UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

“SUPERVISIÓN DE UNA RED DE COMPUTADORAS UTILIZANDO UN EQUIPO DE MONITOREO”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N T A:

LUIS ENRIQUE CORTÉS SAMPAYO

ASESOR DE TESIS:
MAT. LUIS RAMÍREZ FLORES

MÉXICO, 2011.

Agradecimientos

A mi esposa Karina, a mis hijos Luis Fernando y Frida Sofía, por el amor que me dan, ya que es lo que me impulsa para seguir adelante.

A mi mamá y hermanos por el apoyo incondicional que siempre me han brindado a lo largo de mi vida.

A mi suegra por el apoyo que siempre nos brindo en todos los momentos tanto alegres como difíciles.

A mis profesores, a todos aquellos que me ofrecieron su conocimiento a lo largo de mi vida estudiantil, por su apoyo y enseñanzas que me dieron.

Al profesor Luis por su apoyo y consejos, por haber aceptado formar parte de este trabajo, GRACIAS.

A la UNAM, nuestra universidad por hacer de mí y de toda su comunidad personas preparadas para enfrentarse a los retos de la vida.

Índice.

Introducción.

El propósito de esta investigación es dar a conocer la importancia que tiene el obtener un control completo sobre todos y cada uno de los elementos que forman parte de una red de computadoras ya sean redes pequeñas (de área local) o una red más grande (de área amplia).

Identificar los elementos físicos y lógicos que intervienen en la construcción e implementación de redes de computadoras.

Conocer los elementos a tomar en cuenta para el diseño de una red de computadoras.

Enumerar los protocolos de comunicación más comunes utilizados en la transmisión de datos.

Conocer la importancia que tiene la interconectividad de redes de computadoras.

Otro de los propósitos es conocer algunas herramientas o software por medio del cual se puede administrar y controlar todos los elementos que forman parte de la red de computadoras.

Hoy en día la mayor parte de las empresas cuenta con un sistema de computo o por lo menos con alguna computadora personal, a medida que las necesidades de la empresa empiezan a crecer los requerimientos de equipo de computo también comienzan a crecer hasta el punto en el cual el control y administración de su sistema de computo es casi incontrolable. De aquí la razón por la cual se debe apoyar en algunas herramientas o programas que faciliten el control y administración del centro de computo.

Mientras más fuerte sea el crecimiento de nodos instalados en una red, o existan distintos ambientes conviviendo, los problemas en el funcionamiento de la red también se van acrecentando y por lo tanto se va a requerir de diferentes elementos tanto de hardware como de software para que auxilien en el control de la red.

Es necesario tomar en cuenta varios puntos para poder resolver estos problemas.

1) Detectar en donde está el error (Hardware o Software).

2) Conocer el comportamiento de la red.

3) Conocer la utilización de recursos.

4) Realizar pruebas de configuración, sencillas y centralizadas.

Un equipo para monitoreo de la red es un elemento que nos permite ver el estatus general de la red, es decir, qué tanto se está saturando nuestra red y en donde son los puntos con mayor tráfico, cuellos de botella, etc. Con un elemento como éste y con un analizador de protocolos se puede encontrar de una manera más fácil y segura en donde se encuentran los errores del funcionamiento de la red. No se puede olvidar de un detector de fallas en el cable como otros elementos importantes, ya que un gran porcentaje de fallas en las redes se encuentran en el cableado que se utiliza.

Tanto el equipo de monitoreo de redes como el analizador de protocolos, son equipos con una gran tecnología que permite observar y poner al tanto de la situación general de la red. Estos equipos son casi indispensables si se cuenta con un número elevado de estaciones de trabajo y los enlaces que se tienen son de un alto nivel.

Los siguientes equipos para la administración y monitoreo de las redes son algunos de los más conocidos.

- Sniffer (Network General).

- Cable Scanner, entre otros (Microtest).

- HP-Open View (Hewlett Packard).

Los responsables de las redes necesitan de herramientas para administrar a los usuarios, recursos e interconexiones de redes. Si los recursos de las redes se encuentran en lugares remotos, los responsables de la red deberán viajar a estos puntos para configurar o reconfigurar los dispositivos. Anteriormente era necesario tener responsables a mano en diversos lugares, pero los actuales avances en software de red ofrecen los medios necesarios para una administración centralizada. Los responsables de redes que utilizan dichas aplicaciones pueden administrar los dispositivos remotos desde sus propias oficinas.

Con este fin, se ha desarrollado un protocolo de administración de redes OSI, denominado Common Management Information Protocol (CMIP). Este trabaja con los programas de administración de redes de diversos fabricantes, y los responsables pueden trabajar con dispositivos situados en localizaciones remotas sin tener que estar ahí. Una parte del estándar (CIMP) es el Common Management Information Services (CMIS). Con las aplicaciones que utiliza este estándar se obtiene información estadística de los dispositivos, para presentarlas a los responsables para su evaluación. Toda esta información se podrá reunir a partir de los dispositivos de diversos fabricantes en una unidad de gestión centralizada, que se localiza en la oficina del responsable de la red.

Otro protocolo estándar es el Simple Network Manegement Protocol (SNMP), el cual se desarrolló para utilizarlo en redes internas. Este se adapta para usarlo en redes base TCP/IP.

Los protocolos de administración de redes OSI son utilizados en la actualidad por diferentes fabricantes de equipos de cómputo. Por ello, están ganando aceptación a nivel mundial, y los fabricantes han diseñado paquetes de administración centralizada que se comunican y extraen información de los paquetes de administración de otras redes.

El protocolo simple de administración de redes (SNMP) no tiene interés en el servicio con usuarios, más bien con la administración de todos los protocolos de comunicación dentro de cada host y varios detalles del equipo de red que proporcionan estos servicios. En otras palabras el medio ambiente de red.

El SNMP se ha definido para auxiliar al administrador de la red. Para quitar las fallas y mejorar las funciones de manejo.

Existen algunos programas o software que trabajan con el protocolo simple de administración de la red con los cuales se realiza la administración de la red en una forma grafica y estando en una oficina alejada de todos los elementos que componen la red. Algunos de esos programas son el Open View Windows (OVW) y el NetDirector.

I. Conceptos Básicos de Redes de Computadoras.

I.1. Componentes de Redes de Computadoras.

Red. Se define en general, como un conjunto de enlaces de terminales, teléfonos, impresoras, u otro tipo de dispositivos de comunicaciones o de manejo de datos, y a estos dispositivos, los denominamos genéricamente como estaciones.

Se puede decir que en una red existen tres elementos básicos que son los siguientes, como se ve en la figura 1.1:

1.- El equipo que se denomina usuario de la red.

2.- Las interfaces tanto de hardware como de software necesarias para conectarse a la red.

3.- Algún medio de transmisión.

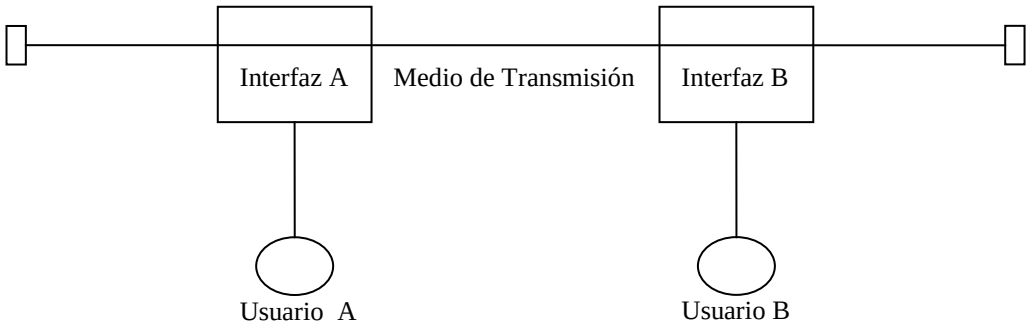


Figura 1.1 Elementos que componen una red

Arquitectura. Es básicamente un conjunto de reglas y convenciones a través de las cuales se construye algo.

Arquitectura de Red. Define las relaciones e interacciones entre los servicios y funciones de una red.

Sistema. Se utiliza para denotar la habilidad de transferir información entre dos sistemas cualesquiera, que están de acuerdo y conforme a los estándares del modelo de referencia OSI (Modelo de Referencia Para La Interconexión de Sistemas Abiertos) de ISO.

I.2. El Modelo OSI.

Para que dos sistemas se comuniquen, deben compartir un conjunto común de reglas (protocolos) para la generación e interpretación de los mensajes que se envíen o reciban. Como este conjunto de reglas no es fácil de entenderse como un todo, se recurrió a una aproximación modular estructurada, por medio de la cual, se puede manejar y comprender mejor a ese conjunto, subdividiéndolo en un número finito de partes.

El modelo de referencia OSI, es un ejemplo de una aproximación modular estructurada. En ese modelo, se define una serie de capas con un grupo de funciones independientes, y los límites de estas capas representan las demarcaciones entre estos grupos de funciones. La idea básica de generar capas, es de que cada nivel superior, agrega valor a los servicios que ofrecen las capas inferiores, por lo que, al usuario de la capa más alta, le es ofrecido un conjunto completo de servicios necesarios para que interactúe con otros usuarios y equipos periféricos que estén distribuidos en la red.

El modelo de referencia OSI, está dividido en siete niveles, en el cual los tres niveles inferiores (capa física, de enlace de datos, y de red), gobiernan las facilidades de comunicación, es decir, las conexiones físicas, el control del enlace, y las funciones de enrutamiento y liberación en la transmisión real de datos. Estos tres niveles, son los que aplican específicamente, a la arquitectura de las redes locales.

Modelos de Redes.

Aunque las funciones de proceso de las distintas aplicaciones que necesitan acceder a una red pueden ser muy diferentes, sólo hay un número limitado de tipos de red, y los problemas de comunicación de un ordenador principal a otro son independientes del proceso de la aplicación.

Una forma simple de ver los problemas de comunicación puede ser la siguiente:

Tiene que haber algún acuerdo sobre la forma de intercambio de las señales físicas que permiten pasar los bits de un ordenador a otro.

Asumiendo que los bits se puedan transmitir y recibir, ¿puede el receptor estar seguro de que los bits que está recibiendo son los que se han enviado? En otras palabras, es necesario disponer de algún sistema de detección y recuperación de errores.

Si un ordenador recibe correctamente un mensaje, ¿es para él el mensaje o debe pasarlo a otro nodo? Y si es así, ¿a cuál?

Si el mensaje es para este nodo, ¿hay algún programa de usuario que pueda y esté dispuesto a recibirlo?

Esta forma tan simplista de ver las cosas introduce el concepto de "niveles" en el proceso de comunicación. Los niveles más bajos se encuentran más cerca de la máquina o de la red. Cada uno de los distintos niveles se pueden imaginar como un conjunto de reglas, o un protocolo, que define cómo se comunican los dos ordenadores a ese nivel.

Esto introduce dos conceptos importantes:

1) Los protocolos que se encuentran en cada nivel y los límites de los niveles deberán estar lo suficientemente bien definidos como para que se puedan introducir los cambios necesarios a un nivel sin que ello afecte al resto de los niveles. Por ejemplo, se podría introducir un nuevo mecanismo de detección de errores sin que el software de los demás niveles sepa que ha tenido lugar un cambio.

2) El protocolo de cada nivel aparentemente sólo se comunica con el protocolo de nivel correspondiente del ordenador remoto.

En la práctica, los datos no se transfieren de una máquina a otra en ningún otro nivel que no sea el "más bajo". Cada nivel sólo se comunica con los niveles que tiene por encima y por debajo, pasando información al nivel más bajo o al nivel más alto.

Este concepto de estructurar el proceso de comunicación en niveles ha sido adoptado por una de las organizaciones de estándares más importantes, la ISO (International Standards Organisation). Esta organización ha desarrollado y publicado una arquitectura formal de protocolos para interconexión de sistemas abiertos (conectando ordenadores heterogéneos) conocida como el modelo de referencia OSI de la ISO. Este modelo está pensado para ser utilizado como estructura para el diseño de protocolos y servicios estándar, en vez de como una definición de protocolos. Es muy probable que sea la estructura a partir de la que van a ser desarrollados los futuros protocolos.

El modelo de referencia OSI de la ISO incorpora siete niveles: el nivel físico, el de enlace de datos, el de red, el de transporte, el de sesión, el de presentación y el de aplicación, como se aprecia en la figura 1.2.1

El nivel físico.

Este nivel es el encargado del mecanismo para transmitir secuencias de bits a través de un enlace o canal de comunicaciones. Es el encargado de los aspectos físicos de cosas como los niveles de voltaje utilizados para representar el 0 y el 1, y las señales de control que indican el estado del circuito físico para que pueda sincronizar el intercambio de datos. También define las propiedades mecánicas de los conectores y de las asignaciones de las patillas de éstos.

El nivel de enlace de datos.

Este nivel usa el mecanismo de transmisión que proporciona el nivel físico, y hace que el canal de comunicaciones parezca estar libre de errores. Incorpora alguna forma de mecanismo de detección de errores y se encarga de los problemas asociados con la retransmisión de la información que se ha corrompido.

El nivel de red.

Mientras que los dos niveles inferiores se encargan esencialmente de la comunicación entre dos máquinas adyacentes de la red, el nivel de red se encarga de conducir los "paquetes" por toda la red. Este nivel toma un mensaje del ordenador, lo divide en paquetes y organiza la transmisión de éstos por la red hasta el destino deseado. Al hacer esto, es el responsable del orden y control de flujo de los paquetes.

El nivel de transporte.

La tarea principal del nivel de transporte es ocultar todas las características dependientes de la red a los niveles que tiene por encima. Esto significa que proporciona una transferencia de datos transparente. Es decir, un usuario de un ordenador se puede comunicar con un usuario de otro sin tener que preocuparse en absoluto por la estructura de la red para poder enviar sus mensajes. La implicación de esto es que todos los protocolos definidos para el nivel de transporte sólo tienen que ser implementados en los mainframes, no en los ordenadores intermedios de la red.

Los servicios proporcionados por el nivel de transporte son la gestión de las conexiones y la transferencia de datos. El usuario del nivel de transporte (es decir, el nivel que hay por encima) puede estar este nivel para establecer y mantener una conexión lógica con el usuario del nivel de transporte correspondiente de un ordenador remoto, y durante este tiempo, el nivel de transporte transferirá datos entre los dos usuarios por medio de esta conexión.

El nivel de sesión.

El período de tiempo durante el que un par (o más) de usuarios permanece lógicamente conectado (aunque no estén continuamente transmitiendo o recibiendo) se conoce como sesión. El nivel de sesión se encarga de establecer y gestionar una vía de comunicación entre dos usuarios. En muchos sentidos, esto se puede considerar como un proceso analógico a los procedimientos de entrada y salida del sistema, necesarios en un sistema de tiempo compartido convencional. Por ejemplo, puede ser necesario comprobar si los usuarios son legales y poder facturar la parte correspondiente de la sesión de comunicación.

El nivel de presentación.

El nivel de presentación se encarga del formato de los datos que se intercambian las partes implicadas en la comunicación. Se podría argumentar que la función del nivel de presentación está en realidad asociada con la aplicación del usuario, pero hay diversas características comunes a muchas aplicaciones que hacen que un nivel de presentación sea importante.

Una de las áreas de interés es la conversión de códigos. Por ejemplo puede ser que una de las partes implicadas en la comunicación utilice código ASCII para almacenar caracteres internamente, mientras que la otra parte use EBCDIC. El nivel de presentación realizaría la conversión correspondiente.

Si un determinado sistema de mensajes que se están intercambiando contuviese un gran número de palabras o expresiones que se repiten, por ejemplo, crédito y débito en un sistema financiero, estas palabras o expresiones se podrían codificar para reducir la cantidad de información que se está intercambiando. Por ejemplo, el uso de un código de ocho bits permite que un byte represente 256 palabras o expresiones diferentes. En este nivel es posible utilizar mecanismos muy sofisticados de compresión de texto.

En una red donde es importante la seguridad de los datos (confidencialidad), el nivel de presentación podría efectuar alguna forma de encriptación inversa en la recepción.

El nivel de aplicación.

Este es el nivel más alto del modelo de referencia, y es el entorno en el que funcionan y se comunican los programas de usuario. Podría parecer que como este nivel es el que se encarga del usuario, los detalles de esta comunicación dependen de la aplicación y son diferentes para todas las aplicaciones. Esto es cierto en algunas aplicaciones, por lo que los protocolos apropiados de este nivel serán diseñados por el usuario. Sin embargo, hay un grupo de áreas de aplicación comunes en las que se está trabajando para definir protocolos estándar para tales aplicaciones. Un requerimiento muy común es el de una aplicación de transferencia de ficheros, es decir, una red de estaciones de trabajo monousuario relativamente pequeñas, cada una de ellas con algún dispositivo de almacenamiento de ficheros de gran capacidad. Una variación de esto sería un protocolo de acceso a ficheros, para acceder a parte de un fichero que está almacenado en un dispositivo de almacenamiento de ficheros de un ordenador remoto. Otros ejemplos pueden incluir la transferencia de documentos por correo electrónico.

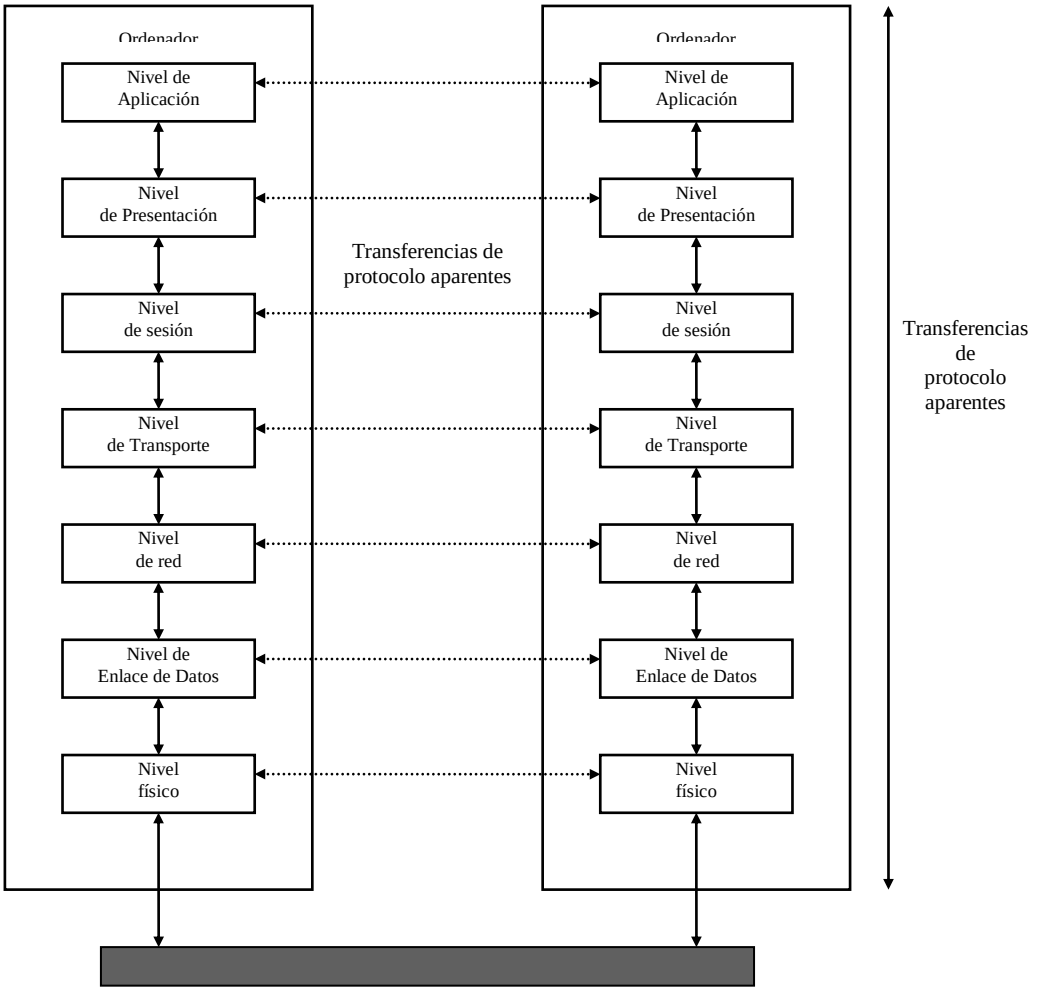


Figura 1.2.1 El modelo de referencia OSI con sus 7 niveles.

I.3 Redes de Área Local y Redes de Área Amplia.

Una definición muy simple de una red seria diciendo que no es otra cosa que varios ordenadores conectados entre sí. Sin embargo, es necesaria una definición más precisa de lo que significa el término ordenador por ejemplo. ¿Se deberá incluir una terminal inteligente? Si se acepta que una red de ordenadores debe excluir un sistema clásico de terminales de tiempo compartido partiendo de la base de que sólo hay un ordenador que controla todos los demás dispositivos entonces una mejor definición incorporaría la noción de que cada dispositivo conectado debe ser capaz de efectuar algún tipo de proceso por si solo. Por tanto una red de ordenadores es un grupo de ordenadores autónomos interconectados entre si.

Por otra parte, un sistema distribuido significa normalmente que hay distribuida alguna otra función, además del hardware, por ejemplo, en una red de ordenadores simple, es muy posible que cada uno de los ordenadores tenga

su propio sistema y su propia copia de todo el software de comunicaciones necesario para comunicarse .Sin embargo en un sistema distribuido sólo hay una copia del sistema operativo, aunque los distintos componentes de ese sistema operativo pueden encontrarse en distintos ordenadores. En este caso puede ocurrir que cuando un usuario utiliza una determinada función del sistema operativo, es muy posible que no sepa que la función la está ejecutando un procesador diferente.

Una red de área local es una red de computadoras que están limitadas a un área geográfica pequeña. Interconecta computadoras, terminales y otros dispositivos digitales dentro del sitio de una planta, las instalaciones de una universidad, un edificio de oficinas, etc.

Una red de área amplia es una red formada por la interconexión de varias redes de área local ya sea que estén estas en un mismo edificio o en lugares distantes.

I.4 Topología de Redes Locales.

Una red de computadoras (ordenadores) puede tener muchas topologías diferentes, independientemente de si son de área local o larga distancia. Como se vera, algunas topologías son más flexibles ante los fallos en ciertos nodos o enlaces de comunicaciones, pero pueden ser más costosas. Generalmente, a lo que hay que llegar para decidir sobre una topología es a un compromiso entre la fiabilidad de la red (lo propensa que sea a los fallos) y el costo de los distintos enlaces.

En términos generales, hay dos tipos de canales de comunicación:

Canales punto a punto.
Canales de transmisión difundida.

Topologías Punto a Punto.

Un canal punto a punto es aquel en el que los ordenadores de una red están enlazados por medio de canales de comunicación a uno o más (pero no necesariamente a todos) de los ordenadores de la red. Si dos ordenadores que están enlazados directamente desean comunicarse, lo pueden hacer directamente. Si dos ordenadores que no comparten un mismo enlace desean comunicarse, lo pueden hacer, pero indirectamente a través de otros ordenadores, véase figura 1.4.1.

En un sistema en estrella los distintos nodos se pueden comunicar con el ordenador central (como en un sistema de terminales), o se pueden comunicar con los demás, pero sólo "atraves" del ordenador central. El coste de añadir un nuevo nodo a la red es bajo, si el ordenador central dispone de un puerto libre, pero en caso contrario es imposible. Si falla un determinado nodo, esto no afecta en absoluto al resto de las comunicaciones, pero si falla el ordenador

central queda inutilizada toda la red. La potencia de proceso del ordenador central es, además, un "cuello de botella" para comunicaciones múltiples y, por tanto, reduce el rendimiento. Sin embargo, muchos de los sistemas de terminales son de este tipo.

En una red totalmente conectada, todos los ordenadores están enlazados con el resto de los ordenadores de la red.

Una red irregular es similar a la red totalmente conectada, excepto que no existe necesidad de conectar todos los ordenadores entre sí.

La topología de árbol (jerárquica) es un caso especial de red irregular. La dificultad inherente a las redes irregulares es el problema de dirigir un mensaje de un ordenador a otro remoto.

En una topología en bucle, un mensaje se pasa al siguiente ordenador del bucle en su totalidad antes de ser retransmitido.

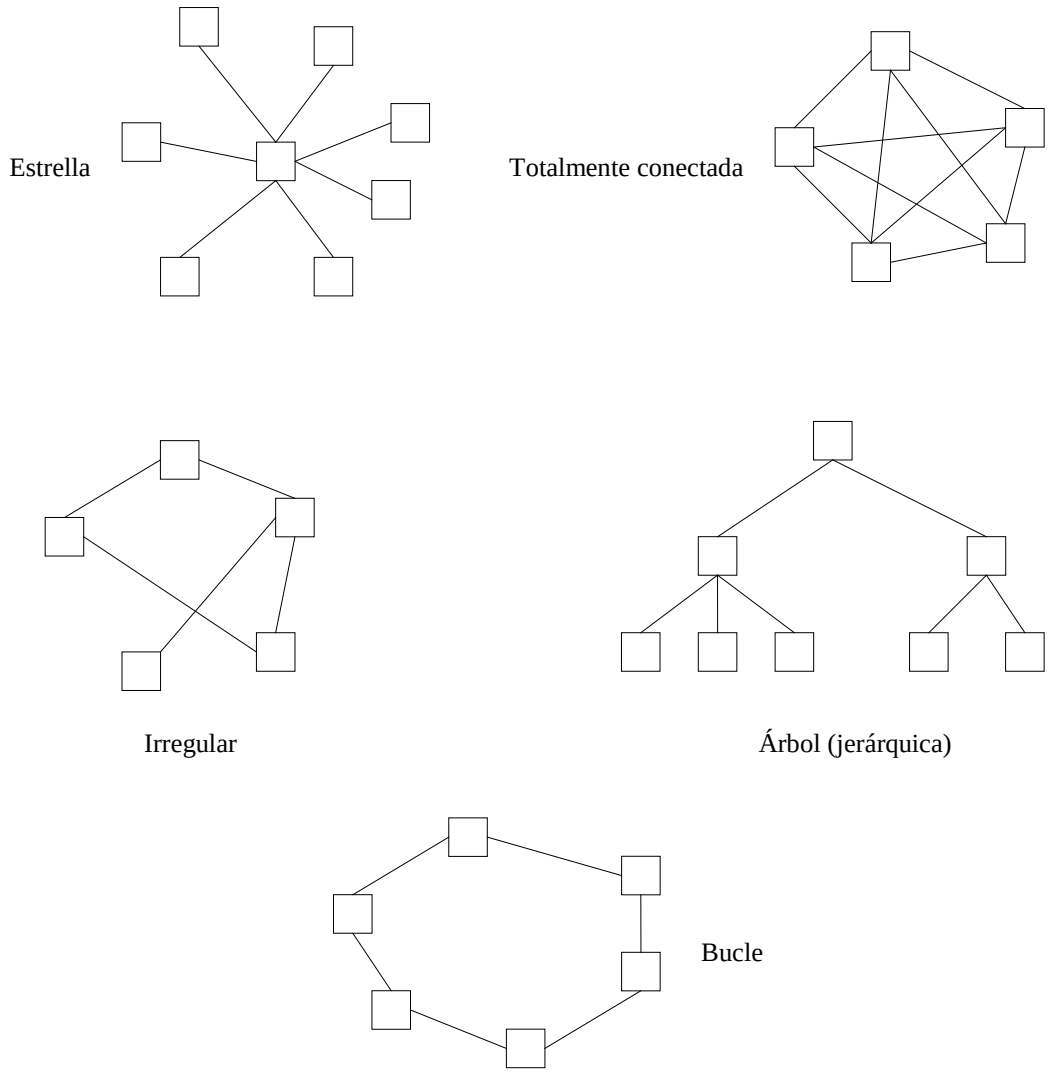


Figura 1.4.1 Representación de Topología Punto a Punto

Topologías de Difusión.

Un canal de difusión es un único canal de comunicación compartido por todos los ordenadores que se comunican a través de él. Cualquier mensaje enviado por un ordenador es recibido por todos los demás ordenadores, por lo que el mensaje ha de contener la dirección del receptor al que va dirigido, de forma que todos los demás ordenadores lo ignoren, véase figura 1.4.2

En una difusión en bus, todos los ordenadores están conectados a un bus o línea común, y en un determinado instante, sólo un ordenador puede transmitir a través del bus y los demás deben estar preparados para recibir. Puesto que puede darse el caso de que dos o más ordenadores deseen transmitir simultáneamente, es necesario que haya algún mecanismo que actúe de árbitro para resolver estos conflictos.

En una difusión en anillo, los bits (o bytes) de un mensaje se transmiten por toda la red sin esperar al resto del mensaje al que pertenecen. En realidad, puede suceder que grupos consecutivos de bits o de bytes pertenezcan a mensajes diferentes y que vayan dirigidos a nodos distintos, con lo cual los mensajes se intercalan y el ancho de banda de la red se comparte por completo. Como en todos los sistemas de difusión, es necesario disponer de algún mecanismo que controle los accesos simultáneos.

Con la difusión vía satélite, cada ordenador puede transmitir y recibir al y del satélite (en la práctica no es necesario que todos los ordenadores de la red estén conectados, sino uno sólo en cada localidad, estando los demás de una localidad conectados de forma más convencional).

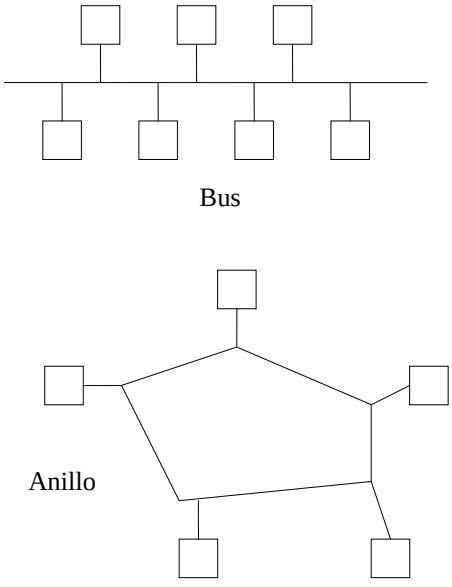


Figura 1.4.2 Representación de Topología de difusión.

I.5 Medios de Transmisión.

Cualquier medio físico que pueda transportar información en forma de señales electromagnéticas se puede utilizar en las redes locales como un medio de transmisión.

Las líneas de transmisión son la espina dorsal de la red, por ellas se transmite la información entre los distintos nodos.

Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: banda base y banda ancha.

Banda Base.

En la transmisión de datos en este tipo de técnica no es necesario el uso de modems y la señal se puede transmitir a alta velocidad.

Banda base significa que la señal no está modulada y, por tanto, esta técnica no es muy adecuada para transmisiones a larga distancia ni para instalaciones sometidas a un alto nivel de ruidos e interferencias. El empleo de esta técnica permite utilizar dispositivos de interfaz y repetidores muy económicos.

La técnica de banda base es especialmente adecuada en la transmisión a corta distancia. El medio de transmisión (el cable) ha de poder cambiar de estado con la rapidez que requiera la transmisión de datos, y los dispositivos de interfaz y los repetidores han de ser capaces de leer y transmitir la información a esa velocidad.

Un canal que trabaje en modo de banda base utiliza todo el ancho de banda, por lo que, en un determinado momento, sólo puede transmitir una señal.

Banda Ancha.

Esta técnica consiste básicamente en modular la información sobre ondas portadoras analógicas. Varias portadoras pueden compartir la capacidad del medio de transmisión mediante técnicas de multiplexación por división de frecuencia. Aunque todos los usuarios utilizan la misma línea, es como si se estuviesen utilizando varias diferentes. El ancho de banda depende de la velocidad a la que se vayan a transmitir los datos.

Los fabricantes de dispositivos de televisión por cable (CATV) vienen utilizando esta técnica desde hace mucho tiempo. A cada canal se le asigna una frecuencia y en los receptores se sincroniza el canal que el usuario desea ver.

Cuando se emplea el sistema de banda ancha para transmitir datos, es preciso el uso de modems para modular la información. Los modems utilizados en las redes de banda ancha son dispositivos muy complejos, pues han de realizar funciones de modulación/demodulación y de transmisión/recepción.

II. Aspectos Básicos para el Diseño de Redes de Computadoras.

II.1 Definición de Necesidades.

El concepto de red se basa en el principio de compartir recursos entre los usuarios de la misma. La principal característica de este tipo de red es el contar con un lugar común de almacenamiento de los datos para compartir la información. En una red de computadoras básica podemos contar con los siguientes elementos.

1.- Servidor de Archivos.
2.- Estación de Trabajo.
3.- Tarjetas de Red.
4.- Cables (Medio de Transmisión).
5.- Sistema Operativo Local.
6.- Sistema Operativo de Red.

El servidor de archivos es la computadora central encargada de compartir los recursos de la red. En ella reside el sistema operativo de red. Adicionalmente existen otros tipos de servidores como pueden ser los servidores de impresión, de base de datos entre otros.

Las estaciones de trabajo son cada una de las computadoras que están conectadas a la red. Estas estaciones de trabajo tienen memoria y procesador propio (terminales inteligentes) es decir que en ellas se procesa cada programa o aplicación que es traído desde el servidor de archivos.

Tarjetas de red es el dispositivo encargado de la comunicación entre el servidor de archivos y las estaciones de trabajo. Se instalan en el servidor y en cada estación.

Los cables es el medio físico a través del cual viaja la información entre los componentes físicos de la red.

Sistema operativo local es el software encargado de controlar la comunicación con todos los elementos internos de la estación de trabajo.

El sistema operativo de red es el software encargado de controlar la comunicación con todos los recursos de la red así como controlar todos los accesos de los usuarios.

II.2 Tipos de Cableado.

Uno de los elementos más importantes y básico para poder realizar la comunicación en la red es el cableado o medio de transmisión.

Los medios de transmisión de banda base son el cable de par trenzado y el cable coaxial de banda base. Los medios de transmisión de banda ancha son el cable coaxial de banda ancha y el cable de fibra óptica.

Cable de Par Trenzado.

El cable de par trenzado es el cable que se utiliza normalmente en las instalaciones telefónicas y para conectar terminales de telex. Este cable se utiliza también en la transmisión de señales digitales, sobre todo en topologías en anillo, pues en esta configuración se pueden compensar fácilmente, por medio de repetidores, los desequilibrios y las atenuaciones producidas por los hilos. Desde el comienzo de la era del ordenador, este cable se ha utilizado para conectar terminales y otros equipos de transmisión de datos de poca velocidad, al ordenador central. El uso del cable de par trenzado está tan extendido que casi todos los edificios disponen normalmente de una instalación con este tipo de cable.

Como su nombre indica, este cable está compuesto por un par de hilos trenzados entre sí. El grosor de los hilos varía, al igual que el número de vueltas (o trenzados) por pulgada. El trenzado mantiene estables las propiedades eléctricas en toda la longitud del cable y reduce las interferencias creadas por los hilos adyacentes en los cables compuestos por varios pares. Este tipo de cable suele estar compuesto por hilos de cobre. Normalmente, el par trenzado no está blindado o, si lo está, el blindaje suele ser muy reducido; debido a esto el cable es muy ligero y relativamente fácil de instalar.

Cable Coaxial de Banda Base.

El cable coaxial se ha estado usando durante muchos años en la red telefónica, en aplicaciones que requieren prestaciones muy similares a las de una red local. También se usa en sistemas de antenas colectivas de televisión. Hay dos tipos de cables coaxiales: el de banda base y el de banda ancha. Aunque ambos están construidos de forma muy similar, su instalación y aplicación son diferentes.

En el cable coaxial de banda base, el hilo conductor central está rodeado de una malla muy fina de hilos de cobre. El espacio que queda entre el hilo y la malla está aislado para separar los dos conductores y mantener las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas. El cable tiene normalmente un diámetro aproximado de 0.94 mm (3/8 de pulgada).

El cable transporta una sola señal digital a una velocidad de transmisión muy alta, 10 ó 12 megabits por segundo. La frecuencia de transmisión es relativamente baja. Los bits se ponen directamente en el cable sin modulación alguna.

Cable Coaxial de Banda Ancha.

El cable coaxial de banda ancha está construido de forma muy similar al cable coaxial de banda base. Tiene varios diámetros diferentes, con diversos grosores de aislamiento. El cable central está protegido por una malla de hilos de cobre o camisa de aluminio. El espacio que queda entre la parte central y la superficie exterior está lleno de material aislante y todo ello está, a su vez, incluido dentro de una capa aislante protectora.

El cable coaxial de banda ancha puede transportar entre 50 y 100 canales de televisión, o miles de canales de voz y de datos a baja velocidad, entre 9.2 y 50 kilobits por segundo.

Cable de Fibra Óptica.

El cable de fibra óptica es un medio de transmisión que se está comenzando a usar en redes locales. Las señales luminosas se transmiten a través de un cable (guía de ondas) compuesto por fibras de vidrio. Cada filamento tiene un núcleo central de fibra con un alto índice de refracción, rodeado de una capa de material similar con un índice de refracción ligeramente menor. El revestimiento aísla las fibras y evita que se produzcan interferencias entre filamentos adyacentes, al mismo tiempo que proporciona protección al núcleo. Todo el conjunto suele estar protegido por otras capas que no tienen más función que la de proteger dichos filamentos.

Hay diferentes tipos de cables de fibra óptica:

Fibra monomodo.

El diámetro del núcleo o fibra óptica es sumamente fino. Este tipo de fibra proporciona un alto rendimiento, pero hace que resulte muy difícil la conexión del cable a transmisores y a otros dispositivos.

Fibra multimodo de salto de índice o índice escalonado.

Estas fibras contienen un núcleo de alta resolución dentro de un revestimiento de resolución más baja. Las conexiones a otros dispositivos son más sencillas que con los otros tipos de fibra.

Fibra multimodo de índice gradual.

Estas fibras varían de densidad y tal variación reduce la dispersión de las señales. Es el tipo de fibra más popular, ya que se utiliza frecuentemente en telecomunicaciones. Tiene un índice de transmisión muy alto, mayor que los otros dos tipos.

Los segmentos de cable han de estar alineados con una gran precisión para que la señal pase de un segmento al siguiente, debido a que la luz tiende a desplazarse de forma ondulada, en vez de en línea recta, como podría

pensarse. Cuantos mayores son las fluctuaciones de la onda luminosa, mayor pérdida y dispersión tiene la señal. Cuanto más fina es la fibra óptica y más estrecho el foco de luz, más recta se mueve la onda luminosa y, por tanto, mayor será la velocidad de transmisión.

II.3 Cableado Estructurado.

Actualmente, en la construcción de edificios destinados a oficinas corporativas se considera necesario incluir un sistema de cableado estructurado para la formación de redes de voz y datos.

La topología de la red es el arreglo físico del cableado estructural y los componentes usados en la interconexión de computadoras y equipos servidores.

Cuando se diseña una red, los factores más importantes para la elección de la topología son los siguientes:

- El patrón de comunicación entre dispositivos.
- El volumen de información que habrá de transmitirse.
- La necesidad de tolerancia a fallas y trayectorias redundantes.
- La frecuencia con que se agregan o eliminan estaciones a la red.
- El tamaño de la red.
- La importancia de la información que se maneja en red (seguridad de datos).
- La distribución que tendrán los equipos en la oficina.

Los estándares de redes (802.3 para ethernet y 802.5 para token ring), tenían hasta hace algunos años definiciones especificas en cuanto al tipo de cableado que podía usarse. Ahora se tienen nuevos desarrollos para satisfacer las necesidades de los usuarios mientras se mantienen o mejoran las especificaciones técnicas. Por ejemplo, para el estándar 802.3 se puede utilizar una amplia variedad de cables:

- 10BASE2: Cable coaxial delgado.
- 10BASE5: Cable coaxial grueso.
- 1BASE5: Cable par trenzado sin malla (UTP).
- 10BASE-T: Cable par trenzado sin malla (UTP).
- 100BASE-T: Cable par trenzado sin malla (UTP).
- 1000BASE-T: Cable par trenzado sin malla (UTP).
- 10BASE-F: Fibra óptica.
- 10BROAD36: Cable coaxial de banda ancha.

Por cada una de de las familias listadas anteriormente, se necesitan conectores y herramientas especiales en la instalación.

Cada tipo de red (token ring o ethernet), establece sus propias reglas y limitaciones en cuanto a la distancia y el número de nodos, aspectos de suma

importancia al momento de efectuar el diseño. Igualmente para interconectar todas las computadoras a instalarse en el sistema.

Los constantes cambios en la ubicación de los equipos, o la necesidad de contar con diferentes tipos de servicios en los puestos de trabajo (conexiones a redes locales, terminales de equipos mayores como mainframes, líneas telefónicas digitales o analógicas, etcétera) ocasionaban gastos elevados de materiales y mano de obra. Además de la suspensión total del servicio hasta que se completaban las modificaciones.

Las Ventajas del Cableado Estructurado.

Una de las principales ventajas del cableado estructurado radica en que los administradores de las redes de voz y datos pueden realizar cambios en la ubicación o tipo de servicios, aun costo sumamente bajo y sin interrupción del trabajo del resto de los equipos.

A continuación se resume en una tabla las diferencias entre las instalaciones de cableado estructurado contra las normales.

Estructurado:	No estructurado:
Independiente de las aplicaciones.	Tiende a ser dependiente de las aplicaciones.
Permite el movimiento del equipo sin recablear.	Se recablea al mover el equipo.
Facilidades para reconfigurar alambrado y equipo.	Difícil hacer reconfiguraciones.
Diseño modular.	No modular.
Permite aislar equipo para la detección de fallas.	Difícil localización de fallas.
Soporta varias plataformas.	Dependiente del tipo de red.

Tabla 2.3.1 Comparativo de redes con cableado estructurado contra no estructurado.

El sistema de cableado estructurado consiste en varias familias de componentes que incluyen medios de transmisión (cables), paneles de parcheo para la administración de los servicios y accesorios como conectores, adaptadores y filtros.

Para la instalación de este sistema se emplea una topología en estrella, con lo cual se tienen las siguientes ventajas:

- Es aplicable tanto a sistemas centralizados como a distribuidos.
- Proporciona una configuración flexible para la introducción de nuevos servicios y segmentación de las redes a fin de dividir el tráfico.
- Proporciona puntos centrales para mantenimiento.
- Permite la expansión del cableado a un costo muy bajo.
- Ofrece facilidades para mudarse a otras tecnologías.

Las nuevas definiciones del tipo de cable que las redes pueden usar (ethernet y token ring, por ser las más comunes), permiten que la topología estrella en el cableado estructurado soporte las configuraciones lógicas de redes: punto a punto, bus, anillo y árbol.

Estos edificios cuentan con una vertical. Esta es la zona en donde se instalan todos los dispositivos de interconexión y los paneles de parcheo. Desde ahí se distribuye el cableado hasta los puestos de trabajo, formando así lo que se llama la horizontal.

En esta horizontal se emplea cable de par trenzado sin protección UTP (Unshielded Twisted Pair, por sus siglas en inglés). Existen varias categorías de UTP, conocidas como de nivel 3, 4 o 5. Cada una de ellas presenta características eléctricas diferentes, básicamente de atenuación de la señal y de velocidad de transmisión a una distancia determinada. Actualmente, el mejor es el nivel 5, con el cual fácilmente se pueden proporcionar servicios de voz y datos.

Para la comunicación entre los pisos del edificio, se instala en la vertical fibra óptica, la cual presenta ventajas significativas sobre el cable, ya que es inmune a las interferencias electromagnéticas, posee un ancho de banda del orden de los cientos de Mhz, atenuación casi despreciable en comparación con el cobre y sistemas de redundancia mejorados. Aunque la fibra es lo más recomendable, puede emplearse también el cobre para la comunicación entre pisos.

Otra de las ventajas del cableado estructurado es la facilidad de incorporar sistemas de administración basados en hardware y software que permitan de manera gráfica detectar los problemas en la red justo en el momento en que éstos ocurren, y de obtener información y reportes para prevenirlos.

Mediante estos sistemas de administración, y dependiendo de la inteligencia de los concentradores de cableado instalados en la vertical, es posible la habilitación o deshabilitación remota de los servicios, por ejemplo para la corrección de fallas o por razones de seguridad.

III. Protocolos de Comunicación.

Cuando dos partes desean intercambiar información es necesario establecer algunas reglas por medio de las cuales pueda tener lugar tal intercambio y asegurar que la información se ha recibido correctamente. Estas reglas son en esencia un protocolo de comunicaciones.

Un protocolo de comunicación es, por tanto, un conjunto de reglas aceptadas por las partes implicadas en la comunicación para poder asegurar que la información que se intercambia se está recibiendo correctamente.

Tareas funcionales de un protocolo.

Hay muchos tipos diferentes de protocolos, algunos sólo se encargan del intercambio de mensajes entre dos partes conectadas a un único enlace, y otros se encargan de la comunicación entre ordenadores conectados a una red. Cada uno de estos protocolos tiene obligaciones diferentes, pero todos ellos incluyen de un modo u otro los siguientes elementos.

1.- Control de Errores.

Todo protocolo tiene un mecanismo de detección de errores que permiten a un receptor detectar si se han producido errores durante la transmisión. Si se ha detectado un error, es necesaria alguna acción para que el receptor obtenga una copia correcta de la información transmitida. Esta acción se conoce como "control de errores". Un ejemplo muy simple es el de un usuario de una terminal que está conectado a un ordenador que usa transmisión asíncrona. Cuando el ordenador recibe un carácter, escribe la secuencia de bits (en forma de carácter) en la pantalla del ordenador o terminal. Si este no es el carácter que quería el usuario, éste puede enviar un carácter especial (por ejemplo un carácter de borrado) para informar al ordenador que ignore el último carácter recibido. Sin embargo, la mayoría de los sistemas de comunicación requieren que este mecanismo esté incorporado, en vez de tener que ser proporcionado por un "usuario inteligente".

2.- Control de Secuencia.

La mayoría de los sistemas de comunicación no intercambian un solo mensaje, sino una serie completa de mensajes, normalmente en una secuencia determinada. Además, el mensaje puede estar dividido en varios bloques más pequeños o paquetes y estos paquetes tienen que estar en una determina secuencia para poder formar el mensaje adecuado. Si un determinado mensaje o paquete se "pierde" o envía a otro lugar de la red, podría suceder que el mensaje fuese recibido en la secuencia incorrecta. Por tanto, el protocolo ha de incluir algún tipo de identificación de secuencia que designe el orden en el que deben ser procesados en el destino el mensaje o los paquetes, puesto que el orden en que han sido recibidos puede ser diferente.

3.- Control de Flujo.

Si en un sistema de comunicaciones la fuente genera información más rápido de lo que el receptor puede aceptarla, se necesita alguna forma de controlar la producción o flujo de información. El control de flujo es la gestión del flujo de información desde la fuente hasta el destino. Esto puede ser muy importante cuando dos ordenadores se comunican por medio de una red de comunicaciones intermedia. La red sólo puede almacenar una cantidad de información limitada, por lo que es necesario controlar la salida del ordenador para que la red no se congestione.

4.- Control de Sincronización.

El control de sincronización se encarga de la acción a tomar en caso de que se detenga el flujo de mensajes. Algunos protocolos, por ejemplo, requieren que después de enviar un mensaje el emisor reciba un “acuse de recibo” de la recepción correcta del mensaje antes de enviar el mensaje siguiente. Si no llega el acuse de recibo (por ejemplo, la línea ha sido desconectada o ha fallado el nodo receptor), el emisor puede esperar para siempre y quedaría bloqueado. Una sincronización es un mecanismo por el que, después de transmitir un mensaje que requiere una respuesta, se pone en marcha un reloj. Si no se recibe una respuesta al cabo de un determinado período de tiempo, la comunicación se “sincroniza”. El mensaje puede entonces ser retransmitido o se abandona la comunicación.

El tiempo de sincronización ha de ser el adecuado para el sistema de comunicaciones. En un sistema punto a punto simple que conecte dos ordenadores, el tiempo de sincronización puede ser muy pequeño. En una red de comunicaciones grande, sin embargo, si los nodos resultan congestionados, la respuesta puede quedar retrasada, y si la sincronización es demasiado pequeña, el emisor podría retransmitir el mensaje innecesariamente, incrementando la congestión de la red.

5.- Control de Puesta en Marcha.

El control de puesta en marcha es el responsable de inicializar la transmisión en un sistema que ha estado parado. Lo mismo que en una conversación telefónica, primero es necesario establecer el enlace físico y después intercambiar información de control para comprobar si en cada extremo se encuentran las partes correctas.

Con un enlace muy corto entre, digamos, un terminal y un ordenador, estas funciones se pueden realizar intercambiando señales en las líneas de control, lo cual se conoce como establecimiento de comunicación.

Cuando los dispositivos que transmiten son ordenadores, el control de puesta en marcha se logra intercambiando un conjunto de mensajes de control o supervisores, o intercambiando paquetes de información. Con un enlace halfduplex, este proceso establece también quién es el maestro quién el

esclavo, por lo que tiene que haber un mecanismo adicional que invierta sus papeles durante el proceso de comunicación.

Niveles de Protocolo.

Cada uno de los niveles o capas del modelo de referencia ISO hace referencia a un protocolo que define un conjunto de reglas, las cuales usan ese nivel para poder comunicarse con un nivel similar del sistema remoto, a continuación veremos algunos ejemplos de protocolos del nivel físico.

Establecimiento de comunicación en el bus de entrada/salida.

Un bus de E/S típico consta de tres tipos de líneas: líneas de datos, líneas de direcciones y líneas de control. Algunas de las líneas de control se usan para coordinar transferencias de datos a través del bus, y éstas son las que vamos a explicar aquí. En las transmisiones asíncronas, el hecho de que no haya un reloj común con el que se puedan relacionar las actividades, significa que es necesario que haya un intercambio de señales, lo que se conoce como saludo. Hay dos líneas de control de sincronización, las llamadas “preparado” y “aceptado”. El protocolo de establecimiento de comunicación hace lo siguiente.

La CPU pone la información de dirección y de modo (entrada o salida) en las líneas apropiadas. Después, indica que lo ha hecho por medio de una señal en la línea preparado. Cuando el dispositivo direccionado recibe la señal de preparado, realiza la operación asignada e indica el final de la misma por medio de una señal en la línea aceptado. La CPU, al recibir la señal aceptado, quita las señales de dirección, de modo y de preparado, y en el caso de una operación de entrada, pone los datos en su buffer de entrada. La sincronización de estas operaciones para una transferencia de salida se muestra en la figura 3.1.

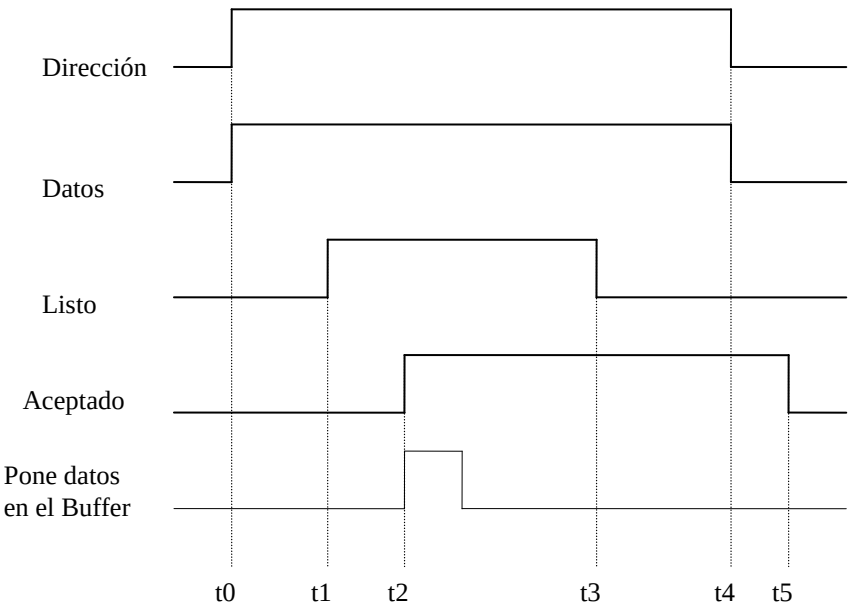


Figura 3.1. Sincronización para una transferencia de salida.

Puesto que ésta es una operación de salida, la CPU pone los datos de salida en las líneas de datos al mismo tiempo que la información de dirección y de modo. El dispositivo direccionado pone los datos en su buffer cuando recibe la señal preparado. La espera t1 - t0 se utiliza para permitir la posibilidad de un desvío y para que los dispositivos efectúen la decodificación de la dirección. También activa la señal aceptado para indicar que ha aceptado los datos. Al recibir la señal aceptado, la CPU corta la de preparado. Después de esto, la CPU quita del bus las señales de datos, de dirección y de modo y cuando el interfaz de dispositivo detecta la transición de la señal preparado quita la señal aceptado. Las señales preparado y aceptado proporcionan un esquema de detección de errores. Si la señal aceptado no se recibe dentro de un plazo de tiempo especificado después de activar la señal preparado, la CPU asume que se ha producido un error. Esto podría hacer que se ejecutara una rutina de error.

Protocolo de Interfaz X21.

A medida que las redes de datos públicas (PDN)-redes establecidas y administradas por una administración nacional de redes específicamente para la transmisión de datos - comenzaron a aparecer, y como éstas a veces necesitaban conectar equipos de distintos fabricantes, estaba claro que tenia que haber algún acuerdo nacional e internacional sobre estándares de interfaces. El CCITT estableció un conjunto de estándares aceptados internacionalmente para usarlos en las redes públicas de datos conocidos como recomendaciones de la serie X. Hay una serie de protocolos conocidos como X25, que han sido definidos para facilitar la comunicación de equipo terminal de datos con una red de datos conmutada de paquetes. En el nivel más bajo del X25 hay un estándar de interfaz, que define el interfaz físico para comunicación con una red totalmente digitada, llamado X21. Puesto que aún hay muchas redes analógicas en uso, se ha definido un segundo estándar de interfaz, conocido como el X21 (bis), para ser utilizado con redes analógicas.

Principio de Protocolos de Enlace de Datos.

Control de errores.

Los diversos esquemas de detección de errores permiten a un receptor detectar cuándo se ha producido un error, pero no disponen de mecanismos para corregirlo. La combinación de un mecanismo de detección de errores y algún medio para corregirlos se conoce como control de errores. Hay dos mecanismos básicos que se usan frecuentemente para manejar la corrección de errores: Comprobación por eco y solicitud de recepción automática (ARQ).

Comprobación por Eco.

La comprobación por eco hace que el receptor devuelva al transmisor los datos que ha recibido. Si el transmisor recibe los mismos datos que ha enviado, asume que éstos han sido recibidos correctamente. Aunque éste es un concepto muy simple, consume mucho ancho de banda, puesto que todo se transmite dos veces. Este sistema se usa principalmente en sistemas

compartidos terminal-ordenador asíncrono. Cuando el usuario escribe un carácter en el terminal, ese carácter no aparece en el terminal, sino que es transmitido al ordenador, el cual lo devuelve para que pueda aparecer en la pantalla y el usuario lo vea. Si el carácter que aparece en la pantalla no es el que quería enviar, el usuario puede enviar un carácter al ordenador indicando que debe ignorar el último carácter enviado.

En realidad, este mecanismo es simple en lo que se refiere al ordenador. Toda la comprobación y corrección de errores la efectúa un usuario inteligente en el terminal. Si el mecanismo de corrección ha de ser automático, entonces se debe usar otro sistema, como el ARQ.

Solicitud de Repetición Automática (ARQ)

La comprobación por eco depende del usuario inteligente que coteja el carácter recibido con el carácter transmitido y lo retransmite si contiene un error. Esta misma función se puede programar en el transmisor en las comunicaciones ordenador-ordenador, pero el método desperdicia mucho ancho de banda, pues todo se transmite dos veces.

Una mejora obvia sobre la transmisión de todo dos veces es que el receptor informe al transmisor cuando se ha detectado un error y pida que se transmitan de nuevo los datos, de aquí el nombre de “solicitud de repetición automática”. Puesto que el bloque de datos que contiene el error se elimina y se retransmite de nuevo, parece que esto funcionaría mejor con bloques lo más pequeños posible. Sin embargo, para poder utilizar eficientemente el canal de transmisión, se necesita una gran velocidad de proceso para comprobar los bits, lo que explica la necesidad de un bloque de tamaño grande. Por tanto, la solución es siempre una decisión importante, aunque la cantidad de almacenamiento disponible en el receptor puede tener un papel principal.

Hay dos mecanismos ARQ de uso común: RQ de espera y RQ continua.

RQ de Espera.

El transmisor envía un solo bloque de datos (incluyendo los bits de comprobación apropiados) y después espera recibir un acuse de recibo (de aquí el nombre de RQ de espera, porque el transmisor está inactivo mientras el receptor comprueba los datos recibidos y enviados y envía un acuse de recibo).

El receptor comprueba el bloque de datos en la recepción y, si no hay errores, devuelve un acuse de recibo positivo (es decir, un carácter ACK del conjunto de caracteres ASCII). Si se detecta un error, el receptor ignora ese bloque y devuelve un acuse de recibo negativo. Si el bloque no llega jamás (o si su formato contiene tantos errores que el receptor no lo reconoce) no se devuelve el acuse de recibo.

Si el transmisor recibe un acuse de recibo positivo, entonces transmite el siguiente bloque de datos. Si recibe un acuse de recibo negativo, entonces retransmite el mismo bloque de datos. Si no recibe ningún acuse de recibo en

el plazo de tiempo especificado también retransmite el mismo bloque. Después de un número determinado de fallos consecutivos con el mismo bloque, el transmisor asume que el receptor no puede continuar y corta la comunicación. Puede haber ocasiones en las que el transmisor vuelve a retransmitir el bloque antes de que el receptor tenga posibilidades de devolver un acuse de recibo, en cuyo caso se transmite una copia doble del mismo bloque de datos. Para permitir que el receptor detecte estos datos duplicados, el bloque de datos contiene normalmente algún tipo de número de orden.

La ventaja de la RQ de espera es que el transmisor y el receptor sólo necesitan tener espacio suficiente para un bloque, por lo que las necesidades de almacenamiento de cada extremo se reducen al mínimo. El sistema es, además, relativamente simple. El inconveniente es que desperdicia ancho de banda, pues el transmisor está parado durante el tiempo siguiente:

Tiempo de propagación de un bloque + Tiempo que tarda el receptor en procesar un bloque + Tiempo que tarda el receptor en enviar un acuse de recibo + Tiempo que tarda el transmisor en procesar el acuse de recibo.

Si esté tiempo de espera es pequeño comparado con el tiempo de transmisión de un bloque, entonces su eficiencia aumenta, y la simplicidad del sistema puede hacerlo muy atractivo. En muchos casos, sin embargo, su inherente pérdida de tiempo (en espera) hace que resulte muy ineficiente.

RQ Continua.

El problema de la RQ de espera es el tiempo que el transmisor desperdicia esperando recibir un acuse de recibo del receptor. Una mejora importante es que el transmisor envía continuamente bloques de datos sin espera al acuse de recibo. A medida que el receptor recibe bloques, realiza las comprobaciones de error apropiadas y acusa recibo igual que en el esquema RQ de espera. La diferencia esencial es que cuando el transmisor recibe un acuse de recibo de un bloque, ya habrá transmitido algunos. Estos tienen dos implicaciones para el remisor:

- Cada bloque necesita un número de orden y cada acuse de recibo necesita incluir el número de orden del bloque del que está acusando recibo, de forma de que si el bloque necesita ser retransmitido, el transmisor sabe cuál tiene que enviar.
- El transmisor necesita guardar una copia de todos los bloques que transmite, por si fuese necesario retransmitir alguno de ellos. La recepción de un acuse de recibo positivo (con su número de orden) se puede usar para eliminar ese bloque de datos en particular de esta área de almacenamiento.

Desde el punto de vista del receptor, la presencia de un error, que dé como resultado la retransmisión de un bloque de datos, significa que los bloques se van a recibir fuera de orden, puesto que el transmisor va a seguir enviando bloques hasta que reciba un acuse de recibo negativo.

Hay dos formas de solucionar esta situación. La primera de ellas es la retransmisión selectiva. Con este procedimiento sólo se retransmite el único bloque incorrecto. Su funcionamiento se puede describir de la siguiente manera:

1) Supongamos que el bloque que tiene el número de orden N tiene errores.

2) El receptor devuelve un bloque de acuse de recibo (un ACK+número de orden) por cada bloque recibido correctamente.

3) Entonces el transmisor recibe bloques de acuse de recibo de los bloques N-2, N-1, N+1, N+2...

4) Al recibir el bloque de acuse de recibo del bloque N+1, el transmisor detecta que éste no es el orden correcto y que por tanto no se ha recibido acuse de recibo del bloque N. Entonces deberá retransmitir el bloque N antes de transmitir el bloque siguiente en el orden original.

Observe que no hay necesidad de un acuse de recibo negativo. El transmisor sabe que un bloque no ha sido recibido correctamente al detectar un acuse de recibo con el orden incorrecto. Esto aún hace necesario que haya un mecanismo de sincronización en caso de que el flujo de acuses de recibo pare de repente, o en caso de que el transmisor no tenga más bloques para enviar por el momento, de forma que no haya acuses de recibo de vuelta.

El receptor necesita almacenar los bloques recibidos por dos razones:

1) Para poder transmitir un mensaje completo (el cual pudo haber sido dividido en bloques o paquetes) en el orden correcto, puesto que algunos bloques pueden no estar en orden.

2) Si el bloque de acuse de recibo contiene errores y por lo tanto no es reconocido, el efecto es que el transmisor volverá a retransmitir ese bloque. Puesto que el receptor puede detectar que se trata de un duplicado (por el número de orden), éste será ignorado (pero, de todos modos, necesita devolver un acuse de recibo para satisfacer al transmisor).

El problema principal asociado con la retransmisión selectiva es la recepción de bloques que no están en orden. El número de bloques que el receptor tiene que guardar no se conoce, y si el receptor está haciendo esto para muchos mensajes, el almacenamiento necesario podría ser bastante grande. Por esta razón, si los mensajes han de pasarse con sus bloques en orden, es más conveniente el otro método, Volver-a-N.

Con este mecanismo, cuando el transmisor es informado de que se ha recibido incorrectamente un bloque, lo retransmite y continúa la transmisión desde ese punto, aunque ya se hayan transmitido algunos bloques.

Su funcionamiento es el siguiente:

1) Se supone que el bloque que tiene el número de orden N tiene un error.

2) El receptor devuelve un bloque de acuse de recibo por cada bloque recibido correctamente.

3) Al recibir un bloque con error, el receptor devuelve un acuse de recibo negativo (NACK), más el número de orden del primer bloque recibido correctamente (N-1). También ignorará todos los bloques recibidos desde el bloque N-1.

4) El transmisor, al recibir un código NACK, retransmitirá todos los bloques a partir del bloque N y continuará la transmisión.

Comparado con la retransmisión selectiva, este mecanismo no necesita mucho espacio de almacenamiento en el receptor, pero de vez en cuando hace que se retransmitan bloques que han sido recibidos correctamente. Es decir, a veces desperdicia ancho de banda. Sin embargo, debido a las mínimas necesidades de almacenamiento, éste es un método muy común en instalaciones en las que es esencial que los bloques se pasen en orden.

III.1 Protocolos de Comunicación más Comunes.

Tipos de Protocolos.

Los protocolos de enlaces de datos han de ser capaces de detectar los errores contenidos en secuencias de bits de las que se desconoce el contenido o significado. No hay ningún método que pueda detectar errores en una secuencia de bits arbitraria continua. Para poder detectar errores, los datos se dividen en bloques y el bloque de datos se transmite junto con los caracteres de control de errores (por ejemplo, una suma de comprobación CRC). Otro término común para estos bloques de datos es el de trama.

Se han desarrollado diversos esquemas para separar datos y formar esquemas listos para ser transmitidos. El propósito de todos ellos es preservar la transparencia de los datos del usuario. Esto significa que si se usan caracteres o secuencias de bits especiales para dar un significado al protocolo, es necesario incorporar otro mecanismo para permitir que la misma secuencia de bits sea transmitida como parte de los datos del usuario sin producir confusión. A continuación se describen tres tipos de protocolos, los cuales se representan en la figura 3.1.1.

Orientado a Caracteres.

Este tipo de formato de estructura asume que el dato enviado es una secuencia de caracteres (grupos de ocho bits) y usa caracteres especiales para indicar el comienzo de la trama, el final de esta y otra información del protocolo. La transparencia se obtiene del modo siguiente: el comienzo de la trama es un par de caracteres de DLE y STX (caracteres ASCII), el final de la trama esta

indicada por DLE y ETX. Para evitar que se produzca una posible coincidencia de esta secuencia de bits en los datos del usuario, el transmisor inserta otro carácter DLE después de cada código DLE que haya en los datos del usuario. El receptor reconoce el final de la trama cuando encuentra los caracteres DLE y ETX. Cada vez que aparezca un carácter DLE (después del comienzo de la trama) éste irá seguido de otro DLE, que suprimirá el receptor.

Orientado a Número de Bytes.

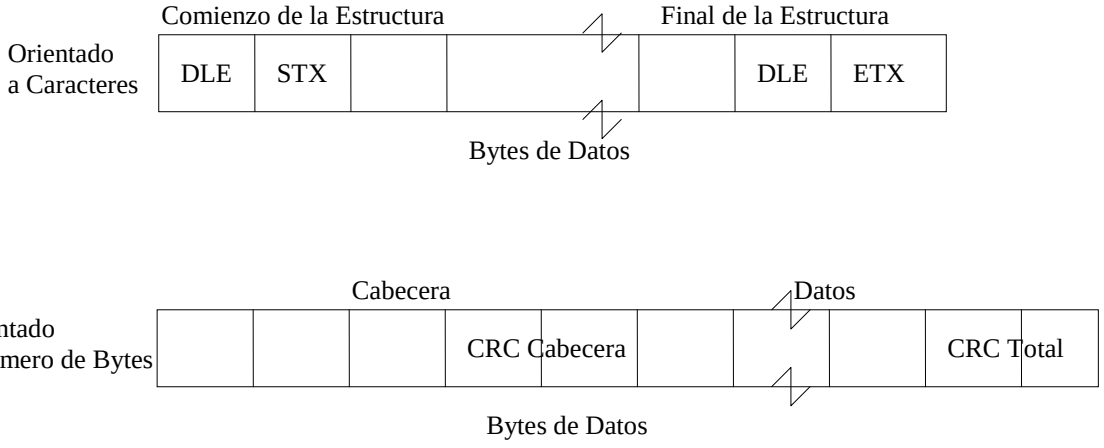
Este formato de trama pone delante de los bytes de datos una cabecera que contiene, entre otra información, un número que indica el número de caracteres (bytes) que hay en el campo de datos de la trama. El receptor sólo tiene entonces que contar el número de bytes de datos, comparándolo continuamente con el número de campo para determinar así el final de la trama. Puesto que la información de la cabecera se ha de utilizar correctamente antes de encontrar el final de la trama, la cabecera termina normalmente con una suma de comprobación CRC, que es confirmada por el receptor antes de comenzar a leer el resto de la trama.

Orientado a Bits (relleno de bits).

Con un formato de trama orientado a bits, el campo de datos no tiene que ser un número entero de bytes (aunque a menudo lo es). El comienzo y el final de la trama están delimitados por un indicador especial de ocho bits consiste en la siguiente secuencia de bits:

01111110

La transparencia (asegurarse de que esta secuencia de bits no se produce en los datos) la obtiene el transmisor insertando un bit cero después de cualquier grupo contiguo de cinco bits uno (1) (además de indicador final que transmite después de haber sido transmitidos todos los bits de datos). El receptor suprime los ceros que haya después de cinco unos (1) contiguos. Esta técnica se conoce como “relleno de bits”.



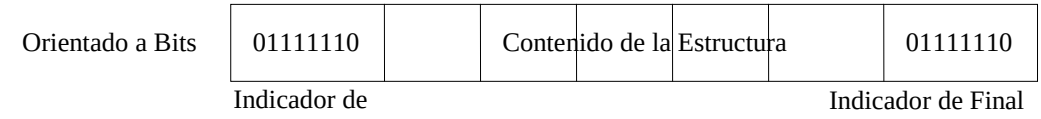


Figura 3.1.1 Estructura de protocolos orientados a caracteres, número de byte y bits.

Estándares de la Capa Física.

Existe una variedad de protocolos para la capa física, algunos muy comunes como el RS-232C y el RS-449 de EIA (Asociación de Industrias Electrónicas de los E.U.A.), secciones de las recomendaciones X.21 y V.24 del CCITT, porciones de los protocolos recomendados por IEEE en su serie 802, los cuales aplican para las redes locales, y los estándares militares que emite el departamento de la defensa de los E.U., en la serie MILSTD-188.

Estos estándares especifican factores tales como circuitos de intercambio y control, niveles de voltajes eléctricos, impedancias, velocidades de transmisión, formatos de conectores y las distancias de transmisión aplicables a la interconexión del DTE con el DCE (Equipo Terminal de Datos, y Equipo de Comunicación de Datos, respectivamente), a esta interconexión se le llama también, "interfaz del usuario con la red".

La Capa de Enlace de Datos.

Los propósitos básicos de la capa de enlace de datos, son: establecer, mantener, y liberar las conexiones entre nodos (cualquier punto de la red en el cual se conmutan datos). Los dispositivos ubicados en los nodos de comunicación, pueden ser terminales, computadoras, equipos de comunicación o cualquier otro considerable dentro de la denominación genérica de equipo de comunicación de datos (DCE).

La estructura básica de un protocolo de control de enlace se deriva de la naturaleza del medio de transmisión utilizado, y toma en cuenta la aplicación y origen de la información, esto es, los requerimientos del usuario, por medio del siguiente conjunto de funciones, que es común a todos los protocolos de enlaces de datos.

1.- Inicialización.
2.- Mecanismo de segmentación (partición) de información.
3.- Verificación de error.
4.- Sincronización de datos.
5.- Control del flujo de datos.
6.- Recuperación desde una condición anormal.
7.- Terminación

Los protocolos de enlace de datos, han evolucionado hacia dos principales clases: "orientados a caracteres" y "orientados a bits".

Los "orientados a caracteres", utilizan un subconjunto definido de estructuras de caracteres de un conjunto predeterminado, realizando la conversión a un formato apropiado para datos, para supervisar su intercambio a través de un en lace de transmisión. Para lo cual, se definen tres tipos de caracteres:

1.- Gráficos, para representar símbolos.
2.- De control, para controlar un ETD.
3.- De comunicación, para controlar funciones en una computadora, tales como la sincronización y la manipulación de mensajes.

Como ejemplo de los más utilizados, podemos mencionar al conjunto ASCII de 7 bits más el bit de paridad, y al EBCDIC de 8 niveles.

En cambio, los protocolos "orientados a bits", los cuales, por su mayor confiabilidad son en la actualidad, los más utilizados. No dependen de caracteres de control, sino de la ubicación de los bits, en campos o bloqueos específicos. Se tienen dos estándares que se emplean en las comunicaciones modernas de datos, son:

ADCCP de ANSI (Advanced Data Comunication Control Procedure).

HDLC de ISO (High-Level Data Link Control).

Los hay también, los generados por fabricantes como IBM, el denominado SDLC (Synchronous Data Link Control).

Protocolos de Acceso de las Redes Locales.

La familia 802 del IEEE, agrupa las funciones de los protocolos de enlaces de datos en una subcapa llamada Control de Enlace Lógico (LLC, de Logical Link Control). Hay una función adicional, que debe realizarse en las redes que tienen muchas estaciones, y es administrar el acceso al medio de transmisión. Esta se realiza en una subcapa separada a la cual se le llama Control de Acceso al Medio (MAC, de Media Access Control). Estos protocolos de acceso, se pueden agrupar en 5 categorías.

1.- Técnicas de Asignación Fija. Ejemplos de ellas son: De Acceso Múltiples por División en Tiempo (TDMA), y de Accesos Múltiples por División en Frecuencia (FDMA).

2.- Técnicas de Acceso Aleatorio. Por ejemplo, la de Accesos Múltiples por Detección de Portadora (CSMA) con sus variantes.

3.- Técnicas de Asignación por demanda con Control Centralizado. Los procedimientos de asignación de canal, se pueden hacer mediante el método de sondeo (polling), en el cual un controlador central pregunta a las terminales si tienen mensajes por enviar; o por técnicas de reservación, en el cual los

requerimientos de canal se inician por el usuario. En ambos casos, un controlador central asigna a los usuarios el espacio, o el tiempo del canal de comunicación.

4.- Técnicas de Asignación por Demanda con Control Distribuido. Son más confiables y de mejor desempeño que las de control centralizado. Por ejemplo, en una topología de anillo, el derecho para acceder al medio, puede ser mediante un patrón de bits con un formato específico, llamado Estafeta de Control (Control Token), que se turna secuencialmente entre los nodos, y cuando uno de ellos tiene algo que enviar, toma la estafeta de control, envía su mensaje y la transfiere el siguiente, que a su vez, la reexpide hasta que llegue a su destino, reiniciándose el ciclo.

5.- Otras Técnicas. En ciertas situaciones, puede ser ventajoso, tener una estrategia de acceso que cambie su naturaleza, conforme a la demanda de tráfico en la red. Por ejemplo, se puede tener una red que utilice CSMA como técnica de acceso, para cargas con tráfico bajo, pero que conmute al esquema de transferencia de estafeta (TOKEN PASSING), al detectarse mensajes frecuentes de colisiones, al crecer la demanda de tráfico de un usuario.

Los Estándares IEEE 802 para Redes Locales.

IEEE, a través de su comité 802, desarrolló una familia de estándares para las redes locales, para promover la conectividad de equipos de diferentes fabricantes. A esta familia se le llamo estándares IEEE 802. Los estándares están en la forma de una arquitectura de comunicaciones de tres capas, que satisface funcionalmente las capas físicas y de enlace de los datos del modelo de referencia OSI. Los estándares 802, definen tres tipos de tecnologías de acceso al medio, y el medio físico asociado, se pueden utilizar en un amplio rango de aplicaciones o sistemas. Las partes componentes son:

802.1 Generalidades, Interconexión, y Administración de Sistemas.

802.2 Control del Enlace Lógico.

802.3 Conductor único (bus) con CSMA/CD.

802.4 Conductor único con estafeta (Token Ring).

802.5 Anillo con estafeta (Token Ring).

802.6 Redes de Área Metropolitana (MANs).

802.7 Grupo de recomendaciones para fibra óptica.

802.9 Redes locales con voz y datos integrados.

El estándar 802.1 describe las relaciones entre diferentes estándares 802, y sus interconexiones con el modelo OSI y los protocolos de alto nivel. Adicionalmente, proporciona indicaciones sobre interconexiones y la

administración de la red. El estándar 802.2 especifica el control de enlace lógico, que es común a los estándares 802.3 al 802.6, el mismo es observado en la figura 3.1.2

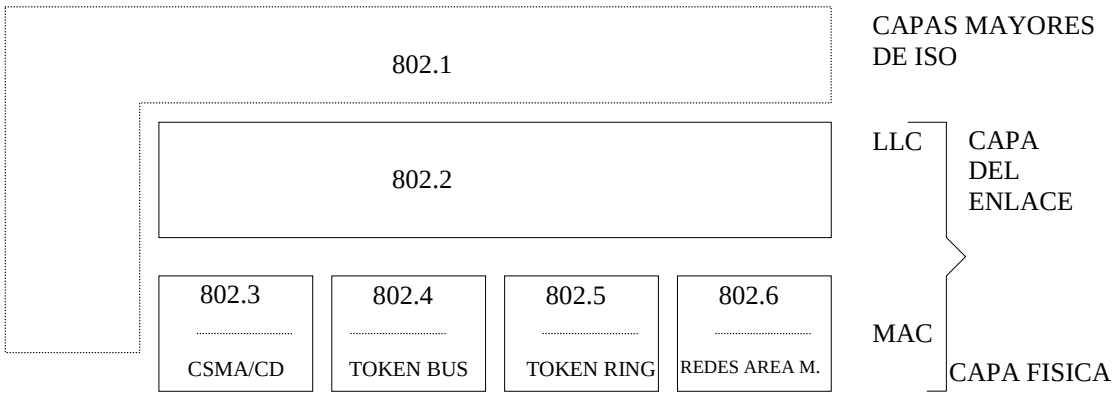


Figura 3.1.2 Relación del estándar 802 y el modelo OSI.

III.2 Protocolo de Comunicación TCP/IP.

III.2.1 Historia de TCP/IP.

El protocolo de comunicación TCP/IP tuvo su origen en una organización gubernamental llamada Advanced Research Project Agenci (ARPA) en la década de los 60's. ARPA, era una agencia del departamento de defensa de los Estados Unidos, dedicada a la búsqueda y experimentación de soluciones que proporcionaran interoperabilidad entre diferentes tipos de computadoras. En 1969 ARPANET fue el resultado de estos experimentos. ARPANET se extendió eventualmente por todo el país y formo la principal red hoy conocida como INTERNET.

La Defense Advanced Research Proyect Agency (DARPA) fue la sucesora de ARPA en 1971, y fue puesta ARPANET en manos de esta. DARPA se enfoco a buscar y experimentar usando tecnología packet-switching enfatizando en los satélites y tecnología de radio para mecanismos de transporte.

En 1973, la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA), de los Estados Unidos, inició un programa para la investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El proyecto tenía por objetivo la interconexión de redes, por lo que se le denominó "Internetting", y a la familia de redes de computadoras que surgió de esta investigación se le denominó "Internet". Los protocolos desarrollados se denominaron el Conjunto de Protocolos TCP/IP, que surgieron de dos conjuntos previamente desarrollados;

los Protocolos de Control de Transmisión (Transmition Control Protocol) e Internet (Internet Protocol).

III.2.2 Componentes de TCP/IP.

Conjunto de Protocolos TCP/IP
Su relación con el Modelo OSI

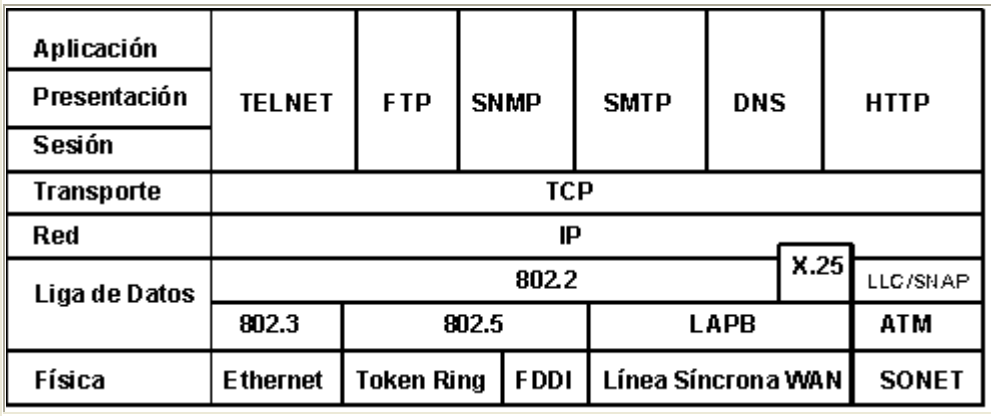


Figura 3.2.2.1 Conjunto de protocolos TCP/IP y su relación con el modelo OSI.
TCP = TRANSFER CONTROL PROTOCOL
IP = INTERNET PROTOCOL

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implementación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en TCP/IP proponen cuatro capas en las que las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Liga de Datos y Física son vistas como la capa de Interface a la Red. Por tal motivo para TCP/IP sólo existen las capas Interface de Red, la de Intercomunicación en Red, la de Transporte y la de Aplicación, figura 3.2.2.2. Como puede verse TCP/IP presupone independencia del medio físico de comunicación, sin embargo existen estándares bien definidos a los nivel de Liga de Datos y Físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo TCP/IP deben considerarse la capa de Interface de Red; siendo los más usuales el proyecto IEEE802, Ethernet, Token Ring y FDDI.

Modelo de capas de TCP/IP

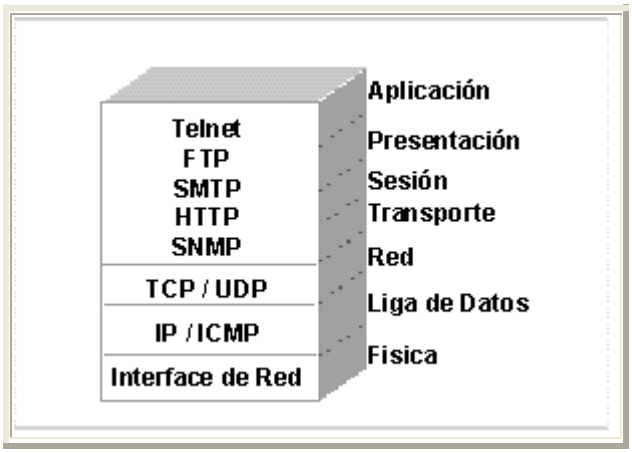


Figura 3.2.2.2 Modelo de capas TCP/IP

Capa de Aplicación.	Invoca programas que acceden servicios en la red. Interactúan con uno o más protocolos de transporte para enviar o recibir datos, en forma de mensajes o bien en forma de flujos de bytes.
Capa de Transporte.	Provee comunicación extremo a extremo desde un programa de aplicación a otro. Regula el flujo de información. Puede proveer un transporte confiable asegurándose que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota, esto lo hace añadiendo identificadores de cada una de las aplicaciones. Realiza además una verificación por suma, para asegurar que la información no sufrió alteraciones durante su transmisión.
Capa Internet.	Controla la comunicación entre un equipo y otro, decide qué rutas deben seguir los paquetes de información para alcanzar su destino. Conforma los paquetes IP que será enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.
Capa de Interface de Red.	Emite al medio físico los flujos de bit y recibe los que de él provienen. Consiste en los manejadores de los dispositivos que se conectan al medio de transmisión.

Tabla 3.2.2.1 Descripción de las capas TCP/IP

Arquitectura de Interconexión de Redes en TCP/IP

Metas

- Independencia de tecnología de conexión a bajo nivel y la arquitectura de la computadora.
- Conectividad Universal a través de la red.

- Reconocimientos de extremo a extremo.
- Protocolos de Aplicación Estandarizados.
- Arquitectura de Interconexión de Redes en TCP/IP Características
- Protocolos de no conexión en el nivel de red.
- Conmutación de paquetes entre nodos.
- Protocolos de transporte con funciones de seguridad.
- Conjunto común de programas de aplicación.

- Arquitectura de Interconexión de Redes en TCP/IP Interconexión de Redes
- Las redes se comunican mediante compuertas.
- Todas las redes son vistas como iguales.

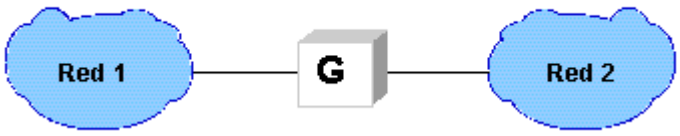


Figura 3.2.2.3 Interconexión de redes.

Para entender el funcionamiento de los protocolos TCP/IP debe tenerse en cuenta la arquitectura que ellos proponen para comunicar redes. Tal arquitectura ve como iguales a todas las redes a conectarse, sin tomar en cuenta el tamaño de ellas, ya sean locales o de cobertura amplia. Define que todas las redes que intercambiarán información deben estar conectadas a una misma computadora o equipo de procesamiento (dotados con dispositivos de comunicación); a tales computadoras se les denomina compuertas, pudiendo recibir otros nombres como enrutadores o puentes.

III.2.3 Direcciones TCP/IP.

- Direcciones IP
- Longitud de 32 bits.
- Identifica a las redes y a los nodos conectados a ellas.
- Especifica la conexión entre redes.
- Se representan mediante cuatro octetos, escritos en formato decimal, separados por puntos, figura 3.2.3.1.

Para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión. Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) de pendiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección internet o dirección IP, cuya longitud es de 32 bits. La dirección IP

identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red, figura 3.2.3.2.

Clases de Direcciones IP

Clases	Número de Redes	Número de Nodos	Rango de Direcciones IP
A	127	16,777,215	1.0.0.0 a la 127.0.0.0
B	4095	65,535	128.0.0.0 a la 191.255.0.0
C	2,097,151	255	192.0.0.0 a la 223.255.255.0

Figura 3.2.3.1 Clases de direcciones IP

Figura 3.2.3.2 Bits de la dirección IP

Tomando tal cual está definida una dirección IP podría surgir la duda de cómo identificar qué parte de la dirección identifica a la red y qué parte al nodo en dicha red. Lo anterior se resuelve mediante la definición de las "Clases de Direcciones IP". Para clarificar lo anterior veamos que una red con dirección clase A queda precisamente definida con el primer octeto de la dirección, la clase B con los dos primeros y la C con los tres primeros octetos. Los octetos restantes definen los nodos en la red específica.

Subredes en IP

Las Subredes son redes físicas distintas que comparten una misma dirección IP.

Deben identificarse una de otra usando una máscara de subred.

La máscara de subred es de cuatro bytes y para obtener el número de subred se realiza una operación AND lógica entre ella y la dirección IP de algún equipo.

La máscara de subred deberá ser la misma para todos los equipos de la red IP.

Se ha mencionado que el enrutamiento sirve para alcanzar redes distantes. También se señaló que las direcciones IP se agrupan en clases. Ahora bien para cada clase se pueden contar con un número determinados de subredes. Las subredes son redes físicas independientes que comparten la misma dirección IP (es decir aquella que identifica a la red principal). La pregunta entonces es ¿cómo se logra que equipos que comparten el mismo identificador de red pero se sitúan en redes físicas diferentes podrán comunicarse usando compuertas? La solución a este problema es determinando una mascara de dirección.

Subredes en Direcciones IP

- Supóngase que la dirección IP de una equipo es 148.206.257.2
- La máscara de subred es 255.255.255.0
- El equipo por tanto está en la subred 148.206.257.0

Mapeo de Direcciones IP a Direcciones Físicas

Estrategia de Conversión	Observaciones
Estática por Tablas	Alto costo en mantenimiento.
Por aplicación de algoritmos	Pude no lograrse una homogénea distribución de direcciones. Remota posibilidad de duplicación de direcciones. Dificultad de elegir el algoritmo más eficiente.
Dinámica	Se consulta, mediante un sólo mensaje, que se emite a todos los equipos en la red, por el poseedor de cierta dirección IP.

Figura 3.2.3.3 Tipos de mapeo de direcciones IP.

Recordemos que los protocolos TCP/IP están enfocados a la transmisión de paquetes de información, buscando la independencia de la arquitectura de la red. Arquitecturas como la Ethernet logran la comunicación sólo mediante el conocimiento de la dirección física de las computadoras. Así en cada computadora que opere con el protocolo IP debe contar con algún procedimiento para la translación de la dirección IP a la dirección física de la computadora con la que establezca comunicación.

Protocolo de Resolución de Direcciones ARP (Address Resolution Protocol)

Le permite a un equipo obtener la dirección física de un equipo destino, ubicado en la misma red física, proporcionando solamente la dirección IP destino.

Las direcciones IP y física de la computadora que consulta, es incluida en cada emisión general ARP, el equipo que contesta toma esta información y actualiza su tabla de conversión.

ARP es un protocolo de bajo nivel que oculta el direccionamiento de la red en las capas inferiores, permitiendo asignar, a nuestra elección, direcciones IP a los equipos en una red física.

Una conversión dinámica de direcciones Internet a direcciones físicas es la más adecuada, debido a que se obtiene la dirección física por respuesta directa del nodo que posee la dirección IP destino. Una vez que la dirección física se obtiene ésta es guardada en una tabla temporal para subsecuentes transmisiones, de no ser así podría haber una sobrecarga de tráfico en la red debido a la conversión de direcciones por cada vez que se transmitiera un paquete.

Implementación del ARP

La interface de red recibe un datagrama IP a enviar a un equipo destino, en este nivel se coteja la tabla temporal de conversión, si existe una referencia adecuada ésta se incorpora al paquete y se envía.

Si no existe la referencia, un paquete ARP de emisión general, con la dirección IP destino, es generado y enviado.

Todos los equipos en la red física reciben el mensaje general y comparan la dirección IP que contiene con la suya propia, enviando un paquete de respuesta que contiene su dirección IP.

La computadora origen actualiza su tabla temporal y envía el paquete IP original, y los subsecuentes, directamente a la computadora destino, figura 3.2.3.4.

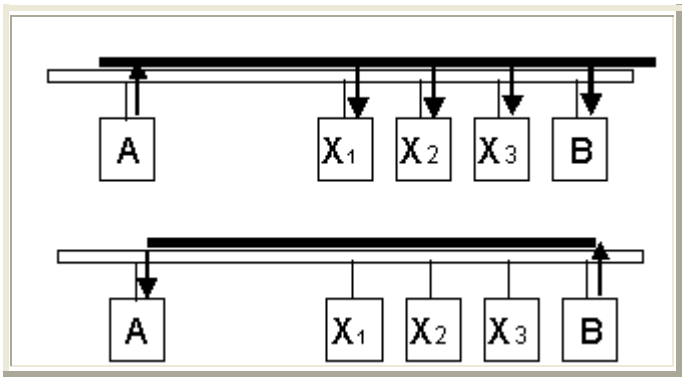


Figura 3.2.3.4 Implementación del ARP

El funcionamiento de ARP no es tan simple como parece. Supóngase que en una tabla de conversión exista un mapeo de una máquina que ha fallado y se le ha reemplazado la interface de red; en este caso los paquetes que se transmitan hacia ella se perderán pues ha cambiado la dirección física, por tal motivo la tabla debe eliminar entradas periódicamente.

Formato de mensaje del ARP

Campo	Descripción
HLEN	Longitud de la dirección del hardware
PLEN	Longitud de la dirección del protocolo
Operación	Indica si es mensaje de consulta o de respuesta
HW Emisor	Dirección Física del Emisor
IP Emisor	Dirección IP del Emisor
HW Destino	Dirección Física del Destino
IP Destino	Dirección IP del Destino

Tabla 3.2.3.4 Descripción del formato de mensaje ARP.

El formato de mensaje de ARP no es fijo, lo que le permite ser usado por otros protocolos de alto nivel.

El ejemplo muestra el formato para un mensaje ARP utilizando Ethernet, en donde la longitud de la dirección física es de 42 bits.

Protocolo Internet (IP)

Características

- Protocolo orientado a no conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones lógicas IP de 32 bits.

- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.
- Realiza el "mejor esfuerzo" para la distribución de paquetes.
- Tamaño máximo del paquete de 65635 bytes.
- Sólo se realiza verificación por suma al encabezado del paquete, no a los datos que éste contiene.

El Protocolo Internet proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable. La orientación a no conexión significa que los paquetes de información, que será emitido a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino. El término no fiable significa más que nada que no se garantiza la recepción del paquete.

Formato del Datagrama de IP

Campo	Descripción
VERS	Versión del IP del datagrama
HLEN	Longitud del Encabezado
Longitud Total	Mide, en Bytes la longuitud del datagrama
Identificador	Identifica los paquetes fragmentados para su reensamble
Flags	Indica si el paquete está fragmentado o no
FOCET	Indica la ubicación de este paquete en uno fragmentado
Opciones	Información usada par administración, longitud variable
Relleno	Ajusta las opciones a 32bits

Tabla 3.2.3.5 Descripción del formato del datagrama de IP.

La unidad de información intercambiada por IP es denominada datagrama. Tomando como analogía los marcos intercambiados por una red física los datagramas contienen un encabezado y un área de datos. IP no especifica el contenido del área de datos, ésta será utilizada arbitrariamente por el protocolo de transporte.

Unidad Máxima de Transferencia MTU (Maximum Transfer Unit)

Indica la longitud de una trama que podrá ser enviada a una red física en particular.

Es determinada por la tecnología de la red física.

Para el caso de Ethernet es de 1500 bytes.

La Unidad de Transferencia Máxima determina la longitud máxima, en bytes, que podrá tener un datagrama para ser transmitida por una red física. Obsérvese que este parámetro está determinado por la arquitectura de la red: para una red Ethernet el valor de la MTU es de 1500 bytes. Dependiendo de la

tecnología de la red los valores de la MTU pueden ir desde 128 hasta unos cuantos miles de bytes.

Fragmentación

La arquitectura de interconexión de redes propuesta por TCP/IP indica que éstas deben ser conectadas mediante una compuerta. Sin obligar a que la tecnología de las redes físicas que se conecten sea homogénea. Por tal motivo si para interconectar dos redes se utilizan medios con diferente MTU, los datagramas deberán ser fragmentados para que puedan ser transmitidos. Una vez que los paquetes han alcanzado la red extrema los datagramas deberán ser reensamblados.

Protocolo de Mensajes de Control de Internet ICMP (Internet Control Message Protocol)

- Reporta sobre destinos inalcanzables.
- Control de flujo de datagramas y congestión.
- Controla los requerimientos de cambio de rutas entre compuertas.
- Detecta rutas circulares o excesivamente largas.
- Verifica la existencia de trayectorias hacia alguna red y el estatus de la misma.

Su función es la de notificar de eventos en los que los paquetes enviados no alcanzaron su destino. Proporciona un medio de transporte para que los equipos compuerta se envíen mensajes de control y error. ICMP no está orientado a la corrección de errores, sólo a su notificación.

Formato del mensaje ICMP

Tipo	Mensaje ICMP
0	Respuesta al eco
3	Destino Inalcanzable
4	Fuente saturada
5	Redirección de ruta
8	Solicitud de Eco
11	Tiempo del datagrama excedido
12	Parámetro problema en datagrama
13	Requerimiento de hora y fecha
14	Respuesta de host y fecha
17	Requerimiento de mascara de dirección
18	Respuesta de mascara de dirección

Tabla 3.2.3.6 Descripción del formato del mensaje ICMP.

El formato de ICMP cambia dependiendo de la función que realice, exceptuando los campos de Tipo, Código y de Checksum. Un 1 en el campo de Protocolo del mensaje de IP indicará que se trata de un datagrama ICMP. La función de un mensaje determinado ICMP estará definida por el campo de Tipo; el campo de Código proporciona información adicional para realizar la función; el campo de Checksum sirve para efectuar una verificación por suma que sólo corresponde al mensaje ICMP.

Enrutamiento de datagramas IP

El enrutamiento se refiere al proceso de determinar la trayectoria que un datagrama debe seguir para alcanzar su destino. A los dispositivos que pueden elegir las trayectorias se les denomina enrutadores. En el proceso de enrutamiento intervienen tanto los equipos como las compuertas que conectan redes (recordar que el termino compuerta es impuesto por la arquitectura TCP/IP de conexión de redes, sin embargo una compuerta puede realizar diferentes funciones a diferentes niveles, una de esas funciones puede ser la de enrutamiento y por tanto recibir el nombre de enrutador).

Tipos de Enrutamiento

Existen dos tipos de enrutamiento; el directo y el indirecto.

Enrutamiento Directo

Debido a que en el enrutamiento directo los datagramas se transmiten de un equipo a otro, en la misma red física, el proceso es muy eficiente. La vinculación entre la dirección física y la IP se realiza mediante el ARP.

Transmisión de datagramas IP entre dos equipos de la misma red física sin la intervención de compuertas. El emisor encapsula el datagrama en la trama de la red, efectuando la vinculación entre la dirección física y la dirección IP, y envía la trama resultante en forma directa al destinatario.

Enrutamiento Indirecto

Las compuertas forman una estructura cooperativa, interconectada. Las compuertas se envían los datagramas hasta que se alcanza a la compuerta que puede distribuirla en forma directa a la red destino.

En el indirecto la transmisión del datagrama se efectúa mediante la intercesión de las compuertas. Aquí la compuerta que actúa como enrutador debe de estar provista de mecanismos para conocer, y por tanto decidir, la trayectoria de la red que se desea alcanzar.

En este direccionamiento un equipo debe enviar a una compuerta el datagrama con destino a una red física distante. La compuerta de la red física envía el datagrama a otras compuertas hasta alcanzar a aquel que puede emitirlo en forma directa a la red destino. La compuerta debe conocer las rutas hacia las diferentes redes externas, ellas pueden utilizar a su vez un enrutamiento

indirecto en el caso de no conocer la ruta a una red específica. Las compuertas conocen las trayectorias a otra red mediante Tablas de Enrutamiento.

Tablas de Ruteo IP

Este es el algoritmo comúnmente utilizado para el enrutamiento de IP. Las tablas de enrutamiento están presentes en todo equipo que almacene información de cómo alcanzar posibles destinos. En las tablas no se almacena la ruta específica a un equipo, sino aquella a la red donde se encuentre. Cada puerto de comunicación de la compuerta debe poseer una dirección IP.

Rutas por Default

Si cada tabla de ruteo conservara información sobre todos los destinos posibles, el espacio sería insuficiente.

Es necesario que con un mínimo de información, el equipo pueda tomar decisiones de ruteo.

Una técnica para mantener tablas de ruteo pequeñas consiste en enviar los datagramas a destinos predeterminados (redes predeterminadas).

Para que en los equipos no exista una tabla excesivamente grande, que contenga todas las rutas a las redes que se interconecta el equipo, es de gran utilidad definir una ruta por default. A través de esta ruta se deberán alcanzar todas las redes destino.
La ruta por default apunta a un dispositivo que actúa como compuerta de la red donde se encuentre ubicado el equipo que la posee.

Enrutamiento entre Compuertas

Arquitectura de Compuerta Núcleo

- Primer esquema de enrutamiento que existió.
- Compuertas de diferentes redes se conectan a una compuerta núcleo.
- La compuerta núcleo es la compuerta por default de las compuertas de las redes locales.
- Las compuertas núcleo no pueden contar con compuertas por default.

Desventajas

- Conveniente sólo para redes administradas centralizadamente.
- Las compuertas núcleo deben almacenar toda la información de las rutas hacia las redes que conectan.
- Complejidad de administración de acuerdo a la complejidad o cambios en la red.

Como se vio en la arquitectura de interconexión de redes de TCP/IP cada par de redes se conectan mediante compuertas. Para que los paquetes alcancen sus redes destino las compuertas deben contar con mecanismos mediante los cuales intercambien la información de las redes que conecta cada uno.

En la Arquitectura de Enrutamiento por Compuerta Núcleo existe una compuerta que centraliza las funciones de enrutamiento entre redes, a esta compuerta se le denomina núcleo.

Cada compuerta en las redes a conectar tiene como compuerta por default a la compuerta núcleo. Varias compuertas núcleo pueden conectarse para formar una gran red; entre las compuertas núcleo se intercambiará información concerniente a las redes que cada una de ellas alcanzan.

La arquitectura centralizada de enrutamiento fue la primera que existió. Sus principales problemas radican no tanto en la arquitectura en sí, si no en la forma en que se propagaban las rutas entre las compuertas núcleo.

Propagación automática de rutas

Establece algoritmos para el intercambio de información entre compuertas.

Contempla el hecho de que las redes son dinámicas.

No obliga a un esquema centralizado de ruteo.

Algoritmos principales: Vector de Distancia y Protocolo de compuerta a compuerta (GGP).

Conforme las complejidades de las redes aumentaron se debió buscar un mecanismo que propagase la información de rutas entre las compuertas. Este mecanismo debía ser automático esto obligado por el cambio dinámico de las redes. De no ser así las transiciones entre las compuertas podían ser muy lentas y no reflejar el estado de la red en un momento dado.

Vector de Distancia

Se asume que cada compuerta comienza su operación con un conjunto de reglas básicas de cómo alcanzar las redes que conecta.

Las rutas son almacenadas en tablas que indican la red y los saltos para alcanzar esa red.

Periódicamente cada compuerta envía una copia de las tablas que alcanza directamente.

Cuando una compuerta recibe el comunicado de la otra actualiza su tabla incrementando en uno el número de saltos.

Este concepto ayudó a definir que tantas compuertas debería viajar un paquete para alcanzar su red destino. Mediante el vector una compuerta podía saber a que otra compuerta enviar el paquete de información, sabiendo que ésta podría no ser la última compuerta por la que el paquete tendría que viajar. Este esquema permite tener varios caminos a una misma red, eligiendo el camino

más corto, es decir aquella compuerta que con menos saltos conduzca a la red destino.

Protocolo de Control de Transferencia

- Proporciona comunicación bidireccional completa mediante circuitos virtuales.
- Desde el punto de vista del usuario la información es transmitida por flujos de datos.
- Confiabilidad en la transmisión de datos por medio de:

- Asignación de números de secuencia a la información segmentada.
- Validaciones por suma.
- Reconocimiento de paquetes recibidos.
- Utiliza el principio de ventana deslizable para esperar reconocimientos y reenviar información.

Proporciona un mecanismo fiable para la transferencia de flujos de información. Aunque está íntimamente relacionado con IP TCP es un protocolo independiente de propósito general. Al ser un protocolo de alto nivel su función es que grandes volúmenes de información lleguen a su destino correctamente, pudiendo recobrar la pérdida esporádica de paquetes.

Fiabilidad en la transferencia de TCP

Cada vez que un paquete es enviado se inicializa un contador de tiempo, al alcanzar el tiempo de expiración, sin haber recibido el reconocimiento, el paquete se reenvía.

Al llegar el reconocimiento el tiempo de expiración se cancela.

A cada paquete que es enviado se le asigna un número de identificador, el equipo que lo recibe deberá enviar un reconocimiento de dicho paquete, lo que indicará que fue recibido. Si después de un tiempo dado el reconocimiento no ha sido recibido el paquete se volverá a enviar. Obsérvese que puede darse el caso en el que el reconocimiento sea el que se pierda, en este caso se reenviará un paquete repetido.

El concepto de la Ventana Deslizante

Se define un tamaño de la ventana, que serían el número de paquetes a enviar sin esperar reconocimiento de ellos.

Conforme se recibe el reconocimiento de los primeros paquetes transmitidos la ventana avanza de posición enviando los paquetes siguientes.

Los reconocimientos pueden recibirse en forma desordenada.

Si el protocolo sólo contara con reconocimientos positivos gran parte de la capacidad de la red estaría desperdiciada, pues no se enviarían más paquetes hasta recibir el reconocimiento del último paquete enviado. El concepto de ventana deslizante hace que exista una continua transmisión de información, mejorando el desempeño de la red.

Protocolo de Datagramas de Usuario

Proporciona de mecanismos primordiales para que programas de aplicación se comuniquen con otros en computadoras remotas.

Utiliza el concepto de puerto para permitir que múltiples conexiones accedan a un programa de aplicación.

Provee un servicio no confiable orientado a no conexión.

El programa de aplicación tiene la total responsabilidad del control de confiabilidad, mensajes duplicados o perdidos, retardos y paquetes fuera de orden.

Este protocolo deja al programa de aplicación a ser explotado la responsabilidad de una transmisión fiable. Con él puede darse el caso de que los paquetes se pierdan o bien no sean reconstruidos en forma adecuada.

Permite un intercambio de datagramas más directo entre aplicaciones y puede elegirse para aquellas que no demanden una gran cantidad de datagramas para operar óptimamente.

IV. Importancia de la Interconectividad de Redes.

IV.1 Conexión entre redes.

No toda la información que se mueve en una red local se genera dentro de la misma área o red. Algunos datos vienen del exterior, ya sea de algunas otros organismos o agencias de servicios que van a estar conectadas con la red de computadoras, los datos pueden haber sido generados en un mainframe o en un miniordenador, o pueden proceder de otra red local que esté conectada con otra red local distante. En cualquier caso, la necesidad de comunicación con el exterior aumenta a medida que también lo hace el número de estaciones y usuarios de la red.

Antes de proceder a establecer conexiones con dispositivos exteriores a la red, es necesario resolver los problemas que existen en las comunicaciones entre dos sistemas distintos (como direccionamiento, formato de los mensajes, control de errores, método de transmisión, etc.). Se necesitan dos tipos de funciones de comunicación:

Funciones básicas: Los servicios de que se ha de disponer en todo momento, incluso cuando las redes que se van a comunicar son del mismo tipo. Aquí se incluye el desvío de mensajes de una red a otra y el direccionamiento de mensajes.

Funciones avanzadas: Los servicios de que se ha de disponer cuando las redes que han de conectarse no tienen las mismas funciones, como detección de errores, conversión de protocolos, etc.

El tipo de funciones de conexión depende de los servicios que sean necesarios:

- Un modem, si el sistema al que se desea acceder está muy lejos y no se accede a él con mucha frecuencia.
- Un gestor de comunicaciones, en redes en las que haya una gran demanda de comunicación con el exterior.
- Puentes o puertas (gateways) para conectar dos redes.
- Un enlace micro-mainframe para obtener datos del mainframe.

IV.2 Modems.

La función básica de los modems es aceptar datos de un ordenador o estación transmisora y convertir las señales digitales en señales analógicas que se puedan transmitir a través de líneas telefónicas de transmisión de voz. En el punto de recepción, el modem (modulador-demodulador) decodifica esas señales y las convierte en señales analógicas que el ordenador o estación receptora pueden entender.

La comunicación se logra mediante la utilización de las redes telefónicas y modems.
El módem puede estar en el gabinete de una PC (interno), o ser externo al mismo. Su función es permitir conectar un computador a una línea telefónica, para recibir o transmitir información.

En relación con la línea telefónica, el módem además de recibir/transmitir información, también se encarga de esperar el tono, discar, colgar, atender llamadas que le hace otro módem, etc.

Respecto del computador al cual está conectado, recibe e interpreta comandos de este (discar, colgar, etc.)

Cuando un módem transmite, debe ajustar su velocidad de transmisión de datos, tipo de modulación, corrección de errores y de compresión. Ambos modems deben operar con el mismo estándar de comunicación.

Dos modems pueden intercambiar información en forma "full dúplex". Esto es, mientras el primero transmite y el segundo recibe, este último también puede transmitir y el primero recibir. Así se gana tiempo, dado que un módem no debe esperar al otro a que termine, para poder transmitir, como sucede en "half dúplex".

El módem que llama, o sea que origina la comunicación se designa "originate" o "local", y el módem que contesta, responde, es el "answer" o "remoto".

Un módem puede contener en su interior dos circuitos generadores de dos frecuencias (tonos) distintas, para enviar ceros y unos, en correspondencia con los que necesite enviar por vía telefónica.

Cuando un módem transmite tonos se dice que modula o convierte la señal digital binaria proveniente de un computador en dichos tonos que representan o portan bits.

Del mismo modo que el oído de la persona que en el extremo de la línea puede reconocer la diferencia de frecuencia entre los tonos del 0 y 1, otro módem en su lugar también detecta cual de las dos frecuencias está generando el otro módem, y las convierte en los niveles de tensión correspondiente al 0 y al 1.

Esta acción del módem de convertir tonos en señales digitales, o sea en detectar los ceros y unos que cada tono representa, se llama demodulación.

El tipo de modulación ejemplificada, con una frecuencia para el uno y otra para el cero, solo permite transmitir hasta 600 bits por segundo.

Denominación Modem:

La palabra módem deriva de su operación como MOdulador o DEModulador.

Un módem por un lado recibe información digital de un computador y la convierte en analógica, apropiada para ser enviada por una línea telefónica, por otro lado, de esta ultima recibe información analógica para que la convierta en digital, para ser enviada al computador.

Frecuencia “Portadora” en la comunicación entre Modems:

Los tonos pueden considerarse como pertenecientes a una única onda que por la línea telefónica viaja de un módem a otro, la cual cambia de frecuencia según se envíen ceros o unos, denominada PORTADORA (carrier), por "portar" los unos y los ceros que se transmiten.

Para que dos modems puedan comunicarse, entre otras cosas deben usar la misma técnica de modulación. Conforme a la Electronic Industries Association (EIA) en cada extremo de la línea, el computador se designa "equipo terminal de datos" (DTE), y el módem, equipo para comunicaciones de datos" (DCE).

Registros de los Modems:

Un módem presenta un centenar de registros no volátiles, designados S0, S1, S2.....S99. Estos guardan distintos parámetros que el usuario puede cambiar mediante comandos, referidos a la fijación de tiempos de respuesta y operación del módem. De esta manera, un modem conectado esta incivilizado de forma deseada. Los modems tienen registros para almacenamiento temporario de datos en curso.

Protocolo de Comunicaciones:

En la comunicación modem-modem se debe cumplir otra secuencia de acciones y señales:

1: El módem local realiza una acción semejante a levantar el tubo, y luego disca el número telefónico del módem remoto.

2: El módem remoto lleva a cabo una acción equivalente a levantar el tubo y emite un tono o serie de tonos particulares que indican que ha respondió el llamado, y que se puede comunicar a una velocidad (bps) y modulación (ambas normalizadas).

3: El módem local responde a la serie de tonos, y negocia con el módem remoto la mayor velocidad de transmisión posible.

En general, un conjunto de procedimientos a cumplir, para llevar a cabo las etapas de una comunicación, constituye un protocolo.

Transmisión asincrónica de datos o protocolo “start-stop”:

Los datos que maneja un módem están organizados en bytes separables, al igual que cuando se almacenan en una memoria principal.

En la transmisión asincrónica los datos se envían como bytes independientes, separados, pudiendo mediar un tiempo cualquiera t entre un byte y el siguiente. Es el modo de transmisión corriente vía módem usado en las PC, siendo en general el empleado por su sencillez para bajas velocidades de transmisión de datos.

Supongamos que se envía X dato de 8 bits, los 8 bits se envían en orden inverso a indicado. Aparecen los bit de control "start" (siempre 0) que indica comienzo de carácter, y "stop"(siempre 1) de final de byte enviado. En total son pues 10 bits (rendimiento del 80%). Para poder distinguir un bit del siguiente cada bit debe durar igual tiempo T.

Para tal fin sirve el bit de start, que permite censar en momentos adecuados (en sincronismo) el valor de los bits siguientes hasta el "stop".

En la transmisión sincrónica se envía un paquete de bytes sin separación entre ellos, ni bits de start y stop (aunque existen bytes de comienzo y final). Así es factible enviar más bytes por segundo.

Bit de paridad:

Supongamos que la PC que transmite envía A=01000001, pero por un ruido en la línea telefónica mientras el módem transmitía, se recibe 01000010, el código recibido será el de la letra C, sin que se pueda notar el error. Dado que ASCII básicamente se codifica en 7 bits, se puede usar el bit restante para detectar si se ha producido un solo error por inversión como el ejemplificado. Entre dos computadores que se comunican, se adopta la convención de que en cada carácter emitido o recibido debe haber un número par de unos. El computador que está enviando, da valor al bit restante citado, de modo que se cumpla dicha paridad. El computador que recibe debe verificar que cada carácter que le llega tenga la paridad convenida. Caso contrario pedirá su retransmisión pues implica que un bit llego errado.

La paridad sirve para detectar si uno de los bits recibidos cambio de valor, que es la mayor probabilidad de errores en transmisión telefónica. Si los bits errados son dos, la paridad par seguirá, y no hay forma de detectar un carácter mal recibido, pues este método supone solo un bit errado. Cuando se usa 8 bits sin paridad ("null parity"), con un bit de stop, se indica 8N1, que es la forma usual de comunicación entre dos PC.

Si como en el ejemplo dado, son 7 bits, con paridad par ("even parity") y un bit de stop, se indica 7E1.

Para el control del envío de archivos de programas existen los protocolos de archivo en los programas Xmodem, Zmodem y otros.

Estos programas dividen al archivo a enviar en bloques de igual tamaño, que se envían (byte a byte con paridad nula) con el agregado de un numero que es el resultado de un cálculo polinomial sobre los bits de cada bloque. En el receptor sobre cada bloque recibido se realiza al mismo cálculo. Si se obtiene

el mismo número agregado se envía un simple OK. De no recibirlo, se vuelve a transmitir el bloque.

Formas más usuales de modulación:

Una onda que cambia entre dos frecuencias para codificar uno y cero, esta modulada en frecuencia (FSK= Frecuency-Shift-Keying= Codificación por cambio de frecuencia)

En el presente este tipo de variación de la forma de una onda se usa en combinación con cambios en la fase de la misma. Cada cambio de fase es como si la porción de onda que sigue a dicho cambio, se adelantara (o atrasara) con relación a lo que debiera ser una forma senoidal continua, pura. Esta forma de cambiar la señal portadora para representar combinaciones binarias, se denomina modulación en fase (PSK=Phase-Shift-Keying=Codificacion por cambio de fase). Resulta ser la más eficaz para transmitir datos binarios en líneas con ruido, siendo que requiere que el emisor y el receptor sean muy complejos.

En un módem actual, los cambios en la portadora pueden ser tanto de amplitud como de fase. La primer técnica conocida como QAM (Quadrature Amplitude Modulation), se concreto en las normas V.22 bis, para portadora modulada a 600 baudios, y con 4 bits por cambio (baudio), con lo cual se podía transmitir hasta 600x4= 2400 bps.

Para superar los 600 baudios, la norma V.32 (QAM) elevo la frecuencia de la portadora, existiendo una sola frecuencia para la transmisión como para la recepción.

Con este método, una portadora se pudo modular a 2400 baudios, y con 4 bits por baudio se llego a 2400x4= 9600 bps. Con la denominada "codificación entramada" o Trellis-TC, que permite al módem receptor corregir errores a medida que recibe datos, agregando un bit extra cada cuatro (norma V.32-TCQAM), se codifican 6 bits por baudio, con lo cual para 2400 baudios se alcanzaron 2400x6= 14400 bps.

Mediante complejas técnicas se logro que la modulación se adaptara a cada instante al estado de la línea telefónica. Se agregaron otras técnicas que requieren efectos compensatorios del mismo tipo en el módem receptor. Se usan cinco velocidades de señalización, siendo la máxima de 3429 baudios, y la mínima de 2400. Cada velocidad implica una frecuencia distinta de portadora, por lo que esta técnica supone la transmisión en un ancho de banda variable según el estado de la línea.

Para 3429 baudios, y con 8,4 bits por cambio de la señal se logra el máximo de 28800 bps. Cuando el módem se comunica con otro, sondea unos 15 segundos la línea, enviando una sucesión de tonos, buscando el mayor ancho de banda utilizable compatible con la taza de error permitida (1 bit errado por cada millón)

Posteriormente, para 3429 baudios se lograron 9,8 bits por cambio, con lo cual se alcanzo una velocidad de 33600 bps.

Software necesario para operar un modem:

Se los denomina "programas de comunicaciones".
Típicamente puede realizar las siguientes funciones:

- Atender el teléfono y transferir archivos hacia otro computador
- Recibir archivos
- Llevar un directorio de números telefónicos y parámetros de otros computadores.
- Hacer que una PC emule una terminal de teclado y pantalla tipo VT100, ANSI o TTY en comunicaciones con grandes computadoras (mainframes)
- Permitir tipear comandos y que sean visibles en el monitor.
- Manejar buffers para guardar la última información que se fue de pantalla (scrollback)
- Ayudar sobre la operatoria en curso.

Al ser inicializado un programa de este tipo, preguntara por la marca o tipo de módem conectado. El usuario tiene a su disposición en el modo comando un conjunto de órdenes para definir los contenidos de los registros S0, S1.... de un módem ante citado. De esta forma se establece como operara un módem.

Para que se le pueda emitir un comando desde el teclado, un módem debe estar en "modo comando". Los comandos se tipean precedidos por la sigla AT (ATtention), y modifican los contenidos binarios de los registros del módem.
Encontramos entre otros:
ATE1; ATV1; ATS0=n; ATB1; ATL2; etc.

Aunque el usuario no ordene comandos, el programa de comunicaciones cuando es llamado inicializa los registros del módem con valores default, que son datos fijos que contiene dicho programa.

Una de las formas de llevar al módem al "modo comunicación", es mediante el comando de discado ATD, que le ordena tomar la línea telefónica, detectar tono, discar y esperar la portadora del módem con el que se comunica.

Hardware de los módems inteligentes actuales:

Hoy en día, en un módem podemos encontrar un microcontrolador, encargado de procesar los comandos que envía el usuario y un microprocesador (el digital signal processor – DSP), dedicado a la demodulacion de las complejas señales analógicas.

Este hardware permite operar a grandes velocidades y que los modems sean multinorma.

IV.3 Routers (puentes).

A medida que aumenta el tamaño y complejidad de las redes, se hace más necesario un medio que se encargue de la demanda de servicio. En general, cuanto mayor es la red, más diversas son las necesidades de los usuarios, y entonces empieza a ser conveniente dividir la red en varias redes secundarias o subredes. Para conectar estas subredes se emplea lo que se conoce como “puente”.

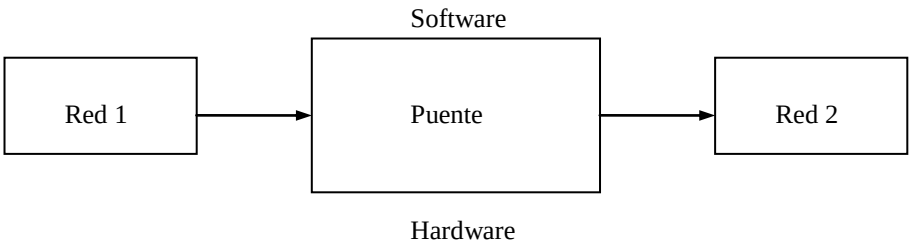


Figura 4.3.1 Conexión entre 2 redes con un router.

Un puente conecta dos subredes que se encuentran normalmente una junto a la otra. Puesto que las subredes son parte de lo que antes era una sola red, las redes conectadas por medio de un puente usan los mismos protocolos.

La función principal de un puente es pasar mensajes de una subred a otra.

Igual que las puertas, los puentes contienen dos interfaces, uno para cada subred, una cierta cantidad de memoria intermedia y la lógica y control suficientes como para saber qué mensajes son los que se han de transmitir a la otra red.

La diferencia principal entre un puente y una puerta es el tipo de redes que conectan. Los puentes conectan redes iguales que una vez formaron parte de una sola red local más grande, mientras que las puertas conectan redes locales distintas y redes de larga distancia. Otra diferencia importante son los tipos de conexión; una puerta efectúa conversiones de protocolo, mientras que el puente no lo hace.

IV.4 Gateways (puertas).

Una puerta o Gateway es un dispositivo que interconecta dos redes. Pero entre dos redes hay muchas incompatibilidades.

Una puede tener un tamaño de paquete mayor que la otra, por lo que será necesario reducir su tamaño. A este proceso se le conoce como fragmentación.

Una red puede utilizar un método muy complejo de detección y recuperación de errores, mientras que la otra puede no disponer de método alguno.

Todas las redes disponen de su propio protocolo de control de acceso de los usuarios y éste puede ser distinto en ambas.

Lo que hace la puerta es servir de intermediario entre las comunicaciones de ambas redes, y está diseñada para reducir problemas de entendimiento entre las redes o los dispositivos. Las redes que enlaza una puerta pueden ser dos redes locales que empleen distintos protocolos o una red local y una red dedicada de larga distancia.

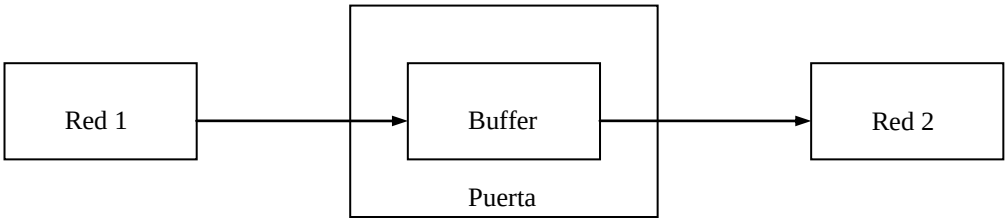


Figura 4.4.2 Conexión entre 2 redes con un gateways.

Una puerta hace lo siguiente:

- Acepta mensajes procedentes de cualquier dispositivo de la red.
- Da a los datos el formato necesario para que la otra red pueda aceptarlos.
- Añade la información de control, dirección y de ruta.
- Lleva el mensaje hasta su destino.

Además de las interfaces de hardware y software, la puerta contiene una cantidad importante de memoria intermedia (buffer). Este buffer es necesario, puesto que cuando la puerta recibe la orden de transmitir un mensaje de una red a otra, tiene que esperar a que se produzca una oportunidad para hacerlo y, mientras tanto, ha de guardar el mensaje en algún sitio. Además, el buffer se utiliza para otras funciones, como regulación de velocidad y conversiones de protocolo.

El buffer forma parte importante del proceso de conversión de protocolos. En un proceso puede haber hasta cuatro procesos de conversión.

Se pueden distinguir dos tipos de puertas: dedicadas y no dedicadas. Las puertas dedicadas son dispositivos de hardware especializado que se encargan únicamente de hacer de “enlace”. Una puerta no dedicada puede ser una estación de trabajo que se dedique a otras tareas, además de servir de “enlace”.

V. Administración de Redes Locales.

En la primera etapa de ARPANET se comprendió que cuando había problemas con la red, la única forma de identificar el problema era ejecutando comandos muy simples como el ping, el cual no brinda suficiente información para resolver rápidamente dichos problemas. En el año de 1990 surge un nuevo estándar llamado: SNMP (Simple Network Managenement Protocol, Protocolo Simple de Administración de Redes). Este protocolo muestra una manera de administrar y supervisar las redes de cómputo para identificar y resolver problemas, así como para planear su crecimiento. Se encuentra implementado en la capa de aplicación y pertenece al grupo de protocolos de TCP/IP.
Hasta el momento existen tres versiones del protocolo: SNMPv1 (versión 1), SNMPv2 (versión 2) y SNMPv3 (versión 3). Las tres son muy parecidas, solo que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión.

V.1. Arquitectura SNMP.

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

V.2. Introducción al Protocolo de Comunicación SNMP.

Podemos decir que SNMP cuenta con 4 componentes principales: Sistema de Administración de Redes (SAR), elementos administrados, un agente SNMP y el protocolo SNMP.

Un Sistema de Administración de Redes (SAR) es un software que ejecuta aplicaciones de administración y monitoreo sobre los elementos administrados, figura 5.2.1.

Los elementos administrados son cualquier nodo de la red que contiene un agente SNMP, son elementos como: servidores, ruteadores, impresoras, etc., los cuales recopilan información administrable para el SAR, tal que es accesada por medio del protocolo SNMP. El agente SNMP es un software que

reside en el elemento administrado, el cual toma la información de administración recopilada por este elemento y la traduce para que sea compatible con el SAR. Y por último, SNMP es el protocolo por medio del cual el elemento administrado proporciona la información de administración al SAR

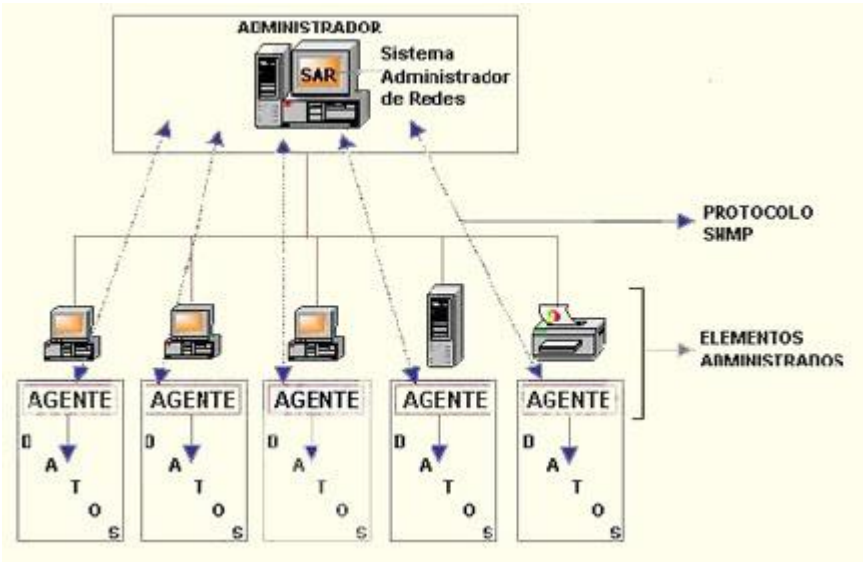


Figura 5.2.1 Relación del SNMP en una red.

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los Administradores de Red usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente SNMP es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Comandos básicos

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

V.3. Variables MIBS.

Base de información de administración SNMP (MIB)

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un ejemplo de un objeto administrado es *atInput*, que es un objeto escalar que contiene una simple instancia de objeto, el valor entero que indica el número total de paquetes AppleTalk de entrada sobre una interfaz de un router.

Un identificador de objeto (*object ID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.

V.4. Aplicaciones.

Mensajes SNMP

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los

administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los puertos comúnmente utilizados para SNMP son los siguientes:

Número	**Descripción**
161	SNMP
162	SNMP-trap

Tabla 5.4.1 Puertos comunes utilizados por SNMP

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

Versión	Comunidad	SNMP PDU

- Versión: Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1);
- Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private";
- SNMP PDU: Contenido de la unidad de datos del protocolo, el que depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la siguiente estructura en el campo SNMP PDU:

Tipo	Identificador	Estado de error	Índice de error	Enlazado de variables

- Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea;
- Estado e índice de error: Sólo se usan en los mensajes GetResponse´(en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:
  - 0: No hay error;
  - 1: Demasiado grande;
  - 2: No existe esa variable;
  - 3: Valor incorrecto;

    - 4: El valor es de solo lectura;
    - 5: Error genérico.
- Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

GetRequest

A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso de la petición. Si la petición fue correcta, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

GetNextRequest

Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto, puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

SetRequest

Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

GetResponse

Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest. En el campo "Identificador de Request" lleva el mismo identificador que el "request" al que está respondiendo.

Trap

Un trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente:

Tipo	Enterprise	Dirección del agente	Tipo genérico de trap	Tipo específico de trap	Timestamp	Enlazado de variables

- Enterprise: Identificación del subsistema de gestión que ha emitido el trap;

- Dirección del agente: Dirección IP del agente que ha emitido el trap;
- Tipo genérico de trap:
    - Cold start (0): Indica que el agente ha sido inicializado o reinicializado;
    - Warm start (1): Indica que la configuración del agente ha cambiado;
    - Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva);
    - Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa);
    - Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad);
    - EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio;
    - Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.
- Tipo específico de trap: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico;
- Timestamp: Indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap;
- Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

GetBulkRequest

Este mensaje es usado por un NMS que utiliza la versión 2 ó 3 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

InformRequest

Un NMS que utiliza la versión 2 ó 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.

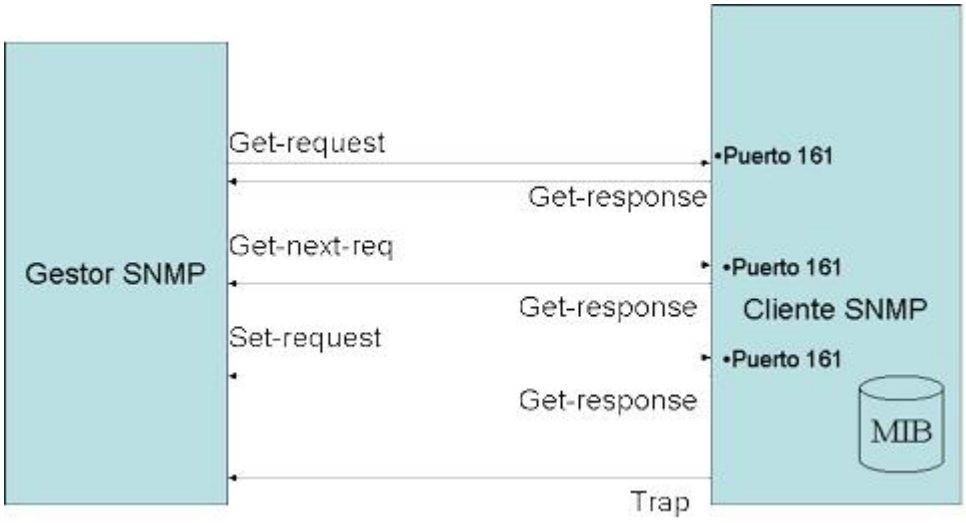


Figura 5.4.1 mensajes entre el gestor y el cliente en el protocolo SNMP.

VI. Equipos de Administración y Monitoreo de Redes.

HP Open View es una familia de productos de software muy amplia, que intenta cubrir la mayoría de las problemáticas de administración de los departamentos de Sistemas.

Existen herramientas orientadas exclusivamente a la administración del rendimiento y la disponibilidad de los sistemas.

HP Open View Operations es la consola central de eventos de HP Open View.

Las principales características son:

- Arquitectura consola-agente, incluye paquetes de software (agentes) para los principales sistemas operativos del mercado y plataformas. Los agentes son independientes de la consola central e informan a la consola solo en casos de excepciones (o sea cuando se detecta alguna situación que requiera informarse), permiten monitorizar ficheros de log, programar tareas, ejecutar programas de control, capturar eventos SNMP (traps), recolectar métricas de rendimiento de sistema y posee interfaces abiertas para envió de mensajes.
- Manejo de usuarios por responsabilidades, cada administrador de Open View solo recibe mensajes de los dispositivos de su interés.
- Vista lógica, permite crear un mapa lógico de los componentes de la infraestructura, dando a los usuarios una mejor visión del estado de los servicios informáticos.
- Escalable e integrable, permite el manejo de una gran cantidad de dispositivos y posee integración con los otros módulos de Open View.
- Interesante manejo de eventos, permitiendo asociar a estos acciones, instrucciones, anotaciones y mantener un histórico para consultas y estadísticas.

VI.1. HP Open View.

El Hp Open View Windows (OVW) es un sistema de monitoreo avanzado que usa interfaces diseñadas para integrar una presentación grafica de todos los elementos de la red administrables y aplicaciones del sistema. El OVW provee una interfaz común para el administrador o gestor de la red y los usuarios finales de la misma. Provee accesos funcionales a los administradores de red, atraves de eficientes menús y cajas de dialogo.

El HP Open View Windows combina la administración tanto de sistemas como de redes en un ambiente de elementos de diversos fabricantes. A continuación se listan algunas ventajas que proporciona a la administración de la red:

- La localización y administración de usuarios, así como los requerimientos de recursos y aplicaciones de la red.

- Integra esas diversas aplicaciones para proveer una consolidada vista de lo que sucede en la red.

- Es un sistema abierto. Puede administrar una red OSI o TCP/IP. Sin importar que sistemas son conectados.

VI.1.1 Introducción al ambiente del HP Open View Windows.

El HP Open View Windows crea y despliega un mapa gráfico que representa la topología actual de la red. El despliegue de los gráficos, o mapa de la red es interactivo. Los cambios de estados en la red son desplegados atraves de cambios de colores en el mapa de la red. El OVW actualiza el estado de la red en un tiempo real, el cual muestra las condiciones del sistema y de la red así como los cambios hechos en ella.

Para cada mapa, OVW crea un ambiente de ventanas interactivas llamadas submapas. Un submapa es una representación esquemática de todo o parte del mapa de la red. Cada submapa tiene una vista diferente del mismo mapa de red. El submapa permite variar la vista del mapa de la red, muestra desde pequeños componentes en un sistema sencillo hasta sistemas más grande como una red mundial.

El mapa da control sobre un conjunto de submapas. Permite direccionar la salida hacia un conjunto de submapas, también permite saber algunos datos como:

- Que estatus guarda cada elemento de la red.

- Como administrar las aplicaciones de objetos en los mapas.

- Como son arreglados jerárquicamente los submapas.

La representación esquemática del submapa de la red es creada por símbolos que representan segmentos y conexiones de la red. Los símbolos pueden representar una variedad de elementos en la red como pueden ser: una tarjeta de PC, una computadora, una impresora, un grupo de computadoras o impresoras, una subred, una conexión entre dos computadoras, una interfaz o una red completa. También se puede elegir como organizar la vista de la red. Se puede incluir o excluir cualquier entidad como se quiera, y se pueden agrupar según las necesidades.

OVW crea un medio de operación y administración para las aplicaciones. Puede crear aplicaciones que administren los sistemas o conexiones en la red

e integrar sus aplicaciones con el HP Open View Windows. HP incluye una aplicación con el OVW, llamada Internet Protocol Map Application (IPMap).

Objetos y Símbolos.

Objetos, mapas, submapas y símbolos son conceptos fundamentales que se usan en Open View. A continuación se definen algunos conceptos.

Objetos (Objects).

En Hp Open View Windows, un objeto es la representación interna lógica de un elemento físico existente en la red. Los objetos están almacenados internamente en la base de datos de OVW. Los objetos representan los recursos para el modelo de características de los recursos.

En OVW, se puede crear objetos, borrar objetos, o modificar las características de los objetos. Un objeto puede representar una pieza física del equipo en la red, los componentes de un nodo en la red, o partes de la misma red. Algunos ejemplos de estos objetos son:

- Una red.
- Una computadora
- Una interface
- Todas las computadoras en un departamento
- Todos los gateways en la red
- Un proceso de software en una computadora.

En OVW, los objetos no son limitados a los recursos de la computadora. Se pueden crear objetos que no tengan que ver con la computación como son lugares y localidades geográficas. Por ejemplo:

- Un edificio
- Una ciudad
- Un estado
- Una región
- Un país

Un objeto puede ser cualquier cosa en el cual un conjunto de características pueden ser definidas.

Símbolo (Symbol).

En OVW, los símbolos están muy relacionados con los objetos. Un símbolo es la representación gráfica de un objeto que es desplegado en un submapa. El OVW usa símbolos que representan un objeto definido y que es almacenado en la base de datos del OVW. En OVW, cuando se crea un objeto, se puede representar con el símbolo que se desee, en un submapa de un mapa. Un objeto puede ser representado por múltiples símbolos. Este puede habilitar múltiples usuarios en diferentes mapas para ver un símbolo del mismo objeto al mismo tiempo. De hecho, el mismo mapa o submapa puede desplegar

múltiples símbolos del mismo objeto. Múltiples símbolos pueden representar el mismo objeto.

En la figura 6.1.1.1 son mostrados algunos símbolos y objetos. Esta figura contiene dos submapas que contienen diferentes símbolos. El objeto Y es representado por un símbolo único en el submapa raíz (root), mientras el objeto X es representado por símbolos en ambos en el submapa raíz y en el submapa 2. Los cambios hechos al objeto X, como un cambio en el status, puede permitir desplegar ambos símbolos en los dos submapas.

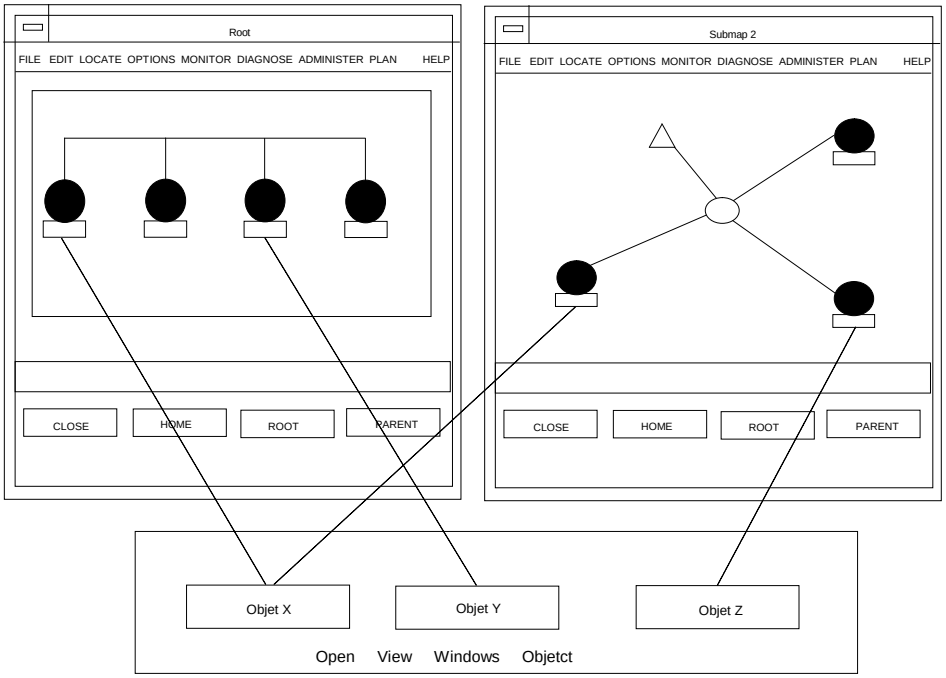


Figura 6.1.1.1 Símbolos y objetos en el OVW.

Aunque un símbolo representa un objeto, un símbolo posee sus propias características que son aparte de las del objeto. Algunos símbolos con estas características son introducidos en la siguiente lista:

- **Tipo de símbolo** (Symbol Type). El tipo de símbolo determina la apariencia visual del símbolo. Se puede escoger un tipo de símbolo para representar gráficamente el objeto. El OVW provee una amplia variedad de tipos de símbolos de los cuales se puede escoger. También, las aplicaciones pueden crear símbolos adicionales al desplegar recursos de un tipo específico.

- **Estado del símbolo** (Symbol Status). Los símbolos pueden desplegar información de su estado por medio del uso de un color. Cuando un recurso representa un objeto que funciona normalmente, el estado del símbolo es representado por un cierto color. El recurso puede fallar en algún momento, el símbolo cambia de color indicando la existencia de algún problema.

Tanto los símbolos de iconos como símbolos de conectores llevan los estados. Estas son cinco condiciones de estados:

Colores de estado de default		
Condición de estados	**Color del Símbolo**	**Color del Conector**
Desconocido - información de estado no disponible	Azul	Negro
Normal - completamente funcional	Verde	Negro
Marginal - al menos un atributo esta disminuido	Amarillo	Amarillo
Critico - no funcional	Rojo	Rojo
No administrado - recurso no usado, estado desconocido	Bronceado	Negro

Tabla 6.1.1.1 Descripción de los estatus de objetos de acuerdo a su color en OVW.

Estado de los componentes de default	
Condición de los Símbolos en el Submapa Hijo	**Estado de los símbolos Representando Objetos Padres**
Todos los símbolos son normales.	Normal
Al menos un símbolo es crítico y los símbolos no están normales.	Critico
Cualquiera de los siguientes: * Todos los símbolos son marginales. * Algunos símbolos normales, y algunos marginales. * Algunos símbolos normales, algunos marginales, y algunos críticos.	Marginal
No símbolo con un estado cualquiera normal, marginal o critico.	Desconocido

Tabla 6.1.1.2 Descripción de los estados en objetos en OVW.

Symbol Behavior. Un símbolo puede tener la función de explorar o ejecutar. Se puede configurar un símbolo para abrir un submapa que muestre con más detalle los componentes del objeto. Alternativamente, se puede configurar un símbolo que desarrolle una aplicación dentro de un objeto, o en un conjunto de objetos. Estos dan rápido acceso a herramientas que se usan más frecuentemente.

El Menú de Símbolos Pop-up

La mayoría de las operaciones en símbolos comunes son accesados usando el menú de símbolos pop-up. Cada icono y símbolo de conexión tiene su propio menú pop-up. El menú de símbolos pop-up, presenta las siguientes opciones:

Menú de Opciones Pop-up	Descripción
Open Symbol...	Causa la misma conducta que dar doble click en un símbolo. Para un símbolo explorable, este abre un submapa hijo. Para un símbolo ejecutable, este corre una aplicación.
Change Symbol Type...	Habilita para cambiar la apariencia de un símbolo icono para cambiarlo a una nueva subclase de símbolo (o nueva clase y subclase).
Describe/Modify Symbol...	Despliega la caja de dialogo **Symbol Description** para el símbolo.
Delet Symbol	Elimina el símbolo común. El objeto representado por el símbolo también es eliminado si otro símbolo no representa el objeto en el mapa.
Hide Symbol	Habilita para ocultar el símbolo para que este no sea desplegado en el submapa.
Set Star Center	Esta acción solo es aplicable a un símbolo en un submapa que esta trazado con asterisco. En tal submapa, esta característica habilita para poner el símbolo electo como el centro del asterisco.
Describe/Modify Object...	Despliega la caja de dialogo **Object Description** para el símbolo electo. Desde esta caja de dialogo, se puede modificar los valores de los atributos de el objeto.

Tabla 6.1.1.3 Funciones en un menú Pop-up.

Mapa (Map).

Un mapa es un conjunto de submapas relacionados que provee una representación gráfica y una presentación jerárquica de la red y sus sistemas. No se puede ver un mapa directamente; en cambio, siempre se ve los submapas que componen el mapa.

Se pueden crear múltiples mapas y almacenar cualquier información acerca del objeto que es desplegado en cada mapa. Múltiples mapas pueden desplegar información acerca del mismo objeto por que los mapas obtienen esta información de la misma fuente, de la base de datos de objetos del OVW. En OVW, se pueden crear nuevos mapas, borrar mapas, y cerrar los mapas desde los mapas ya existentes.

Cuando se ejecuta el OVW, un mapa especifico es automáticamente abierto. El mapa que es abierto en la pantalla es llamado el mapa abierto (open map). La

red y los sistemas administradores de aplicaciones actualizan el mapa abierto. Otros mapas que el mapa abierto no ha contemplado activamente actualiza la información hasta que son abiertos. Cuando otro mapa es abierto, OVW y sus aplicaciones integradas actualizan ese mapa.

Aunque se pueden crear múltiples mapas, en OVW, solo un mapa puede estar abierto en una sesión que dura algún tiempo. Diferentes usuarios pueden abrir el mismo mapa (al mismo tiempo) por medio de diferentes sesiones del OVW.

El primer usuario que abre un mapa puede leer-escribir (read-write access) en el mapa. Habilita el acceso de lectura-escritura al usuario para editar el mapa para crearlo, borrarlo y modificar los atributos de los objetos, y símbolos, submapas, y características de los mapas. Subsecuentemente, el usuario que abra el mismo mapa está habilitado al acceso de solo lectura (read-only) a el mapa. Con un mapa de lectura-escritura, los usuarios pueden monitorear el mapa para ver su estado y otros cambios, pero no pueden editar el mapa.

Submapa (Submap).

Un submapa es una vista particular del ambiente de la red. Este consiste de relacionar símbolos que son desplegados en una ventana única. Cada submapa despliega una perspectiva diferente del mapa. El OVW crea un submapa raíz por cada mapa. La raíz del submapa provee de un estándar, un submapa de alto nivel para cada mapa. Frecuentemente los submapas son organizados en un uso jerárquico por un mapa dado, con la raíz del submapa en primer término. También se pueden crear submapas independientes.

Se puede abrir y desplegar múltiples submapas del mapa abierto en cualquier momento, cualquiera de todos los mapas de la lista del mapa abierto y seleccionar el mapa a abrir, o transportarse de un mapa a otro. Se puede transportarte entre submapas del mapa abierto, solo dando doble click al mouse sobre el símbolo a explorar. El doble click en el símbolo abre un submapa que despliega más detalles u otras vistas.

Se puede crear, borrar y modificar las características de un submapa en el mapa abierto. Se puede crear un submapa que despliegue más detalles del sistema en la red. Se puede continuar creando e incrementando detalles de los submapas del mapa de la red.

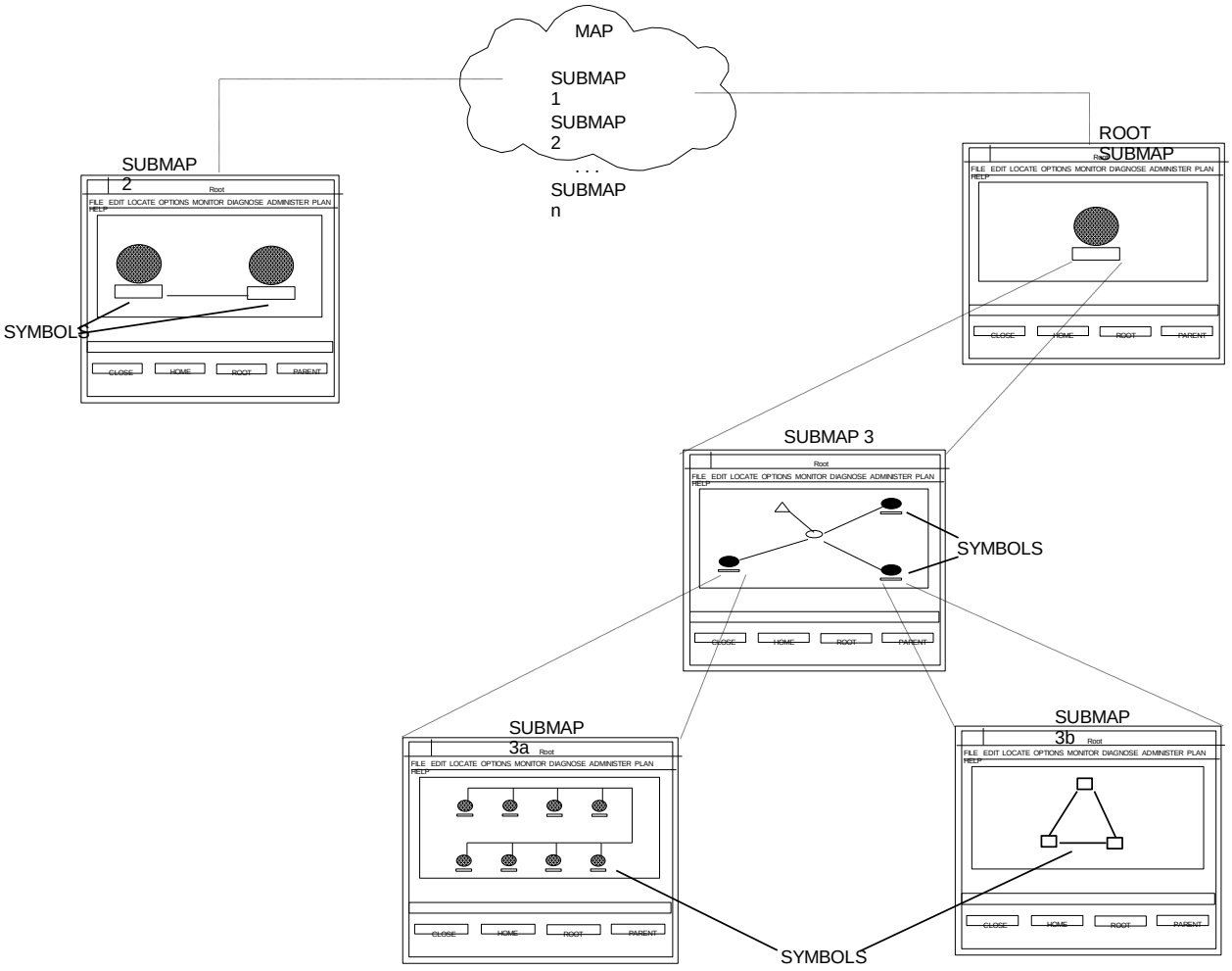


Figura 6.1.1.2 Submapas en OVW.

El Plano Background (plano de fondo).

El plano de fondo permite agregar un gráfico para el mapa de red. Los símbolos en el plano de aplicación y el plano del usuario aparecen encima del gráfico. El plano de fondo es un plano activo que puede ser usado para desplegar un gráfico de fondo, en el fondo de una presentación de un submapa. El plano de fondo puede estar vacío. La siguiente ilustración muestra tres planos combinados en todo el submapa.

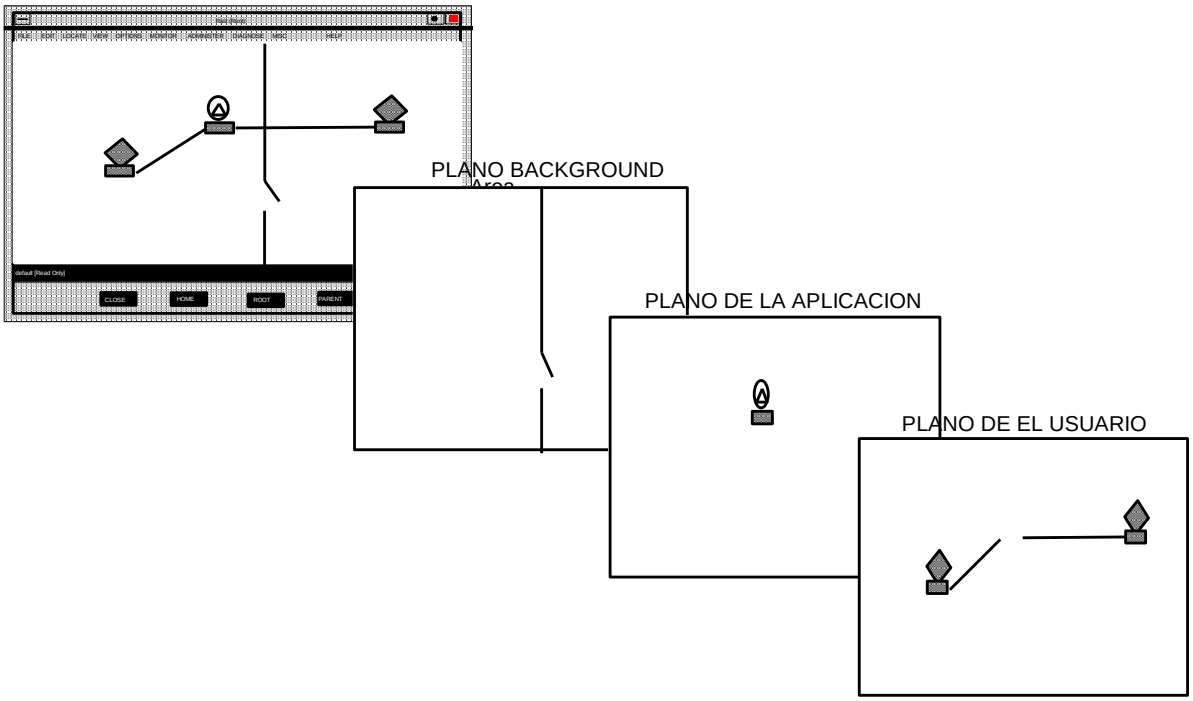


Figura 6.1.1.3 Plano de fondo en OVW.

Background Graphics (Gráfico de Fondo).

Un gráfico de fondo es un gráfico, semejante a un mapa o ilustración, este puede ser desplegado en el plano de fondo en un submapa. El gráfico de fondo puede ser diferente para cada submapa.

Se puede especificar qué fondo deberá tener el aspecto del plano de acuerdo con un submapa dado. El OVW soporta los siguientes formatos de archivos para gráficos de fondo:

- GIF(tm) -CompuServe Graphics Interchange Format
- XBM -X11 monochrome bitmap format.

Fotografía de aplicación del Mapa (Map Snapshots)

Un snapshots es un mapa particular congelado en ese momento. Un snapshots despliega el estado de la red en el momento en que se acciona el snapshot. Un snapshot puede ser útil para comparar versiones de la red y del mapa de sistemas o para detección de ruido. Un snapshots preserva el estado y colocación de todos los símbolos, y contiene todos los submapas que existen en el mapa.

VI.1.2 Archivos Principales para poder Correr el HP Open View.

Para comenzar HP Open View Windows se usa el comando ovw. HP Open View Windows automáticamente comienza la aplicación que es instalada y registrada. Inicializar OVW es un simple procedimiento de un paso.

Requisitos.

- El procesador del administrador de red que trabaja con OVW debe estar corriendo. Si el procesador del administrador de red no está corriendo, se puede comenzar por ejecutar el comando */usr/OV/bin/ovstart*. Ese proceso corre en modo oculto. Se puede verificar el estado de ese proceso tecleando *ovstatus*.

- La estación de trabajo debe estar corriendo con X Windows, o HP VUE (el cual corre en X Windows) para correr Open View Windows. Se puede comenzar X Windows por teclear *xllstart*.

- El directorio */usr/OV/bin* debe estar en el PATH. Si no está, se puede teclear */usr/OV/bin/ovw* para comenzar HP Open View Windows.

Procedimiento.

Para correr Open View Windows, se debe teclear *ovw* y presionar Enter.

Al empezar a correr OVW, un mapa por default es creado y abierto. Cuando OVW está corriendo, siempre está abierto un mapa. Después de inicializar OVW, se pueden crear mapas adicionales y especificar cualquiera de ellos como el mapa que OVW abrirá al comienzo en el OVW Graphical User Interface. Cuando un mapa es abierto, OVW despliega un submapa del mapa. Nunca se cierra el mapa (de hecho, no es desplegada ninguna operación de cerrar mapa) por que OVW cierra un mapa automáticamente cuando se abre otro mapa o cuando se sale de OVW.

El Comando OVW.

La mayoría de las veces, es necesario escribir ovw para iniciar una cesión con HP Open View Windows. A continuación se trataran detalles del comando ovw que se usan con más frecuencia.

Cuando se inicializa HP Open View Windows en la estación de trabajo, se comienza en la sesión OVW. La sesión OVW abarca desde correr hasta salir de HP Open View Windows o apagar la estación de trabajo. Se puede comenzar una nueva sesión OVW corriendo OVW nuevamente. Se puede variar la forma de comenzar una sesión de OVW. A continuación se trata sobre el comando ovw y se da un ejemplo de cómo puede usarse.

Opciones.

El comando ovw contiene las siguientes opciones:

ovw [*-ro* / *-rw*] [*-map* map_name]

Opción(Option)	Significado
-ro	Abre todos los mapas para solo lectura (read-only)
-rw	Abre todos los mapas para lectura-escritura (read-write). Esta opción es la default. Es necesaria usarla solo si el X-recurso especifica solo-lectura (read-only) como default.
-map_name	Abre el mapa map_name o crea el mapa, *map_name*, si es que no existe.

Tabla 6.1.2.1 Opciones del comando OVW.

Ejemplos:

Comando introducido	Efectos
ovw	Corre OVW y abre el mapa asignado por el usuario como mapa default
ovw -map Admin Map 1	Corre OVW y abre el mapa, *Admin Map 1*. *Admin Map 1* no necesita ser el mapa de default
ovw –ro	Corre HP Open View Windows y abre el mapa asignado por el usuario como default. El mapa default, y todos los mapas subsecuentes que se abren durante esa sesión, son abiertos con acceso de solo lectura.
ovw -ro -map Europe2	Corre Hp Open View Windows y abre el mapa llamado *Europe2*. Todos los mapas durante esta sesión de OVW son abiertos con acceso de solo lectura.

ovw –rw	Corre HP Open View Windows y abre el mapa asignado como el mapa default por el usuario. Los mapas pueden ser abiertos con acceso de lectura escritura si la licencia lo permite. La opción -rw es la default y es necesario solo si X-recursos especifican solo-lectura (read-only) como comportamiento por default.

Tabla 6.1.2.2 Ejemplos de la utilización del comando ovw.

VI.1.3 Partes que Componen una Ventana del HP OVW

La Ventana del Submapa.

Todo el tiempo un mapa está abierto, OVW despliega un mapa único. Se puede abrir un submapa adicional para ver múltiples submapas al mismo tiempo. Todos los submapas son desplegados en este mismo submapa. Una ventana de submapa consiste de las siguientes partes físicas.

- La barra de menú
- El área visible
- La línea de condiciones
- La caja de botones

La siguiente figura despliega el submapa raíz de un mapa de una red. En esta figura, el submapa raíz contiene un símbolo único que representa un IP Internet.

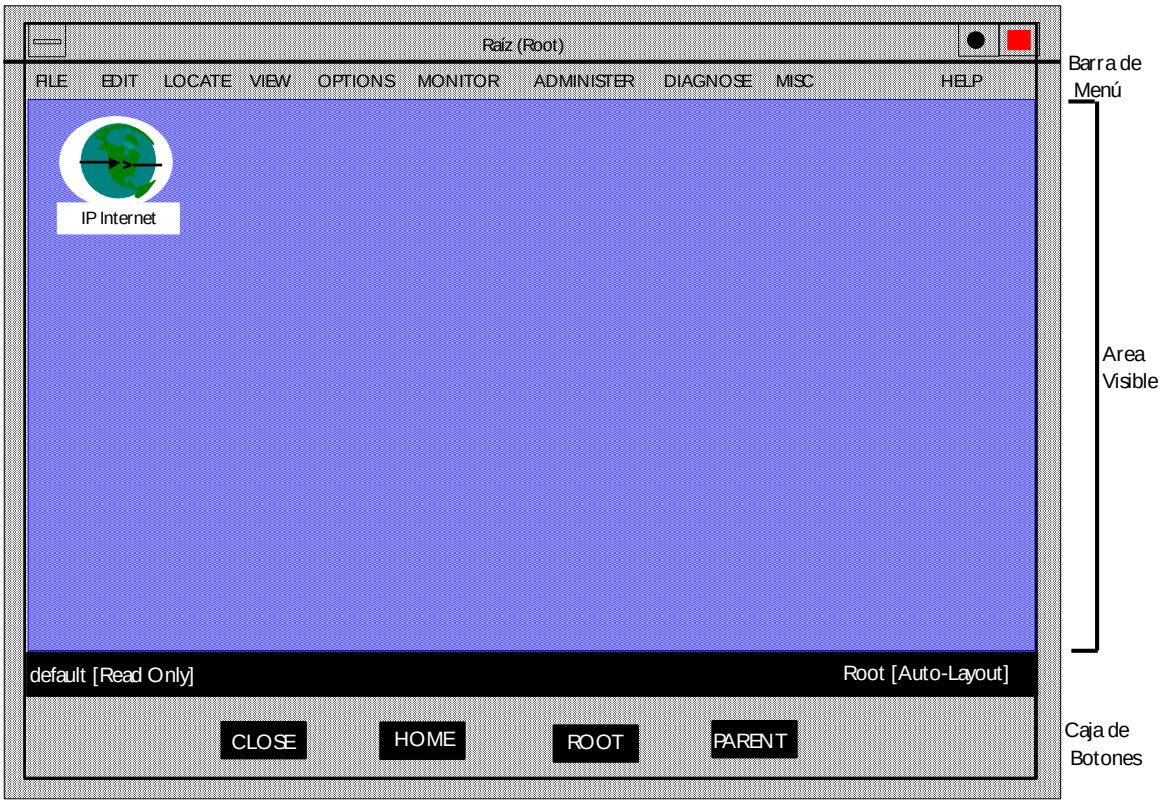


Figura 6.1.3.1 Ventana de un submapa en OVW.

Si un IP Internet, o cualquier otro símbolo, aparecen en el submapa, se puede transportarte a otro punto de vista del mapa de red.

Usando un mouse, dando doble click en el símbolo IP Internet, otro submapa puede ser desplegado. La siguiente gráfica mostrada es un submapa hijo. Del mismo modo se puede abrir un submapa hijo para el símbolo desplegado presionando el botón 3 de el mouse (o el botón 1 y 2 simultáneamente) en el símbolo IP internet y seleccionando el menú *Open Symbol*.

Se pueden crear submapas que desplieguen regiones geográficas del mundo en el cual estén recursos que sean necesarios administrar.

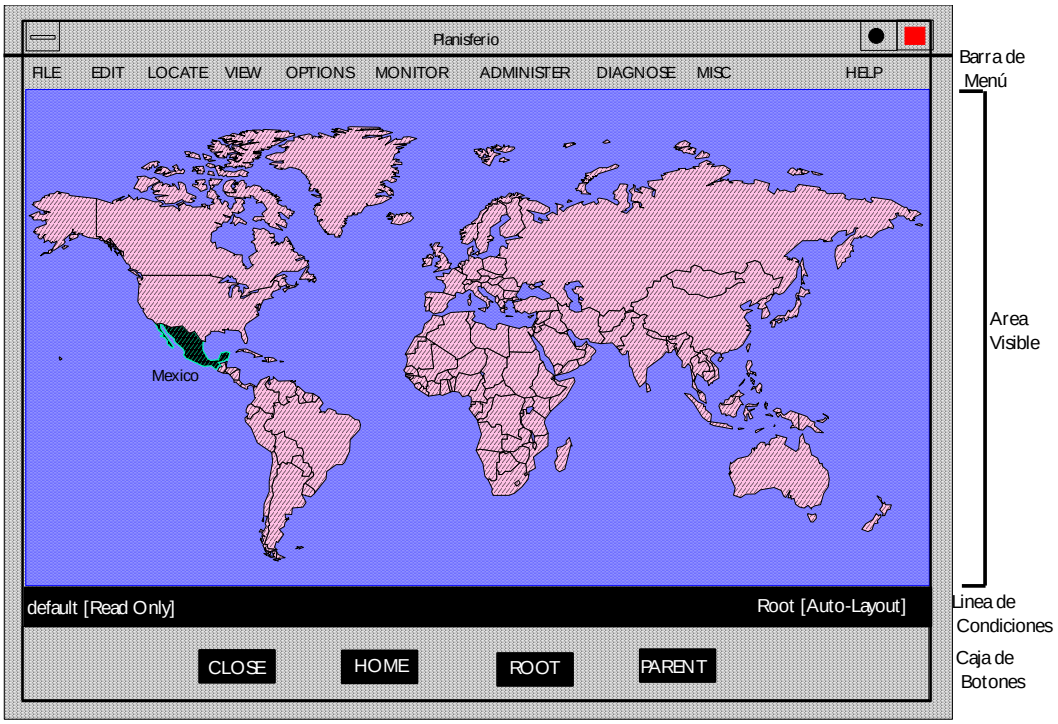


Figura 6.1.3.2 Ejemplo de un submapa que despliega una región geográfica en OVW.

Doble click en el símbolo etiquetado, México, puede abrir un submapa que despliegue recursos en el país de México.

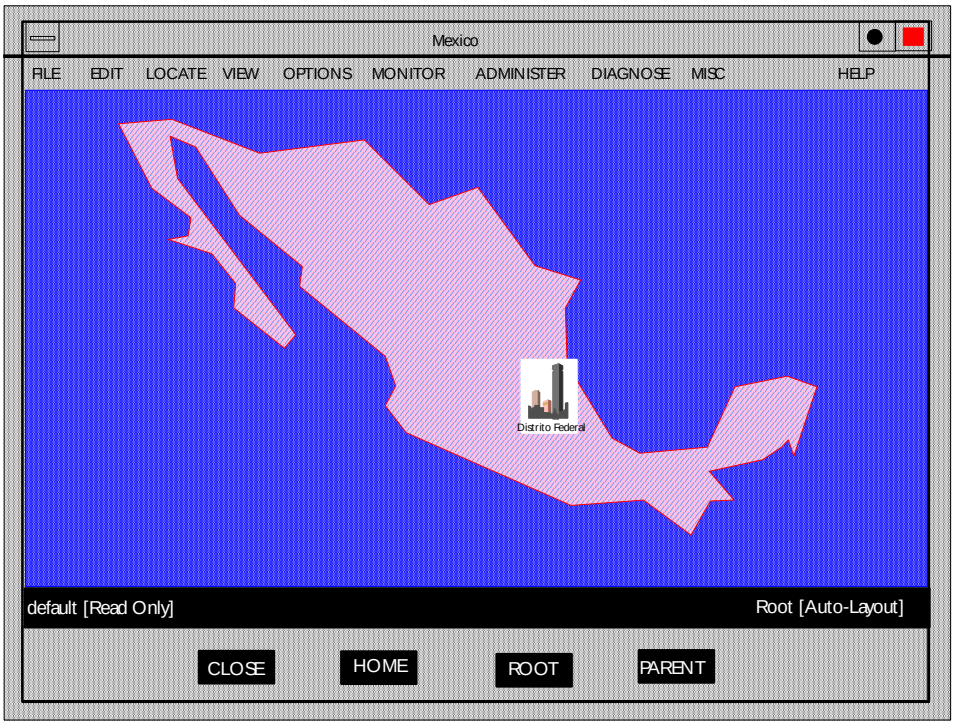


Figura 6.1.3.3 Submapa que despliega la región geográfica México en OVW.

A continuación se tratara sobre las partes físicas de un submapa.

La Barra de Menú.

La barra del menú aparece hasta arriba de la venta del submapa, y este contiene la opción del menú del OVW que permite el acceso y control de las operaciones de la estación administradora de red. Las opciones en la barra de menú son organizadas de acuerdo al tipo de función que se provee. A causa de que las aplicaciones pueden registrar nuevas opciones de menú en la barra de menú, las opciones en la barra pueden variar.

Explorando la barra de menú en el submapa. Desde la barra de menú, se despliega un submenú. El submenú desplegado contiene opciones de funciones similares. Si se observa las letras de la lista del menú que están subrayadas, estas son llamadas nmonicos. Se pueden usar nmonicos para realizar tareas en el OVW desde el teclado. Se puede desplegar el menú Fail con el mouse. Se lista el mapa disponible en el sistema OVW Presionando la tecla "O". Este abre una caja de dialogo del mapa disponible.

Adicionalmente a los mnemónicos, OVW despliega caracteres especiales, los cuales habilitan para realizar tareas desde el teclado. Esos caracteres aparecen en la barra de menú, y en los submenus marcados. La siguiente tabla lista los tipos de símbolos que OVW despliega y explica el funcionamiento de esos símbolos.

Símbolo en las opciones del menú	Funcionamiento
Opción del menú seguida por puntos suspensivos: ...	Seleccionando esta opción del menú enseña un dialogo de cajas.
Opción del menú seguidas por flecha a la derecha ->:	Seleccionando esta opción enseña en cascada más opciones de menú específicas.
Un mnemónico. (Un carácter subrayado en la barra de menú o un submenú desplegado).	Presionando estas teclas cuando el menú es desplegado inicia la selección para opciones en la barra de menú o submenú. Un submenú debe ser activado para activar un mnemónico en la barra de menú.
Un acceso aleatorio.	Una tecla o secuencia de teclas para accesar a la opción directamente.

Tabla 6.1.3.1 Descripción de las opciones utilizadas en el menú principal en OVW.

La siguiente tabla provee una breve descripción de las opciones por default en la barra de menú.

OPCIONES DEL MENÚ	DESCRIPCIÓN
File	Las opciones del menú File son generalmente asociadas con la manipulación de archivos (los mapas son almacenados como archivos). Por ejemplo, en este menú se puede abrir un mapa, listar los mapas disponibles, copiar un mapa (usando Save Map As ...), borrar un mapa, describir un mapa, representar acciones relacionadas para el cierre de un mapa, y salir de Open View Windows.
Edit	Las opciones del menú Edit habilitan para editar símbolos, objetos y submapas en el mapa abierto. El editar incluye tareas tales como sumar, borrar, copiar, cortar y pegar.
Locate	Las opciones del menú Locate proveen herramientas para localizar objetos y submapas dentro del mapa abierto. También se puede desplegar una lista de toda la selección de objetos.
View	Las opciones del menú View habilitan para cambiar todo y/o la aparición del dato que está desplegado en el submapa o en el mapa abierto.
Options	Las opciones del menú Options son asociadas con la configuración y lo más común en el mapa de red. Por ejemplo se puede especificar que objetos se pueden administrar o no administrar.
Monitor	Las opciones del menú Monitor permiten el acceso para aplicaciones que presentan información relevante para la selección de objetos. La información puede consistir de opciones tales como el nombre de un nodo y descripción, estado o todos los datos del objeto.
Diagnose	Las opciones del menú Diagnose permiten probar la conectividad del sistema.
Misc	Las opciones del menú Misc consta de una variedad de funciones que no son asociadas directamente con las otras categorías de menú.

Help	Las opciones del menú Help contiene varios métodos para que se pueda accesar detallada información de ayuda en HP Open View Windows e información general acerca de las aplicaciones que se están integrando con OVW.

Tabla 6.1.3.2 Tabla que describe brevemente las funciones en la barra de menú principal en OVW.

El área visible.

Es el área donde OVW despliega el submapa. El submapa muestra símbolos y gráficas que contienen información acerca de los sistemas, conexiones y otras partes de la red.

La barra de estados.

La barra de estados se encuentra en la parte de abajo del área visible. La barra de estados despliega información acerca del mapa de red y ciertas condiciones de estado del OVW y aplicaciones integradas.

Estado de OVW

OVW despliega la siguiente clase de información en la barra de estado:

- El nombre del mapa abierto.
- El tipo de acceso que está permitido en el mapa abierto, solo lectura (read only) o lectura-escritura (read-write).
- El nombre del submapa.
- Si una característica OVW llama un dibujo automáticamente está habilitado para el submapa. El mensaje [auto-layout] pertenece al submapa, no a todo el mapa. OVW despliega [auto-layout] cuando el dibujo automático está habilitado para el submapa.

Estado de aplicaciones.

OVW despliega condiciones de estados que pertenecen a aplicaciones integradas si la aplicación informa acerca de estos estados. Por ejemplo, IP Map está en aplicaciones integradas que HP transporta con OVW.

Estado IP Map.

Cuando un mapa es abierto, IP Map comienza sincronizando la fase, si IP Map es habilitado por el mapa. Mientras Ip Map esta sincronizándose, OVW despliega [Synchronizing] en la barra de estado de todos los submapas

desplegados. Durante esta fase, IP Map busca el Open View Topology Manager Database, y las características por cambiar desde que fue abierto el mapa. Si son descubiertos nuevos objetos, IP Map lleva al frente el mapa para poner fecha a los dibujos de símbolos nuevos.

Mientras IP Map esta sincronizándose, las siguientes funciones no pueden realizarse:

- El OVW restringe el uso de sumar o borrar símbolos, objetos, o submapas.

- IP Map no podrá aparecer en la lista de aplicaciones configurables en la caja de dialogo Add Objet o Object Description hasta que se completa la sincronización.

- Se puede presentar el administrador de objetos y operaciones de objetos no administradas, pero no podrán hacer efecto hasta que la sincronización es completada.

- Cuando la fase de sincronización es terminada, IP Map regresa para llenar la configuración funcionalmente.

La Caja de Botones

El OVW despliega una caja de botones exactamente debajo de la barra de estados en cada submapa. La caja de botones contiene varios botones que habilitan para serrar el submapa desplegado, o desplegar un submapa diferente sobre el mapa abierto. Los botones son descritos brevemente a continuación:

En esta forma aparecen colocados.

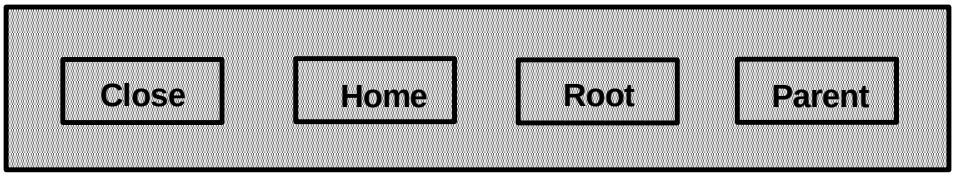


Figura 6.1.3.4 Caja de botones en OVW.

Botón	Acción
Close	Cierra este submapa
Home	Despliega el submapa hogar
Root	Despliega el submapa raíz
Parent	Despliega el mapa de primer orden de este submapa

Tabla 6.1.3.3 Descripción de las opciones en la caja de botones en OVW.

Convenciones de uso del Mouse.

El mouse habilita para realizar rápidamente una variedad de tareas en OVW. Cualquier mouse, de 3 botones, de 2 botones, o de 1 botón puede ser usado.

Selección: usado para seleccionar una opción en un mapa o menú.
Arrastrar: usado para mover símbolos dentro del submapa.
Propósitos de rutina: usado para activar un submenú que despliega otras características del símbolo.

Los botones específicos a oprimir dependen del número de botones que tiene el mouse.

Tipo de Mouse	Acción que realiza el botón
De 3 botones	Botón 1 es usado para selección. Botón 2 es usado para arrastrar. Botón 3 es usado para propósitos de rutina.
De 2 botones	Botón 1 es usado para selección. Botón 2 es usado para arrastrar. Botón 1 y 2 son usados para propósitos de rutina.

Tabla 6.1.3.4 Descripción del uso del mouse en OVW.

El mouse ayuda a realizar tareas en los submapas.

Seleccionando uno o más objetos. Oprimiendo el botón 1 en un símbolo selecciona un objeto.

Moviendo un símbolo en una ventana. Para mover un símbolo en una ventana, se presiona el botón 2 en el símbolo y se puede arrastrar este a una nueva posición. Si se usa mouse de 2 botones, se presionan los botones 1 y 2 al mismo tiempo en el símbolo y se arrastra este a la nueva posición.

Abriendo un submapa hijo. Para abrir un submapa hijo desde un símbolo, se presiona doble vez el botón 1 en un símbolo explorable.

Cajas de dialogo.

Una caja de dialogo permite obtener información o cambiar parámetros operacionales. Se puede ver y modificar esta información con los campos, listas y botones que aparecen en una caja de dialogo. Se pueden modificar datos en una caja de dialogo con el mouse. Si el uso de una opción particular no es permitido, ese control es visualmente obscuro. Esta opción esta gris. La siguiente figura muestra la caja de dialogo con descripción del mapa (map

description), la cual es desplegada cuando se selecciona Edit:Describe/modify Map... desde la barra de menú de OVW.

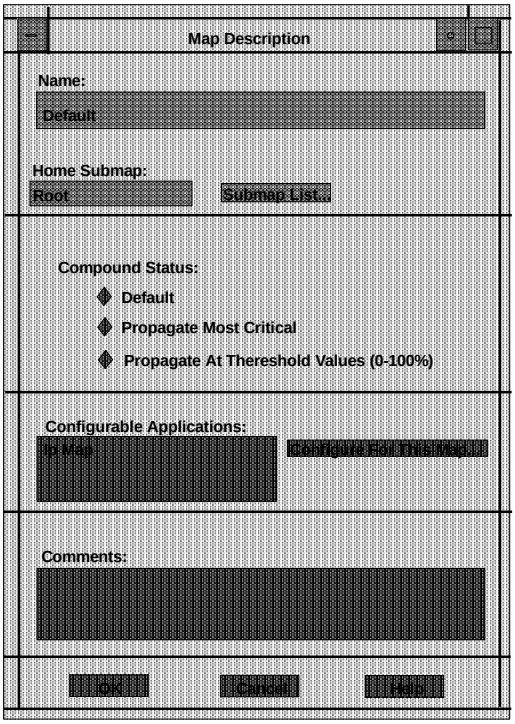


Figura 6.1.3.4 Muestra de una caja de dialogo en OVW.

A continuación se tratara la lista de cajas de dialogo que aparecen con mayor frecuencia en OVW y los tipos de botones que pueden aparecer en estas.

Lista.

Muchas cajas de dialogo despliegan una lista que contiene opciones que se pueden seleccionar. Frecuentemente aparecen botones a la derecha de la lista. Esos botones pertenecen a la lista.

Botones.
El HP Open View Windows usa varios tipos de botones que pueden aparecer en cajas de dialogo, en submapas, o en herramientas accesadas desde aplicaciones. Todos los tipos de botones son definidos por OSF/Motif. A continuación se van a tratar algunos tipos de botones.

Push Buttons.

Los botones push (en forma rectangular) aparecen en cajas de dialogo para todas las operaciones ejecutables asociadas en la caja de dialogo.

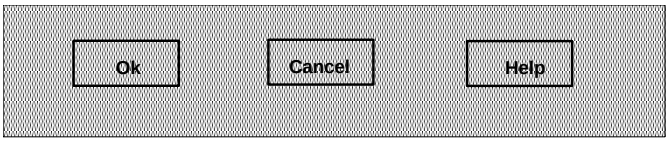


Figura 6.1.3.5 Muestra de los push buttons en OVW.

Radio Buttons.

Los botones radio (en forma de rombo) son usados para seleccionar una de varias opciones. Los botones radio usualmente despliegan información del estado asociada con un pequeño número de mutuos estados exclusivos (de dos a cuatro). Los botones radio frecuentemente se encuentran en pares, tales como opciones yes/no u on/off.

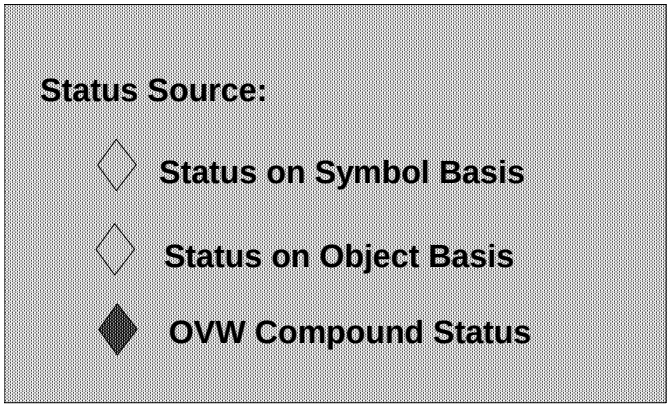


Figura 6.1.3.6 Muestra de Radio Buttons en OVW.

Check Buttons.

Las cajas check (en forma cuadrada) son usadas para seleccionar varias opciones simultáneamente. Las cajas check pueden estar verificando con cualquier combinación, incluyendo todas las cajas al mismo tiempo.

Option Buttons.

Dando click con el mouse en un botón de opción despliega un menú de opciones desde el cual se puede elegir solo una opción. Los botones de opción son usados cuando una lista de opciones es exclusiva.

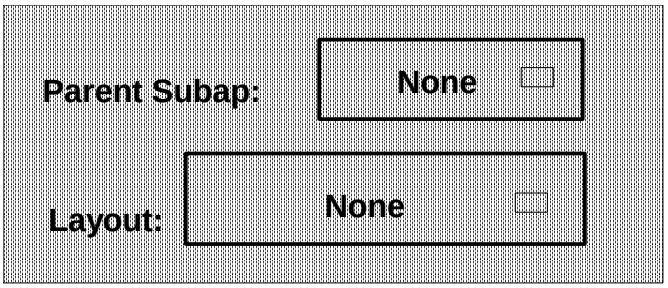


Figura 6.1.3.6 Muestra de Option Buttons en OVW.

A continuación se describirá una breve referencia de las opciones que contiene la barra de menú.

Menú File.

Contiene opciones que habilitan para realizar operaciones en mapas y fotos de fondo. Por convención, el menú File contiene opciones que son generalmente asociadas con archivos. Los mapas y fotos de fondos están almacenados como archivos. El menú File también habilita para salir de OVW. También se puede realizar operaciones como las siguientes:

- Crear un mapa nuevo.
- Listar los mapas existentes y abrir alguno de esos mapas.
- Copiar un mapa.
- Borrar un mapa.
- Describir o modificar las características del mapa abierto.
- Crear, abrir, listar, describir y borrar fotos de fondo del mapa abierto.
- Salir de HP Open View Windows.

Figura 6.1.3.8 Muestra del menú de opciones File en OVW.

Menú Edit.

Contiene opciones para editar símbolos y objetos en submapas del mapa abierto. Del mismo modo se pueden realizar tareas en los submapas. Tareas tales como las siguientes son disponibles:

- Agregar objetos y conexiones para submapas del mapa abierto.
- Cortar (o copiar) y pegar símbolos entre dos submapas del mapa abierto.
- Borrar símbolos u objetos.
- Ocultar símbolos por tanto no aparecerán en el submapa ni en ninguno de los submapas del mapa abierto.
- Mostrar los símbolos ocultos en un submapa o en todos los submapas del mapa abierto. Esta acción no esconde los símbolos.
- Crear, describir, listar, abrir o borrar submapas del mapa abierto.

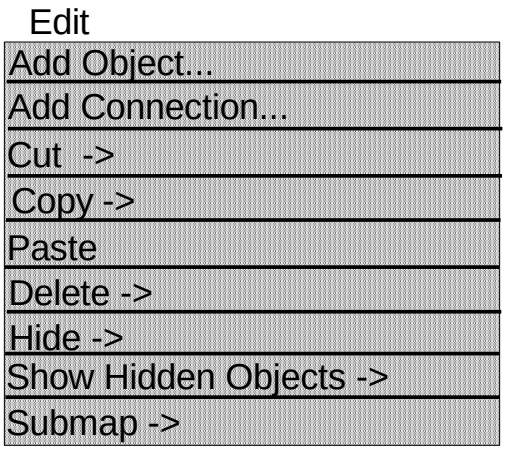


Figura 6.1.3.9 Muestra del menú de opciones Edit en OVW.

Menú Locate

Contiene opciones de menú que habilitan para localizar objetos en el mapa abierto, por ejemplo:

- Listar todos los objetos seleccionados dentro de la lista de selección de objetos.
- Localizar submapas específicos, desplegando los submapas en caja de dialogo Map y búsquedas por nombre de submapas.

- Localizar objetos basándose en la siguientes características de objetos y símbolos:

  - Seleccionando nombre
  - Atributos
  - Comentarios
  - Estado del símbolo
  - Tipo de símbolo
  - Etiqueta de símbolo

Esta opción despliega el siguiente submenú:

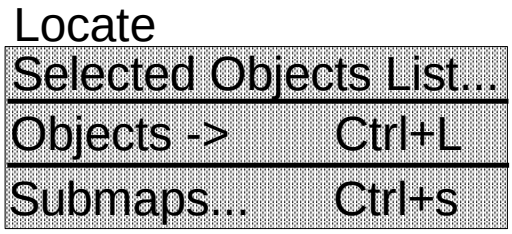


Figura 6.1.3.10 Muestra del menú de opciones Locate en OVW.

Menú View

Contiene opciones que permiten cambiar en forma total la apariencia del dato que se está viendo en el submapa.

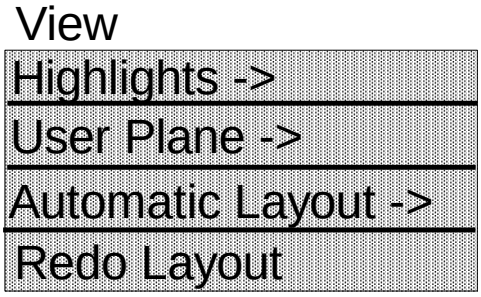


Figura 6.1.3.11 Muestra del menú de opciones View en OVW.

Menú Options

Las opciones en este menú son asociadas con la configuración y lo más común del ambiente general del HP Open View Windows como son:

- Activar la capacidad de administrar objetos.

- Desactivar la capacidad de administrar objetos.

- Ver o modificar las características del mapa abierto.

Esta opción despliega el siguiente submenú:

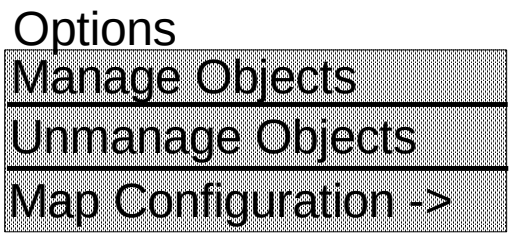


Figura 6.1.3.12 Muestra del menú de opciones Option en OVW.

Menú Monitor

Las opciones en este menú permiten accesar a herramientas de aplicaciones que presentan información relevante de los objetos seleccionados. La información puede ser información de estado que es permanente o de cambios, tal como descripción, o esta puede ser información que continuamente cambia como una función de tiempo o uso, tal como el ascenso del tráfico de una LAN, la carga de un CPU, etc. Esta opción despliega el siguiente submenú.

Figura 6.1.3.13 Muestra del menú de opciones Monitor en OVW.

Menú Diagnose

Las opciones en este menú permiten accesar a aplicaciones de diagnostico como molestias de ruido, probando y diagnosticando problemas con los sistemas en la red.

Menú Misc

Las opciones en este menú permiten accesar a aplicaciones las cuales funcionalmente no ajustan bajo los otros menús del OVW.

VI.1.4 Procedimientos con HP Open View.

Open View está organizado en Mapas o ventanas con determinados símbolos. Por defecto, la primera vez que se inicia OVW descubre todos los elementos con dirección IP a los que tiene acceso desde la máquina donde gestiona. Una

vez descubiertos, los inserta al mapa Internet, donde los conecta según la información que obtiene a partir de los nodos de direcciones IP, tablas de routing, etc.

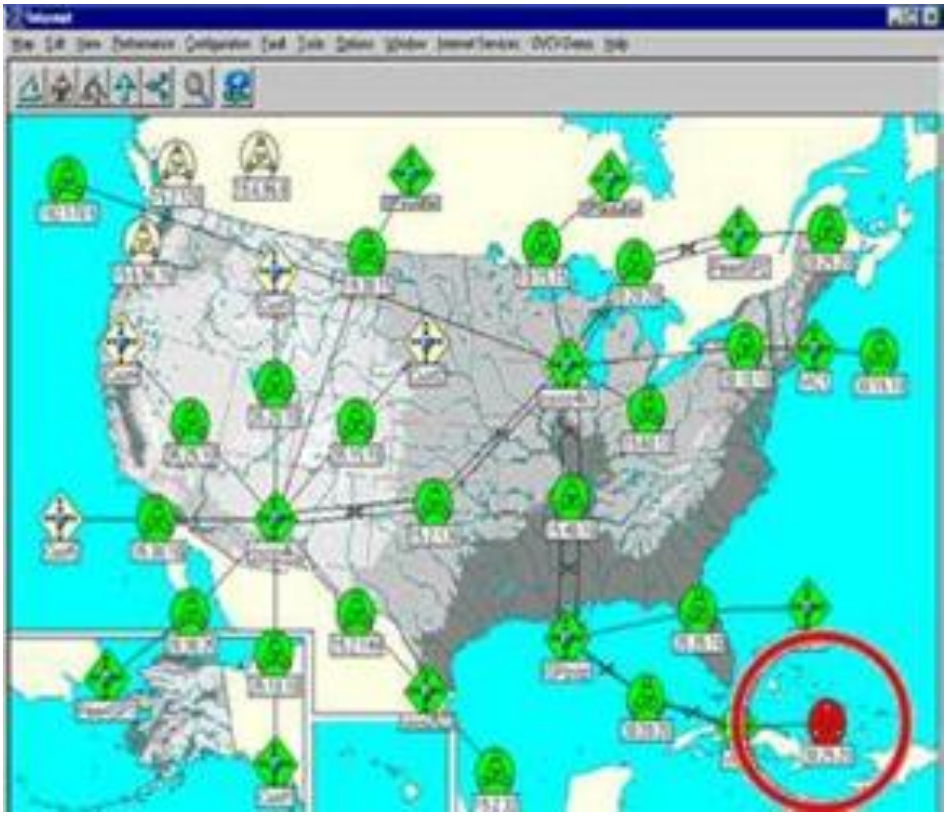


Figura 6.1.4.1 Muestra de un submapa con redes interconectadas.

Cuando se instala HP Open View lo primero que hace el sistema es un autodescubrimiento de la red a la cual está conectado con la finalidad de detectar los hosts, routers, y otros dispositivos de nivel 3 OSI con los cuales se tiene conectividad directa.

Pero obviamente es posible añadir todos los nodos que se requieran aunque no estén conectados directamente al Servidor local, aunque pertenezca a otra red distinta.

En la imagen 6.1.4.2 tenemos el primer mapa (root) que podemos ver una vez instalado Open View, este mapa tiene un único elemento que sería una red llamada Internet, y todos los submapas se alojarían colgando de este mapa principal.

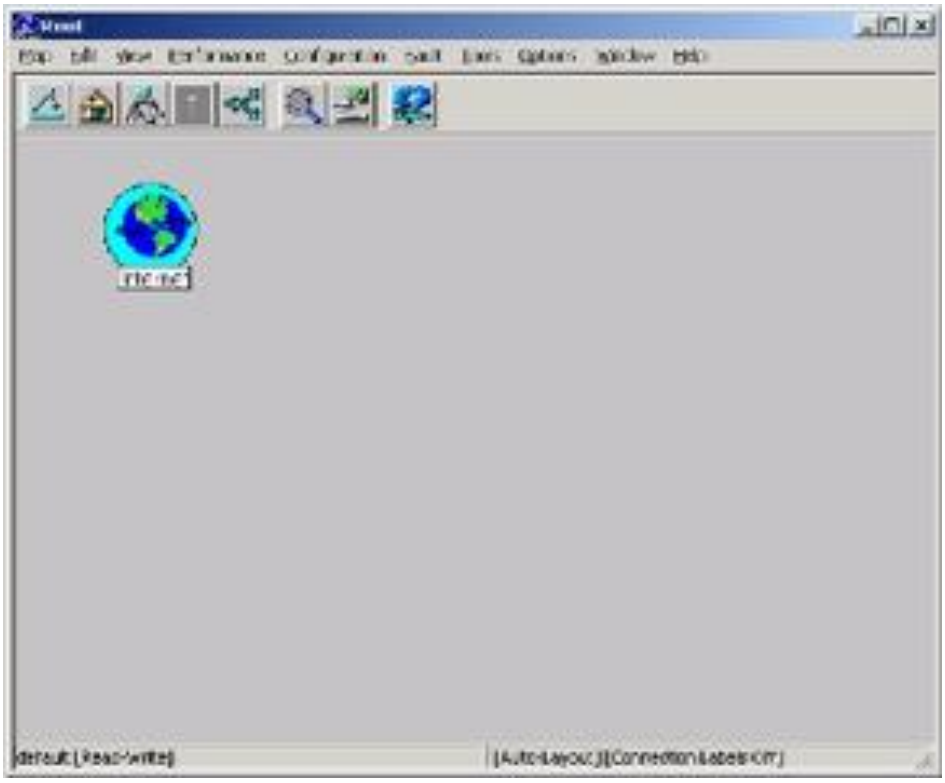


Figura 6.1.4.2 Muestra de un mapa Root en OVW.

Personalización

Hasta ahora muy bien, pero, ¿Se puede personalizar el HP-Open View para que sea mucho más eficiente para la red que se está administrando?, se necesita saber a simple vista donde están ubicados los equipos, qué equipos son, se quiere que al apretar sobre un icono haga algo que no sea mostrar sus interfaces.

Ahora se puede personalizar todo esto.

Supóngase que se está trabajando en una red compuesta por 4 subredes, una en Madrid, otra en Valencia, otra en La Coruña y otra en Barcelona.

El resultado del auto layout de HP - Open View sería el de la figura 6.1.4.3, bastante poco significativo y no ofrece información visual instantánea sobre, en cuál de las cuatro subredes se tiene algún problema (color rojo)

Se ha puesto de fondo un mapa de España, y se ha renombrado cada una de las redes al nombre de la ciudad donde se encuentran y se han dispuesto esas redes encima de su posición geográfica dentro de España.
Para llegar a este resultado en el que se tienen las redes con un nombre más descriptivo, situadas en una posición concreta y con un dibujo de fondo que puede ser un mapa se ha seguido el siguiente procedimiento:

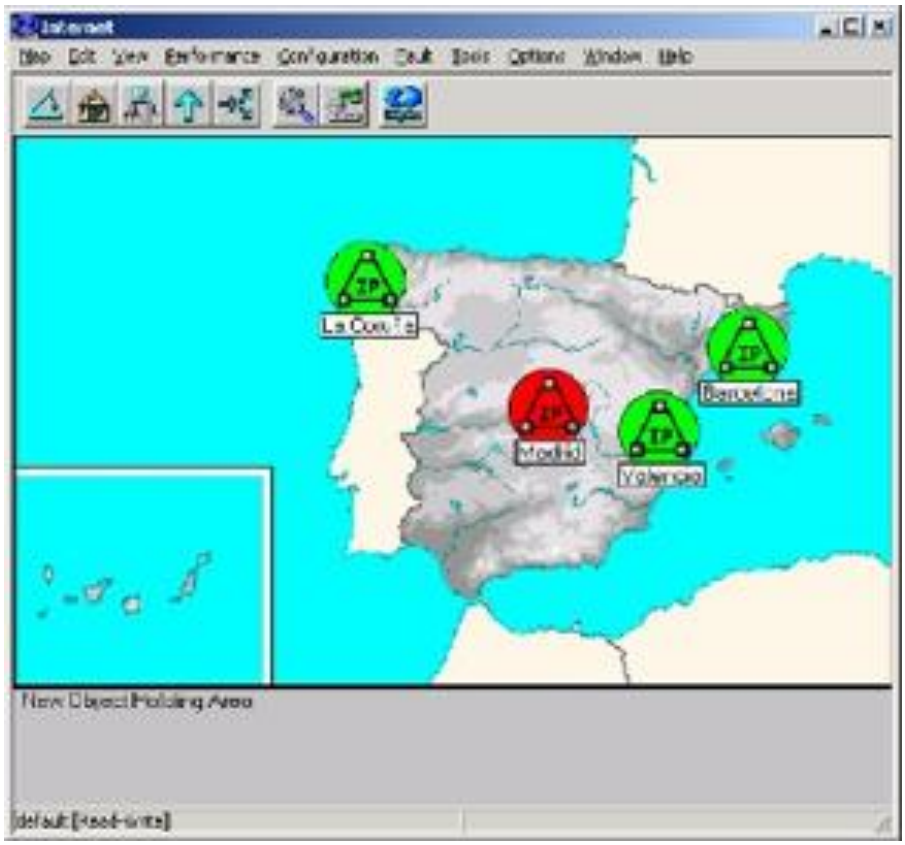


Figura 6.1.4.3 Muestra de un mapa en OVW.

Se han renombrado las redes

- Botón derecho encima de cada una de las redes y se presiona el mouse en Symbol Properties
- Y en Label se escribe el nombre que se desea ver, por ejemplo Madrid.

Se ha seleccionado una imagen de fondo

En el menú de la aplicación (arriba) se presiona el mouse haciendo lo siguiente

- Map
- Submap
- Properties
- Dentro de Properties se selecciona la pestaña View y en Background Graphics se selecciona la imagen deseada, en este caso el mapa de España (La imagen no tiene porque ser un mapa).

Se ha deseleccionado la opción AutoLayout de la misma ventana donde se ha seleccionado la imagen de fondo, esto permite mover los iconos de un sitio a otro y situarlos en el mapa en la posición que se requiera.

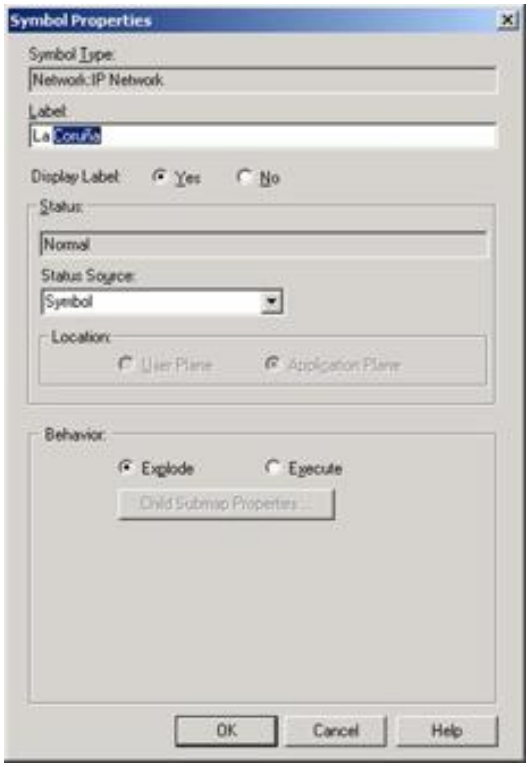


Figura 6.1.4.4 Menú para configurar un símbolo en OVW.

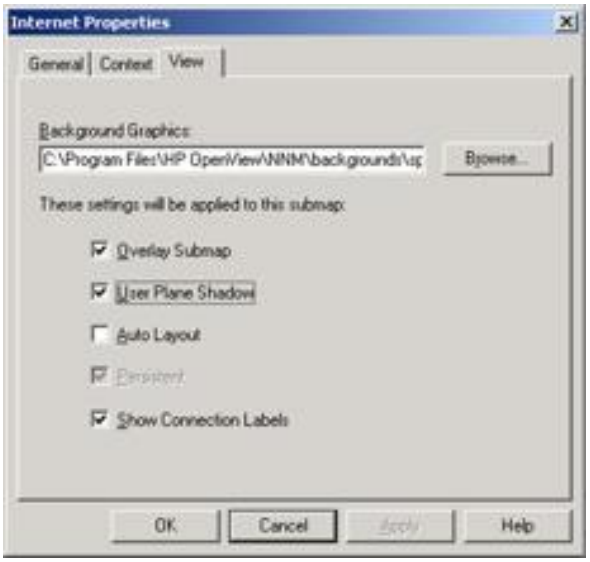


Figura 6.1.4.5 Menú para agregar un gráfico a un mapa en OVW.

Configuración

Llegado a este punto ya se sabe cómo hacer que Open View sea más amigable, pero aún no se ha visto como se añaden mapas, nodos, etc.

Unas de las cualidades principales de HP – Open View es que es capaz de monitorizar cualquier equipo que responda a peticiones SNMP o incluso de forma muy limitada a equipos que respondan a peticiones ICMP, en este caso sólo se puede saber si el equipo está conectado o no (en muchos casos más que suficiente), pero no es suficiente en determinados casos en los que se necesita una información más detallada y precisa de un equipo o nodo, como podría ser por ejemplo un router de acceso que es crítico para la comunicación en cualquier compañía, en este caso se necesita saber casi todo lo que le pueda pasar al router o a un servidor crítico para cualquier administrador de red o usuario de la misma.

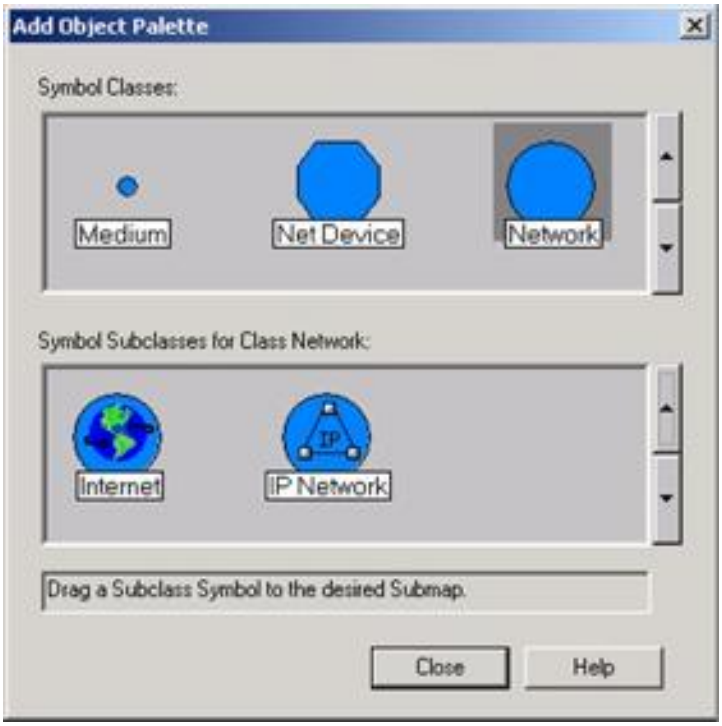


Figura 6.1.4.6 Menú para agregar un objeto al submapa en OVW.

HP – Open View como software de gestión que es, recibe una serie de traps que se tienen que organizar según severidad y categorizarlos en distintas clases, o incluso se puede requerir que una alarma determinada muestre un pop-up o incluso se puede querer traducir los traps al Español.

En Open View se puede añadir como nodo cualquier cosa, desde un PC Windows hasta un gran router en un Core IP de un gran operador de Internet, pasando por supuesto por servidores UNIX, Mac, etc., routers Cisco, Lucent, etc, las posibilidades del gestor son enormes y el interés de todos es explotarlas al máximo debido a su elevado precio y sobre todo posibilidades.

Para añadir un nuevo elemento que esté en una nueva red se tiene que crear la red y posteriormente añadir el elemento, para ello se realizara el siguiente procedimiento:

1.- Se añadira la red en el submapa deseado, para ello se realizara en el menú de Open View lo siguiente:

- Edit
- Add Object
- Se selecciona en Symbol Classes el grupo de elementos, en este caso Network
- En la ventana inferior se selecciona el tipo de red a insertar, por ejemplo IP Network.
- Se arrastraría la red al mapa correspondiente
- Al arrastrar la red al mapa se abrirá la siguiente pantalla en la que se agrega la dirección de la red con su máscara y en Label se escribe el nombre de la red.

2.- Ahora se entraría dentro de la red creada y se crearía el nuevo nodo en los mismos menús, pero con la diferencia de que en el menú de Add Object se selecciona el elemento en cuestión, que puede ser o no otra red.

Figura 6.1.4.7 Menú para personalizar un objeto dentro de OVW.

El resultado de añadir un PC a la nueva red sería el de la figura 6.1.4.8.

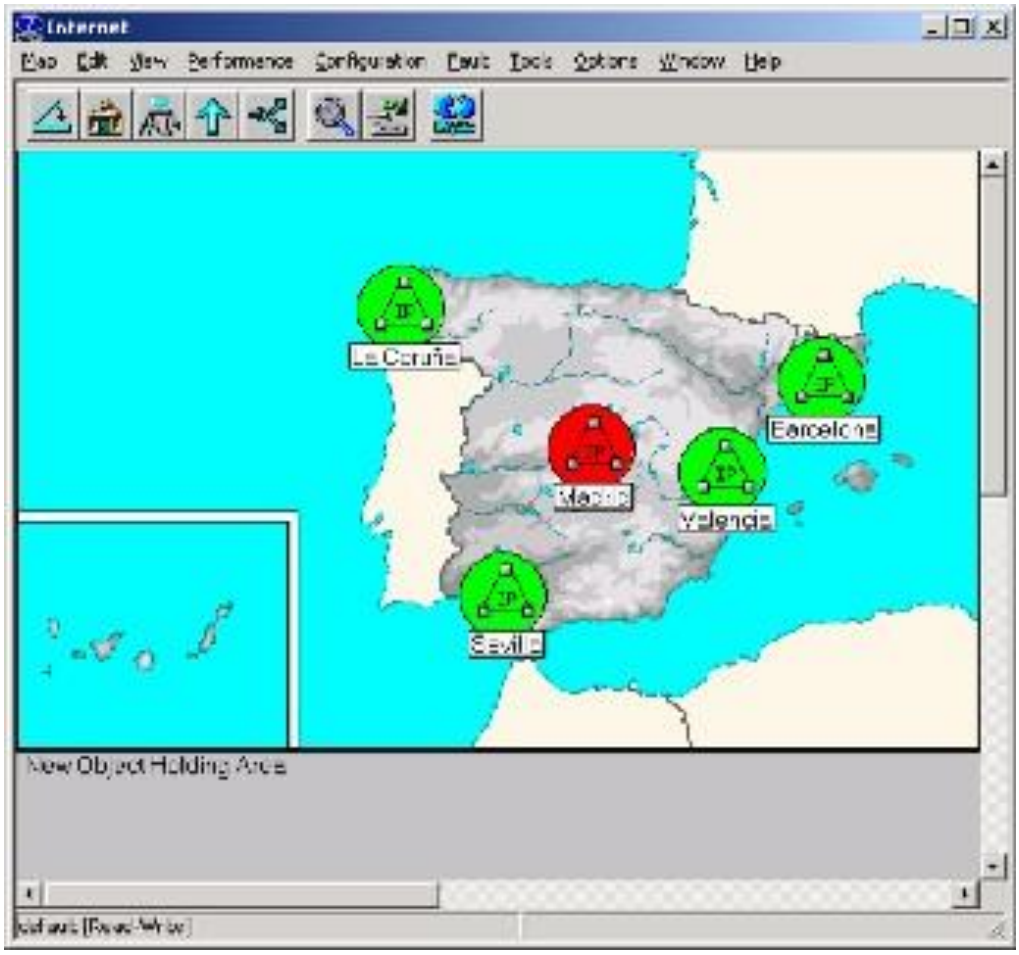


Figura 6.1.4.8 Submapa que visualiza la nueva red *dentro de OVW.*

Lo explicado aquí obviamente es lo más sencillo que se puede hacer con Open View, ya que es un software muy potente, para como primera visión puede servir.

Conclusiones.

En la conclusión de este trabajo hemos reconocido la importancia de tener controlados todos los elementos que forman parte de una red de computadoras, ya que de esta forma podemos determinar si existen problemas en la misma y poder resolverlos a la brevedad.

Es importante tener conocimiento sobre los elementos o componentes que conforman una red de computadoras, saber que topologías son las más eficientes y adecuadas para realizar los enlaces de los diferentes equipos que formaran parte de nuestra red.

Debemos seleccionar el medio físico, es decir el tipo de cable más adecuado que nos de las mejores ventajas y el mejor costo que vaya de acuerdo a nuestras necesidades de compartir recursos entre los usuarios de la red.

Es importante reconocer que mientras mejor planeada sea la estructura de la red, mas fácil será la administración y el control de la misma, el diseño de la misma con un cableado estructurado nos permitirá tener varias ventajas como el poder reacomodar los equipos sin necesidad de volver a cablear, nos permitirá detectar fallas aislando los equipos, soportará la implementación de diferentes plataformas o sistemas operativos en nuestra red, se reducirán los costos de mantenimiento, entre otras ventajas.

Reconocemos la importancia de utilizar los medios de comunicación más adecuados en la red, al igual que la estructura ideal de acuerdo a nuestras necesidades en cantidad de usuarios, optimización de recursos de red, así como los tipos de archivos y paquetes que utilizarán los usuarios de la misma.

Hemos probado la importancia de tener herramientas tanto de software como de hardware que apoyen en la administración de la red, que mientras más potentes sean estas herramientas nos ayudarán a administrar los recursos y los usuarios, aun estando el administrador de la red a distancias considerables de los usuarios finales.

Hoy en día es importante contar con algún equipo que nos apoye en la administración y el monitoreo de la red, en el caso tratado en este trabajo vemos que el HP Open View es una herramienta de software muy potente que además de estar diseñado en un ambiente muy amigable como lo es Windows, nos proporciona una serie de opciones y vistas que nos permiten llevar un control completo de todos los elementos de la red.

A continuación se presenta un breve estudio costo beneficio sobre el diseño de una red estructurada de 50 nodos, tomando en cuenta todos los elementos necesarios para la adecuada implementación de la misma, así como un equipo de monitoreo que permita la supervisión y administración de la red, haciendo la aclaración que se supone ya se cuenta con los equipos de usuarios, así como sus respectivas licencias de software.

COTIZACION DE ESTRUCTURACION Y CABLEADO DE RED E INPLEMENTACION DE EQUIPO DE MONITOREO					
CANTIDAD		**PRECIO POR PIEZA**	**SUBTOTAL**	**IVA**	**TOTAL**
610	CABLE UTP DE PAR TRENZADO CAT5E CONDUMEX	7.60	4,636.00	741.76	5,377.76
120	JACK RJ45 CAT5E	15.50	1,860.00	297.60	2,157.60
60	CAJA DE REGISTRO SENCILLA	26.00	1,560.00	249.60	1,809.60
60	PLACA KEYSTONE DE 1 CAVIDAD	10.35	621.00	99.36	720.36
400	CONECTOR 8 CONTACTOS P/CABLE DE RED UTP	1.70	680.00	108.80	788.80
3	PANEL DE PARCHEO DE 24 PUERTOS	420.00	1,260.00	201.60	1,461.60
1	RACK VERTICAL DE 19" ANCHO POR 4 PIES ALTO	1,637.94	1,637.94	262.07	1,900.01
100	CINCHO SUJETABLE DE NYLON	0.40	40.00	6.40	46.40
3	SWICH DE 24 PUERTOS	1,200.00	3,600.00	576.00	4,176.00
1	REGULADOR DE 4 ENTRADAS	600.00	600.00	96.00	696.00
1	ROUTER CISCO RV082 RUTEADOR DE 8 PUERTOS ETHERNET 10/10	2,200.00	2,200.00	352.00	2,552.00
1	COMPUTADORA PERSONAL (CONSOLA)	34,500.00	34,500.00	5,520.00	40,020.00
1	SOFTWARE HP OPEN VIEW CON LICENCIA	125,000.00	125,000.00	20,000.00	145,000.00
50	MANO DE OBRA EN INSTALACION	400.00	20,000.00	3,200.00	23,200.00
1	CAPACITACION Y SOPORTE EN EL USO DE HP OPEN VIEW	50,000.00	50,000.00	8,000.00	58,000.00
	TOTAL		**248,194.94**	**39,711.19**	**287,906.13**

Los beneficios que tendremos sobre nuestra red son:

- Tendremos un control completo sobre cada uno de los elementos que forman parte de la red.
- Permite el movimiento de equipos sin necesidad de volver a cablear.
- Proporciona puntos centrales para mantenimiento.
- Permite aislar equipos para la detección de falla.
- Soporta varias plataformas.

Podríamos mencionar un sinfín de beneficios pero es claro que de acuerdo al costo del estudio anterior, el implementar toda esta tecnología es conveniente en redes grandes y complejas, donde los tiempos de respuesta sobre cualquier falla de la red deben ser inmediatos y oportunos por que pudieran haber grandes pérdidas económicas por la falta de servicio, aclarando que muy probablemente sobre redes pequeñas no es conveniente esta implementación por su gran costo.

Glosario.

10 BASE 2	Implementación de Ethernet de 10 Mbps en cable coaxial delgado. Su máximo segmento es de 200 metros.
10 BASE 5	Implementación de Ethernet de 10 Mbps en cable coaxial grueso. Su máximo segmento es de 500 metros.
10 BASE F	Especificación para red Ethernet de 10 Mbps en fibra óptica.
10 BASE T	Estándar de transmisión de Ethernet sobre MIT a 10 Mbps.
100 BASE FX	Especificación para correr Ethernet 100 Mbps sobre fibraóptica.
100 BASE T	Estándar de transmisión sobre MIT de velocidad 100 Mbps.
100 BASE T4	Especificación para correr Ethernet 100 Mbps sobre cable 3,4 y 5 MIT de 4 pares.
100 BASE TX	Esquema que ofrece 100 Mbps sobre cable categoría 5 MIT.
Address	En redes, la palabra dirección se refiere a un distintivo único para cada nodo de la red.
Administrador	Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman superusuario.
Algoritmo	Serie de pasos para realizar una tarea específica.
Ancho de banda	Relación de velocidad para la transmisión de datos medidos en Kbps (kilo baundios por segundo) y que representa la capacidad del canal de comunicación para transportar datos.
ANSI	Organización encargada de la documentación de los estándares en Estados Unidos. director.
Application Server	Computadora destinada a brindar los servicios de una aplicación específica a los usuarios de una red.
ARCNet	Red de computadoras y recursos compartidos creado por Datapoint muy popular en los años setenta, cuyas características eran: bajo costo, cableado en estrella y velocidad hasta 2.5 Mbps.
ARP	Proceso en donde se asigna al número de la tarjeta una dirección formato TCP/IP.
ARPA	Agencia militar de Estados Unidos encargada de proyectos tecnológicos como las redes computacionales militares.
ARPANET	Proyecto del Departamento de Defensa de los Estados Unidos que utiliza protocolos tipo X.25 donde la cantidad de información (paquetes) no es fija. La

	dividieron en dos: Milnet para uso militar e Internet para uso público.
ASCII	Código utilizado para representar los caractere de escritura en formato binario (7 bits para 128 caracteres o el modo extendido de 8 bits para 256 caracteres).
Asíncrona	Forma de trasmisión de datos donde no se necesita señal adicional de reloj. La señal contiene la informació de cuándo cambia cada dato.
AT	Tecnología de 16 bits, utilizada en la tercera generación de computadoras personales 286.
ATM	Tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad, con tecnología de paquetes retrasados. Se considera la arquitectura del futuro en comunicaciones digitales.
AUI	Conexión utilizada para poder cambiar de tipo de cables en topologías Ethernet.
BIT	Dígito binario, unidad mínima de información de los dos estados 0/1. Abreviación de Binary Digit que puede ser 0 o 1. Es la unidad básica de almacenamiento y proceso de una computadora. 8 bits = 1 byte.
BPS	Bits por segundo. Velocidad de transmisión serial.
Bridge	Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.
Broadcast	Transmisión abierta. Mensajes que se mandan sin destino específico.
Buffer	Espacio físico de memoria destinado a guardar datos temporalmente.
BUS	Circuito de interconexión eléctrica para transmitir información.
Byte	Conjunto de 8 bits. Representa un carácter en lenguaje binario.
CABLE NIVEL 3	Cable tipo MIT 2 pares que soporta 10 MHZ.
CABLE NIVEL 4	Cable tipo MIT que soporta 20 MHZ.
CABLE NIVEL 5	Cable tipo MIT 4 pares que soporta 100 MHZ. ser la que más se ocupa.
Carrier o portadora	Señal eléctrica que permite la modulación de otra señal que contiene la información. Se utiliza para la transmisión remota vía la infraestructura de comunicaciones.
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía. Encargado de los estándares internacionales de comunicación.
Cliente	Producto o presentación de *front end* (directamente con el usuario) que interactúa con otros servidores o productos de *back end* (sin presentación directa con el usuario). El cliente realiza solicitudes y presenta los

	resultados. No realiza los procesos ni los cálculos, eso se los deja a los programas de *back end* que son más poderosos pero no tienen la capacidad de comunicarse directamente con el usuario.
Cocentrador	Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.
Conectividad	Estado que permite la transferencia de datos entre dos computadoras.
CSMA/CD	Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.
DDP	Tipo de conexión a Internet creado por Datasys de América. Se lleva a cabo por medio de una línea telefónica que comunica a la computadora del cliente con el ruteador que da acceso a Internet. Mantiene velocidades de 56.4 Kbps y tiene la capacidad de alimentar una red de hasta 10 computadoras. Para su instalación, el DDP necesita: dos modems idénticos de 28.8 Kbps conectados a la computadora cliente y al ruteador del proveedor; instalación de Windows NT en la computadora cliente, y de una configuración especial para el ruteador del proveedor. Este producto elimina el ruteador del lado del cliente.
Dial Up	Circuito de comunicación que se establece vía telefónica.
Dirección Destino	En el lenguaje de redes es la computadora que envía los datos de una transmisión.
Dirección Fuente	En el lenguaje de redes es la computadora que recibirá los datos en una transmisión.
DLC	Protocolo para el manejo de datos a través de líneas de comunicación.
Dominio	Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.
DTE	En redes, son los equipos en donde los datos tienen origen y destino.
Estación	Computadora que puede realizar procesos.
Ethernet	Estándar de red más popular e implementado. Utiliza *CSMA/CD* con una velocidad de 10 Mbps.
Fast Ethernet	Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.
FDDI	Estándar de transmisión de datos vía fibra óptica hasta de 100 Mbps con topología parecida a Token

	Ring/Token Passing.
File Server	Computadora dedicada a proveer y almacenar los archivos.
FTP	Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.
Full Duplex	Característica de un canal de comunicación en el que dos terminales pueden mandar y recibir información simultáneamente.
Gateway	Dispositivo que permite conectra dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.
Gigabyte	*GB*, 1 073'741 824 bytes, formalmente es 1 K de MB.
Half duplex	Característica de un canal de comunicación en el que dos terminales mandan y reciben información turnándose, una a la vez.
Hamming Code	Código de detección de errores de comunicación que consiste en enviar bits adicionales con la información acerca de los datos transmitidos para poder compararla en su destino.
Hardware	Referente a dispositivos reales, físicos. Todos los componentes electrónicos, magnéticos y mecánicos de las computadoras.
HDLC	Protocolo para redes X.25.
Host	Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.
Hub	Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con funciones inteligentes de retraso de señal *(retiming)*, y retransmisión de la misma *(repeating)*.
ICMP	Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.
IEEE	Agrupación de ingenieros que, entre otras funciones, documenta todos los desarrollos tecnológicos.
IEEE-802.1	Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
IEEE-802.2	Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI) llamado LLC.
IEEE-802.3	Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).
IEEE-802.4	Define cuadros Token Bus tipo ARCNET.
IEEE-802.5	Define hardware para Token Ring.
IEEE-802.6	Especificación para redes tipo MAN (de área metropolitana).

IEEE-802.7	Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.
IEEE-802.8	Especificación para redes de fibra óptica tipo Token Passing/FDDI.
IEEE-802.9	Especificaciones de redes digitales que incluyen video.
IEEE-802.11	Estándar para redes inalámbricas con línea de vista.
IEEE-802.12	Comité para formar el estándar de 100 base VG que sustituye CSMA/CD por asignación de prioridades.
IEEE-802.14	Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.
Interface	Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.
Internet	Red de redes con base en TCP/IP y acceso público mundial.
Interoperabilidad	Término referente a la capacidad de diferentes redes para comunicarse entre sí.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.
IPX	Protocolo definido para redes Netware que tienen direcciones en tres campos (nodo, red y socket), lo cual le permite mantener varios enlaces entre redes y procesos en varios servidores.
ISO	Organización que especifica estándares de calidad internacionales.
Kilobyte	KB. 1024 bytes.
Link	Término utilizado para referirse a los componentes lógicos y físicos que permiten la comunicación entre dos sistemas.
LLC	Controla las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI).
Login	Proceso de entrada a la red utilizado como término para indicar que la estación está dentro de la red.
Logon	Proceso de entrada a un host. Utilizado para indicar que en realidad el trabajo se desarrolla en el host.
MAC	Capa de control de acceso a medios. Capa del modelo de comunicación OSI, que es la encargada del control lógico del medio físico.
Mainframe	Cuadro principal o computadora principal en la cual se llevan a cabo todos los procesos.
MAN	Red de Area Metropolitana.
Marcado por pulsos	Técnica utilizada para mandar la señal del número telefónico al que queremos contactar mediante cambios de intensidad en el voltaje.
Marcado por tonos	Técnica utilizada para mandar la señal del número

	telefónico al que queremos contactar mediante cambios de frecuencia del voltaje.
MAU	Dispositivo utilizado en topologías de estrella física para generar un círculo lógico. Todos se conectan a él, y él asigna quién tiene el Token Passing o derecho de transacción.
Megabyte	MB. 1'048,576 bytes. Formalmente es 1 K de KB.
MIT	Cable de par trenzado sin blindaje.
Módem	Modulador-Demodulador. Dispositivo que convierte señales binarias a tonos transmitibles por vía telefónica.
NetBios	Interface estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
Netware	Sistema operativo de red desarrollado y propiedad de Novell.
NFS	Sistema de archivos de red. Genéricamente es un sistema que permite el acceso a un servidor de archivos.
Nodo	Estación de trabajo con identificación propia que puede ser fuente y destino en la red.
OSI	Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.
Packet	Unidad de información a transmitir. No contiene dirección ni destino, tan sólo ruta (el siguiente punto a llegar).
Patch Panel	Centro de empalme. Lugar donde llegan todos los cableados para conexión a la infraestructura de red.
Path	Nombre asignado a la variable que nos indica las rutas lógicas de los datos.
PDN	Redes públicas de conmutación de paquetes.
Peer-to-peer	Igual a igual. Forma de comunicación de red donde cada uno tiene las mismas tareas en el proceso.
Ping	Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.
Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.
Pulso	Cambio en el nivel o intensidad de la señal de voltaje.
Repetidor	Dispositivo que transmite y amplifica la señal de la red.
Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje.
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
SNA	Arquitectura de protocolos para redes.
SNMP	Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.

SPX	Trabaja en el cuarto nivel de OSI. Brinda apoyo a IPX garantizando la llegada y controlando las secuencias.
STP	Cable de par trenzado con blindaje o aislamiento magnético.
Supervisor	Usuario de la red con autoridad para realizar las tareas de alto nivel de cliente-servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman administrador.
TCP/IP	Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.
TELNET	Utilería de TCP/IP que permite un *logon* remoto sobre un *host*.
Terminador	Componente del cableado que empata la impedancia característica del cable para regular las señales eléctricas en la red.
Tiempo de acceso	Intervalo entre el tiempo de una solicitud de datos por el sistema y el tiempo en que el dispositivo los tiene disponibles.
Token Passing	Estafeta. Método de comunicación en red en el que cada elemento debe recibir el permiso para hablar o la estafeta.
Token Ring	Red local en la que el permiso para transmitir es secuencial o en anillo.
Tono	Cambio en la frecuencia de la señal de voltaje.
Topología	Descripción de las conexiones físicas de la red, el cableado y la forma en que éste se interconecta.
TP	Cable de pares trenzados.
Transciever	Dispositivo de Ethernet que permite el cambio de medio físico a cable.
WACK	Describe el estado de espera hasta que se recibe confirmación de que la transmisión se realizó con éxito.
WAN	Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.
X.21	Protocolo usado en las redes telefónicas digitales para voz y datos en transmisión síncrona Full Duplex.
X.25	Protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.
X.28	Estándar para la forma en que las terminales asíncronas tienen acceso a los paquetes de la red y sus comandos.
X/WINDOWS	Protocolo cliente-servidor de ambiente gráfico para UNIX. Originalmente desarrollado en el proyecto Athena por el MIT.

Índice de Figuras.

Índice de Tablas.

Bibliografía.

Autor: Beltrao Moura José Antao
Redes Locales de Computadoras: Protocolos de Alto Nivel y Evaluaciones de Presentaciones
Editorial: McGraw-Hill
Primera Edición. Año 2007.

Autor: Black Uyless
Redes de Computadoras: protocolos, normas e interfaces.
Editorial: Macrobit
Tercera Edición. Año 1997.

Autor: Friend-Fike; Baker-Bellamy
Transmisión de Datos y Comunicaciones
Editorial: McGraw-Hill
Primera Edición. Año 2006.

Autor: Krugliski.
Guía a las Comunicaciones de IBM/PC
Editorial: McGraw-Hill
Tercera Edición. Año 1995.

Autor: Rabago José Félix.
Redes Locales: Conceptos Básicos.
Editorial: Anaya Multimedia.
Cuarta Edición. Año 2005.

Autor: Tanenbaum Andrew. S.
Redes de Computadoras
Editorial: Prentice Hall.
Tercera Edición. Año 1997.

Páginas de Internet:

Apuntes y trabajos de temas de informática en general.
Varios autores
http://www.cybercursos.net/

Curso rápido de OpenView
Eduardo Collado
http://www.monitorizando.com/

Los Sistemas Operativos de red
Varios autores
http://www.monografias.com/