardware son distintas y su asignación depende del fabricante.

Direcciones lógicas y de hardware.

Cuando se conectan dos redes utilizando un ruteador, se acaba con dos tipos distintos de trafico de datos: por un lado, con un trafico de datos local, donde los nodos de una misma subred se comunican entre si; y, por otro, con un trafico de red donde los nodos de las distintas subredes establecen comunicación. Este último tipo de tráfico es el que tiene que gestionar por el ruteador.

Comunicación en la misma subred.

Si por ejemplo dos computadoras incluidas en la misma subred se comunican, el Nodo A de la subred 1 tiene que enviar los datos al Nodo B de la subred 1. El nodo A sabe que los paquetes tienen que dirigirse a la dirección lógica 1B en una dirección real de hardware.

Ahora bien, es posible que el nodo A ya sepa que la dirección lógica 1B se refiere a la dirección de hardware X2. De hecho, las computadoras suelen tener pequeñas memorias caché donde guardan este tipo de información para la resolución de direcciones de hardware. Si el Nodo A no conoce la dirección de hardware correspondiente a la dirección lógica 1B en una dirección de hardware. Cuando reciba la información enviada a los paquetes al nodo de, que los aceptará sin problemas ya que cuentan con su dirección de hardware, X2.

Comunicación entre subredes diferentes.

Veamos ahora situación en que de una computadora se decide enviar datos a otra computadora ubicada en otra subred.

El nodo A de la subred 1 desea enviar datos al Nodo A de la subred 2. Esto significa que el Nodo A de las subred 1 desea enviar datos a la dirección lógica 2A. El Nodo A de la subred 1 sabe que la dirección 2A no se encuentra en la subred local, por lo que pasa a enviar los paquetes a su pasarela determinada, de en es más que la interfaz del ruteador está conectada a la subred 1. En este caso, de dirección lógica de la pasarela del Nodo A (de la subred1) es 1C. Sin embargo, como ocurría antes, esta dirección lógica tienen que resolverse en una dirección

de hardware, es decir, convertirse en la dirección de hardware de la interfaz 1 del ruteador.

Los nodos recogen información de direccionamiento.

Las computadoras utilizan mensajes de difusión y tablas de información (que elaboran a partir de la información de difusión ubicada fuera de la red por otras computadoras) para determinar que direcciones son locales y cuáles son remotas dentro de una conexión entre redes. Una vez más, y sirviéndose de mensajes de difusión, el Nodo 1 de la subred 1 recibe la información dirección de hardware relacionada con la dirección lógica 1C (la dirección de hardware es X3) y pasa a enviar los paquetes al ruteador 1 a través de su interfaz 1. Ahora que el ruteador tiene los paquetes, debe determinar el modo en que deberá red en pedirlo con el fin de que lleguen al nodo de destino. Para ello, consultará la tabla de encaminamiento y después conmutada los paquetes a la interfaz que está conectada a la subred de destino.

Conmutación de paquetes.

Cuando los paquetes llegan ruteador, se opera la conmutación de los mismos. Esto quiere decir que el ruteador moverá paquetes desde la interfaz del ruteador por la que entraron y los conmutará hasta la interfaz de ruteador conectada a la subred a la que deben dirigirse. Sin embargo, en determinados casos, es posible que los paquetes tengan que pasar por más de un ruteador para alcanzar su destino final. En este ejemplo sólo participa un ruteador, el Ruteador 1, que sabe que la dirección lógica 2A se encuentra en la Subred 2, por lo que pasa a conmutar los paquetes desde la interfaz 1 de ruteador a la interfaz 2 de ruteador.

Una vez más, se recurre a los mensajes de difusión para resolver la dirección lógica 2A en la dirección de hardware X4. Se asigna a los paquetes la dirección apropiada y el ruteador pasa después a reexpedirlos a la subred 2. Cuando el Nodo A de la Subred 2 ve los paquetes con la dirección de hardware X4, pasa a apropiarse de ellos.

El encaminamiento de datos supone tanto el uso de direccionamiento lógico como el direccionamiento de hardware para transmitir paquetes desde una computadora emisora a otra computadora receptora. Todos los protocolos de encaminamiento utilizan un esquema ligeramente distinto para resolver direcciones lógicas en

direcciones de hardware, pero siguiendo prácticamente en el mismo método (direccionamiento de TCP/IP).

Tablas de encaminamiento.

Los ruteadores utilizan software para crear tablas de encaminamiento, estas tablas contienen información sobre que interfaz de hardware del ruteador es la ruta de inicio (para el ruteador) que recibirá a los paquetes para después reexpedirlos a su dirección de destino.

Sin embargo el equipo, no toma en cuenta las direcciones de nodos particulares al construir sus tablas encaminamiento; tan sólo consideran el modo de reexpedir un determinado número de paquetes a la red pertinente. Por ejemplo:

Las tablas de encaminamiento proceden, en realidad, de dos fuentes distintas. En un encaminamiento estático, el administrador de la red introduce en la tabla las distintas rutas disponibles entre los segmentos interconectados. Para ello, el administrador de red utiliza una serie de comandos de ruteador con el fin de elaborar una tabla parecida a la Tabla 2.3.1. Las tablas encaminamiento también pueden construirse de forma dinámica utilizando protocolos de encaminamiento RIP e IGRP.

Nombre lógico de la subred	Interfaz del ruteador
1	1
2	2

Tabla 2.3.1 Tabla básica de encaminamiento para el ruteador 1.

Cuando en la interconexión participan varios ruteadores, como ocurre en las grandes redes corporativas, las tablas de encaminamiento contienen más información. Por ejemplo, podemos tomar la anterior red compuesta por dos subredes y un ruteador, y ampliarla a una red que integre cinco subredes y dos ruteadores. La figura 2.3.2 muestra esta red ampliada.

Dirección lógica 1B dirección de

Dirección lógica 1A dirección de

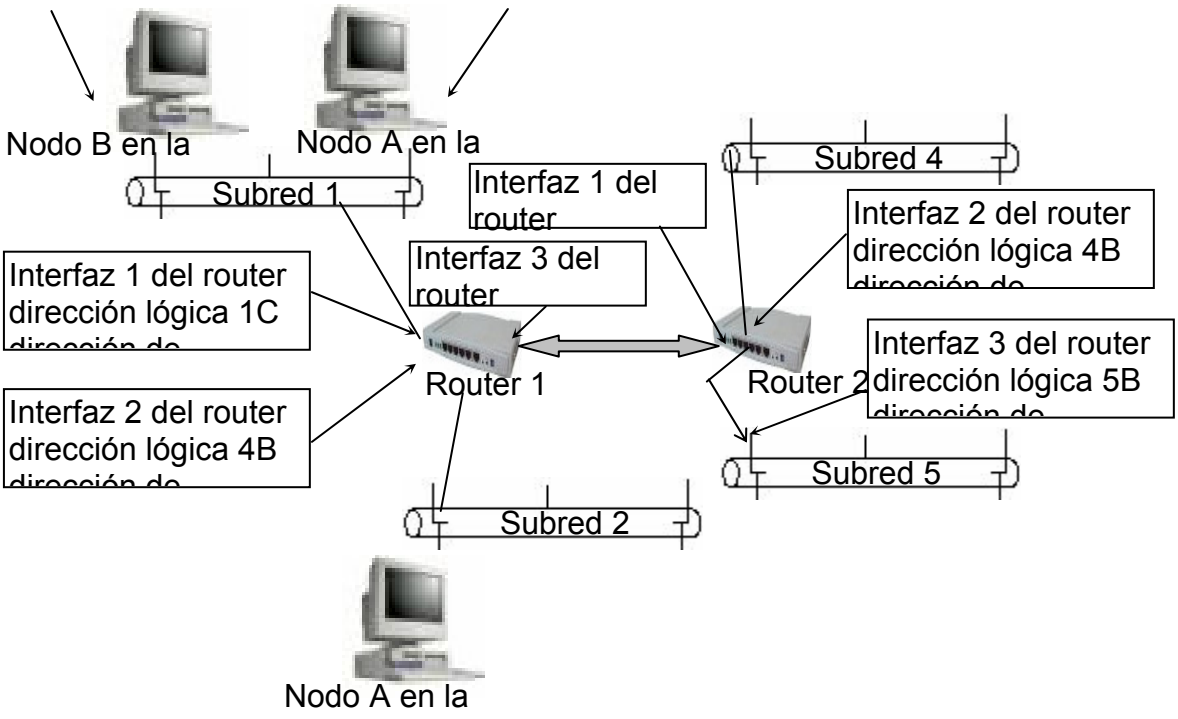


Figura 2.3.2 Una red dividida en cinco subredes que utiliza dos ruteadores.

Es posible que ahora sólo se vean cuatro subredes. Pero de hecho, cualquier conexión serie entre dos ruteadores conforma una subred aparté y se le debe asignar una dirección lógica única.

La figura 2.3.3 muestra una red de área local que incluye un ruteador entre sus componentes operativos y lo que se debe hacer para ponerlo en funcionamiento es:

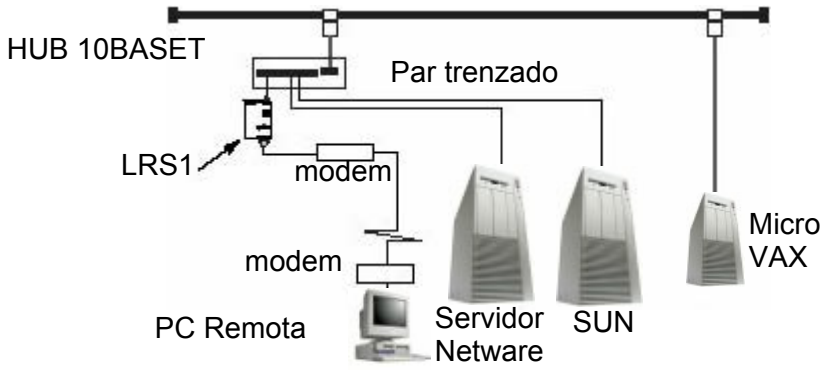


Figura 2.3.3 Red local con un ruteador LRS1.

1. Primero hay que definir es donde se va a colocar el ruteador, atendiendo todas y cada una de las medidas de protección que exige el fabricante, ya que una mala ubicación del mismo puede ocasionar funcionamiento errático que por ejemplo puede reflejarse en perdida de datos.
2. Conectarlo mediante el conector RJ45, que esta en el panel trasero, a la red Ethernet mediante un cable para 10BASE-T.
3. A continuación, conectarlo a un dispositivo de comunicación serie.
El LRS1 esta diseñado para comunicarse con otros dispositivos que gestionen comunicaciones en serie mediante un puerto RS232, para lo cual se emplea un conector DB25.
El puerto serie esta configurado inicialmente para operar a una tasa de 9600 bauds, 8 bits, un bit de parada y sin paridad.
4. Poner en funcionamiento el LRS1.
Solo se debe usar la fuente de voltaje del LRS1 que es de 6 volts, ocupar otras fuentes que cumplan con el voltaje, pero no con otros parámetros necesarios para su funcionamiento puede ocasionar daños irreversibles.
Se debe verificar que los LEDs de encendido y enlace se iluminan. Si no es así, hay que desconectarlo y verificar su conexión de voltaje y Ethernet y volverlo a poner en operación.
El procedimiento de arranque para el LRS1 consta de los siguientes tres pasos, y cuando está operando normalmente el arranque requiere de 30 segundos aproximadamente para completarse:
1.- Al encenderlo se ejecuta, un procedimiento de diagnostico que dura aproximadamente 5 segundos. Los LEDs de encendido y enlace se iluminan en verde intenso. Los LEDs de estado OK y señal serie se iluminaran alternativamente e indican que se están realizando auto pruebas. Los LEDs de encendido y enlace se iluminan en verde si el LRS1 está correctamente conectado tanto a la fuente de voltaje como a una red de comunicaciones valida.
2.- El LRS1 obtiene información de la configuración TCP/IP por medio del BOOTP y el RARP. Esto tarda aproximadamente 20 segundos si el equipo anfitrión (consola del ruteador) acepta la petición de llamado. Durante este lapso de

tiempo, el LED de OK parpadeara en verde tres veces por segundo, ocasionalmente parpadea en amarillo cuando se envían o se reciben datos.

3.- Determinara si el código cargado en la memoria Flash RAM es válido. Si es así, se cargara el código y continuara su ejecución normal. Esto lo realiza en 5 segundos aproximadamente.

Cuando la unidad opera normalmente, el LED de OK parpadeara dos veces, una vez por segundo. Si hay datos que se estén transmitiendo en el puerto Ethernet, el LED de OK parpadeara en amarillo. El LED serie parpadeara en rojo cuando se este transmitiendo información por el puerto serie, en verde cuando se este recibiendo información y en amarillo cuando este tanto recibiendo como transmitiendo datos.

Almacena su código ejecutable en una memoria Flash ROM reescribible, para hacer posible las subsecuentes actualizaciones. Sólo es necesario que se obtenga dicho software para cargárselo al LRS y de esta manera tener al día el código en la memoria ROM con una nueva versión del código de configuración inicial.

Aunque mediante el EZWebCon es la manera recomendada para configurar el servidor de acceso remoto, el equipo también puede ser configurado usando cualquiera de los métodos siguientes:

Por medio de las conexiones de Telnet/Rlogin al ruteador.

Al conectarse vía BOOTP a un sitio TCP/IP (se direcciona la IP, se establece el equipo anfitrión del los datos para que se pueda transmitir el archivo.)

Por medio de un archivo de configuración transmitido vía TCP/IP o NetWare e introducido al aparato al momento de su puesta en marcha.

2.4 Configuración.

Establecer la configuración básica de un ruteador consiste en activar sus distintas interfaces y configurar los parámetros vía software para los protocolos encaminados y de encaminamiento. Por ejemplo, si se esta encaminando IP, las interfaces tienen que tener asignadas las direcciones IP correspondientes. Los protocolos de encaminamiento también tienen que estar debidamente configurados (si se va a utilizar RIP o IGRP, deberán configurarse estos dos protocolos). Lo mismo que cualquier interfaz en serie que vaya a emplearse y deberá utilizarse con el correspondiente protocolo WAN de capa 2 (como DIC o el Relé de trama). Entre la información acerca de la configuración básica deberá asimismo incluirse el ancho de banda y la sincronización para conexiones WAN.
El código de configuración del ruteador se sirve de parámetros de software para indicarle lo que debe encaminar y el modo en que debe hacerlo. Existen distintas formas de llevar a cabo la configuración del ruteador, ya sea utilizando directamente la consola del ruteador, o bien de forma indirecta, cargando un archivo de configuración ubicado en un servidor de Protocolo Trivial de Transporte de Archivos TFTP (Trivial File Transport Protocol) dentro de la red. El listado siguiente muestra algunas de las opciones disponibles para cargar la información de configuración dentro de un ruteador:

- Consola del ruteador. Puede configurarse directamente desde un PC que esté conectado al puerto correspondiente por medio de cable trenzado. El PC tiene asimismo que ejecutar algún tipo de software de emulación de terminal que le permita conectarse con el ruteador a través del puerto serie del PC.
- Terminal Virtual. Si ya se configuró a nivel básico activando algunas de las interfaces en la red (como un puerto Ethernet), se puede configurar vía Telnet por medio de una terminal virtual. Esto significa sencillamente que una computadora de la red que esta ejecutando un programa Telnet se conectará con el ruteador y pasara a configurarlo (siempre que se faciliten las contraseñas correctas).
- Estación de trabajo para la gestión de la red: También pueden configurarse desde una estación de trabajo incluida en la red que ejecute un software

especial para la gestión de redes, como la Cisco Works de Cisco o el HP Open View de Hewlett Packard.

- Servidor TFTP. Se puede cargar una configuración de ruteador desde un servidor TFTP incluido en la red. Si se guardan las configuraciones en un servidor de este tipo, después podrán descargarse sin problemas para otros ruteadores.

De entre todos estos métodos de configuración, probablemente el más sencillo y directo sea el de conectar un PC directamente al puerto de la consola del ruteador. Con ello no solo se puede construir rápidamente una configuración básica gracias a los cuadros de dialogo que presenta el software, sino que además permite ajustar los parámetros de configuración en el modo de configuración.

El PC que se utilice como consola se comunica con el ruteador por medio del software de emulación de terminal. Existen varios paquetes de software de este tipo, como HyperTerminal (que viene en sistemas operativos de Microsoft) o ProComm plus (un programa comercial de comunicaciones que integra funciones de fax, emulación de terminal y otros servicios de comunicación). También existen otros paquetes de software disponibles en Internet que pueden descargarse como freeware o shareware, como Tera Term Pro que es un emulador bastante funcional.

Hay que asegurarse de que el software de emulación de terminal soporta la comunicación en serie ya que hay algunos de ellos que funcionan vía Telnet. Esto significa que no soportan o permiten la configuración del software de terminal para comunicaciones a través de puertos serie.

Una vez instalado un determinado paquete de software de emulación de terminal, se deben configurar los parámetros del puerto serie elegido para comunicarse con el ruteador. La tabla 2.4.1 refiere un listado de los parámetros de comunicación que debe utilizar el software.

Parámetro	Configuración
Emulación de terminal	VT100
Velocidad en Baudios	9600
Paridad	Ninguna

Bits de datos	8
Bits de parada	1

Tabla 2.4.1 Parámetros a configurar en el puerto serie.

2.4.1 Trabajar con el software de emulación de terminal remota.

Configuración con el EZWebCon

El programa EZWebCon, se distribuye con el LRS1 y es la manera más fácil de configurar el servidor. La interfaz de selección y puesta a punto con EZWebCon ayuda a configurar el equipo para aplicaciones en general y tareas especificas.

El EZWebCon se realizo para dar soporte en sistemas que funcionan bajo las plataformas operativas de UNÍX, Machintosh, Windows/Windows NT, y Novell Netware, todas las versiones están incluidas en el CD-ROM que incluye el equipo.

Configuración mediante la línea de comandos.

Si se desea se puede configurar con la interfaz de línea de comandos (disponible en sesiones Telnet/Rlogin) por medio de EZWebCon, o bien conectándolo a una terminal mediante el puerto serie. Este método nos es tan gráfico e intuitivo ya que exige el conocimiento de las opciones de la tabla 2.4.2. Las modificaciones que se hagan a la configuración que esta definida por el fabricante del servidor solo se verán reflejadas al reiniciar el equipo.

OPCION	DESCRIPCIÓN
IP Adress	Aquí se le define la dirección IP
Load Host IP Adress	Aquí se define la dirección IP del equipo anfitrión
Second IP Host	Se define una dirección IP de un equipo anfitrión de respaldo
IP Subnet Mask	Dirección IP de la mascara de sub red.
Scan Settings	Muestra la versión del software con que opera, la dirección IP, el nombre del archivo del programa de operación, dirección IP del equipo de respaldo y la mascara de sub red.
Reboot	Reinicializa y pone los valores por defecto

Tabla 2.4.2 Opciones de la configuración.

2.5 Interfaces

2.5.1 Generalidades

Una interfaz suministra la conexión física entre el ruteador y un tipo de medio físico de la red. Las interfaces a menudo se denominan puertos y cada puerto viene designado físicamente de acuerdo con la topología de red a la que sirve. Por ejemplo, una interfaz de Red de Área Local (LAN) ,como un puerto Ethernet en se compone de un conector hembra RJ45 (que está conectado a un repetidor (hub) Ethernet) por medio de un cable de par trenzado con conectores machosRJ45 en cada extremo).

Los puertos incorporados se designan por tipo de conexión seguido de un número. Por ejemplo, si el primer puerto Ethernet en un ruteador se designa como E0, el segundo se designará E1, y así sucesivamente (en determinados casos, el puerto Ethernet se configurará como repetidor (hub)). Los puertos serie se designan siguiendo este mismo procedimiento, donde S0 corresponde al primer puerto serie.

No sólo pueden conectarse distintos tipos de tarjetas de interfaz (como LAN o WAN), sino que además puede seleccionarse el número de puertos deseados en cada tarjeta. Por ejemplo, en una de las tres ranuras que tienen disponibles algunos modelos de ruteadores de la serie LRS.

Para saber que interfaces (así como su actual estado) se están utilizando en un determinado ruteador se utiliza el comando show interfaces. El estado de los distintos puertos dependerá de si están conectados (físicamente a la red) y de si han sido configurados.

Los ruteadores de gama alta, utilizan tarjetas de Procesador de interfaz Versátil (Versatile Interface Processor o VIP). Cada tarjeta VIP puede disponer de dos ranuras para tarjetas de interfaz. Este tipo de ruteadores se construyen de forma personalizada, y sus Interfaces se ajustan directamente a las necesidades de interfaz que pueda requerir una interconexión amplia de redes.

La configuración de una determinada interfaz depende del tipo de protocolo de red de utilice la red al que esta conectado el puerto de la interfaz. Por ejemplo, un puerto Ethernet conectado a una red IP tendrá que configurarse para el

encaminamiento IP. En cambio, un puerto Ethernet conectado a una red Apple Talk deberá configurarse para el encaminamiento Apple Talk.
Los ruteadores LRS soportan varias redes LAN, ampliamente utilizadas. Las Interfaces de ruteador mas comunes para redes LAN son Ethernet, Fast Ethernet, Token Ring de IBM y la Interfaz de Datos Distribuidos por Fibra Óptica (Fiber Distributed Data Interface o FDDI).
Todos estos protocolos de Red de Area Local (LAN), utilizan el mismo sistema de direccionamiento físico de la capa de enlace de datos (es decir, la dirección MAC de hardware el NIC, o la dirección MAC de hardware ubicada en el controlador de la interfaz de ruteador). Estas direcciones son únicas para cada dispositivo.
Se puede gestionar más de un protocolo de red (como el IP e IPX/SPX) a la vez. También es capaz de ejecutar varios protocolos de encaminamiento al mismo tiempo (algo que en ciertos casos exigen los protocolos de red que deben encaminarse).

Interfaces en serie.
Permiten conectar varias redes LAN utilizando tecnologías WAN. Los protocolos WAN transmiten datos a través de interfaces asíncronas y sincronas en serie (dentro de los ruteadores), están conectadas entre si mediante líneas contratadas y otras tecnologías de conectividad suministradas por terceros.
Las conexiones sincronas en serie utilizan un dispositivo de sincronización que propicia una correcta transmisión de los datos cuando estos se transmiten del emisor al receptor a través de una conexión en serie. Las comunicaciones asíncronas sirven de los bits de inicio y de parada para garantizar que la interfaz de destino ha recibido todos los datos.
Las tecnologías WAN de la capa del enlace de datos que más se utilizan en la actualidad son el Control de Enlace de Datos de Alto Nivel (High Level Data Link Control o HDLC). El X.25, el Relé de trama (Frame Relay), la Red Digital de Servicios Integrados (Integrated Services Digital network o IDSN) y el protocolo de punto a punto (Point to Point Protocol). Todos estos protocolos WAN se configuran en determinadas interfaz es de ruteador cuando éste se encuentra en el modo de configuración.

Interfaces lógicas.

Las interfaces lógicas no existen como tales, es decir, no son interfaces de hardware de un ruteador.

Es una interfaz únicamente de software que se crea mediante el IOS de un ruteador. Para entender el concepto, se puede considerar como una interfaz virtual creada por medio de una serie de comandos del software del ruteador. Los dispositivos reconocen estas interfaces virtuales como interfaces reales, lo mismo que una interfaz de hardware, como un puerto serie por ejemplo. Se pueden configurar distintos tipos de interfaces lógicas en un ruteador, como interfaces de retrobucle, Interfaces nulas e interfaces de túnel.

Interfaces de retrobucle: Emula una Interfaz física real en el ruteador. Los retro bucles suelen configurarse en un ruteador de gama alta utilizado como ruteadores de núcleo entre dos interconexiones corporativas de redes o entre una red corporativa e Internet. Los ruteadores que sirven como ruteadores de núcleo se configuran con un protocolo externo de pasarela, como el Protocolo de Pasarela Fronteriza (BGP), que encamina a los paquetes entre dos interconexiones distintas de redes.

Puesto que el ruteador sirve como enlace fundamental entre interconexiones de redes, los paquetes de datos no deberían volcarse si una determinada interfaz física del ruteador deja de funcionar. Por esto mismo, la interfaz virtual de retro bucles recrea y configura como la dirección de finalización para las sesiones del Protocolo de Pasarela Fronteriza (BGP). De esta forma, el tráfico se procesa localmente en el ruteadores, lo que garantiza la recepción integra de los paquetes en su destino final.

Interfaces nulas. Esta Interfaz se configura en un ruteador utilizando determinados comandos y sirve como un muro de contención para impedir el paso de un determinado tráfico de la red. Por ejemplo, si no desea que el tráfico de una determinada red pase por un determinado ruteador (y que lo hagan por otros ruteadores incluidos en la interconexión) se puede configurar la interfaz nula de forma que reciba y vuelque todos los paquetes que la red envíe a dicho ruteador. Por lo general, los listados de acceso se utilizan para filtrar el tráfico en una interconexión de redes y definir los ruteadores que pueden utilizarse para determinadas redes. Comparada con los listados de acceso, la interfaz nula sería como no utilizar una herramienta adecuada para realizar una tarea muy específica.

Interfaces de túnel: Puede utilizarse para conducir un determinado tipo de paquetes a través de una conexión que normalmente no soporta dicho tipo de paquetes. Por ejemplo, se puede configurar una interfaz de túnel en cada uno de los dos ruteadores que se encargan de encaminar paquetes Apple Talk desde sus respectivas Redes de Área Local (LAN). Ambos ruteadores estarían conectados por medio de una conexión en serie, como se muestra en la figura 2.5.1. La interfaz del túnel se configuraría para encaminar IP. Y aunque Apple Talk no puede encaminarse normalmente a través de una interfaz IP, los paquetes Apple Talk se encapsularían (es decir, se meterían todos dentro de un sobre genérico) y después de conducirían a través del túnel como si fueran paquetes IP.

Si se configura a nivel básico con el fin de que lo reconozca la red, se puede conectar después el ruteador a sus distintas conexiones físicas y completar posteriormente la configuración del ruteador utilizando una terminal virtual a través de la red.

Cuando se adquieren los cables para conectar las interfaces del ruteador a las distintas conexiones en serie, se debe asegurar la compra de configuraciones de pines apropiadas. Todos los cables parecen iguales a simple vista, por lo que se debe especificar al distribuidor las características exactas del cable que se desea instalar y si la instalación es de exigencias limite en cuanto a la limpieza de la señal, se debe tomar en cuenta también el material con que se elaboran.

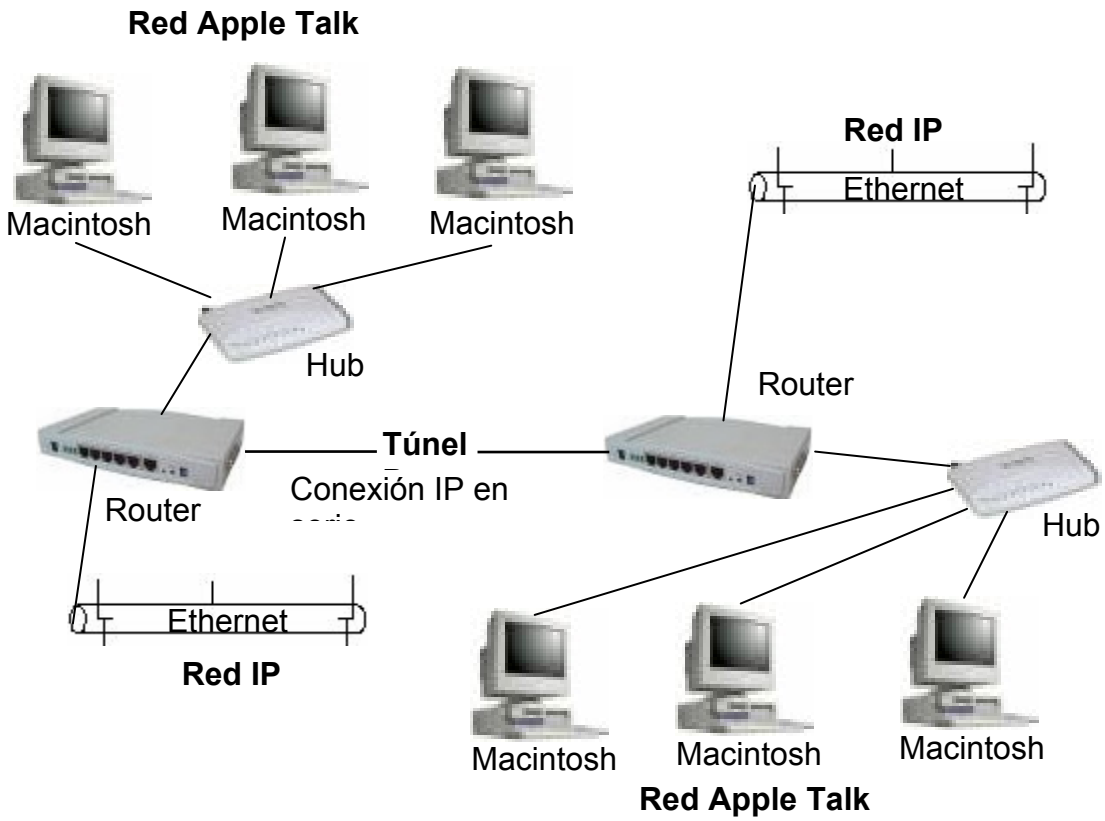


Figura 2.5.1 Los paquetes AppleTalk se encaminan a través de un túnel IP virtual.

Si se conecta a los distintos dispositivos de LAN y WAN antes de configurarlo, las conexiones podrán configurarse íntegramente y probarse inmediatamente. Sin embargo, si el ruteador está ubicado en un área de difícil acceso (como en una ranura de la carcasa del hub), es posible que resulte algo complicado conectar directamente el PC al ruteador con lo que se dificulta la configuración.

2.6 Carga del software.

Cuando se pone en funcionamiento el ruteador, la memoria ROM ejecuta una autoprueba de encendido post (Power On Self Test) que comprueba su hardware es decir el procesador, las interfaces y la memoria. Esta autoprueba es muy parecida a la que se ejecuta al encender una PC (en el que también se comprueba la RAM, el CPU y demás elementos de hardware).

El paso siguiente en la secuencia de arranque es la ejecución de un programa de carga que se encuentra almacenado en la ROM. Este programa de carga busca el IOS de Lantronix. El IOS puede cargarse directamente desde la ROM (los ruteadores incluyen una copia parcial o íntregra del LRS IOS en la ROM), desde la Flash RAM del ruteador o desde un servidor TFTP incluido en la red.

Una vez cargado el IOS, este pasa a buscar el archivo de configuración. Este normalmente se encuentra almacenado en la memoria NVRAM (se utiliza un comando de copiado para transportar la configuración de ejecución en la NVRAM). Al igual que el IOS, el archivo de configuración puede cargarse desde un servidor TFTP y una vez más la ubicación del archivo de configuración dependerá de la información almacenada en la NVRAM del ruteador.

Una vez cargado el archivo de configuración, la información incluida en este activa las interfaces y proporciona los parámetros relacionados con los protocolos encaminados y de encaminamiento vigentes en el equipo.

Si se carga el IOS desde otra fuente que no sea la memoria Flash RAM, se tiene que incluir una anotación en el registro de configuración de la ROM. Igualmente para cargar el archivo de configuración desde otra fuente distinta a la memoria NVRAM, debe incluirse en la NVRAM información acerca de la ubicación del archivo.

Si no se encuentra un archivo de configuración en la NVRAM o en cualquier otro lugar previamente especificado (como un servidor TFTP), se iniciara el modo arranque (setup) y aparecerá el cuadro de dialogo para configurar el sistema (System Configuration) en la pantalla de la consola del ruteador.

Lantronix tiene su propia herramienta de confoguracion llamada, EZWebCon que es una interfaz gráfica de usuario que proporciona la manera más fácil de manejar los ruteadores de Lantronix. Todos los ruteadores LRS tienen memoria Flash por lo que pueden reprogramarse "in situ" con una simple carga de la nueva versión. Numerosos y nuevos productos de gestión de redes no tienen este rasgo, lo que dificulta o imposibilita sus posibilidades de actualización. Lantronix fue uno de los pioneros en proporcionar actualizaciones gratuitas de software a través de Internet y la Web de Lantronix (www.lantronix.com) guía al usuario a través del proceso con facilidad.

2.6.1 Sistema Operativo de Interconexión de redes.

Trabajar con el software de emulación de terminal.

Cada paquete de emulación de terminal opera de distinta forma, pero todos proporcionan un sistema de menús y cuadros de diálogo para acceder a los distintos parámetros del software. Los parámetros de comunicación se configuran utilizando cuadros desplegables donde vienen incluidas las distintas opciones.

El sistema operativo de interconexión de redes IOS (Internetworking Operating System) es el software que permite al hardware del ruteador encaminar paquetes por una conexión entre redes. El IOS como cualquier otro sistema operativo, proporciona el conjunto de comandos y funciones de software con los que puede controlarse y configurarse el ruteador, además de ofrecer la funcionalidad que requieren los distintos protocolos tanto de encaminado como de encaminamiento, para hacer realidad la interconexión de redes.

Para esto se deben activar las distintas interfaces y protocolos que lo integran. Deben utilizarse una serie de comandos para que interfaces como Ethernet o en serie puedan ejecutarse. También debe suministrarse información de configuración para los protocolos que se encaminan, como IP o IPX/SPX. Y tienen que configurarse igualmente los protocolos de encaminamiento, como RIP e IGRP. Una vez configurado, deben gestionarse los archivos de configuración. El listado que se ofrece a continuación presenta algunas de las tareas que tiene que ejecutar con el conjunto de comandos del IOS:

Configurar las interfaces de Red de Área Local (LAN): Esto se debe hacer después de realizar las conexiones físicas, ensamblar el hardware del ruteador y conectar los distintos cables a las redes LAN o WAN. Las interfaces del ruteador deben configurarse para su uso en estas redes. Por ejemplo, en una red que encamine IP, cada interfaz Ethernet que se utilice debe configurarse con la dirección IP y la mascara de subred que proceda.

Configurar las conexiones en serie y los protocolos WAN. En aquellos casos en que el ruteador este conectado a una red WAN por medio de una línea contratada o cualquier otra tecnología WAN, el protocolo WAN que se utilice en las interfaces en serie del ruteador debe configurarse con mucha atención.

Gestionar los archivos de configuración del ruteador. Una vez configurado, conviene guardar alguna copia del mismo. Su configuración de ejecución del se

almacena en la memoria NVRAM donde viene incluida como la configuración de arranque. También puede resultar oportuno conservar una copia de un archivo de configuración en un CD como se puede hacer actualmente o cargarlo desde un servidor TFTP.

Controlarlo y mantenerlo. También tendrá que utilizarse el conjunto de comandos del IOS para controlar y resolver los posibles problemas que puedan surgir con el equipo. Asimismo, pasado un tiempo, resultará necesario actualizar el IOS dentro de la memoria Flash RAM. El conjunto de comandos proporciona todas las herramientas que se requieren para controlarlo y actualizar su IOS y el conjunto de características que éste incluye.

EzwebCon es el programa propio de Lantronix y proporciona una interfaz grafica de usuario para configurar y verificar el LRS1. Esta desarrollado en lenguaje JAVA y puede operar normalmente en cualquier plataforma del tipo terminal virtual que soporte Java 1.2 o superior.

El EZWebCon se obtiene desde la dirección electrónica de Lantronix donde se debe seleccionar la liga de descargas, aquí seleccionaremos el producto del cual queremos información para después elegir ya sea el programa de instalación o una actualización del IOS.

Si ya se obtuvo el software hay que instalarlo en la consola del ruteador (PC al que este conectado), para esto solo basta con ejecutar el archivo ezwebcon.exe como hacemos con la mayoría de instaladores de software. No se necesita instalar ningún otro programa. Una terminal virtual Java esta incluida en la instalación realizada.

Cuando se configuran interfaces en serie con un determinado protocolo WAN, está utilizando de hecho el comando de encapsulación seguido del nombre del protocolo. La encapsulación es el proceso de empaquetar datos en un determinado encabezado de protocolo. Por ejemplo, los datos Ethernet se encapsulan en un encabezado Ethernet antes de ser transmitidos por la red. En aquellos casos en que se transmiten tramas Ethernet por una conexión WAN, toda la trama se ubica (o encapsula) en un tipo de trama determinado por el protocolo WAN utilizado, como DIC o PPP.

Los comandos de configuración van de lo general a lo específico. Primero se hace saber al IOS que se desea configurar algo; después se le indica ese algo que se

desea configurar y por último se introducen los parámetros de configuración específicos.
Los comandos de configuración del ruteador pueden clasificarse en tres categorías:

1.- Comandos globales. Como su nombre lo indica, son comandos de una sola linea que afectan a toda la configuración del ruteador. Ejemplos de comandos globales son hostname y enable secret (que establece la contraseña secreta para el modo privilegiado). Este tipo de comandos se denominan globales porque se aplican a un parámetro que afecta a la funcionalidad general del ruteador, como su nombre o la contraseña para acceder al modo privilegiado.
2.- Comandos de puerto. Son un conjunto de comandos que permiten especificar una determinada interfaz o controlador para su configuración; a estos comandos deben seguirle una serie de subcomandos que proporcionan la información de configuración adicional relativa a una determinada interfaz o controlador. Por ejemplo, un comando de puerto para especificar que debe configurarse la interfaz en serie 0 sería interfase serial 0.
3.- Subcomandos. Estos proporcionan la información específica de configuración para la interfaz o controlador que se ha especificado en un determinado comando de puerto. Por ejemplo, para proporcionar una dirección IP para una determinada interfaz en serie, tiene que escribir IP Address seguido de una dirección IP específica y una mascara de subred.

TEMA 3. ACCESO REMOTO A LA SUBESTACIÓN.

3.1 Introducción.

Existen requerimientos importantes para los sistemas de telecomunicación utilizados por una subestación, que en general no son satisfechos por las compañías que ofrecen el servicio público. Dichos requerimientos son:

a) Confiabilidad. Significa la minimización de pérdidas de comunicación y de errores en transmisión de datos, aun en el caso de condiciones ruidosas adversas.
b) Disponibilidad. El sistema debe sufrir solamente una degradación mínima en el caso de falla de circuitos debido a deficiencias del Hardware y del Software.
c) Oportunidad. Es esencial una respuesta en tiempo real especialmente con las señales de teleprotección. Las transmisiones de datos se originan por las instalaciones en el sistema eléctrico y esto da origen a la necesidad de transmisiones de corta duración (en el rango de los milisegundos).
d) Transparencia. El sistema de telecomunicaciones debe ser compatible con todos los elementos que estén asociados al mismo, tanto en lo relativo a la electrónica como en su programación y debe ser capaz de interconectarse a los sistemas existentes, independientemente de los protocolos utilizados.
e) Flexibilidad. A medida que el sistema eléctrico evoluciona, se hace necesario que la red de telecomunicaciones en sí, sea capaz de ser modificada para cubrir estos nuevos requerimientos. La normalización y la compatibilidad apegadas a las tendencias tecnológicas son formas que facilitan siempre los cambios.
Además de la capacidad de modificación, debe contemplarse la capacidad de reserva que permita la incorporación de nuevos servicios y/o nuevas instalaciones.
f) Mantenimiento. La planeación del sistema debe considerar métodos y equipos que hagan mínimas las demandas de mantenimiento. Por ejemplo, en algunos casos las condiciones atmosféricas pueden impedir el acceso a repetidores no atendidos en ciertas estaciones del año.

g) Seguridad. La seguridad en la operación del sistema eléctrico está basada fundamentalmente en los sistemas de comunicación que permitan detectar, diagnosticar y decidir sobre las acciones que corrijan o mejoren el comportamiento

del sistema eléctrico de ahí que los sistemas de comunicación deben contar con la suficiente redundancia que garantice la operación segura de dicho sistema.

3.1.1 Teleprotección

Se refiere a requerimientos funcionales del usuario (Basados en la recomendación del grupo 57 del IEC y la recomendación IEC 834-I). Existen dos tipos básicos de información que es necesario transmitir entre las terminales en los extremos de la línea de potencia protegida:

a) Información tipo comando
Los esquemas de protección de distancia y de comparación direccional ayudados por equipos de comunicación se basan en la transmisión de información tipo comando entre los extremos de la línea protegida. La señal transmitida puede ser codificada y compleja, pero siempre se usa como una señal tipo comando y por lo tanto contiene información de comando más que información cuantitativa.
A continuación se definen algunos términos importantes para la teleprotección tipo comando:

Seguridad: es una función de la probabilidad de ocurrencia de un comando no deseado.
Dependabilidad: es una función de la probabilidad de pérdida de un comando. Los diversos sistemas que utilizan información tipo comando tienen mucho en común. El comando de disparo o bloqueo se debe transmitir y recibir correctamente dentro de un tiempo determinado con una seguridad dada en un tiempo dado y con una dependabilidad dada.
El usuario de un esquema de teleprotecciones requiere una alta dependabilidad del esquema, con frecuencia se da una cifra de 10^2 a 10^4 para la probabilidad de pérdida de un comando. Esto tendrá significado solamente cuando estas cifras se condicionen a una relación de señal a ruido.

Tiempos de transmisión: tiempo que transcurre desde que se cierra el contacto del relevador de entrada en el emisor hasta que se activa el relevador o dispositivo de salida del receptor del extremo alejado. Incluye el tiempo propio del equipo emisor/receptor los filtros, el tiempo propio de canal y el tiempo adicional de decisión debido al ruido.

Los diversos esquemas de protección tienen diferentes requerimientos para el tiempo de transmisión. Este tiempo se debe cumplir en el equipo utilizado en relación a los otros parámetros dados, tales como: relación señal a ruido, probabilidad de pérdida de un comando, probabilidad de ocurrencia de un comando no deseado y el ancho de banda del canal.
Al hablar de tiempos de transmisión, se deben mencionar tres términos:

a) Tiempo total de desconexión de un sistema de protección
Éste es el intervalo de tiempo desde el momento en que ocurre una falla en la línea de transmisión hasta que un interruptor opera con la ayuda de un sistema de teleprotección.
b) Tiempo de transmisión nominal para un canal de teleprotección (t).
Éste es el intervalo de tiempo desde que se inicia la señal de entrada al transmisor de la teleprotección hasta que el receptor de la teleprotección da su salida, medida en condiciones libres de ruido.
c) Tiempo de transmisión real para un canal de teleprotección (t_0)
Éste es el intervalo de tiempo máximo desde que se inicia la entrada de un transmisor de teleprotección hasta que el receptor de teleprotección da una salida, medido bajo condiciones de ruido para una relación de señal a ruido previamente definida. Para un canal libre de ruido: $t = t_0$
Los valores típicos de t_0 para algunos esquemas son de entre 4 y 20 ms para un esquema permisivo, y entre 20 y 40 ms para un esquema directo.

Se da la disponibilidad como un porcentaje del tiempo que el equipo está disponible para transmitir o recibir una señal de mando o de guarda.
Los diversos medios de transmisión utilizados para teleprotección (OPLAT, radio, fibra óptica cable, etc.) proporcionan diferentes características de transmisión. Las propiedades del circuito de telecomunicación requerido varían entre los diferentes esquemas de protección.
b) información cuantitativa
La información cuantitativa se usa para la protección diferencial de un enlace entre dos o más terminales. Por ejemplo la amplitud o fase, de las terminales tiene que ser comparada en cada una de ellas y la decisión que identifica y dispara la sección de línea fallada o bloquea la sección de línea sana respectivamente, depende solamente de la diferencia entre la información cuantitativa de las terminales.

El incremento en el tamaño y complejidad del sistema eléctrico ha cambiado gradualmente los requerimientos para los sistemas de control y monitoreo, además, el efecto de los costos de mano de obra más altos tiende a reducir el grado de control manual. Este desarrollo se inició con el control remoto de una sola estación de potencia o transformación y hoy en día, es una práctica común controlar hasta cincuenta (50 ó aún más estaciones desde un centro de control). La necesidad del monitoreo ha obligado al desarrollo de sistemas analógicos sencillos hasta sistemas basados en computadoras para la adquisición de datos, análisis y control.

La estructura de los sistemas de telecontrol tiene una influencia en el diseño de la red de telecomunicaciones. Es muy importante minimizar esta influencia diseñando la red de telecomunicaciones hasta donde sea posible de una manera flexible, de tal forma que, pueda acomodar los cambios tanto en el tamaño como en la estructura de los sistemas de telecontrol.

Comunicaciones de emergencia para operación.

Dependiendo de los tipos de canales utilizados, es conveniente proporcionar instalaciones de respaldo que permitan el uso continuo de las telecomunicaciones de operación más esenciales en caso de falla del sistema normal. Cuando existe una segunda opción, tal como lo es una compañía de telecomunicaciones externa, que proporciona el grueso de los canales normales, es posible reducir a un mínimo la capacidad de la infraestructura propia en comunicaciones para emergencias. En forma similar, se puede echar mano de sistemas privados de microondas, es posible que la falta de reservas esenciales se pueda crear la necesidad de tener algunos sistemas alternos al presentarse condiciones de emergencia. Otra categoría de emergencias surge en el caso de desastres naturales, tales como inundaciones, tornados o temblores. En éstos casos los sistemas de telecomunicaciones existentes pueden quedar fuera de servicio y la restauración del suministro de energía puede depender de las previsiones de una adecuada instalación de telecomunicaciones para casos de emergencia.

Durante condiciones de falla que afecten las redes de telecomunicaciones, la mayoría de los sistemas de control podrían volver a métodos de operación menos eficientes pero aun seguros, con algún costo extra hasta que la emergencia haya pasado.

Se deben usar diversos tipos de canal y utilizar, en lo posible, diferentes rutas de telecomunicación, de tal manera que se reduzcan las fallas del modo común.

Tales medios se complementan con un plan de emergencia que hace uso masivo de unidades de radio móviles desviando las unidades normalmente involucradas en trabajos comerciales no esenciales, para reforzar las unidades de operación de sistema e ingeniería.
Para los circuitos punto a punto de distancias más grandes, los sistemas de microondas propios, enlazados con los sistemas OPLAT y circuitos de radio de alta frecuencia, también son utilizados durante condiciones de emergencia. El utilizar redes de radio militares, y aun de radio aficionados, no debe pasarse por alto en casos de desastre donde ambas pueden ser de utilidad.

Lectura remota de medidores.

Existen básicamente dos subdivisiones principales, la medición remota de medidores integradores en las estaciones de transformación o en las estaciones de potencia, y la lectura remota de los medidores de los consumidores. La primera presenta un problema de transmisión directa de información, y los mensajes necesarios solamente forman una parte del total del flujo de información desde una subestación La última aplicación que se está volviendo muy importante, requiere la comunicación de las lecturas de los medidores de cada consumidor a intervalos predeterminados con una tasa de error baja. Los principales requerimientos son: el uso de equipo de bajo costo, de alta confiabilidad a prueba de vandalismo, con bajo consumo de potencia que cubran las necesidades de los consumidores.
En el sistema eléctrico de alta tensión, la lectura remota de medidores en las estaciones de transformación y de generación presenta problemas comunes a todos los sistemas de telecontrol; generalmente puede ser satisfactoriamente proporcionada con los mismos métodos que se utilizan en el esquema de telecontrol. En el sistema eléctrico de alta tensión, la lectura remota de los medidores de los consumidores se puede hacer en varias formas, utilizando señales de transporte superimpuestas en las líneas telefónicas desde el medidor de cada consumidor, interrogando por radio y utilizando frecuencias de transporte superimpuestas en la red de suministro. El último método mencionado es el que se utiliza más frecuentemente a nivel mundial.
Un sistema telefónico corporativo propio de la empresa eléctrica, se utiliza cuando las compañías que suministran el servicio de telecomunicaciones no tienen la disponibilidad para proporcionar tal servicio, o cuando es más económico para la empresa eléctrica operar su propio sistema telefónico. Sin embargo, la posibilidad

para hacerlo depende de las políticas nacionales en materia de telecomunicaciones.
Las aplicaciones corporativas contemplan todas las necesidades que a nivel nacional, divisional, regional ó residencial de obra, cubren actividades directivas, de construcción, comerciales, financieras, de abastecimiento, de personal y otras.
Para estas aplicaciones se consideran sistemas de telecomunicación cuyo diseño cubra las necesidades generales, jerarquizando los servicios.
La infraestructura de los sistemas de telecomunicación corporativos considera la transmisión de señales de voz, teleinformática, fax y otras.

Funciones de control y adquisición de datos.
Para empezar se definirá el concepto de dispositivo electrónico inteligente, ya que este es el que toma los datos de los dispositivos con los que cuenta la subestación.
La gran cantidad de dispositivos convencionales así como los extensos cableados de cobre en paralelo han quedado en el pasado sustituyéndolos actualmente por dispositivos electrónicos inteligentes y comunicaciones seriales.
Muchos fabricantes ofrecen una tecnología universal y uniforme para todo un campo de aplicación funcional en equipos de protección, control y medición, así como en la fabricación y conexión de los mismos. Esto resulta en la normalización de diseño, interfases y concepto de operación para la automatización de subestaciones.
Todos los dispositivos son altamente compactos e inmunes a interferencias, y por lo tanto son adecuados para instalación directa en celdas de transmisión y distribución. Además todos los dispositivos y sistemas son completamente automonitoreados, lo cual significa que los costos previos de mantenimiento pueden ser considerablemente reducidos.
Cada dia más fabricantes ofrecen una gama completa de relevadores multifuncionales para todas las aplicaciones en el campo de las redes y protección de máquinas con lo cual se facilita tanto la obtención del producto como una mayor variedad de precios.
En el caso de reelevadores microprocesados, un diseño uniforme y construcción libre de interferencia electromagnética en cajas metálicas con terminales de conexión convencionales de acuerdo a los requerimientos del usuario asegura un sistema de diseño simple y un uso similar al obtenido con los relevadores convencionales.
Las técnicas de medición numéricas aseguran una operación precisa con menor mantenimiento gracias a su capacidad de automonitoreo.

La integración de protección adicional y otras funciones, tales como mediciones de operaciones en tiempo real, registro de eventos y fallas, unidades todo en uno, nos permite economizar en espacio y en costos de diseño e instalación. El ajuste y programación de los dispositivos puede llevarse a cabo a través de un display de operador integral de texto en lenguaje claro y guía de menú, o usando programas de PC cuyas interfaces de usuario son cada vez más intuitivas.
Las interfaces seriales abiertas, IEC 870-5-103, permiten una libre comunicación con sistemas de control de más alto nivel, con lo que se pueden estructurar instalaciones con productos de los más diversos fabricantes.
De esta manera, las mediciones en línea y los datos de falla registrados en los relevadores de protección pueden ser usados para el control local o remoto, o pueden ser transmitidos vía módem al lugar de trabajo del ingeniero de servicio.
Los mejores fabricantes suministran dispositivos individuales así como sistemas de protección completos en celdas terminadas de fábrica. Para aplicaciones complejas, por ejemplo en el campo de transmisión de tensiones muy grandes, están disponibles las facilidades de pruebas de diseño con un modelo amplio de red usando las técnicas de simulación y evaluación más modernas.
La instrumentación o dispositivos de medición, esta constituida por dispositivos electrónicos inteligentes (DEI´s) que constan principalmente de un sensor de medición y un transductor. Estos elementos también poseen integrado un elemento de comunicación que les permite integrarse en una red de medidores a un sistema de adquisición centralizado, pudiendo recibir comandos y enviar datos por solicitud. Una de las últimas innovaciones en este campo es el desarrollo de chips que permiten la comunicación de esta instrumentación vía Internet con el centro de control sin la necesidad de utilizar una red de área local (LAN) o una computadora con módem conectado a una línea telefónica. La gran capacidad de estos equipos de medición permiten la adquisición y envío de otras variables que pueden ayudar a mejorar la calidad del servicio prestado. El desarrollo tecnológico alcanzado por las compañías dedicadas al suministro de esta instrumentación ha crecido notablemente en los últimos tiempos, permitiendo un abaratamiento en la fabricación de los mismos y haciendo atractiva la implantación de esta forma de medición.
El desarrollo de la instrumentación inteligente permite tener disponibles en el mercado dispositivos, que son capaces de recolectar y enviar hasta siete variables relativas al consumo eléctrico y sobre la calidad del servicio. También las capacidades de la instrumentación inteligente pueden ser aprovechadas para ejecutar programas de mantenimiento. En la figura 3.1.1 se aprecia el aspecto de

un DEI, el SEL-351 que es un relevador direccional de sobrecorriente con funciones de recierre y localización de fallas.

Figura 3.1.1 Dispositivo electrónico inteligente.

La comunicación o integración de la instrumentación inteligente con el centro de control o facturación se hace de diversos modos y utilizando diversos medios. El desarrollo de las redes de comunicación ha hecho posible que se implementen diversas formas de comunicación aprovechando las diversas plataformas públicas existentes, es decir, la comunicación entre los instrumentos de medición y su centro de control, puede hacerse a través de medios diversos tales como cable coaxial, fibra óptica, o inalámbrica y utilizando los canales utilizados por pagers, CDPD, telefonía tradicional, telefonía celular, PCS e Internet.

Para las funciones de control y adquisición de datos, el DEI debe tener entradas y salidas digitales que se asocian al equipo que supervisan. Las funciones de control son salidas digitales y las funciones de adquisición son entradas digitales.

Para las funciones de la subestación que no tienen un DEI asociado y para DEI's que no cubran totalmente las funciones de control y adquisición suficientemente detallados, se debe adicionar un UCAD que cubra las funciones mencionadas, además de un 20 % adicional de capacidad en cuanto a manejo de puntos, para expansiones futuras. Este dispositivo debe tener la capacidad de ejecutar funciones lógicas tipo PLC, de registrador de eventos y mandos remotos no presentes en los DEI's.

Se requiere que las entradas digitales se puedan programar para proporcionar la siguiente información:

a) Estado de la entrada digital (abierto/cerrado) "status".
b) Detección de cambio momentáneo entre exploraciones del CPS.
c) Registro de eventos.

Las salidas digitales para comandos del tipo pulsado, deben ser ajustables por programación de 0,1 a 5 segundos.
Para el caso de comandos subir/bajar se requiere duración de pulsos programables de 0,1 a 10 s con incrementándose 0,1 segundos.

Arquitectura de Comunicaciones.
Las comunicaciones que utiliza el sistema en su arquitectura final están estructuradas en 5 niveles. Sin embargo debido a los alcances de este trabajo, únicamente se consideran 3: nivel inferior, red subestación y red zona.

a) nivel inferior.- Es la comunicación de los DEI´s con sus periféricos tales como sensores u otros DEI's, como un proceso propio de la operación de estos dispositivos. Los protocolos de comunicación empleados para estos propósitos, pueden ser del tipo propietario.
b) red de subestación.- Es la red que comunica los DEI's hacia el CPS a través de los puertos RS-485 o fibra óptica, utilizando alguno de los protocolos siguientes: DNP 3.0, Ethernet o alguno de los basados en UCA o IEC 60870-5,
c) red de zona.- En este nivel se operan dos tipos de comunicaciones; la de la red del centro de operación distribución zonal y la red del SCADA.

Red del centro de operación distribución zonal.
Es la red que comunica a los CPS's de las subestaciones de una zona, con un servidor ubicado en el centro de operación distribución zonal, en donde se encuentran concentradas las bases de datos y resultados de tareas específicas de cada uno de los CPS's.
El CPS debe proporcionar una salida a una red de área amplia (WAN) para el intercambio de información que reside en la base de datos de la subestación, pudiendo ser TCP/IP, X-25, entre otras.

Protocolo DNP 3.0
El protocolo DNP (Distributed Network Protocol), originalmente desarrollado por Westronic Inc. en 1990, actualmente GE Energy Services, documentado y puesto al público en 1993, es un protocolo basado en los estándares de comunicación IEC 870-5 diseñado para la industria en aplicaciones de telecontrol, especialmente enfocado hacia el sector eléctrico por la precisión y calidad de la información que transporta.
Es un protocolo de comunicaciones abierto y no propietario diseñado basándose en un modelo que incluye tres de las capas del modelo OSI (Open Systems

Interconnections), denominado EPA (Enhanced Performance Architecture): Capa de Aplicación, Capa de Enlace de Datos y Capa Física.
Es muy eficiente por ser un protocolo de capas, mientras que asegura alta integridad de datos. Es adecuado para aplicaciones en el ambiente SCADA completo: RTU-IED, Maestra–Remota, punto-punto y aplicaciones de red. Sus características son:

- Pueden existir más de 65000 dispositivos con direcciones diferentes en un mismo enlace.
- Confirmaciones al nivel de la Capa de Enlace y/o Capa de Aplicación garantizando así alta integridad en la información.
- Solicitudes y respuestas con múltiples tipos de datos en un solo mensaje, y permite objetos definidos por el usuario incluyendo la transferencia de archivos.
- Segmentación de los mensajes en múltiples tramas para garantizar una excelente detección de errores y recuperación de tramas con errores.
- Puede incluir solo datos que hallan cambiado en el mensaje de respuesta (Reporte por excepción).
- Asigna prioridades a un grupo de datos (clases), y los solicita periódicamente basándose en las mismas.
- Los dispositivos esclavos pueden enviar respuestas sin solicitud (Respuestas no Solicitadas).
- Soporta sincronización temporal con un formato de tiempo estándar.

3.2 Componentes para establecer el acceso remoto.

En primer lugar se definirán las tareas que los componentes principales realizan. Las funciones del control supervisorio deben tener las siguientes prioridades:

- Controles.
- Diagnóstico periódico del sistema.
- Cambios de estados y alarmas.
- Telemediciones.
- Programas de aplicación específica.
- Respaldo de la información en forma periódica a disco.
- Programas de presentación de información.
- Programas de impresión.

Funciones de la unidad de procesamiento central que son:

- Control de periféricos.
- Control de la interfase hombre/máquina (consola de control, diagramas unifilares e impresoras).
- Administración de los datos de las UTR (recepción de datos y envío de comandos).
- Administración de archivos (alarmas. telemediciones. etc.).
- Cálculos de ingeniería.
- Ejecución de programas de aplicación.

La unidad debe incluir por lo menos el siguiente equipamiento:

- Reloj de tiempo real
- Monitoreo de fuente de alimentación
- Reinicio automático/falla de alimentación
- Acceso directo a memoria
- Protección de memoria
- Expansión de memoria suficiente para alcanzar los requisitos establecidos
- Carga automática de programación con cargador de programa de iniciación del sistema (boots trap)

- Panel de control de operador, para los controles de operación, programación y pruebas, terminal conversacional (teletipo)
- Vigilancia de operación de memoria UPC.

La UPC debe incluir un contador sencillo, externo y confiable que pueda ser controlado en cualquier momento por una instrucción de programa. Este mecanismo debe tener la finalidad de monitorear la operación de la UPC en línea.
El sistema necesita contar con dispositivos de almacenamiento de información, los cuales deben tener capacidad suficiente para todos los procesos a desarrollar, los respaldos de información deben ser programables y los tiempos de acceso deben ser menores de 21 milisegundos. Dichos dispositivos ópticos y/o magnéticos deben considerar respaldos de largo, mediano y corto plazo y utilizar la tecnología de vanguardia; por ejemplo: cartuchos de cinta magnética, CD-ROM y mas recientemente DVD ROM. Las unidades deben estar diseñadas para operación continua (24 horas por día), y ser de tipo compatible con sistemas comerciales.

Controlador de comunicaciones.
Debe controlar el intercambio de información entre la estación central y la UTR, el centro de control de nivel superior y todos los procesos internos. La unidad debe consistir de:

- controlador de enlaces de alta velocidad (DB-25, X-25 o superior)
- modems
- conmutadores de líneas de comunicaciones
- dispositivos manejadores de protocolos de comunicación (varios)
- manejo de datos digitales y analógicos hacia los equipos de comunicación con manejo individual (a nivel de puerto) de la velocidad, la cual debe ser seleccionable por programación

El equipo debe ser provisto en gabinetes cerrados, en el caso de que no se localice con el resto del equipamiento del sistema supervisorio.
En cuanto a la operación de los modems, su operación debe apegarse a los estándares CCIIT y/o BELL y debe considerar lo siguiente:

a) Sensibilidad, debe operar en el intevalo de -30 a -45 dB
b) El nivel de transmisión debe operar de -35 a + 2 dBm
c) Facilidades para efectuar lazos de prueba analógico y digital

d) Facilidad para poner tonos continuos de marca y espacio
e) Relación señal a ruido mayor a 25 dBm

Enlace con el centro de control de nivel superior.
Se debe tener la posibilidad de establecer comunicación bilateral a través de un puerto de comunicación dedicado con una o más Estaciones Maestras de nivel jerárquico superior, comportándose en este caso como terminal remota. El intercambio de información debe ser parte o la totalidad de la información adquirida de sus UTR y podrá utilizar el mismo, o diferentes protocolos de comunicación, mediante comunicación en red o con la utilización de enlaces de comunicación y protocolos, como el X.25.

Unidad de programación.
Esta unidad debe ser utilizada para el desarrollo de programación y evaluación de la misma. Debe operar tanto dentro como fuera de línea, utilizar lenguajes comerciales a través de terminal inteligente con protocolos normalizados.

Características de la Programación.
Las siguientes descripciones indican las características generales que se consideran necesarias para la funcionalidad del sistema.
La programación en consideración debe incluir los siguientes grupos:

a) Programación básica (sistema operativo).
b) Programación de aplicación (normalizada y específica).
c) Programación de mantenimiento y exploración.

El sistema operativo debe considerarse del tipo de módulos unidos entre sí, para formar un paquete apropiado a la configuración del sistema y a los requisitos de operación.
Este paquete de tipo modular debe permitir a los programas de aplicación ser añadidos, quitados o revisados sin afectar otras partes de la programación.
El sistema operativo debe estar diseñado para proveer los niveles requeridos de comportamiento para la configuración máxima total de las UTR’s del sistema y operar en la filosofía de Sistema Abierto.

Subsistema de programación.
Debe permitir al programador desarrollar las siguientes operaciones en línea (a través de la terminal conversacional para programación asignada a la UPC y la consola de mantenimiento):

a) Cambio de prioridades.
b) Asignación al equipo.
c) Monitoreo de la frecuencia de ejecución de tareas.
d) Definición del sistema (dentro de los límites preescritos para la generación del sistema) es decir, adición o borrado de unidades, adición y borrado de terminales remotas, adición de puntos de reserva, modificación de alarmas o factores de escala, generación o alteración de pantallas ("displays") con el generador de imágenes, generación o cambios en general del banco de datos.

Adquisición de datos.
Programa independiente para barrer cada tipo de datos de entrada y a ser ejecutado cíclicamente, de acuerdo a un tiempo de actualización específico. Las prioridades deben ser dadas siempre al ciclo más rápido. Con el fin de tener un ciclo de obtención de datos más eficiente, se consideran factores de la técnica de barrido, tales como reporte de datos por excepción de las UTR tanto para indicaciones, alarmas o mediciones seleccionadas; agrupación de datos en diferentes ciclos (lentos y rápidos).

Procesamiento de datos.
Todos los datos recibidos de las UTR deben ser validados y analizados antes de ser enviados al banco de datos. Cada una de estas tareas para las diferentes funciones, deben ser efectuadas en módulos de programación separados.

a) Manejo de errores de comunicación.
Los errores en transmisión deben ser registrados por cada UTR. Cuando la frecuencia de un error en una UTR específica alcance un número predeterminado, una alarma debe ser enviada al operador. En tales casos (y cuando las UTR no contesten), el dato o datos correspondientes en el sistema deben ser marcados o etiquetados (con bloqueo), como no actualizados.
b) Detección de cambios de estados.
Un nuevo estado debe ser comparado con el estado anterior, aún cuando en la correspondiente UTR el dato sea procesado, si es el caso de remotas inteligentes.

En el caso que exista disparidad en la comparación, se debe efectuar, adicionalmente, una revisión para ver si el cambio es por autorización (un comando), o un cambio no autorizado (disparo). En el último caso se debe iniciar una alarma al sistema.

c) Conversión de telemediciones y monitoreo de límites.

En el caso de puntos analógicos pueden existir 3 casos de datos transmitidos de las UTR, a la estación central: datos transmitidos a la estación central en ciclo rápido, datos transmitidos a la estación central en ciclo lento y datos transmitidos a la estación central por excepción.

En los tres casos debe considerarse el contar con límites para los analógicos, los cuales pueden ser tratados en el procesador central o en las UTR, y los que al ser violados deben generar una alarma al operador del sistema.

d) Actualización de archivo de datos.

Después de una validación y análisis de datos, éstos deben ser enviados a los archivos apropiados donde deben ser ordenados de acuerdo a su origen (UTR), y tipo (como indicaciones y telemediciones) Cada entrada debe poder ser acompañada de información complementaria como estado de la alarma, número de cambios, dato no actualizado o bloqueo.

e) Almacenamiento de datos, preparación para teletransmisión y recepción al/del centro de control de nivel superior.

f) Almacenamiento de datos y preparación para la pantalla y mímico reducido en el TRC.

Programación para la simulación de telemediciones.

El sistema debe incluir la programación y la capacidad de almacenaje para simular la adquisición de datos a partir de una unidad terminal remota, incluyendo el almacenamiento de los datos y generación de alarmas.

Programación de puntos calculados.

El sistema debe incluir la programación y la capacidad de almacenaje para la definición de un mínimo de 300 puntos calculados. Las entradas para estos cálculos podrán ser cualquiera de los puntos definidos en el sistema como estados, telemediciones o acumuladores.

Se debe incluir como mínimo: funciones aritméticas (suma, resta, multiplicación, división); funciones lógicas (AND, OR, NOT, OR exclusivo); logaritmos común y natural; X a la potencia Y; exponencial a la potencia A; funciones trigonométricas

(seno, coseno, arco seno, arco coseno); funciones misceláneas, (máximo, mínimo, valor absoluto, raíz cuadrada); sentencias condicionales (IF,GOTO).
Estos puntos pueden ser incluidos, de acuerdo a las necesidades, en reportes y desplegados del sistema, junto con los datos telemedidos.
Debe ser posible definir límites para los puntos analógicos calculados y condiciones de alarma, tanto para analógicos calculados como para los estados calculados.
La periodicidad de los cálculos puede ser definida como mínimo, de acuerdo a la frecuencia con que se obtengan sus entradas.
El sistema debe incluir la programación y la capacidad de almacenaje para la generación y mantenimiento de reportes, cuya impresión debe poder ser bajo demanda del operador y/o de acuerdo a una programación predefinida, por mes, día, hora o minuto. Los reportes deben contener información de puntos telemedidos, calculados y resultados de programas de aplicación.
El sistema debe tener una capacidad de cuando menos 100 reportes, con un mínimo de 50 páginas de longitud cada uno. La salida de estos reportes puede ser dirigida, de acuerdo a las necesidades, a cualquiera de las impresoras, disco o cinta magnética.
La generación y mantenimiento de los reportes debe ser por medio de una interfase interactiva, similar a la descrita para la generación de desplegados.

Programas especiales para fallas de alimentación.
En el caso de fallas de alimentación, el detector de interrupción debe inicializar la ejecución de un programa que debe conservar todos los datos recuperables después que el sistema llegue a detenerse. El programa también debe levantar el sistema (Warm Start).

Arranque e inicialización.
Después de una transferencia, regreso de alimentación y orden de arranque, deben ejecutarse automáticamente los siguientes puntos:

- revisión de equipo.
- selección del sistema principal.
- inicialización de todas las tareas.
- actualización del banco de datos.
- lectura de tiempo presente.
- pantalla de mensajes de información al operador por reinicio de operación del sistema.

Cualquier comando iniciado con anterioridad debe ser inhibido hasta que las operaciones anteriores hayan sido exitosamente completadas.
Generalmente se utiliza el siguiente equipo para configurar el acceso remoto:
Un modem V.92 para conectarlo al controlador principal o computadora gestora del sistema. Las opciones en cuanto a este tipo dispositivo son muy variadas y la elección viene dada en función de las prestaciones que tenga el aparato.
Un servidor de acceso remoto del cual existen diferentes marcas y precios, como el LRS1 ejecutando la versión de BIOS V1. ¾ o superior. Al igual que el modem este dispositivo se eligió en concordancia a la exigencia muy particular del sistema, ya que también en este caso, las opciones son varias.
Un concentrador (Hub) Ethernet con la característica de repetidor. Este aparato es seleccionado para dar cabida a tantos nodos como sean necesarios, ademas de proporcionar un excedente de puertos para futuras ampliaciones.
Un modem V.92 que se conecta al servidor de acceso remoto LRS1 mediante el puerto serie.
Un tranceptor Ethernet para cada tarjeta de control en los nodos remotos. La selección de este equipo se define más en cuanto a lo referido a costo, ya que el funcionamiento en general es muy similar en todos los fabricantes, pero entre más estricto sea el nivel de seguridad del sistema, se necesitaran tarjetas más estables en su funcionamiento y por lo mismo, más costosas.
Cable Ethernet 10BaseT para la interconexión entre el nodo remoto y el concentrador y entre este y el servidor de acceso remoto.
Esto además del equipamiento necesario para la adquisición de datos generados por los dispositivos que están conectados directamente a la red electrica y otros que están interconectados entre sí. De los cuales se indican algunos de ellos a continuacion, y que asimismo, aparecen en el diagrama a bloques de la subestación, como es el caso del módulo OPT-8B que se muestra en la figura 3.2.1.

Figura 3.2.1 Módulo de 8 puertos RS-232 modelo OPT-8B.

Tarjetas de adquisición de datos.

Las tarjetas de adquisición de datos se conectan directamente al bus del controlador principal de subestación, permiten adquirir y procesar datos en tiempo real.

Cada tarjeta presenta funcionalidades diferentes, lo que da la posibilidad de utilizar una tarjeta para aplicaciones muy variadas, como podría ser el cuenteo de eventos, la generación de señales de salida, o la adquisición de señales de entrada. Su apariencia es como la mostrada en la figura 3.2.2.

Figura 3.2.2. Tarjeta de adquisición de datos.

En este caso se trata de la tarjeta PCL-844+PLUS; es una tarjeta de interface para aplicaciones de laboratorio e industriales, se instala en una ranura PCI de la computadora para comunicarse con terminales, modems u otros instrumentos.

Su funcionamiento esta basado en su procesador RISC, que libera de trabajo al procesador principal de la computadora donde este instalada, ademas de ser capaz de transmitir información a 921.6 Kbps.

Normalmente una tarjeta de adquisición de datos solamente aporta los bloques de encaminamiento de la señal, así como la medida de esta (con posibilidad de amplificación), las funciones de cálculo, memoria y visualización las tiene que realizar la computadora al cual está conectada la tarjeta.

Una ventaja importante en las tarjetas de adquisición de datos es que se evita la duplicidad de diferentes bloques en el instrumento y en la computadora, como pueden ser memoria o funciones de cálculo. También es importante la facilidad de instalación, de puesta en marcha y su flexibilidad de uso en muchas aplicaciones.

Características.

Una tarjeta de adquisición de datos se caracteriza por una serie de parámetros que permiten decidir su utilización. Los parámetros se fijan a partir de un conjunto de funciones y dispositivos internos de la placa entre los cuales destacan el número de canales de entrada y el de salidas analógicas y digitales, los convertidores analógico-digitales, los sistemas de multiplexación y los márgenes dinámicos de entrada y salida.

Las entradas analógicas.

El número de canales analógicos ha de distinguir entre los que permiten entrada diferencial de los de entrada unipolar. Las entradas unipolares están referenciadas a una tierra común y se utilizan en el caso de trabajar con señales de alto nivel (tensión superior a 1v) dónde no haya grandes problemas de interferencias. En caso de utilizar entradas diferenciales, cada entrada tiene su propia referencia de forma que el posible ruido en modo común que se pueda introducir queda rechazado.

La conversión analógico digital.

Este elemento fija muchas de las características de la tarjeta. Cuanto mayor sea el proceso de conversión, mayores serán las posibles frecuencias de muestreo.

Las señales de entrada han de ser muestreados según el criterio de Nyquist por lo que es importante que el convertidor analógico-digital pueda convertir la señal en palabras digitales en el menor tiempo posible.

Un proceso rápido adquiere más valores en un tiempo dado que uno de lento y esto permite el poder representar mejor las señales originales.

Otro parámetro muy importante en el conversor analógico-digital es la resolución, que se puede definir como el número de bits que utiliza el conversor para representar la señal analógica.

En la actualidad existen diferentes tipos de convertidores analógico-digitales. El más popular es el de aproximaciones sucesivas, ya que ofrece la máxima velocidad y resolución a un precio razonable

Márgenes dinámicos de entrada.

Para conseguir una mejor resolución en los sistemas de medida, se ajusta el rango de la entrada que se pretende adquirir al rango del instrumento. Los rangos de la señal de entrada se refieren a los niveles mínimos y máximos de tensión de entrada que el convertidor puede cuantificar. La mayoría de las tarjetas ofrecen la

posibilidad de seleccionar diferentes ganancias y así poder configurar diferentes niveles de rango de tensión de entrada.
El rango dinámico de la entrada, la resolución y la ganancia disponible determinan la variación más pequeña detectable de señal de entrada.

Los sistemas de multiplexación.
Con esta técnica se pueden medir diversas señales con un único convertidor analógico-digital. Consiste en el hecho que el convertidor analógico-digital obtiene una muestra de un canal e inmediatamente después conmuta al siguiente canal de entrada, por lo que un sistema de adquisición solo necesita un convertidor para muchos canales. Esto significa que la velocidad de muestreo de cada canal individual es inversamente proporcional al número de canales muestreados.
Si nuestra aplicación necesita trabajar con muchas señales de entrada, se ha de decidir que método de encaminamiento de la señal es el más correcto. El método más común es el denominado muestreo continuo, en el cual conmuta cada canal de entrada a las funciones internas en intervalos de tiempo constante.
Otro método es el de muestreo simultáneo, en el que todos los canales de entrada son muestreados al mismo tiempo (con una diferencia de nanosegundos) ya que cada canal tiene su propia circuiteria de muestreo. Este método es importante cuando las relaciones de tiempo de cada señal con las otras es importante.

Las salidas analógicas.
Estas salidas se utilizan para proporcionar señales de estímulo y de prueba al sistema de adquisición. Uno de los elementos más importantes de esta circuitería es el conversor digital-analógico que determina la calidad de la señal analógica de salida. Los parámetros que miden esta calidad son el tiempo de asentamiento de la señal, el slew rate y la resolución.
El tiempo de asentamiento y el slew rate determinan con que velocidad puede variar el nivel de la salida del conversor digital-analógico. El tiempo de asentamiento es el tiempo que necesita la salida para llegar al grado de precisión deseado. El slew rate es el valor máximo de variación de señal que el conversor puede generar a la salida.
Por otro lado, la resolución a la salida es similar al concepto que ya se ha introducido de resolución a la entrada.

Entradas y salidas digitales.
Se utilizan para controlar procesos, generar patrones de prueba y posibilitar la comunicación con el periférico. Los parámetros más relevantes de esta especificación son el número de líneas digitales, la velocidad con que los datos pueden entrar y salir y la capacidad de control en los canales.

Circuitos de cuenteo y temporización de entrada y salida.
Esta circuitería es útil para el conteo de eventos, medidas temporales de pulsos digitales y la generación de señales cuadradas y de pulsos. Además son necesarios para adquirir las señales en el momento preciso. La señal de disparo (trigger) se utiliza para iniciar y parar la adquisición en función de acontecimientos externos y para sincronizar un proceso de adquisición con otros posibles. Dicha señal se puede obtener de diferentes fuentes, ya sean internas generadas por las funciones del instrumento que se utiliza, o también pueden provenir de generadores externos.
Existen también los llamados simuladores de tarjetas de adquisición de datos que en un principio no eran del todo fiables, pero dado el avance en las técnicas de programación y en los cada vez más robustos sistemas operativos, aparecen ahora como una opción interesante.
Estos simuladores permiten el desarrollo y prueba de aplicaciones de adquisición de datos sin necesidad de tener instalado el hardware.
El propósito del simulador es imitar las señales físicas que se conectan a los terminales de una tarjeta de adquisición de datos. Así, se puede desarrollar y probar un programa que use una determinada tarjeta de adquisición de datos sin tener que recurrir a instalar la tarjeta y sin tener que montar ningún tipo de dispositivos en las entradas/salidas de la tarjeta. Una vez terminado el programa se puede probar sobre un computador que posea la tarjeta de adquisición de datos y conectar a dicha tarjeta los dispositivos que se desee controlar.

Unidad Inteligente Distribuida.
El visual BOH es una unidad inteligente distribuida de señalización y control, que se utiliza ampliamente en aplicaciones SCADA (Control Supervisorio y Adquisición de Datos), control de subestaciones eléctricas, restauradores, alimentadores, seccionalizadores, pozos, tanques, estaciones de rebombeo, plantas de agua de tratamiento y aplicaciones similares. Su diseño incluye los últimos avances tecnológicos proporcionando la confiabilidad, versatilidad y facilidad de mantenimiento necesaria en este tipo de aplicaciones. Incorpora su propio

protocolo de comunicaciones interno y soporta fácilmente emulaciones de los principales protocolos utilizados en este ramo, tiene la habilidad de ser programada para contestar dos protocolos a la vez. Por medio de un puerto dedicado al frente o posterior del dispositivo se establece un dialogo completo de configuración, monitoreo y diagnostico, utilizando para ello una terminal de servicio, por ejemplo un simulador de protocolos. La transferencia de la información adquirida por el visual BOH puede ser configurada para manejo de reporte por excepción, si el protocolo a utilizarse así lo requiere.

El visual BOH puede ser utilizado para conformar conjuntos concentrados de adquisición/control o como un elemento de un sistema distribuido de adquisición/control, instalado en tableros de protección convencional o gabinete intemperie tipo kiosco.

Las funciones básicas de la unidad inteligente distribuida visual BOH son las de adquirir información de las entradas de estado digitales y transmitir dicha información al controlador principal de subestación (CPS), asimismo a solicitud del CPS efectuar los mandos (control). A las funciones básicas de adquisición y control se agregan las de prueba y autodiagnóstico auxiliares en el análisis de fallas del sistema y además la verificación de la integridad de los mensajes enviados/recibidos al CPS.

Los paquetes de software proporcionados pueden ser estándares o especialmente diseñados para el sistema. Toda la programación es almacenada permanentemente en memoria no volátil (flash rom). Las funciones incluyen manejo de interrupciones por medio de lo cuales el microprocesador soporta funciones dinámicas de tiempo real.

Cada visual BOH se configura en base a software de personalidad residente en la memoria de solo lectura y cuenta con una gran flexibilidad para expandir o reconfigurar el sistema mediante módulos de software que permiten desarrollar las funciones deseadas:

Software Desarrollado

Remoto de adquisición/control
Registrador de eventos con resolución de 1 milisegundo
Cuadro de alarmas
Controlador lógico programable (PLC)
Funciones combinadas

Arquitectura

El visual BOH se encuentra configurado en base a una arquitectura de tipo modular cuyos principales componentes son:

Modulo de procesamiento (cpu).
Modulo de entrada digital (estados, alarmas, registro de evento).
Modulo de cuadro de alarmas.
Modulo de control (salidas digitales, comandos).
Modulo de comunicación.
Modulo de monitoreo y diagnostico.
Modulo de alimentación.

Las entradas/salidas del visual BOH cuentan con circuitos de protección ópticos y filtros para evitar que señales de ruido, transitorios o inducciones electromagnéticas provenientes del campo que ocasionen un funcionamiento incorrecto o daño al equipo electrónico.
La totalidad de las funciones de comunicación se realizan mediante un protocolo que cuenta con un código de seguridad altamente confiable. Con el auxilio de la interfaz adecuada se realiza el enlace de comunicaciones hacia el controlador principal de subestación (CPS). Existen varias opciones para la conexión física de los canales de comunicación según sean las necesidades particulares de la instalación: interfaz tipo RS-232, interfaz tipo red RS-485, enlace ethernet LAN/WAN, línea telefónica privada o conmutada, enlace fibra óptica, enlace vía radio, microondas. En el nuestro caso, el Visual BOH se enlaza hacia el CPS por medio de una interfaz RS-485.

Modulo de procesamiento

El modulo de procesamiento tiene a su cargo las tareas de monitorear continuamente las entradas de estado, acumuladores y con la información adquirida configurar una base interna de datos. Bajo interrogación del CPS y por reporte por excepción transmite la información requerida de su base de datos, en el formato especificado por el protocolo utilizado, con el fin de que este actualice su base de datos. Al recibir comandos de control del CPS el visual BOH los decodifica y efectúa la acción de control requerida y retransmite el nuevo estado de la información proveniente del campo hacia el CPS. El microprocesador ejecuta constantemente un autodiagnóstico global interno, comunicando los resultados de dicho autodiagnóstico al CPS.

En caso de detección de eventos de cambios de estado los almacena con su horario de ocurrencia en tiempo real, para posteriormente transmitirlos al CPS. Los eventos detectados no serán dados de baja hasta recibir confirmación de recepción de parte del CPS. Con el fin de evitar disparidad de horarios, el reloj de tiempo real propio del visual BOH, es sincronizado periódicamente con el del CPS.
El modulo de procesamiento efectúa en forma cíclica un diagnostico interno y comunica los resultados del autodiagnóstico al CPS. Continuamente se verifica la presencia de los módulos de adquisición/control que deben estar de acuerdo a la configuración establecida por el usuario. La información de diagnostico adquirida la reportara al CPS.
El visual BOH incorpora un microprocesador de 32 bits de alta tecnología como la parte básica de su unidad lógica, aunado su alta velocidad de operación 43 Mhz, así como la confiabilidad de su funcionamiento. El microprocesador encuentra verificado su correcto funcionamiento mediante un circuito de guardia (watch-dog) el cual al detectar un mal funcionamiento del microprocesador o una falla de la alimentación al microprocesador (+/- 5%), ejecuta las siguientes acciones:

- Bloqueo instantáneo de salidas de control.
- Restablecimientos (resets) continuos al microprocesador con el fin de obligarlo al reinicio de su funcionamiento normal.

Modulo de entrada digital (estados, alarmas, registro de evento).
El modulo de entrada digital permite censar el estado (ejemplo: abierto/cerrado) de grupos de 32 contactos secos o bien la presencia de voltaje (nominal de alimentación del visual BOH). Acopladores ópticos protegidos contra inversión de polaridad son utilizados para aislar las entradas de campo de la electrónica del visual BOH. Todas las entradas/salidas cuentan con protección contra transitorios esto con el fin de evitar daños al equipo o comportamientos anormales.
El visual BOH adquiere los datos relativos a los estados de entrada mediante una exploración cíclica que se realiza periódicamente. Las características de adquisición tienen que ver básicamente con el filtrado digital que se realiza a todas y cada una de las entradas. Este filtrado impide reportar eventos transitorios básicamente relacionados con fenómenos de rebote de contactos o ruido inducido. El filtrado es idéntico para todos los eventos y permite tomar en cuenta cualquier cambio de estado, pero después de algunos milisegundos (barridos) en los que se ha confirmado dicho cambio.

La transmisión de los datos de las entradas digitales al CPS se puede realizar según el protocolo elegido, con bit de estado y bit de cambio o con un solo bit y con las funciones de registro de evento deseadas incluyendo hora y fecha de captura de evento en tiempo real. Para el registro de eventos y detección de cambios momentáneos entre exploraciones del CPS, se proporciona una resolución de 1 milisegundo en todas las entradas. El visual BOH almacena, en un buffer circular 10000 alarmas/eventos (cambios de estado) sin limite de tiempo.
El modulo de entrada utiliza dos tarjetas Advantech PCL-720 como interfaz de entrada. La tarjeta Linc PC97211 se emplea para optoacoplar y proteger cada una de las entradas de campo, en grupos de 16 entradas. Los conectores CN2 y CN4 de la tarjeta PCL-720 son utilizados para las entradas digitales.

Modulo de cuadro de alarmas.

El modulo cuadro de alarmas exhibe las condiciones de alarma presentes en el sistema así como las leyendas correspondientes a cada uno de los puntos de entrada digital configurados como alarma. La indicación luminosa permite identificar las diferentes condiciones de registro de alarmas (apagado, encendido, parpadeo) en el tiempo. La versión visual BOH estándar consta de 16 ventanas de alarma al frente, las cuales se presentan por un ciclo de 8 x8 alarmas que integran el modulo de entrada digital.
La señalización de alarmas se efectúa por medio de la tarjeta PC97212A situada en la parte frontal con la leyenda estado de alarmas la cual se interconecta a la tarjeta de entrada/salida advantech PCL-720 por medio del conector PC97212A.
El modulo de cuadro de alarmas utiliza dos tarjetas advantech PCL-720 como interfaz de salida. La tarjeta linc PC97212A es la interfaz de leds empleada para señalización.

Modulo de control (salidas digitales, mandos).

El modulo de salidas digitales proporciona al usuario 32 salidas de control a través de contactos secos para cada una de ellas.
En las salidas de control se cuenta un nivel de desacoplamiento al campo por medio de los contactos del relevador asociado. Con el fin de evitar la aparición de energía electromagnética inducida, que puede ocasionar pérdida o comportamientos inadecuados en el microprocesador, cada una de las salidas cuenta con varistores de protección con capacidad de 130 joules. Como se menciono anteriormente, el microprocesador encuentra verificado su correcto funcionamiento mediante un circuito de guardia el cual al detectar un mal

funcionamiento del microprocesador o una falla de la alimentación al microprocesador (+/- 5%), bloquea instantáneamente de las salidas de control. La bobina de los relevadores de control es alimentada mediante 12 vcd, la capacidad de contactos de salida de los relevadores de control es de 3 amperes a 125 vcd.
Las salidas de control tienen el siguiente modo de operación:
Pulsante fija.- Se proporciona un pulso de duración fija que el usuario selecciona de antemano entre un rango de 0.1 a 5 segundos con intervalos de .1 segundos (100 Milisegundos).
El modulo de salida utiliza dos tarjetas advantech PCL-720 como interfaz de salida. La tarjeta linc PC97210 es la interfaz de relevadores empleada para interconexión al campo en grupos de 16 salidas.

Modulo de comunicación.
El visual BOH con referencia al CPU cuenta con dos puertos serie, uno del tipo RS-232 y el otro configurado como RS-485 por medio del cual se encuentra enlazado a un Procesador de Comunicación CP BOH el cual a su vez representa el enlace con el controlador principal de subestación (CPS). Esta facilidad permite instalar el visual BOH en un tablero de protección convencional o en un gabinete externo intemperie tipo kiosco.
Además de los dos puertos anteriores, el visual BOH cuenta con ocho puertos serie adicionales RS-232, que se encuentran identificados con las leyendas JD1 a JD8 en la parte posterior, por medio de los cuales se enlaza a los dispositivos electrónicos inteligentes (DEI´s) que se asignen: SEL-351, SEL-501, SEL-287V, SEL-251, SEL-267, SEL-279, SEL-321, GE DFP 100, SIEMENS 7SD511, SIEMENS 7UT512, ION 7300, ION 7700, BASLER BE1-851, BASLER CDS 220, y otros. Para la implementación de los ocho puertos serie adicionales, se emplea una tarjeta advantech C168P. Los conectores asignados a estos puertos corresponden al tipo DB25 macho, la asignación de puntos es la siguiente:

Modulo de monitoreo y diagnostico.
El puerto serie utilizado para propósitos de monitoreo y diagnostico se encuentra ubicado en la parte frontal por medio de un conector RJ-11, y en la parte posterior por medio de un conector DB-9 Macho JM1.
La asignación de puntos de conexión del conector RJ-11, es la siguiente:

1 detector de barrido de datos
2 recepción RD

3 transmisión TD
4 referencia a tierra (Ground)

Viendo de frente el conector, la terminal superior es la 1.
La asignación de puntos de conexión del conector DB-9 se analizará un poco mas adelante.
Los parámetros de configuración del puerto serie RS-232 dedicado a monitoreo y diagnostico de interface hombre maquina son: 19200 bauds, 8 bits de datos, 1 bit de stop, no paridad.

Función enlace transparente
En el visual BOH, se cuenta con la función de enlace transparente, mediante la función de puerto transparente, el visual BOH actúa como un enrutador de la comunicación de CPS hacia un DEI seleccionado. En el BOH CPS se ejecuta la aplicación propietaria del DEI requerido (Ejemplo: MLINK de General Electric, DIGSI de SIEMENS, Analytic Assistant de SEL, Power View de los multimedidores ION, Power Measurements, y otros).
Su conexión esta dada por el modulo de multipuertos del CPS hacia cada uno de los visual Boh en el puerto 8 (JD8), por cables independientes dedicado exclusivamente para este enlace.

Modulo de alimentación
El visual BOH tiene un bajo consumo de energía, su fuente conmutable es de una gran eficiencia y baja generación de calor. Puede ser programada para alimentar periódicamente los circuitos o en aplicaciones que corran interrumpidamente.
El sistema de alimentación esta previsto para trabajar, según características particulares, con un voltaje de alimentación de 12, 24, 48, 125 o 250 vcd, respaldado con 127 vca.

3.3 Conexiones y cables.

Los cables se utilizan para conectar los equipos, ya sean conexiones entre Hubs, de PC a Hub, o de PC a PC. 10BASE-T ó bien UTP, o RJ45 o cable de par trenzado. Externamente es igual que el cable telefónico, incluso en los conectores (los RJ45), aunque no deben confundirse nunca. Con una longitud máxima de unos 100 m por tramo, es muy cómodo de usar, resistente y fácil de diagnosticar errores.
El cable utilizado es par trenzado UTP Categoría 5 (Cat. 5) de 8 hilos para 100BaseTX, con sus respectivos conectores RJ45, uno para cada punta.

Conector RJ45.
El conector RJ-45 visto por el lado de los contactos se aprecia en la figura 3.3.1, los contactos se numeran del 1 al 8 empezando por la izquierda, los colores de los pares trenzados son los que normalmente traen los cables de categoría 5, es decir: naranja y blanco-naranja, verde y blanco-verde , azul y blanco-azul, marrón y blanco-marrón, si se utiliza un cable con colores diferentes es importante no olvidar el utilizar un par para cada dirección de la transmisión, porque si los mezclamos, es decir, si utilizamos por ejemplo dos hilos de pares diferentes para una dirección, la comunicación no se establece sobre todo si el cableado tiene una longitud superior a 5 metros.

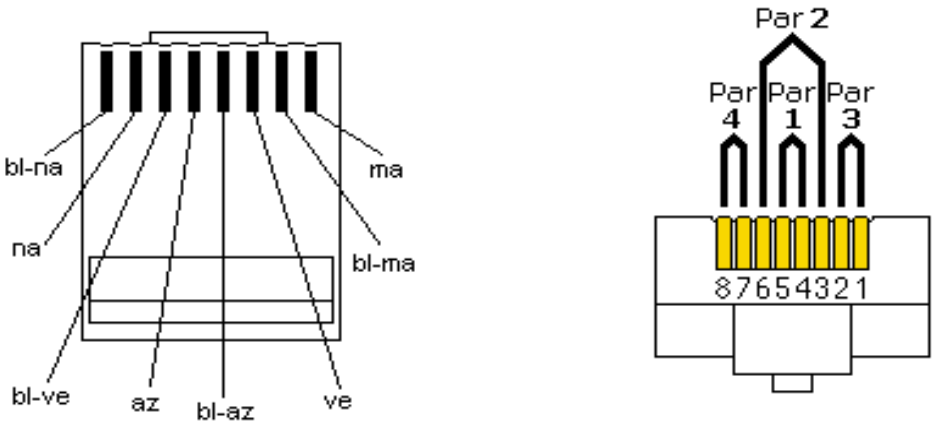


Figura 3.3.1 Contactos del conector RJ45.

La función de cada uno de los contactos se muestra en la tabla 3.3.1.

PIN	A	CONCENTRADOR
1	Recepción de datos +	Transmisión de salida +
2	Recepción de datos -	Transmisión de salida -
3	Transmisión de datos +	Recepción de datos +
6	Transmisión de datos -	Recepción de datos -
4,5,7,8	Sin conexión	Sin conexión

Tabla 3.3.1 Asignación de pines del conector RJ45.

Puerto serie del servidor de acceso remoto

El puerto serie que trae el ruteador se debe conectar a un modem V.92 y las asignaciones de sus patillas se muestran en la figura 3.3.2.

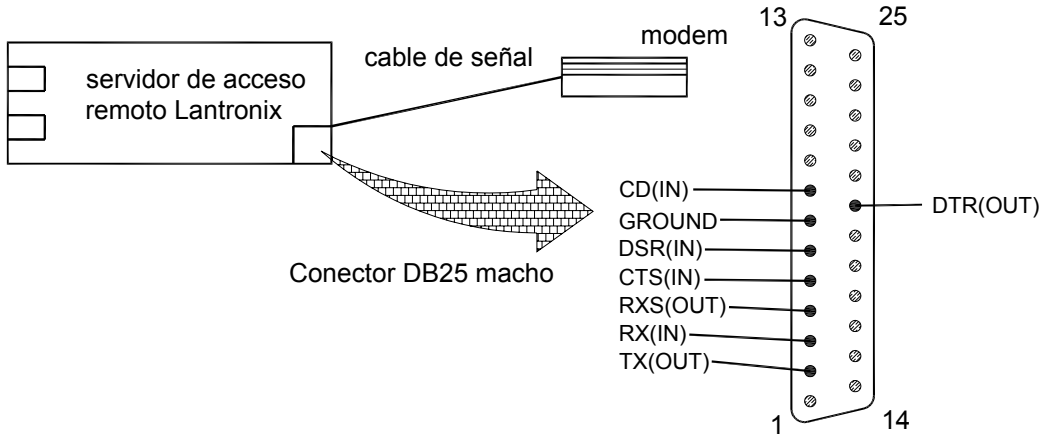


Figura 3.3.2 Asignación de pines en el puerto serie.

El ruteador viene equipado con sus respectivos aditamentos para ser fijado en el rack correspondiente, bajo las normas que correspondan para su correcto funcionamiento.

3.4 Configuraciones.

En este punto se conecta y se realiza la prueba correspondiente de comunicación entre la subestación y un puesto de control remoto que puede ser la central de control o una computadora que se conecte a la línea telefónica para entrar al sistema.

El modem elegido se conecta al sistema sin cambiar sus configuraciones de fábrica, que deben ser compatibles en lo referente al control de flujo de la información, incluyendo la corrección de errores y la compresión de datos. En caso de que los valores de fábrica no sean compatibles hay que ajustarlos conforme al manual de usuario para que el funcionamiento sea correcto.

Para asegurarnos de lo anterior se pueden efectuar las siguientes pruebas de compatibilidad entre el modem y el ruteador.

1. Con el ruteador en funcionamiento con valores predefinidos, y el modem configurado como el párrafo anterior lo indica, verificar si se establece comunicación con este mediante el comando ras-start-c, esto se realiza desde el controlador principal de subestación.
2. Con el ruteador funcionando con los valores asignados por el usuario y con el modem configurado para funcionar con el ruteador, verificar si se establece comunicación con el modem mediante el comando ras-start-s.

Estas pruebas son necesarias para determinar plenamente la compatibilidad entre el modem y el ruteador.

El software que hace posible la comunicación remota esta dividido en cuatro rutinas que son:

ras-config: para la configuración del ruteador.

ras-start: para establecer la comunicación con el equipo huesped.

ras-stop: para terminar la conexión.

Si se le adiciona el modificador –help a cada uno de los comandos, aparecerán en la pantalla las distintas opciones de los comandos.

Ahora se debe configurar el ruteador para asignarle los valores de red con los que ha de funcionar, para lograrlo se deben seguir los siguientes pasos:

En la consola de control dentro de la línea de comandos se debe cambiar a super usuario mediante el comando “su”.

A continuación se debe escribir el comando ras-config para entrar al modo de configuración del equipo.
Se selecciona la opción 2 del menú que es crear una configuración de acceso remoto (RAS).
Aquí necesitaremos proporcionar la siguiente información:
1. Nivel (RAS label). Es un nombre que se le dará al acceso remoto y puede ser alfanumérico de máximo 10 caracteres, este nombre se ocupara cada vez que se quiera acceder al sistema, o se puede cambiar según se necesite.

2. Clave de acceso (login password). Es una cadena de caracteres alfanuméricos con una longitud máxima de 6 y es solicitada cada vez que un usuario intenta conectarse al sistema en cuestión. Este password es insensible a las letras mayúsculas o minúsculas.
3. Nivel de acceso (privileged password). Es una contraseña de máximo seis caracteres alfanuméricos y nos permite definir los privilegios que los distintos usuarios tienen al entrar al sistema.
4. Tipo de modem (modem type). Aquí se precisa el modem que se instaló y está definido por un listado de marcas de modems que aparece con el comando ras-config.
5. Número telefónico de conexión (phone number). Se debe escribir el número telefónico al que esta enlazado el modem y que a su vez esta conectado el ruteador.
6. Dirección del protocolo de internet (IP address). Se le asigna una dirección en notación decimal que se haya definido para su ubicación lógica dentro de la instalación.
7. Mascara de subred (IP subnet mask). Se le asignan una mascara de subred en notación decimal, la cual está definida por los administradores de red.
Las configuraciones elegidas se graban en el archivo $RASUSER/lrs1-cust <ras_label>.cmd y en otros que definen las contraseñas, los privilegios, los modos de acceso y diversos listados que definen otros parámetros.

3.4.1 Creación de una configuración personalizada de acceso remoto.

Entrando al menú principal mediante el programa ras_config aparece la pantalla siguiente:

Main Menu
– – – – – – –
[0] Exit
[1] Create Host Serial Config
[2] Create Remote Access Server Config
[3] Create Remote Target Config
[4] List Remote Access Servers
[5] List Remote Targets
[6] Delete Remote Access Server Config
[7] Delete Remote Target Config

Selection [0–7]: 2

Create Remote Access Server Config
– –
Si seleccionamos la opción número 2 estamos listos para crear un archivo de configuración personalizada llamado $RASUSER/lrs1'label'.cmd. En donde label es el nombre de la configuración que estamos creando.
Esta acción también modifica los archivos $RASUSER/Systems, $RASUSER/asppp.com, $RASUSER/asppp.gen y $RASUSER/asppp.sup, mismos que son necesarios para conexiones punto a punto.
Aquí se necesita proporcionar la siguiente información:

Un nombre para el ruteador.
Una contraseña de acceso para la consola remota.
Una contraseña que define los privilegios para los usuarios.
El tipo de modem que esta conectado.
El número telefónico de la línea a que esta conectado el modem y a su vez el ruteador.
La dirección IP que le fue asignada a la interface de red del ruteador.
La mascara de subred asignada para la interface de red.
Una contraseña de usuario que se aloja en la cuenta de usuarios de soporte.

Una dirección IP que se aloja en el segmento cuenta usuarios de soporte.
Una contraseña de usuario que se aloja en la cuenta de usuarios general.
Una dirección IP que se aloja en el segmento cuenta usuarios general.
Ahora el sistema nos pregunta si deseamos crear una configuración de acceso remoto, si contestamos que si, nos pide el nombre que deseamos asignarle a nuestra configuración. Las palabras en negrita de esta sección son las respuestas que el usuario debe dar al sistema, a continuación se muestra dicho proceso:

Do you wish to continue to create remote access server config ? [y/n] **y**
Label for RAS ? **acceso1**
Login password of RAS remote console ? **seguro**
Privileged password of RAS remote console ? **privado**

El ruteador esta configurado para reconocer a una buena cantidad de marcas y modelos de modem por ejemplo, Intel, Cisco, Hayes, etc. Y solo hay que elegir el modelo del nuestro en la lista que se presenta. En este caso se elige el número 4 que corresponde a un Motorola.

Modem type to which the RAS is connected [1–35] ? **4**
Phone number of RAS modem ? **26518513**
IP address of RAS ethernet interface ? **147.137.24.242**
IP subnet mask of RAS ethernet interface ? **255.255.255.0**
Password of RAS ”support” account ? **soporte001**
IP address of RAS ”support” account ? **172.16.254.254**
Password of RAS ”general” account ? **general001**
IP address of RAS ”general” account ? **147.137.24.243**

La configuración para RAS-server-acceso1 fue creada con los siguientes datos.

login password = **seguro**
privileged password = **privado**
modem type = **4**
modem phone number = **26518513**
ethernet IP address = **147.137.24.242**
ethernet IP subnet mask = **255.255.255.0**
”support” account password = **soporte01**
”support” account IP address = **172.16.254.254**

”general” account password = **general01**
”general” account IP address = **147.137.24.243**

A continuación se nos pregunta si deseamos crear la configuración personalizada de acceso remoto y contestamos si.

3.5 Establecer una conexión remota.

Para establecer una conexión a un nodo remoto, se tienen que seguir los siguientes pasos:

1. En la interfaz de comandos de la P.C. que se va a conectar, ejecutar el programa ras-start y cambiar a super usuario “su”.
2. Iniciar el programa ras-start con el modificador “s” o “g” según corresponda y la dirección IP a la que se desea acceder:
Ejemplo: $RASROOT/ras-start –s 147.137.24.241
3. Salir del modo super usuario.

Modos de servicio.
El acceso remoto se puede realizar en dos modalidades: soporte y general que se identifican por los modificadores –s y –g, uno de los cuales se utilizó en el ejemplo próximo anterior.

En el modo de soporte, se busca un usuario en el listado de cuentas de soporte, ese modo se usa generalmente para establecer la comunicación entre nodos, además de ser el modo de servicio por default y proporciona acceso a los nodos Ethernet de la red a la que accedamos.

En el modo general, se busca un usuario en el listado de cuentas general, con esta modalidad estamos en capacidad de acceder no solo a nodos de red sino a servidores de red en algunas redes de área local.

Ejemplo:
Usando el programa ras-start:

$RASROOT/ras–start –s 147.137.24.241

aparece en la pantalla:
info: moved /etc/asppp.cf to /etc/asppp.cf.sav.ras
info: moved /etc/uucp/Systems to /etc/uucp/Systems.sav.ras
info: moved /etc/uucp/Devices to /etc/uucp/Devices.sav.ras
info: moved /etc/uucp/Dialers to /etc/uucp/Dialers.sav.ras
Starting PPP daemon.
Starting PPP interface ipdptp6.
Waiting for connection to remote access server.
Waiting for connection to remote access server.
Waiting for connection to remote access server.
Connected to remote access server, 147.137.24.242.
Adding static routes for target nodes. . .
add host 147.137.24.241: gateway 147.137.24.242

Al cabo de unos instantes de procesamiento se establece la conexión y estamos enlazados con la terminal remota de nuestro interés.

Terminar una conexión remota.
Para terminar una sesión de acceso remoto se debe hacer lo siguiente:

1. En la interfaz de comandos cambiarse a superusuario: “su”
2. Ejecutar el programa ras-stop:
$RASROOT/ras-stop
3. Salir del modo superusuario.

Ejemplo:

$RASROOT/ras–stop
aparece en la pantalla:

Deleting static routes for targetnodes. . .
delete host 147.137.24.241: gateway 147.137.24.242
Stopping PPP interface ipdptp6.
Stopping PPP daemon.
info: moved /etc/asppp.cf.sav.ras to /etc/asppp.cf
info: moved /etc/uucp/Systems.sav.ras to /etc/uucp/Systems
info: moved /etc/uucp/Devices.sav.ras to /etc/uucp/Devices

info: moved /etc/uucp/Dialers.sav.ras to /etc/uucp/Dialers

Después de unos momentos, este programa interrumpe la conexión y quedamos desvinculados del sistema al que accedimos.

TEMA 4. SUPERVISIÓN OPERATIVA DE LA SUBESTACIÓN.

4.1 Introducción.

Las tecnologías de adquisición de datos no pueden ser explotadas óptimamente a menos de que se tengan las herramientas adecuadas de análisis de información. En otras palabras, el conocimiento que se obtiene de los datos de medición es más útil cuando se presenta en una forma fácil de interpretar y por lo tanto de usar. Para tal efecto existe software orientado al procesamiento de información obtenida de mediciones. Ellos son escalables y abiertos en sus bases de datos, de tal manera que se pueden enlazar a otros sistemas de las compañías de electricidad, para apoyar las funciones de facturación y servidores de mercado.
En el esquema general de medición que se está implantando en los mercados se distinguen tres bloques principales que, con variantes en sus denominaciones, son: instalaciones de medición, medios de comunicaciones y centros de control.
El esquema puede variar de país a país en función de los requerimientos operativos del modelo de mercado.
En el centro de control se lleva a cabo la administración del sistema de medición. El centro está integrado por equipos de cómputo, bases de datos cliente/consumo, interfaces a los medios de comunicaciones y herramientas de aplicación. Los medios de comunicaciones, integrados por canales y protocolos de comunicaciones, constituyen el enlace entre el centro de control y las instalaciones de medición. Estas últimas constituyen el punto donde nace la medición y están formadas, básicamente, por transformadores de medición, medidores de energía, concentradores de datos e interfases a los medios de comunicaciones.
Existen puntos críticos de las redes de transmisión y distribución de los que se necesitan obtener mediciones en sitios geográficamente distantes a lo largo de estas. Al igual que en los puntos de entrega/recepción, se utilizan medidores electrónicos multifunción con capacidad de comunicación remota a través de teléfono o radio, y con funciones avanzadas de medición. La medición en estos puntos se realiza comúnmente para propósitos de balance de energía, análisis de pérdidas y de evaluación de la calidad de la energía.

4.2 Acceso al controlador principal de subestación.

Al establecer la comunicación vía remota con la subestación de interés mediante una terminal de computadora, lo que se muestra es la pantalla del programa de control del controlador principal de subestación, el cual mediante su interfaz gráfica de usuario nos permite observar la configuración de la instalación así como el estado de los dispositivos, esto es, si están operando normalmente o se ha disparado alguna alarma.
Debido a que el presente trabajo gira en torno a la supervisión operativa de la subestación, solo haré referencia a cuatro secciones del menú del programa

controlador, mismas que se observan en la figura 4.2.1, ya que estas se refieren a cuestiones meramente operativas, mientras que otras secciones del mismo tratan de su configuración, tema que no es objetivo de este trabajo explicar. Dichas secciones son: clave de acceso, presentación, acceso al DEI y diagnostico.

Figura 4.2.1. Secciones del menú principal.

El acceso a la subestación se logra dependiendo del nivel que corresponda a la persona que se está comunicando, se define desde el menú clave de acceso o desde el botón nivel acceso de la presentación unifilar y nos habilita la ventana de la figura 4.2.2.

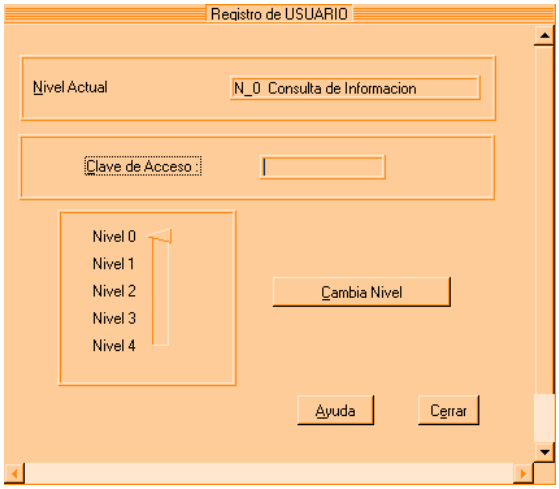


Figura 4.2.2. Ventana de registro de usuario.

Donde se observan los diferentes niveles cuya descripción es la siguiente:

- Nivel 0 Consulta de información general.
- Nivel 1 Operación con acceso a control.
- Nivel 2 Sesión directa con DEI.
- Nivel 3 Ajustes de protección.
- Nivel 4 Configuración del sistema.

Estos niveles se determinan según la jerarquía de la persona que va a utilizar el servicio de comunicación remota, a cada uno de las cuales se les asigna un

nombre de usuario y una contraseña para establecer la conexión con el controlador principal de la subestación.
Por lo que podemos intuir que, un usuario de más alto nivel puede consultar más eventos que su predecesor y el de más alta jerarquía puede intervenir en todos los procesos del sistema.

4.3 Diagrama unifilar.

Al acceder al controlador principal de subestación, una vez que hemos entrado en sesión de red, lo que observamos es la pantalla del programa de control que para nuestro caso se llama BOH CPS, misma que nos muestra un diagrama unifilar de subestación, mismo que se observa en la figura 4.3.1.

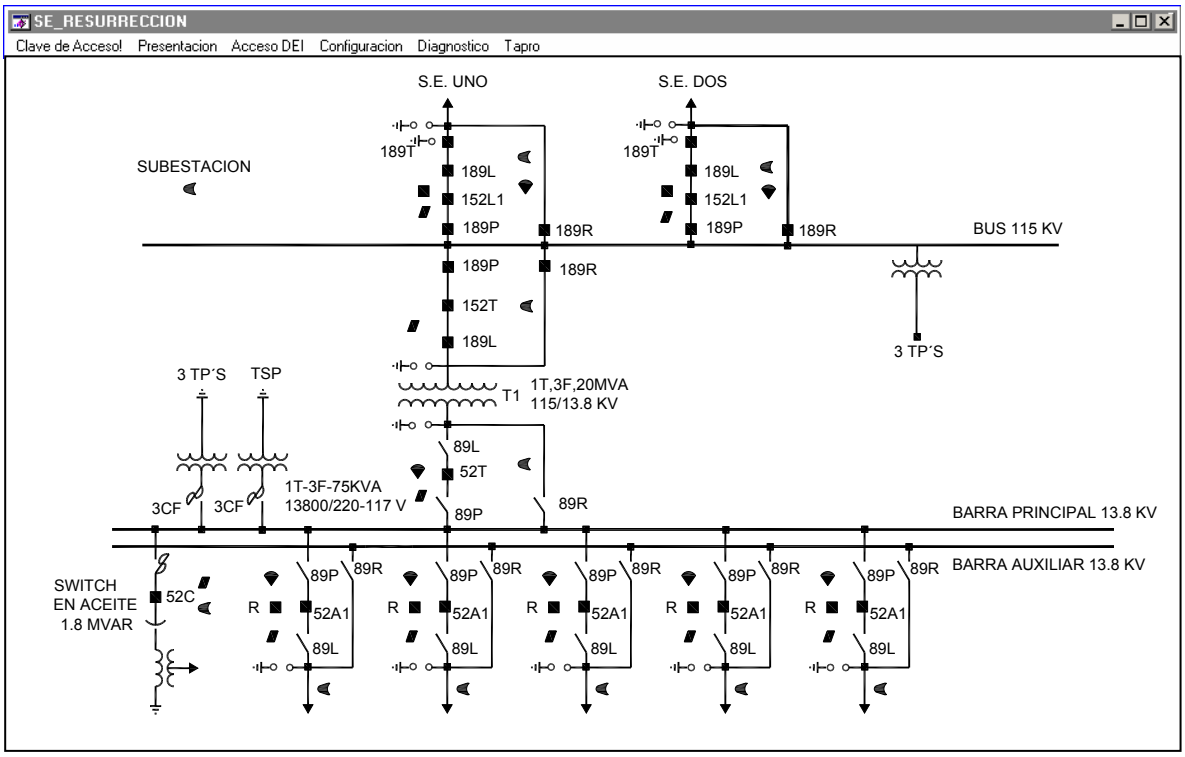


Figura 4.3.1 Presentación unifilar de la subestación.

La presentación unifilar es la presentación principal del sistema, en esta se presenta al operador en forma gráfica y dinámica, la información obtenida de los dispositivos electrónicos inteligentes (DEI´s), variables digitales (posición de interruptores, cuchillas, información de contactos de entrada/salida, elementos internos, etc.) y mediciones (corrientes, voltajes, potencia activa, potencia reactiva, etc.) por medio de diagramas esquemáticos formados por una parte estática (representación gráfica de la instalación) y una parte dinámica cuya representación varía según la información recolectada del campo.

Campos de exhibición.

Son las ventanas que muestran información dentro de las secciones del programa, de las que a continuación se hace una descripción.

Nivel de Acceso.- Es el nivel de acceso en el cual se encuentra actualmente el sistema.
Unifilar.- Nombre de Unifilar.
Puerto transparente.- Exhibición/Modificación de Puerto Transparente actual.
TX.- Exhibición de datos de último Telegrama de Transmisión correspondiente al puerto de comunicación actual. Si la transmisión fue correcta el color de fondo será verde, en caso contrario el color de fondo será rojo.
RX.- Exhibición de datos de último Telegrama de Recepción correspondiente al puerto de comunicación actual. Si la transmisión fue correcta el color de fondo será verde, en caso contrario el color de fondo será rojo.
Ultimos eventos.- En la parte inferior se exhiben los últimos dos eventos ocurridos en el sistema. Cuando se presenta un evento en el sistema se actualizan los datos del evento y enseguida comienza a flashear. Al accionar el botón RECONOCE se detiene el flasheo.

Variables de tipo dinámico.

Las Variables de Tipo Dinámico representan los cambios que ocurren continuamente en el campo relativos a la variable digital o analógica que representen. En el sistema se tienen definidos los siguientes tipos de variables dinámicas, las cuales se presentan en la tabla 4.3.1.
Si existe un evento generado (cambio) relativo a alguna variable dinámica, la representación correspondiente (icono o valor) se actualizara y aparecerá parpadeando hasta que se oprima el botón Reconocer.

Funciones de variables tipo dinámico.

Para cada uno de los iconos que representan las variables del Unifilar se tienen definidas las siguientes funciones:

Por ejemplo al oprimir el puntero del ratón sobre el icono que esta debajo de la palabra subestación, nos aparece la ventana siguiente, que corresponde a la figura 4.3.2 que es un panel de alarma de subestación en el cual se observan tres variables que son Detección de Humo/Fuego en Caseta, Detección de Intruso en Caseta y Bajo Voltaje en Banco de Baterías. Estas variables pueden accionar alarmas y se tiene la posibilidad de controlarlo, accionando los botones inferiores que son: callar, reponer o cerrar, según sea necesario.

VARIABLE	REPRESENTACION	ICONO NORMAL	ICONO ALARMA
64 Variables Alarma		Verde	Rojo

32 Variables Panel de Alarma		Verde	Rojo
64 Variables medición Valor número punto flotane		Amarillo sobre negro	Fuera de barrido: azul sobre negro. Alarma ALTO-ALTO: Rojo sobre negro.
16 Variables interruptor licencia		Blanco	Rojo
32 Variables panel de medición		Blanco	Rojo

Tabla 4.3.1 Variables tipo dinámico.

Figura 4.3.2 Panel de alarma de subestación.

Si seleccionamos el menú presentación nos aparecen las opciones de la figura 4.3.3.

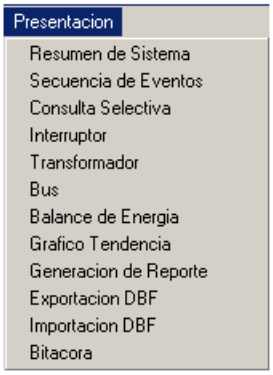


Figura 4.3.3. Opciones del menú Presentación dentro del programa controlador de subestación.

4.4 Resumen de sistema.

En la presentación resumen de sistema aparece una matriz con los 64 DEI´s y se muestra el estado que guardan en relación a la comunicación que establece con el sistema, cuyo aspecto es como el de la figura 4.4.1, pero en la que solo se muestra un arreglo de 16 DEI´s, pero para fines explicativos con esta representación es suficiente, ya que en ella están presentes los botones de operación correspondientes.

Variables de tipo dinámico

Las Variables de Tipo Dinámico representan los cambios que ocurren continuamente en el campo que representan. En la Presentación RESUMEN de SISTEMA se tienen definidos los siguientes tipos de variables dinámicas, mostradas en la tabla 4.4.1.

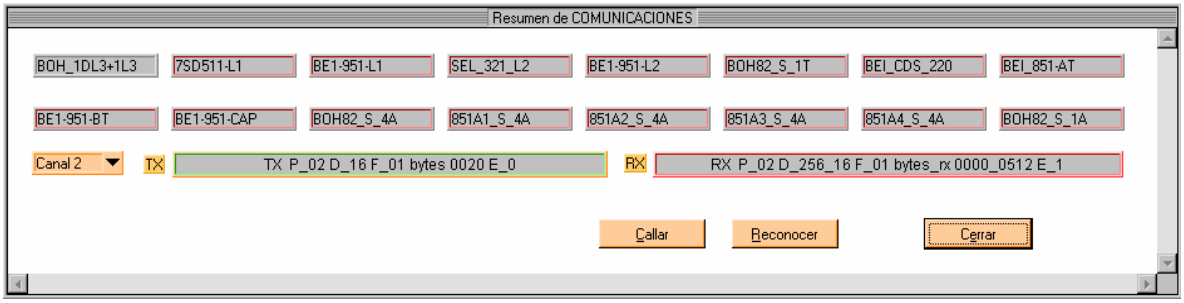


Figura 4.4.1 Ventana Resumen de comunicaciones.

VARIABLE	REPRESENTACION / COLOR
64 variables DEI	En Barrido: negro sobre fondo verde. Fuera de barrido: negro sobre fondo rojo Falla de Barrido: negro sobre fondo magenta
Puerto transparente	Negro sobre fondo azul

Tabla 4.4.1 Variables de tipo dinámico.

Si existe un evento generado relativo a alguna variable dinámica, la representación correspondiente (icono o valor) aparecerá parpadeando hasta que se oprima el botón reconocer.

Funciones de variables tipo dinámico.

Al accionar sobre algún DEI del resumen de comunicaciones aparece la Presentación ESTADISTICA DE COMUNICACION del DEI correspondiente, ver figura 4.4.2, en donde se exhibe el número del DEI, el nombre del DEI a observación y las variables de estadística de comunicación siguientes:

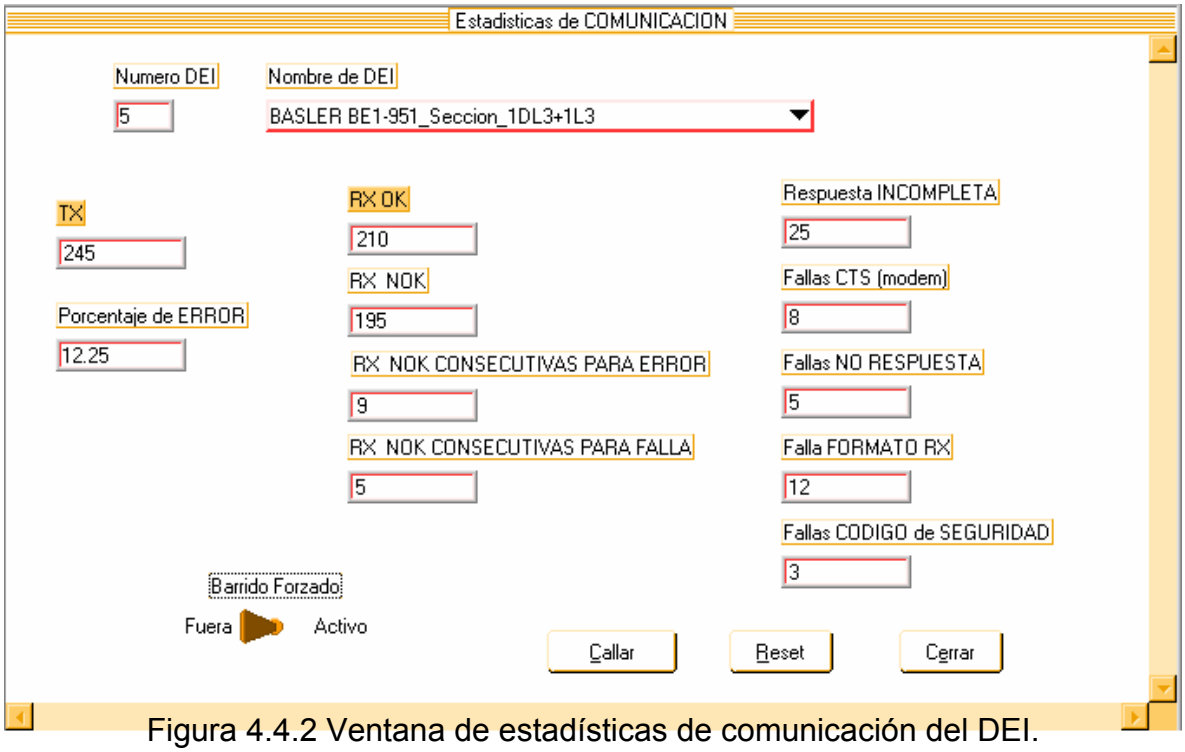


Figura 4.4.2 Ventana de estadísticas de comunicación del DEI.

TX.- Número de Transmisión.
Porcentaje de ERROR.- Errores totales entre número de transmisiones.
RX OK.- Recepciones correctas.
RX NOK.- Recepciones con error totales.
RX NOK CONSECUTIVAS.- Recepción con error consecutivas.
RESPUESTA INCOMPLETA.- Recepción incompleta.
Fallas CTS (módem).- Falla por ausencia de señal CTS modem.
Fallas NO RESPUESTA.- No recibido respuesta.
Fallas FORMATO RX.- Se recibió respuesta con errores de formato.
Fallas CODIGO DE SEGURIDAD.- Se recibió respuesta con código de seguridad incorrecta.
Canal.- Exhibición/Modificación de puerto de comunicación actual.
TX.- Exhibición de datos de último Telegrama de Transmisión correspondiente al puerto de comunicación actual. Si la transmisión fue correcta el color de fondo será verde, en caso contrario el color de fondo será rojo.

RX.- Exhibición de datos de último Telegrama de Recepción correspondiente al puerto de comunicación actual. Si la transmisión fue correcta el color de fondo será verde, en caso contrario el color de fondo será rojo.

Botones de operación
Los botones de operación que se presentan en la parte inferior tienen asignadas las siguientes funciones:

- Barrido Forzado Simulación dentro de barrido del DEI elegido.
- Calla Calla alarma audible.
- Reset Puesta a cero de estadísticas de comunicación.
- Cerrar Regresa a Presentación UNIFILAR.

4.5 Presentación Interruptor.

La presentación interruptor nos indica los datos importantes del interruptor seleccionado: Marca, Modelo, Numero de Serie, Capacidad, Fechas de mantenimiento anterior y próximo, Disparos para Vida Util, Monitoreo del balance de corriente, estado de Libranza, datos de desgaste por fase relativos a I2T o equivalente. Su apariencia es como la de la figura 4.5.1.

Campos de exhibición
- Marca.- Marca de interruptor seleccionado.
- Modelo.- Modelo de interruptor seleccionado.
- Numero de Serie.- Numero de serie de interruptor seleccionado.
- Capacidad.- Capacidad interruptiva del interruptor

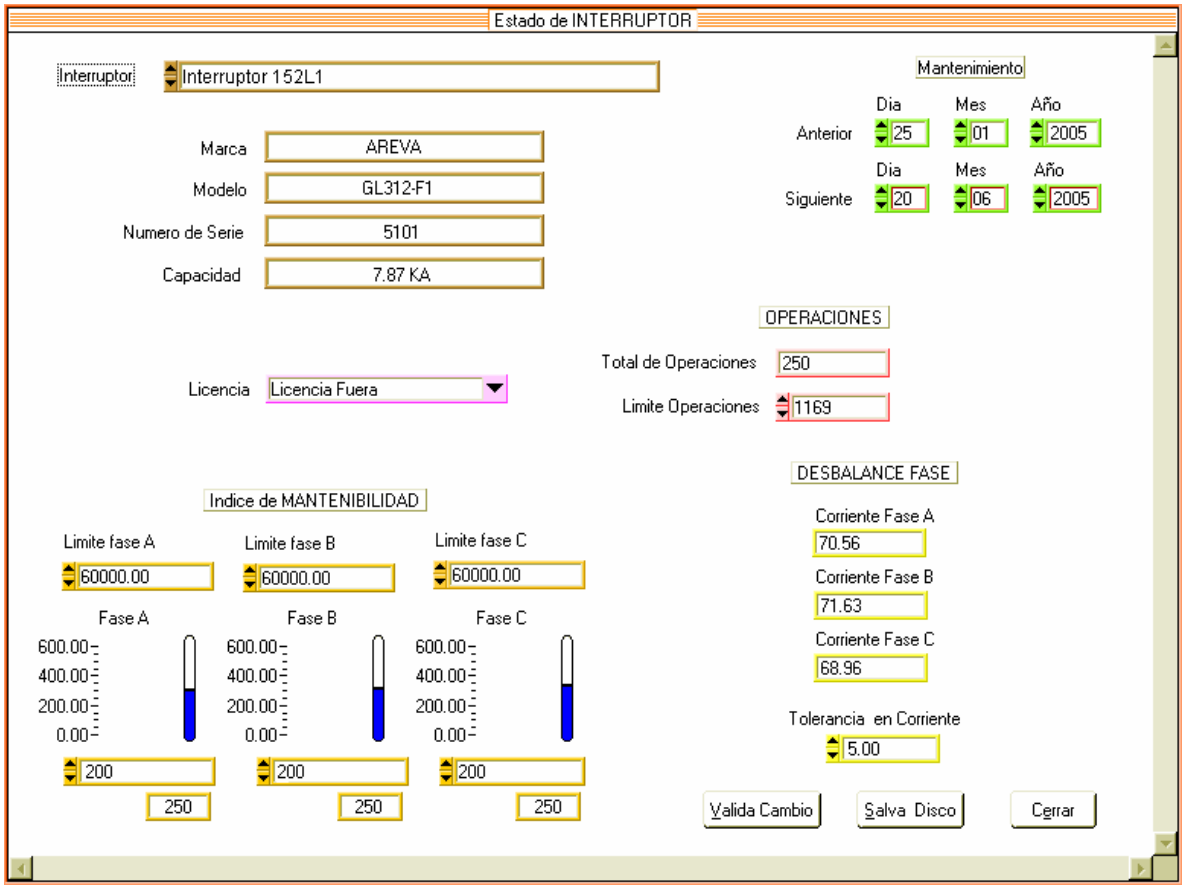


Figura 4.5.1 Ventana Estado de interruptor.

Variables de tipo dinámico.

Las Variables de Tipo Dinámico representan en forma gráfica y numérica los cambios que ocurren continuamente en el campo relativos al interruptor seleccionado de acuerdo con la tabla 4.5.1.

VARIABLE	REPRESENTACIÓN
Disparos Actuales	Valor numérico entero
Indice de Mantenibilidad Fase A, B y C	A.- Limite de Fase A, B y C: Valor numérico tipo flotante B.- Diagrama de barra de color: Azul = Normal Amarillo = Alerta Rojo = Alarma

Tabla 4.5.1 Variables tipo dinámico para interruptores.

Los valores de rango bajo y alto de la barra representativa de las variables de índice de mantenibilidad, corresponden a los valores de rango bajo y alto que se definen en la forma de Configuración de MEDICION de las variables de medición asignadas a los índices de mantenibilidad de Fase A, Fase B, Fase C, en la forma de Configuración de INTERRUPTOR.

Campos de selección/exhibición
Las Variables de selección permiten modificar los parámetros de diagnostico del interruptor seleccionado y son las siguientes:

Interruptor.- Selección de los interruptores ya previamente configurados, del cual se puede observar sus características y estado.
Libranza.- Selección del estado que debe guardar el interruptor por concepto de libranza.
Disparos para Mantenimiento.- Son las operaciones que ha efectuado el interruptor y que se presentan para vigilar su ciclo de mantenimiento por concepto de operaciones. En caso de cumplirse el limite de operaciones enviara una alarma y el fondo cambiara a rojo.
Mantenimiento Anterior.- Fecha de realización del último mantenimiento que se proporciono al interruptor.
Próximo Mantenimiento.- Fecha de la realización del próximo mantenimiento que se realizará al interruptor. En caso de cumplirse la fecha enviara una alarma y el fondo cambiara a rojo.
El valor de Disparos para Mantenimiento corresponde al límite alto definido para la variable de alarma asignada a Disparos en la forma Configuración de INTERRUPTOR Mantenimiento.

Botones de operación.
Los botones de operación que se presentan en la parte inferior tienen asignadas las siguientes funciones:

Valida Cambio.- Guarda los cambios efectuados en memoria temporal
Salva Disco.- Guarda los cambios en disco
Cerrar.- Regresa a Presentación UNIFILAR

4.6 Presentación transformadores.

La presentación transformador nos indica los datos importantes del transformador seleccionado: marca, número de serie, capacidad, fecha de mantenimiento anterior y próximo, temperatura del aceite por fase, temperatura devanados por fase y posición de taps. Su aspecto es como el de la figura 4.6.1.

Campo de exhibición.

- Marca.- Marca del transformador seleccionado
- Modelo.- Modelo del transformador seleccionado
- Número de serie.- Número de serie del transformador seleccionado
- Capacidad.- Capacidad en MVA que tiene el transformador seleccionado

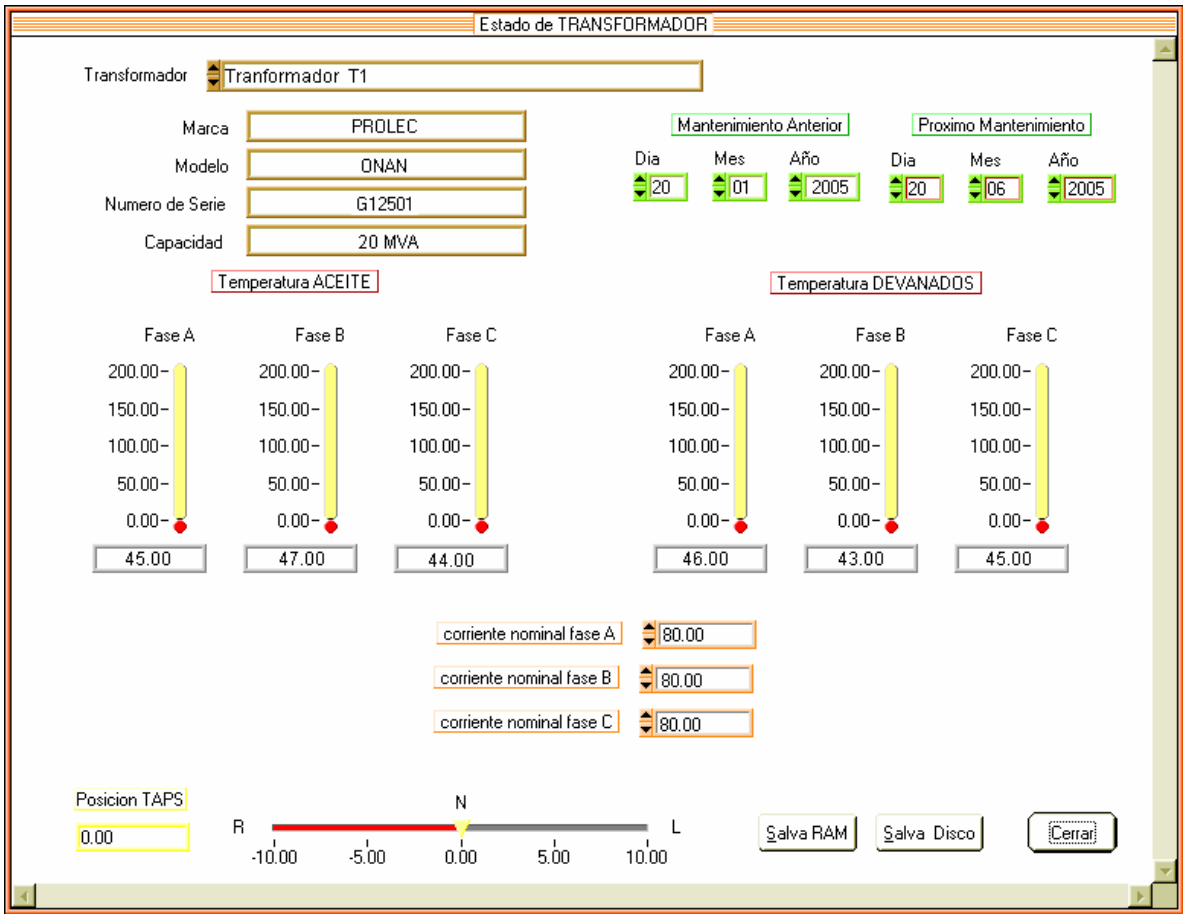


Figura 4.6.1 Ventana estado de transformador.

Las variables tipo dinámico presentan en forma gráfica y numérica los valores que ocurren continuamente en el campo relativo al transformador seleccionado, en la tabla 4.6.1 se muestra el reglaje de colores de las temperaturas de aceite y devanados.

	NORMAL	ALERTA	ALARMA
TEMPERATURA ACEITE	AZUL	AMARILLO	ROJO
TEMPERATURA DEVANADOS	AZUL	AMARILLO	ROJO

Tabla 4.6.1 Código de colores para la temperatura de aceite en transformador.

Los valores de temperatura de aceite y temperatura de devanados y posición de taps se obtienen del monitoreo de señales que definen en la forma de configuración de medición de las variables asignadas a la tarjeta analógica.

Campos de selección/exhibición
Las Variables de selección permiten modificar los parámetros de diagnostico del transformador seleccionado y se describen en la tabla 4.6.2.

FECHAS	DESCRIPCION	TIPO DE SELECCIÓN
Mantenimiento Anterior Día/Mes/Año	Fecha de realización del ultimo mantenimiento que se proporciono al transformador	Campo de Exhibición Numérico
Próximo mantenimiento Día/Mes/Año	Fecha de realización del próximo mantenimiento que se proporcionara al transformador	Campo de Exhibición Numérico

Tabla 4.6.2 Información para mantenimiento del transformador.

Botones de operación
Los botones de operación se presentan en la parte inferior, tienen asignadas las siguientes funciones:

Valida Cambio.- Guarda los cambios efectuados en memoria temporal.
Salva Disco.- Guarda los cambios en disco.
Cerrar.- Regresa a Presentación UNIFILAR.
Cerrar.- Regresa a Presentación UNIFILAR.

4.7 Barras del BUS

La presentación de bus, misma que se muestra en la figura 4.7.1, nos indica la lectura de los voltajes de las barras del bus seleccionado y la tolerancia permitida de desbalance entre ellos. Cuando se excede la tolerancia el color de fondo de la variable cambia a rojo.

Variables tipo dinámico

Las variables tipo dinámico representan en forma numérica los cambios que ocurren continuamente en el campo relativos a la medición de los valores de voltaje del bus. En la tabla 4.7.1 se observan dichas variables.

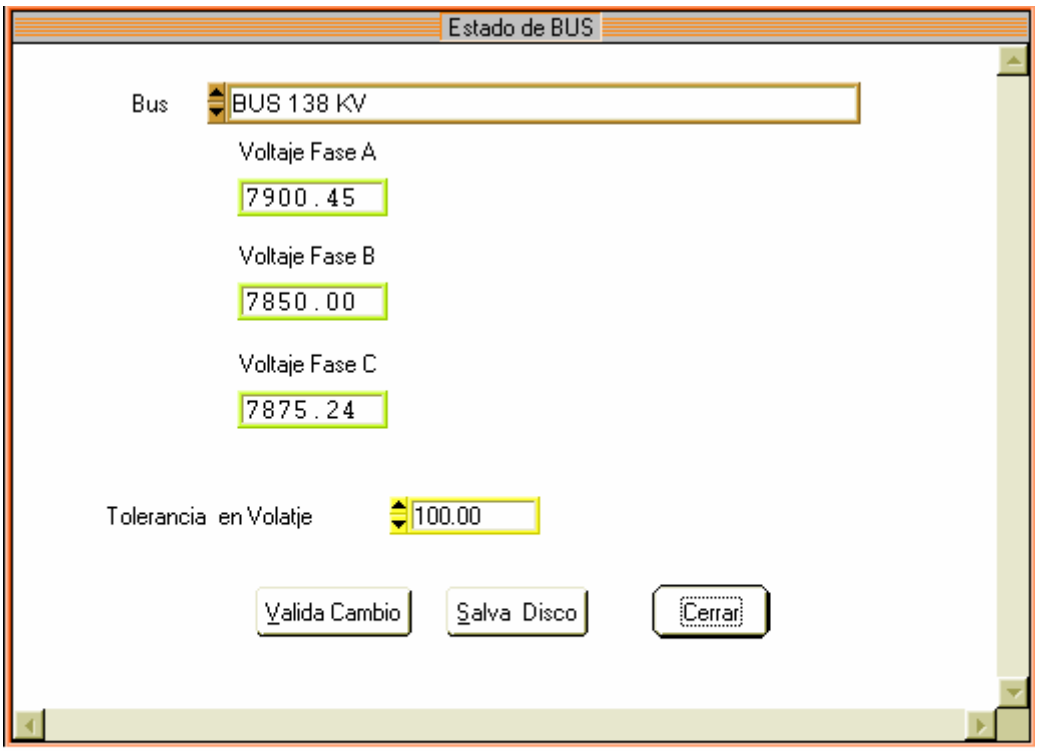


Figura 4.7.1 Ventana de estado de BUS.

VARIABLE	PRESENTACION
VOLTAJE FASES A,B Y C	A.- Valor numérico tipo flotante B.-Fondo: Rojo=Alarma, tolerancia excedida Amarillo=normal

Tabla 4.7.1 Variables tipo dinámico para BUS de subestación.

Campos de selección/exhibición.
Bus.- Selección del bus el cual presentara su estado.
Tolerancia en voltaje.- Es el valor permitido de diferencia entre los voltajes mediante una comparación entre fases, es decir, de A contra B, B contra C y A contra C.

Botones de operación.
Los botones de operación que se presentan en la parte inferior, tienen asignadas las siguientes funciones:

Valida Cambio.- Guarda los cambios efectuados en memoria temporal.
Salva Disco.- Guarda los cambios en disco.
Cerrar.- Regresa a Presentación UNIFILAR.

4.8 Supervisión del dispositivo electrónico inteligente (DEI).

Presentación TABULAR ALARMA
En la presentación TABULAR ALARMA se tiene acceso a una presentación tabular ordenada de las variables de Alarma, tal como se aprecia en al figura 4.8.1.

En el TABULAR ALARMA aparecen, en forma ordenada, el icono de alarma, número de la alarma, el nombre de la alarma, la leyenda de estado de la alarma, el número de cambios de 0 a 1 y de 1 a 0 todos estos correspondientes al Visual Boh elegido.

Campos de exhibición
DEI actual.- Lista de Selección del DEI actual, solo Visual BOH contiene tabular de alarmas.
INDICE.- Exhibición/Modificación de índice de variables actual, ejemplo: Variables 1-32,33-64.

Botones de operación
Los botones de operación que se presentan en la parte inferior derecha tienen asignadas las siguientes funciones:

- Prueba.-Hace una prueba de Sincronización a los Visual Boh
- Calla.- Callar alarma audible
- Reconoce.- Reconocer los eventos y detiene el flasheo de variables
- Cerrar.- Regresa a Presentación UNIFICAR

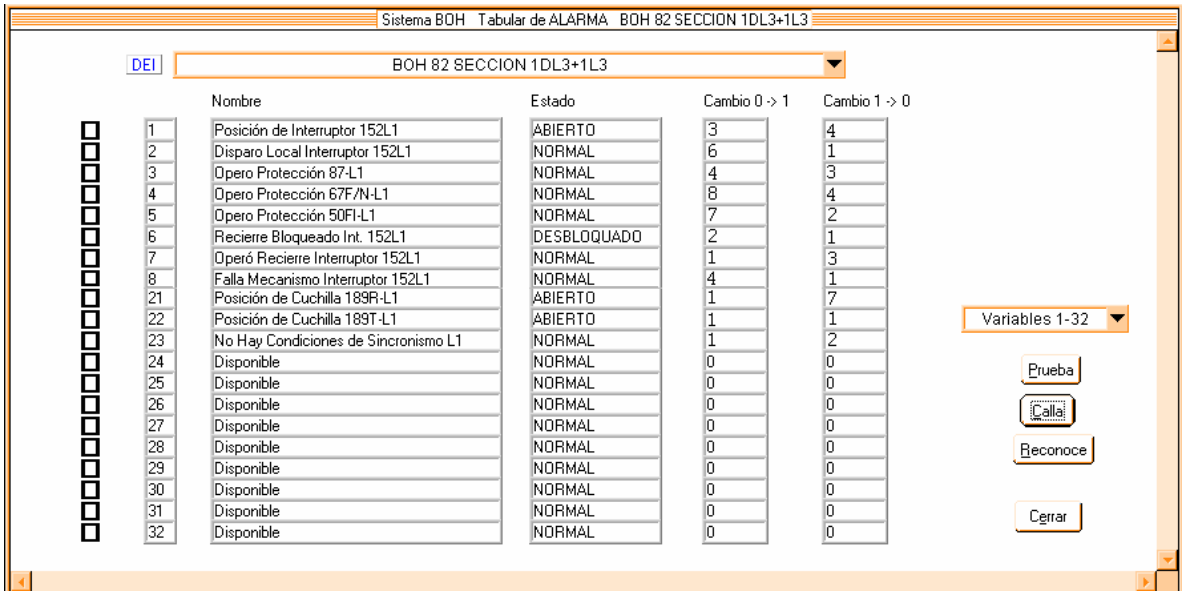


Figura 4.8.1 Tabular de alarma.

Presentación TABULAR MEDICION

En la presentación TABULAR MEDICION se tiene acceso a una presentación tabular ordenada de las variables de Medición, como se puede observar en la figura 4.8.2 En el TABULAR MEDICION aparecen, en forma ordenada, el número de medición, nombre de la medición, el valor de la medición y la leyenda de unidades correspondientes, este tabular es aplicable a los DEI´s que recaban alguna medición.

Campos de exhibición.

DEI actual.- Lista de Selección del DEI actual

INDICE.- Exhibición/Modificación de índice de variables actual, ejemplo: variables 1-32,33-64.

Botones de operación

Los botones de operación se presentan en la parte inferior derecha tienen asignadas las siguientes funciones:

- Calla Callar alarma audible
- Reconoce Reconoce los eventos y detiene el flasheo de variables
- Cerrar Regresa a Presentación UNIFILAR

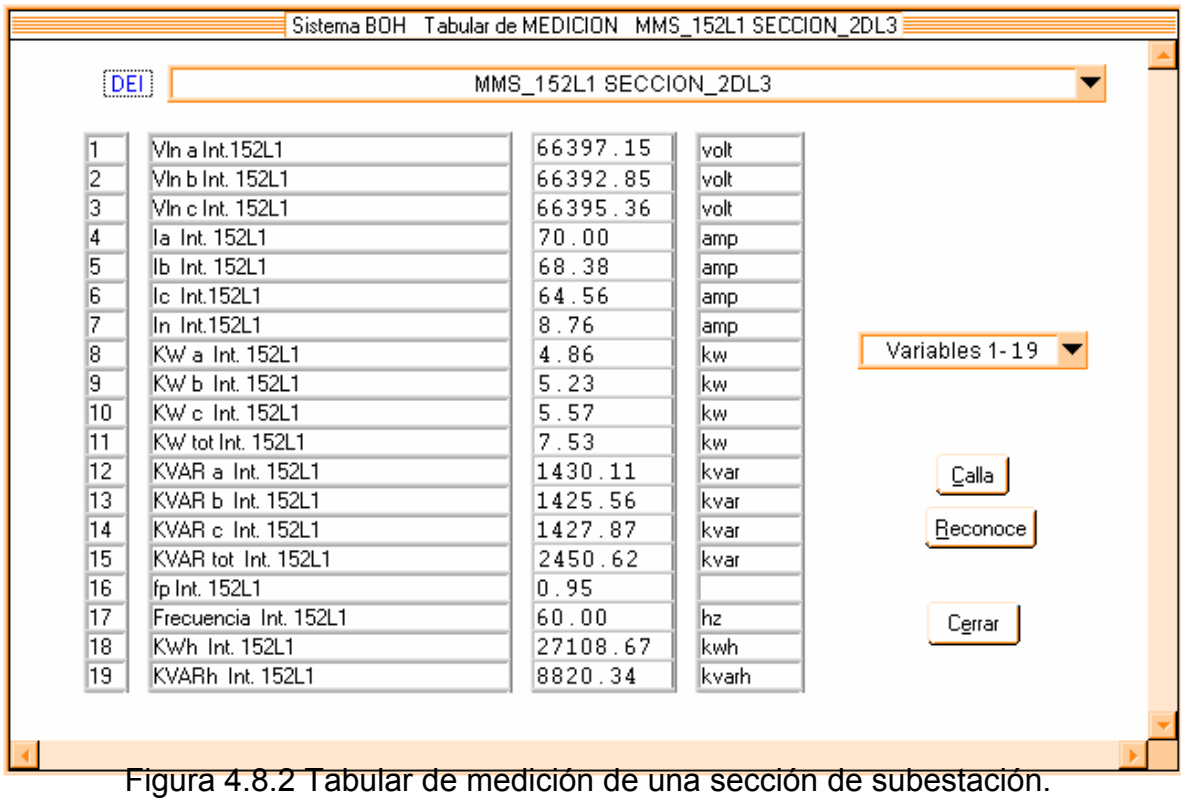


Figura 4.8.2 Tabular de medición de una sección de subestación.

Presentación TABULAR de MANDO.

En la presentación TABULAR de MANDO se tiene acceso a una presentación tabular ordenada de las leyendas de Mando, como se aprecia en la figura 4.8.3.
En el TABULAR de MANDO aparecen, (en forma ordenada) el número de mando y nombre del mando, el número de veces que se ha ejecutado desde el CPS (Controlador Principal de Subestación, Local) y el número de veces que se ha ejecutado desde Nivel Superior (Remoto) estos mandos son ejecutados físicamente en los Visual Boh.

Campos de exhibición

- DEI.- Lista de Selección del DEI actual.
- INDICE.- Exhibición/Modificación de índice de variables actual, ejemplo: variables 1-32.

Botones de operación

Los botones de operación se presentan en la parte inferior derecha, tienen asignadas las siguientes funciones:

Calla Callar alarma audible.
Reconoce Reconocer los eventos y detiene el flasheo de variables.
Cerrar Regresa a Presentación UNIFILAR.

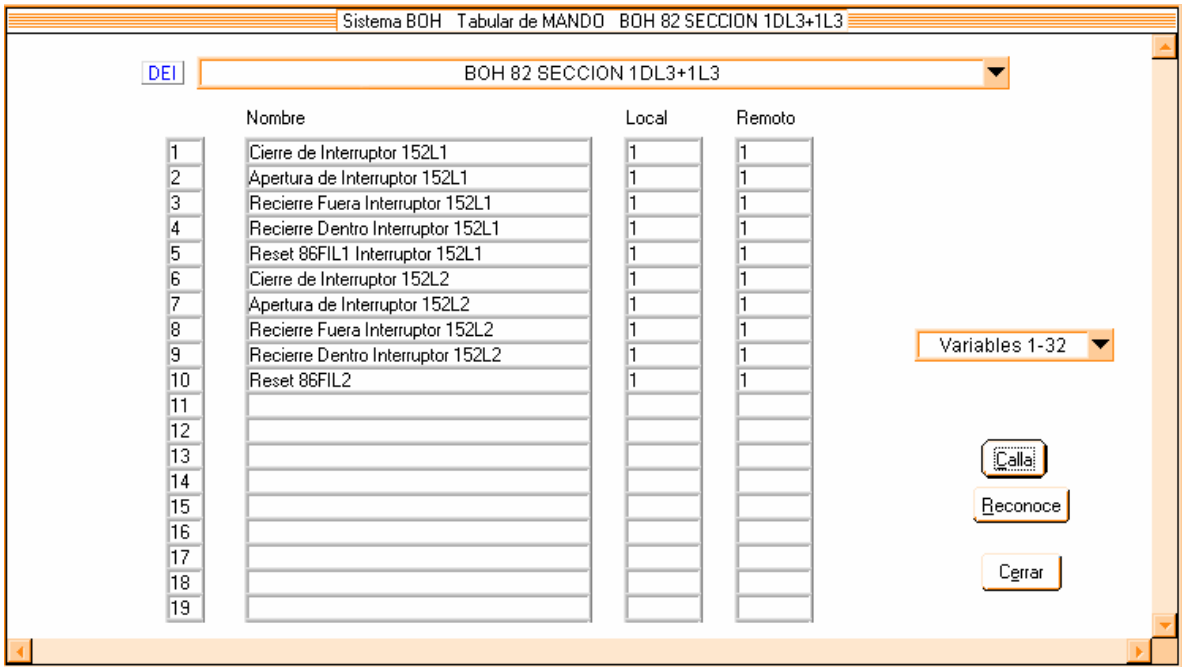


Figura 4.8.3 Tabular de mando.

Presentación EVENTOS RELEVADOR

Presenta el resumen corto (últimos 10,000 eventos) de los eventos de los relevadores de protección, ver figura 4.8.4, asociados al algoritmo localizador de falla, como es el DEI SEL 351 BT y los alimentadores, en esta misma pantalla se muestra la distancia a la cual ocurre una falla en cualquiera de los alimentadores después de realizado el algoritmo correspondiente.

Campos de exhibición

INDICE.- Exhibición de eventos registrados actualmente, ejemplo: Eventos 1-500 hasta 9500-10,000.

EVENTOS.- Exhibición del número total de eventos del relevador registrados.

Botones de operación

Los botones de operación se presentan en la parte inferior, tienen asignadas las siguientes funciones:

Limpia Buffer	Borra todos los 10,000 eventos e inicia nuevamente el registro de los eventos
Calla	Callar alarma audible
Cerrar	Regresa a Presentación UNIFILAR

Figura 4.8.4 ventana de últimos eventos de apertura del interruptor 152L1.

Presentación ULTIMOS EVENTOS
En la presentación ULTIMOS EVENTOS se exhiben los últimos 10,000 eventos registrados en el sistema, según un formato de índice de evento, fecha, hora, descripción del evento, y dependiendo del grado de urgencia establecido para algún evento o alarma se tendrá o no un fondo de color rojo.

Variables de tipo dinámico
Los eventos registrados se actualizan automáticamente.

Campo de exhibición

- INDICE.- Apuntador de eventos relativos al buffer circular de 10,000 eventos.
- EVENTOS.- Número de eventos en el buffer circular.

Campo de exhibición/modificación.

- INDICE.- Exhibición/Modificación de índice de variable actual, Ejemplo: Variable de 1-500 hasta 9500-10,000.

Botones de operación.
Los botones de operación que se presentan en la parte inferior tienen asignadas las siguientes funciones:

Limpiar Buffer.- Borrar todos los 10,000 eventos generados, para iniciar nuevamente el registro de los eventos.
Calla.- Calla alarma audible.

Cerrar.- Regresa a Presentación UNIFILAR.

Presentación CONSULTA SELECTIVA.

En la presentación CONSULTA SELECTIVA se exhibe el resultado de la consulta selectiva sobre los 10,000 eventos registrados en el sistema. Los criterios de consulta están basados en un DEI inicio/fin, punto inicio/fin, fecha dia_mes_año inicio/fin y hora_minuto_segundo inicio/fin.

Las consultas de datos se pueden realizar aplicando los siguientes filtros:

Dei inicio/fin.- Número de Dei donde se inicia y termina la búsqueda (Mínimo 1 DEI, Máximo 64 DEI´s).

Punto inicio/fin.- Número de Punto donde se inicia y termina la búsqueda (Mínimo 1 Punto, Máximo 64 Puntos).- Grado de Urgencia.- Selección de Grados de Urgencia: Todos, Información, Alerta, Urgencia.

Día inicio/fin.- Día donde se inicia y termina la búsqueda (Mínimo 1 día, Máximo 31 días).

Mes inicio/fin.- Mes donde se inicia y termina la búsqueda (Mínimo 1 mes, Máximo 12 meses).

Año inicio/fin.- Año donde se inicia y termina la búsqueda (Mínimo 1999 año, Máximo 3000 año).

Hora inicio/fin.- Número de Horas donde se inicia y termina la búsqueda (Mínimo 1 hora, Máximo 24 horas).

Minuto inicio/fin.- Número de Minutos donde se inicia y termina la búsqueda (Mínimo 1 min., Máximo 60 Minutos.

Segundo inicio/fin.- Número de Segundos donde se inicia y termina la búsqueda (Mínimo 1 seg. Máximo 60 segs.).

Si es necesario obtener impreso un listado de eventos de interés, se tiene la posibilidad de generar reportes en formato .txt, los cuales son:

Reporte de ALARMA.- Estado actual de alarmas de DEI seleccionado.

Reporte de MEDICION.- Estado actual de mediciones DEI seleccionado.

Reporte de COMUNICACIÓN.- Estado actual de comunicación de DEI seleccionado.

Reporte de EVENTOS.- Buffer de últimos 10,000 eventos de sistema.

Reporte de MANTENIMIENTO.- Estado actual de mantenimiento de interruptores.

Reporte de LIBRANZA.- Estado actual de libranzas de interruptores.

Reporte de CONFIGURACION DEI.- Configuración de DEI seleccionado.

Reporte de CONFIGURACION UNIFILAR.- Configuración de UNIFILAR seleccionado.

Reporte de CONFIGURACION NIVEL SUPERIOR.- Estado actual del mapeo de variables a nivel superior.

Los reportes se pueden programar en forma horaria eligiendo el intervalo correspondiente en el campo ajuste de hora.

La presentación bitácora consiste en un pequeño editor de textos que permite introducir informes relativos a Libranzas, Mantenimientos, Maniobras, o información general de cualquier tipo, relativas a la operación de la Subestación.

Posteriormente, estos datos son almacenados con el nombre que el usuario elija, en el directorio que el usuario elija, pasando a formar parte de una Bitácora General de la Subestación. Asimismo, la presentación bitácora sirve para leer esta información.

Presentación EXPORTACION DBF.

Mucha de la información generada debe ser concentrada para su posterior análisis, para lo cual se utiliza la presentación EXPORTACION DBF que genera archivos tipo DATABASE para su utilización en ambientes EXCEL, PARADOX, ORACLE, SYBASE, etc. La pantalla de exportación de bases se muestra en la figura 4.8.5.

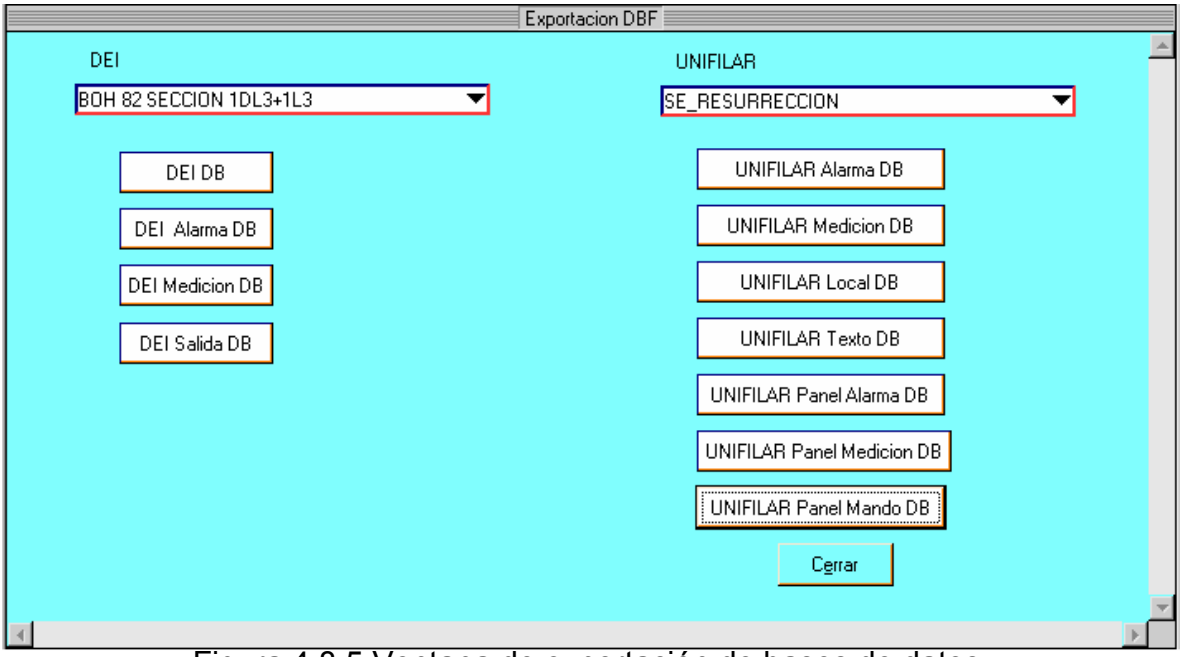


Figura 4.8.5 Ventana de exportación de bases de datos.

Los archivos de base de datos que es posible exportar se enumeran en la tabla 4.8.1.

DEI DB	Genera archivo DEI_DB.DBF
DEI Alarma DB	Genera archivo DEI_XX_ALARMA_DB.DBF
DEI Medición DB	Genera archivo DEI_XX_MEDICION_DB.DBF
DEI Mando DB	Genera archivo DEI_XX_MANDO_DB.DBF
UNIFILAR Alarma DB	Genera archivo UNIFILAR_XX_ALARMA_DB.DBF
UNIFILAR Medición DB	Genera archivo UNIFILAR_XX_MEDICION_DB.DBF
UNIFILAR Local DB	Genera archivo UNIFILAR_XX_LOCAL_DB.DBF
UNIFILAR Texto DB	Genera archivo UNIFILAR_XX_DB.DBF
UNIFILAR Panel Alarma DB	Genera archivo

	UNIFILAR_XX_PANEL_ALARMA_DB.DBF
UNIFILAR Panel Medición DB	Genera archivo UNIFILAR_XX_PANEL_MEDICION_DB.DBF
UNIFILAR Panel Mando DB	Genera archivo UNIFILAR_XX_PANEL_MANDO_DB.DBF

Donde: XX = DEI ó UNIFILAR seleccionado

Tabla 4.8.1 Archivos de bases de datos que se pueden exportar.

La utilidad de la información recabada radica en la posibilidad que se tiene para aplicar técnicas de análisis de información que hagan posible un mejor funcionamiento de la subestación aprovechando los recursos tanto humanos como económicos de la mejor manera posible.

CONCLUSIONES.

Cuando se diseña el sistema de control de una subestación, los objetivos principales son la confiabilidad y la reducción de costos. Actualmente la utilización de la tecnología disponible, basada en el uso de dispositivos electrónicos inteligentes con microprocesadores y las facilidades de comunicación utilizando redes de área local de alta velocidad, permiten desarrollar un nuevo concepto para los sistemas de control, protección y monitoreo en una subestación eléctrica de alta tensión. La comunicación a su vez permite la integración del control, la protección y el monitoreo en un sistema integrado común, brindando diversas ventajas en comparación a los sistemas convencionales.
La tendencia en el ámbito mundial hacia la desregulación y privatización de los servicios de generación, transmisión, distribución y comercialización del servicio eléctrico, se encuentra centrada en la creación de mercados competitivos. Esto hace que el rendimiento a corto plazo de las inversiones realizadas y la reducción de los costos asociados a todos los proyectos del sector eléctrico sea de vital importancia.
Entre los componentes claves de una red de control numérico se debe tener especial cuidado en determinar las características deseadas para:

- Los relés de protección y los dispositivos electrónicos inteligentes en general.
- La red LAN de comunicación de la subestación.
- Interfaces hombre-máquina

De manera que se satisfagan los requerimientos propios del sistema eléctrico y que al mismo tiempo se busque la mejor relación precio-valor para el sistema de control numérico implementado.
En la tabla siguiente pueden observar los datos obtenidos por empresas especializadas en el ramo, que demuestran cuantitativamente el grado de reducción en costos que se puede obtener en los nuevos sistemas eléctricos de potencia con sistemas de control numérico ya instalados.
Con el uso de controladores numéricos se influye también significativamente en la reducción de costos de equipos de comunicación en la subestación, ya que permite eliminar múltiples líneas de comunicación (cableado) entre los dispositivos electrónicos inteligentes y la red de area local de la subestación, gracias a la integración en el controlador de una sola base de datos, permitiendo su acceso desde la red LAN de la subestación.
La facilidad de tener centralizada en las estaciones de operación la posibilidad de realizar la configuración de los diferentes dispositivos electrónicos inteligentes de la subestación y la capacidad de diagnosticar el estado de los mismos puede ser un factor importante en la reducción futura de los costos de mantenimiento del sistema.

Se pueden ejemplificar las conclusiones para un elemento importante de una subestación: el transformador y conocer la importancia de su monitoreo. Para ello nos basamos en una experiencia adquirida en la Comisión Federal de Electricidad.
El desarrollo e instalación de los 5 sistemas de monitoreo en línea de 15 autotransformadores de potencia de la CFE, permitieron detectar fallas en proceso durante la instalación de los mismos y dar un seguimiento estrecho del comportamiento de cada una de las variables monitoreadas en función del tiempo y de esta manera conocer la condición del sistema aislante aceite/papel.

	Reducción en %
Perdidas en Volt y Var	4
Mantenimiento de equipos de la subestación	8
Número de salidas de alimentadores en la subestación	10
Tiempos sin servicio para los consumidores	10
Costos de nuevas construcciones	25
Costos de equipos	30
Aplazamiento de gastos importantes de capital	50

En forma general, se puede concluir que los transformadores de potencia son parte vital de los sistemas de transmisión de energía y que debido a restricciones económicas para realizar mantenimientos periódicos en función a las recomendaciones de los fabricantes, existe una fuerte tendencia a realizar mantenimiento basado en la condición real, mediante la detección oportuna de degradaciones incipientes. Para cumplir con este requerimiento, los sistemas de monitoreo en línea para transformadores de potencia proporcionan las herramientas requeridas para incrementar la confiabilidad de los transformadores por medio del monitoreo continuo de los parámetros más importantes.
Los beneficios de los sistemas de monitoreo en línea son los siguientes:

• Proporcionan información sobre la condición operativa de los transformadores.
• Crean un historial de datos.
• Permiten en algunos casos, sobrecargar los transformadores sin reducir su vida útil.
• Cambian de mantenimientos periódicos a mantenimientos basados en la condición real del equipo.
• Auxilia en la toma de decisiones.
• Reducen el riesgo de fallas catastróficas y los costos asociados con ellas.

• Verifican los cambios en las condiciones operativas y del estado del sistema aislante después de un mantenimiento y de esta manera justificar la realización de mantenimientos a las demás unidades del banco.

Una vez analizados los beneficios que resultan al contar con sistemas de monitoreo vía remota que en principio parecen bastante onerosos, a mediano y largo plazo demuestran sus enormes ventajas.

BIBLIOGRAFIA

Comer, Douglas E.
Redes Globales de Información TCP/IP, Principios básicos, protocolos y Arquitectura, Ed. Prentice Hall.

Guijarro Coloma Luis
Redes ATM principios de interconexión y su aplicación, Ed. Alfaomega / ra-ma.

Halsall Fred
Comunicacion De Datos, Redes De Computadores Y Sistemas Abiertos, Pearson Education, Tercera Edición 1998.

Stallings, William
Comunicaciones y redes de computadores, quinta edición. Prentice Hall, 1997.

Tanenbaum S. Andrew
"Redes de Computadoras", Prentice Hall Hispanoamericana, Tercera Edición, 1997.

RECURSOS ELECTRONICOS

Protocolos de comunicación.
http://fing.uncu.edu.ar/catedras/archivos/electronica/tema11r.pdf

Curso de protocolos TCP/IP
http://www.saulo.net/pub/tcpip/index.html

Categoría Protocolos de dmoz.org:
http://dmoz.org/World/Español/Computadoras/Internet/Protocolos/
[Selección de páginas web en castellano que tratan sobre los protocolos de Internet]

Redes
http://www.htmlweb.net/redes/redes.html
[Página web dedicada programación y diseño web.

Protocolo fast ethernet, acceso remoto
http://www.consulintel.es/Html/Tutoriales/Articulos/fast_eth.html
[Página web de asesores en telecomunicaciones]

Funcionamiento de un ruteador, aspectos basicos
http://informatica.uv.es/iiguia/2000/AER/Tema2.pdf

Manual del ruteador Lantronix LRS1
http://www.lantronix.com/pdf/legacy/lrs1_2.pdf
[Página web del fabricante]

Sistemas de lectura remota, breve revisión
http://neutron.ing.ucv.ve/revista-e/No7/Jorge%20Gudi%C3%B1o%5CSistemas%20de%20Lectura%20Remota.htm

Aplicación de redes lan en subestaciones
http://www.selinc.com/techpprs/SEL_Moore_Talacci_Dey_ApplyingEthernetLAN_6198.pdf

Sistemas SCADA
http://html.rincondelvago.com/scada.html