UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
"ARAGÓN"

"DISEÑO DE LA INFRAESTRUCTURA DE UNA RED LAN PARA LA ESCUELA SECUNDARIA 425 LICENCIADO JESÚS REYES HEROLES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A N :

PAOLA VANESSA COBOS SANTES

GUILLERMO VILLANUEVA RODRÍGUEZ

ASESOR :
ING. PABLO LUNA ESCORZA

MÉXICO 2006

DEDICATORIAS

A MIS PADRES

Por el amor, la fuerza, enseñanzas, regaños y valores que me han dirigido por la vida y me han dado las alas que necesitaba para volar. Por tener siempre los brazos abiertos cuando necesito un abrazo y por tener un corazón que sabe comprender.

A MIS PADRINOS

Por ser unos padres para mí que han sabido guiarme y aconsejarme a lo largo de este camino y por mostrarme esas lecciones que he necesitado en la vida para aprender.

A MIS ABUELITAS

Por cuidarme como una madre, quererme, mimarme y adorarme.

A MIS HERMANOS

Por ser tan lindos conmigo y darme la responsabilidad de ser un buen ejemplo para ellos.

A MI TIA GENOVEVA

Por cuidarme cuando más lo necesite, apoyarme y enseñarme a lo largo de mi vida.

A MI ESPOSO

Por ser la luz que ilumina mi vida y me inspira a ser mejor cada día. Por todo su amor, paciencia, compresión y ternura. Por enseñarme nuevas cosas cada día y por compartir su vida conmigo.

A DIOS

Por la vida tan maravillosa que me dio, llena de bendiciones, con unos padres y hermanos que me quieren, unos padrinos que me cuidan, una abuela que me adora, un hombre que me ama y por los amigos sinceros que tengo a mi alrededor.

Paola Vanessa

Tomado de su mano inicie mi aprendizaje en la vida, con su mirada de ternura logre sortear la infinidad de obstáculos que llega a tener un estudiante para lograr sus objetivos, ahora casi todo lo que soy se los debo a ustedes por su ejemplo de tenacidad y valor, por su respeto y cariño que se que nunca me falta y por la familia tan hermosa que hemos logrado formar, por que en los momentos mas difíciles de mi vida, ahí cuando ustedes se dieron cuenta que el cúmulo de dudas estaban por vencerme, llegaron con sus palabras de aliento que fueron y son el origen de este logro que hoy culmina con esta tesis que es suya, Papás…

Con ustedes he aprendido el valor de compartir desde la mas honda tristeza hasta la mas efusiva alegría, y me han alimentado de fuerza para afrontar cada día con esa seguridad de que a pesar de que todos los planes hechos para mi vida se desplomen, ustedes estarán ahí como mis mas fieles amigos y mis mas silenciosos confesores, gracias por su cariño fraternal y por soportar esos días de arduas tormentas, por nunca olvidarme y por perdonar hasta lo imperdonable; son la base de mi esfuerzo, espero ser un buen ejemplo para ustedes, pues ustedes lo son para mi, Roge, Víc esta tesis es para ustedes, pues sin su presencia las cosas en mi vida no serian, ni tendrían el valor que tienen día a día…

Cuando te fuiste a tu misión comprendí que para encontrar a alguien en quien confiar fuera de mi familia seria una misión imposible, gracias por todos esos momentos en los que creí que el mundo de afuera terminaría por quitarme del paso, por ser la única persona a quién puedo llamar amigo, gracias por permitirme guardar los secretos mas inconfesables en ti, gracias por ser ese tercer hermano que puede llegar a comprender hasta lo incompresible, esta tesis no estaría completa sin que apareciera tu nombre aquí Ramón…

Cuando comencé mi ruta hasta esta meta sus esperanzas estaban puestas en que su primer nieto terminara una carrera, les confieso que no fue nada fácil y por momentos estuve apunto de claudicar, pero esa semilla de experiencia y sus relatos de cómo es la vida de aquellos que dejan pasar oportunidades me impulsaron para llegar a este momento en donde encontré que toda aquella felicidad que ustedes soñaron para mi se vuelve realidad y esta de sobra decir que sin su apoyo o si alguno de ustedes me hubiera faltado esta tesis no tendría el mismo sabor de triunfo, gracias Abuelitos…

Hay un momento que de mi mente no puedo olvidar, ese que quizás hubiera cambiado la ruta de mi destino; hemos vivido tantos momentos juntos, tantos secretos, tantas sonrisas que era imposible olvidarme de ti, de mi tío y de mis primos a los que adoro, sabes que son mis favoritos y espero que algún día pueda regresarles cada sonrisa de apoyo y cada difícil decisión; Ale, Rodrigo gracias por ser los mejores tíos del mundo y gracias por permitirme ser yo mismo cuando estoy con ustedes; Nancy, Mónica, Daniel espero que este esfuerzo lo sientan suyo, estamos mas unidos que lo que cualquiera pudiera imaginar, espero ser una buena imagen para ustedes pero sobre todo pueda ser el apoyo que sus padres fueron para mí, está tesis se las dedico desde el fondo de mi corazón..

Cuando te conocí no imaginaba que serias la piedra angular de mi existencia, aquella presencia que lo puede todo, ese impulso de ternura y amor que amanece y se duerme conmigo; estuviste ahí cuando las cosas en los salones de clase se volvía oscuramente imposibles, pero tu mano me llevo siempre hasta una rivera segura en donde poder comprender los números de una formas mas sencilla. Gracias por abrirme las puertas de tu casa, pero sobre todo gracias por abrirme las puertas de tu corazón, pues en él encontré esa inspiración que me permitió llegar a este momento con el cual ambos soñamos con dedicación, fuerza y determinación, esta tesis es para ti pues se que sin tu apoyo este momento nunca hubiera llegado. Pao mi bella esposa no tengo mas que decirte mas que mil gracias por cada momento compartido, por los desvelos que a tu lado son maravillosos, por enfriar el temperamento que siempre me acompaña y por no dejar que mis ojos se cierren cuando hay mucho por aprender…

Gracias por tu existencia que me da la energía y el espíritu, por tu presencia cuando las lagrimas de frustración ruedan por mi cara, por estar ahí sin decir nada aguardando a que me acuerde que nunca estaré solo y que por sobre todas las cosa esta tu mano guiando y vigilado mi sendero, esta tesis te la doy como ofrenda de mi cariño y devoción gracias DIOS por darme tanta felicidad…

… Guillermo

INDICE

OBJETI VO

El objetivo de esta tesis es diseñar una red de comunicaciones para la Escuela Secundaria 425 mediante la cual los alumnos tengan acceso a servicios como:

- **Consulta de libros, mediante una biblioteca virtual.**
- **Consulta de boletas**
- **Consulta de información.**

Así también, se piensa en un beneficio para los profesores, de manera que tengan acceso a servicios como:

- **Asentar calificaciones en línea**
- **Solicitud de trabajos y tareas**
- **Exámenes y calificación de los mismos de manera automática.**

JUSTIFICACION

Nosotros consideramos que nuestra tesis es justificable porque proponemos un proyecto que va a renovar a la red existente y va a otorgar varios servicios (señalados en el objetivo) que la red por sus características no puede ofrecer.

INTRODUCCION

A través de los diferentes desarrollos informáticos y computacionales hemos podido observar que la información es lo que mueve al mundo y que ninguna Empresa o institución que quiera sobrevivir al desarrollo de estas nuevas tecnologías no puede, ni debe quedarse estancada en sistemas de comunicación obsoletos, a demás, se tiene la obligación de ofrecer nuevos y mejores servicios para sus clientes o bien para sus miembros.

La utilización de las redes para el acceso a la información remota existe en muchas formas, desde las compras en el hogar hasta el acceso a las instituciones financieras, los periódicos se pueden consultar con la comodidad de un clic y sin ensuciarse los dedos, las video conferencias son cada vez mas de uso común, ya que permiten que un grupo de personas se encuentren en puntos distantes y puedan mantener una discusión acerca de algún tema en especifico, compartir conocimientos de forma inmediata y sin la necesidad de tener que hacer un viaje largo.

Dadas las corrientes de servicios otorgadas por las diferentes escuelas en nuestro país y debido a que todavía en la secundaria no se tienen estos servicios, hemos decidido que la mejor opción que podíamos presentar para nuestro trabajo de tesis era el mejorar la red existente en la Escuela Secundaria #425, con lo cual podríamos tener varias posibilidades de alcance.

Nuestro proyecto se basa en la utilización de la seguridad SSL(Secure Socket Layer) como medio principal de protección de la información personal de cada estudiante, y también nos permitiría ofrecerles a los profesores la posibilidad de entregar sus calificaciones desde la comodidad de su hogar o bien desde los ordenadores que estarían ubicadas en los diferentes laboratorios y salones de clase.

Por años el hombre a intentado comunicarse de una manera mas eficiente y eficaz, teniendo la seguridad de que sus datos no van a ser pirateados o jaqueados, en el mundo de la red global, debido a que la información de cada alumno debe ser confidencial y además debe de estar segura en un banco de datos, hemos decidido utilizar los medios de encriptación y firewall mas confiables como lo es Integrity Desktop, que es una herramientas que posibilita compartir la información de un equipo a otro sin perder sus características de encriptación y seguridad, con ello lograríamos hacer mas personal el manejo de dichos datos.

Para nosotros como estudiantes es gratificante poder contribuir en algo para la mejora de esta escuela, a su vez hemos quedado totalmente conformes con el trabajo que nos hemos planteado y esperamos que durante el transcurso puedan disfrutarlo tanto como nosotros lo hemos hecho.

Además de obtener todos los benéficos mencionados que otorga una red local, otro de los objetivos de nuestra tesis es ahorrar dinero en la innovación a la red existente, en la actualidad los componentes computacionales han tenido una reducción notable en sus precios permitiendo

que mas gente tenga la oportunidad de conocerlos y manejarlos, pensamos que como estudiantes de las nuevas generaciones creemos que cada alumno debe tener la posibilidad de contar con los diferentes dispositivos de hardware corno lo son escáneres, cámaras digitales, impresoras láser y grabadores de CD en cada salón de clase. Y con el consentimiento y administración de los profesores.

Ya con estas nuevas herramientas computacionales en casi cada salón de clase se tendrá la posibilidad de poder permitir que los alumnos se acerquen de una forma mas personal a la información y a los a los profesores les dará la posibilidad de dar una clase mas completa o en su momento mas actualizada.

Esta es una idea general de nuestro concepto de innovación a la red de la Escuela Secundaria N° 425.

CAPITULO I. AMBIENTE DE RED

OBJETIVO PARTICULAR

Conocer los elementos necesarios para diseñar una red, así como su funcionamiento, de manera general, dentro de la misma.

1.1 GENERALIDADES

Una red de comunicaciones es un sistema de nodos (ordenador, módem, hub) interconectados por enlaces a través de los cuales fluye la información.

Los objetivos principales de una red son:

- Posibilidad de compartir periféricos costosos como son: impresoras láser, módem, fax, etc.; además de compartir grandes cantidades de información a través de distintos programas, bases de datos, etc., de manera que sea más fácil su uso y actualización.

- Reducir e incluso eliminar la duplicidad de trabajos.

- Permitir utilizar el correo electrónico para enviar o recibir mensajes de diferentes usuarios de la misma red e incluso de redes diferentes.

- Reemplazar o complementar mini computadores de forma eficiente y con un coste reducido.

- Establecer enlaces con mainframes. De esta forma, un computador de gran potencia actúa corno servidor haciendo que los recursos disponibles estén accesibles para cada uno de los computadores personales conectados.

- Posibilidad de mejorar la seguridad y control de la información que se utiliza, permitiendo la entrada de determinados usuarios, accediendo únicamente a cierta información o impidiendo la modificación de diversos datos.

- Tolerancia ante fallos, si un computador de la red falla, otro puede asumir sus funciones y su carga.

- Es accesible al ambiente de trabajo, un empleado puede recibir y transmitir información fuera de la oficina.

1.2 ESTRUCTURA DE UNA RED DE COMUNICACIONES

El propósito fundamental de cualquier sistema de comunicaciones es intercambiar información entre dos partes.

Un ejemplo de un modelo simple de una red de comunicaciones puede ser el intercambio de información entre una estación de trabajo y un servidor a través de la red pública telefónica o el intercambio de información entre dos estaciones de trabajo a través del mismo medio. Los elementos fundamentales de un modelo como éste son:

- Fuente: es el dispositivo que genera los datos que van a ser transmitidos, y que pueden ser una terminal o un servidor.

- Transmisor: los datos generados por las fuentes algunas veces necesitan ser modulados, esto es, convertidos de señales digitales a analógicas y viceversa. Un transmisor emite señales digitales que serán convertidas en analógicas, un módem realiza esta modulación para que dos computadoras que utilizan la red pública telefónica puedan comunicarse.

- Medio de transmisión: es el medio físico por donde viajan los datos y que conecta a las terminales.

- Receptor: éste dispositivo recibe las señales analógicas que viajan a través del medio y las convierte en señales digitales para que la computadora pueda entender la información, el módem es también el que se encarga de demodular dicha información.

- Destino: sólo recibe la información proveniente de la fuente.

Diagrama a bloques de una red de comunicaciones

Figura 1.1. Estructura de una red de comunicaciones

En un ambiente técnico de red a la fuente/destino se le llama ETD (equipo terminal de datos), los cuales utilizan los transmisores/receptores llamados ETCD (equipo de terminación de datos) para comunicarse a través de la red.

1.2.1 CLASES DE REDES

Por su cobertura las redes se clasifican en:

- REDES DE AREA LOCAL (LAN): son redes privadas donde los ordenadores se encuentran en un mismo edificio, la velocidad de transmisión en muy grande (decenas de Mbits) y la tasa de error es muy pequeña.

- REDES DE AREA METROPOLITANA (MAN): también son redes privadas, pero los ordenadores pueden estar en diferentes edificios que no sobrepasen el ámbito urbano.

- REDES DE AREA AMPLIA (WAN): es una red pública donde los ordenadores pueden estar en diferentes edificios que se encuentren en la misma o distinta localidad, ciudad o país, tienen una velocidad de transmisión baja (decenas de Kbps hasta 2 Mbps) y una tasa de error elevada.

1.2.2 CONSIDERACIONES EN EL DISEÑO DE UNA RED

Para el diseño de una red se deben tomar en cuenta varios factores, los cuales serán característicos del tipo de aplicación de la misma, estos son:

- Lugar de instalación: se debe de analizar la dimensión del lugar de instalación para conocer la cantidad de cable a utilizar, así como, las condiciones climatológicas del lugar, para adaptar un sistema acondicionador de temperatura para el (los) equipo(s) servidor(es).

- Numero de servidores y terminales: es necesario conocer el número de equipos que se interconectaran para poder reconocer los recursos que compartirán y así reconocer el nivel de tráfico.
- Dispositivos de interconexión: el poder conocer que tipos de dispositivos se van a implementar resulta útil para definir los alcances de la red, ya que, éstos nos ayudan a amplificar y direccionar la información, a establecer la misma entre dos redes de protocolos diferentes y evitar errores en la transmisión.

- Medios de transmisión: el análisis de medio de transmisión a utilizar es muy importante, debido a que, se puede anticipar la compra de artículos extra para evitar la pérdida de información en el medio elegido, ya que una fuente de corriente o de iluminación puede causar que la información que fluya a través del medio se pierda.

- Tarjetas de red: hoy en día los ordenadores cuentan con la tarjeta de red integrada, es importante conocer sus características de velocidad de transmisión, porque de ella depende que la conexión de la computadora a la red pueda realizarse.

- Software: es importante conocerlo para que nuestra red hable en un mismo idioma y no se tengan problemas de protocolos que eviten que la información pueda ser entendida por el receptor.

- Estándares: es necesario tomarlos en cuenta para prevenir problemas de compatibilidad entre los componentes interiores y exteriores de los equipos, así como, para evitar problemas con las comisiones encargadas de reglamentar el uso del espacio para la comunicación a través de microondas y radiofrecuencias.

1.3 REDES DE AREA LOCAL

Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo. Las topologías usadas para LAN son anillo, bus, árbol y estrella. Las topologías en bus y en árbol son secciones pasivas de cable a las que se encuentran conectadas las estaciones, de modo que la transmisión de una trama por parte de una estación puede ser escuchada por cualquier otra estación. Una LAN en anillo consiste en un circuito cerrado de repetidores que permite la circulación de los datos alrededor del anillo. Un repetidor puede funcionar también como un punto de conexión de dispositivo, realizándose la transmisión generalmente en forma de tramas. Por su parte, una red LAN en estrella incluye un nodo central al que se conectan las estaciones.

Una configuración común de red LAN es aquella que consta de computadores personales. Dado el relativo bajo costo de estos sistemas, algunos gerentes administradores de organismos adquieren frecuentemente computadores personales para aplicaciones departamentales tales como hojas de cálculo y herramientas de gestión de proyectos, y acceso Internet.

Pero un conjunto de procesadores departamentales no cubren todas las necesidades de un organismo, siendo también necesarios servicios de procesamiento central. Algunos programas, como los modelos de predicción económica, son demasiado grandes para poder ejecutarse en un computador pequeño. Ficheros de datos corporativos de gran tamaño, como los correspondientes a contabilidad y nóminas, precisan de un servicio centralizado al tiempo que deberían ser accesibles por parte de distintos usuarios. Además, hay otros tipos de ficheros que, aunque especializados, deben compartirse entre diferentes usuarios. Existen también razones de peso para llevar a cabo la conexión de estaciones de trabajo inteligentes individuales no sólo a un servicio central sino también entre sí. Los miembros del equipo de un proyecto o de un organismo necesitan compartir trabajo e información, siendo digitalmente la forma más eficiente para hacerlo.

Algunos recursos caros, tales como un disco o una impresora láser, pueden ser compartidos por todos los usuarios de una LAN departamental. Además, la red puede servir de nexo entre servicios de red corporativos mayores; por ejemplo, la compañía puede disponer de una LAN a nivel de

edificio y de uña red privada de área amplia. Un servidor de comunicaciones puede proporcionar acceso controlado a estos recursos.

El uso de redes LAN para dar soporte a computadores personales y estaciones de trabajo se ha con vertido en un hecho casi universal en todo tipo de organizaciones. Incluso aquellos lugares en que aún existe una fuerte dependencia de un computador principal, se ha transferido parte de la carga de procesamiento a redes de computadores personales. Quizá el mejor ejemplo de la forma en que se utiliza un computador personal sea la implementación de aplicaciones cliente/servidor.

1.3.1 COMPONENTES BASICOS DE UNA RED LAN

Las redes de área local están compuestas por una mezcla de software y hardware como dispositivos de computación, tarjetas de interfaz de red, sistema de cableado, concentradores y software de red, los cuales se encargan del buen funcionamiento de la red.

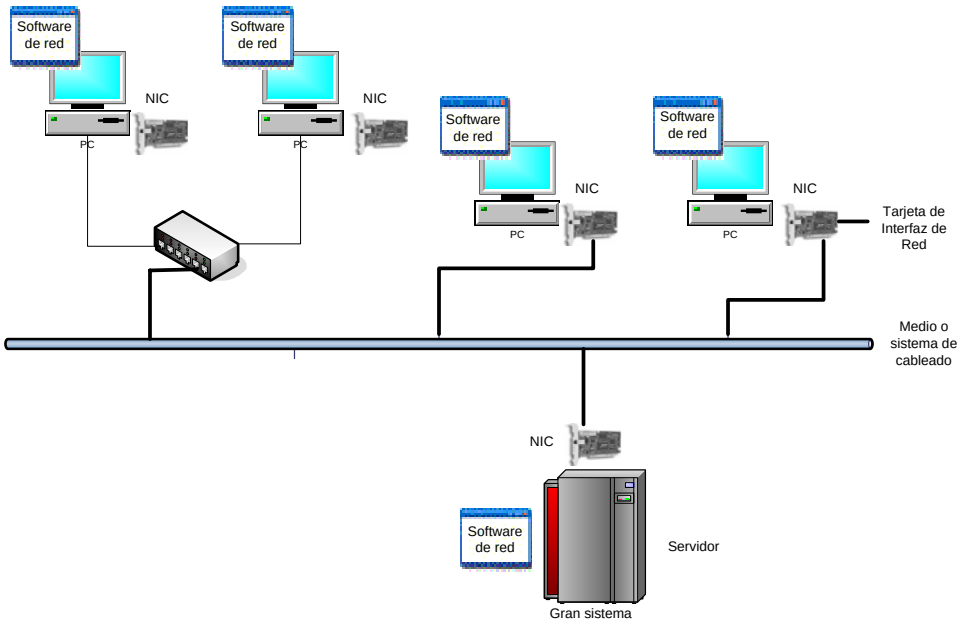


Figura. 1.2 Componentes básicos de una red LAN

1.3.2 HARDWARE Y SOFTWARE

Como componentes de hardware tenemos:

Dispositivos de computación: una red de área local es típicamente usada para interconectar dispositivos de computación de propósito general, como son computadoras personales o estaciones de trabajo, así como, dispositivos de propósito especial, como son impresoras y dispositivos usados para interconectar LAN‘s individuales.

Tarjetas de interfaz de red (NIC): Se colocan en una ranura de expansión de cada Terminal de la LAN, una NIC frecuentemente es llamada adaptador de red debido a que es la interfaz entre el computador y el cable de red. La NIC se encarga del envío de los datos hacia la red a través del bus con una dirección única, controlando el flujo de datos entre el computador y cable de red.

Sistema de cableado: es el medio de transmisión por donde va a fluir la información, que puede ser alámbrico o inalámbrico. Entre los medio alámbricos podemos citar el cable coaxial, el UTP y la fibra óptica. En los medios inalámbricos tenemos la radio, las microondas, el infrarrojo y el láser. En el sistema de cableado se incluyen unidades de aditamento (conectores) que permiten a los dispositivos de computación conectarse al cable de red.

Concentradores: Algunas LAN usan dispositivos llamados concentradores o unidad de acceso los cuales permiten que múltiples dispositivos de computación se conecten al sistema de cableado a través de un punto central. Conectar dispositivos a través de un concentrador frecuentemente facilita la instalación y el mantenimiento de la red local.

Como componentes de software tenemos:

Software de red: El software de red realiza funciones de alto nivel que proporcionan a los usuarios finales facilidades como acceso a impresoras y archivos remotos.

1.4 TOPOLOGIA DE RED

Se denomina topología a la forma geométrica en que están distribuidas las terminales, nodos y enlaces que conforman una red.

El objetivo de la topología es buscar la forma más económica y eficaz de conectar los diferentes elementos de una red para facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, permitir un mejor control de la red y permitir de forma eficiente el aumento de las estaciones de trabajo.

Podemos distinguir dos aspectos diferentes al momento de considerar una topología:

- La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado en la red.

- La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

LAN-Red de Area Local
UTP- Cable de Par Trenzado Sin Apantallar

1.4.1CONFIGURACIÓN EN BUS

En ella todas las estaciones comparten el mismo canal de comunicaciones, toda la información circula por ese canal y cada una de ellas recoge la información que le corresponde.

En ésta topología no hay un ordenador principal, es fácil de instalar, la cantidad de cable a utilizar es mínima, tiene una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones y el fallo de una estación no repercute en la red.

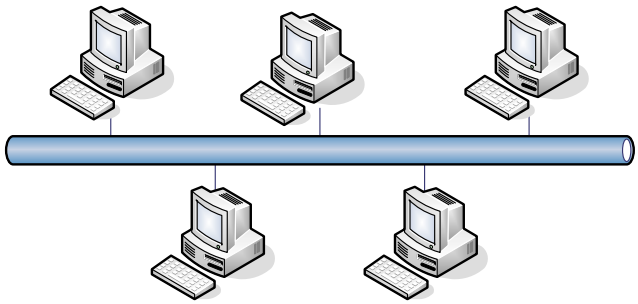


Figura 1.3 Topología bus

Sin embargo, es fácil de intervenir por usuarios ajenos de la red, sin perturbar el funcionamiento normal; una ruptura en el canal de comunicación afectaría toda la red, la longitud no puede sobrepasar los 2,000 metros.

El control del flujo, se ve afectado cuando varias estaciones intentan transmitir a la vez, como hay un único bus, sólo una de ellas podrá hacerlo, por lo que mientras mayor sea el número de estaciones la red tendrá más complicaciones para el control del flujo.

Es la configuración lógica más extendida actualmente y está usada por la red ETHERNET.

1.4.2 CONFIGURACIÓN EN ESTRELLA

Esta topología se originó en los años 70’s, es una de las más antiguas y en ella todas las estaciones están conectadas directamente al servidor u ordenador principal, aunque también pueden estar conectados a un concentrador o un switch, de tal forma que todas las comunicaciones se han de hacer necesariamente a través de él.

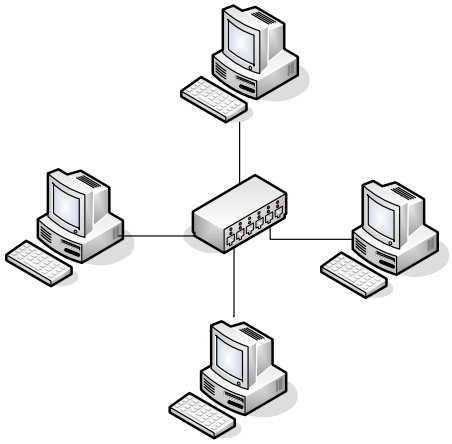


Figura 1.4 Topología Estrella

Esta topología permite incrementar y disminuir fácilmente el número de estaciones, si se produce un fallo en alguna de las estaciones de trabajo no repercutirá en la función general de la red, pero, si se produce un fallo en el servidor, la red completa se vendrá abajo.

Tiene un tiempo de respuesta rápido en las comunicaciones de las estaciones con el servidor y lenta en las comunicaciones entre las distintas estaciones de trabajo.

No es muy conveniente para grandes instalaciones y su coste es caro debido a la gran cantidad de cableado y a la complejidad de la tecnología que se necesita para el servidor. Sin embargo el mantenimiento es más fácil, debido a que la atención se concentra en el servidor, además de que es la topología física más usada por las empresas.

Existen modificaciones para esta topología:

Topología en estrella extendida

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

Topología en árbol

La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. El enlace troncal es un cable con varias capas de

ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

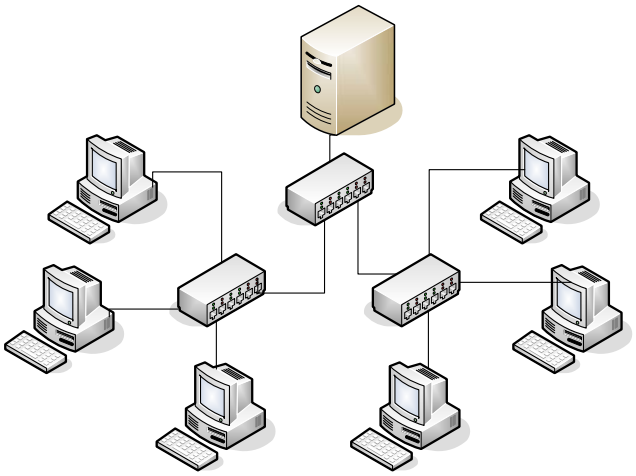


Figura 1.5 Topología Arbol

1.4.3 CONFIGURACIÓN EN ANILLO

Esta topología se originó en los años 80 ‘s. En ella todas las estaciones están conectadas entre sí formando un anillo, de manera que cada estación sólo tiene contacto directo con otras dos y tampoco posee un ordenador principal.

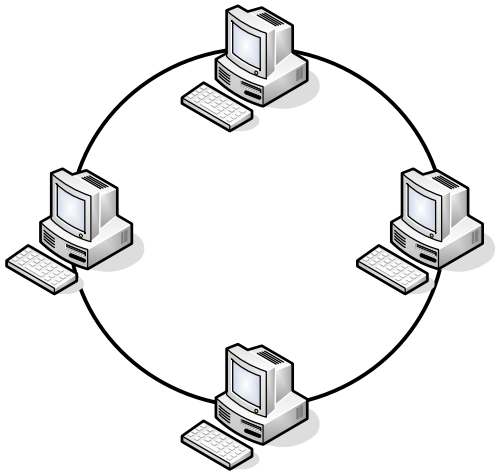


Figura 1.6 Topología Anillo

Entre sus inconvenientes destacan:

Este tipo de redes permite aumentar o disminuir el número de estaciones sin dificultad; pero, a medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red.

Un fallo en una estación puede dejar bloqueada la red, pero un fallo en un canal de comunicaciones la dejará bloqueada en su totalidad.

Su instalación es compleja y su uso está extendido por el entorno industrial. Está usada por la red TOKEN RING de IBM.

1.4.4 FACTORES DE EVALUACION

Se ha escogido la topología lógica bus o ethernet para nuestro diseño, debido a que es el estándar en las redes de áreas locales, permite una buena comunicación entre los ordenadores y es compatible con el protocolo más extendido en todo el mundo, TCP/IP.

La topología física empleada es la de estrella extendida y árbol, debido a que la atención esta en el servidor y es más barato mantener el servidor en un buen estado, con su respaldo, que mantener todas las computadoras. Con un buen servidor no se tiene problemas de tráfico, hoy en día los equipos de cómputo tienen precios accesibles, además de que los dispositivos de comunicación (switch, routers) ayudan a segmentar la red y mantener un buen control de tráfico y accesibilidad, por lo que la comunicación entre las computadoras y el servidor se vuelve muy rápida.

Otro factor importante es que si uno de los nodos falla, la red se mantendrá funcionando y para garantizar la confiabilidad de la red no se necesita de un excesivo cableado como en la topología doble anillo o malla.

1.5 TRANSMISION DE DATOS

La transmisión de información se lleva a cabo a través de distintos medios, los cuales debido a sus característica físicas necesitan de técnicas de transmisión especiales.

La transmisión de datos esta totalmente ligada a la naturaleza del mismo, la cual puede ser analógica o digital.

Los datos digitales se caracterizan por tener un espectro discreto y finito, formado por dos estados binarios (unos y ceros), éste tipo de datos es fácilmente manejable, debido a que se pueden mezclar y transmitir datos de voz, video y fuentes de datos con un sistema de transmisión digital común, con la ventaja de preservar la intimidad con el uso de codificación criptográfica, además de que los errores en los datos pueden ser pequeños y hasta cierto punto corregibles, incluso cuando existe una gran cantidad de ruido en la señal recibida. Los inconvenientes de manejar datos digitales es que se necesita mayor ancho de banda y sincronización.

Los datos analógicos se caracterizan por tener un espectro continuo y un intervalo infinito de valores, son poco manejables para su transmisión porque a distancias largas y frecuencia altas son propensos a perder información

irrecuperable en la transmisión. La gran ventaja que presentan es que requieren menor ancho de banda y no necesitan sincronización.

De acuerdo a la naturaleza de los datos existen dos técnicas de transmisión:

Banda base

En la transmisión banda base las señales son transmitidas a través del medio físico en forma de pulsos discretos, eléctricos o luminosos. Las señales que se transmiten no son moduladas, por lo que utiliza todo el ancho de banda en cada transmisión, lo que implica que sólo se puede enviar una señal simultáneamente.

Como los pulsos viajan a través de todo del medio de comunicación, éstos pueden distorsionarse debido a que el medio de transmisión es muy largo o la velocidad de transmisión es muy alta, lo que provoca que los datos puedan ser inteligibles y erróneamente interpretados por el receptor.

Para evitar estos problemas existen dispositivos llamados repetidores que se encargan de recibir la señal digital y retransmitirla con su forma y potencia original. Con la señal regenerada cualquier ruido agregado a la misma se nulifica. Los dispositivos de comunicaciones de la red pueden actuar como repetidores en algunas LAN geográficamente separadas.

Los elementos de conexión que se pueden utilizar son: el cable de par trenzado y el cable coaxial de banda base.

Banda ancha

En la transmisión banda ancha se envía señales analógicas a través del medio modulando las señales digitales sobre ondas portadoras, la cuales pueden compartir el ancho de banda del medio de transmisión mediante multiplexación por división de frecuencia. Es decir, actúa como si en lugar de un único medio se estuvieran utilizando líneas distintas.

Las señales son transmitidas en forma de ondas electromagnéticas y el ancho de banda depende de la velocidad de transmisión de los datos.

Este método hace imprescindible la utilización de un módem para poder modular y demodular la información.

La distancia máxima puede llegar hasta los 50 km y permite usar además los elementos de conexión de la red para transmitir otras señales distintas de las propias de la red como pueden ser señales de televisión o señales de voz.

Los elementos de conexión que se pueden utilizar son: el cable coaxial de banda ancha y el cable de fibra óptica.

1.6 TECNICAS DE CODIFICACION

Las técnicas de codificación consisten en cambiar:

- Datos digitales, señales digitales
- Datos digitales, señales analógicas
- Datos analógicos, señales digitales
- Datos analógicos, señales analógicas

Los factores que se deben de tener en cuenta para utilizar un buen sistema de codificación:

- Espectro de la señal: La ausencia de componentes de altas frecuencias disminuye el ancho de banda. La presencia de componente continua en la señal obliga a mantener una conexión física directa (propensa a algunas interferencias). Se debe concentrar la energía de la señal en el centro de la banda para que las interferencias sean las menores posibles.

- Sincronización: para separar un bit de otro, se puede utilizar una señal separada de reloj (lo cuál es muy costoso y lento) o bien que la propia señal porte la sincronización, lo cuál implica un sistema de codificación adecuado.

- Detección de errores: es necesaria la detección de errores ya en la capa física.

- Inmunidad al ruido e interferencias: hay códigos más robustos al ruido que otros.

- Costo y complejidad: el costo aumenta con el aumento de la razón de elementos de señal.

Dependiendo de la aplicación y el medio de transmisión de la señal es como se escoge el tipo de codificación a utilizar.

Para nuestra tesis, consideramos conveniente solo mencionar las dos primeras técnicas de codificación, que son las utilizadas en las redes de comunicación de área local para la transmisión de los datos

1.6.1 CODIFICACION DIGITAL (Datos digitales representados por datos digitales)

Una señal digital es una secuencia discreta de pulsos discontinuos de voltaje, cada pulso es un elemento de la señal y se codifican para transmitir los datos binarios de la misma. Son los códigos de línea los que se encargan de dar un formato de señalización a los unos y ceros. En el caso más simple con

un elemento de señal representamos un bit, es decir, un 0 binario se representa con un pulso negativo y un 1 binario con un pulso positivo.

Con esto decimos que un bit se puede representar por más de un elemento de señal, siendo necesario definir la taza de datos y la taza de modulación.

La taza de datos es la cantidad de bits que se transmiten por segundo y se mide en bits/seg. La taza de modulación es la cantidad de elementos de la señal por segundo y se mide en baudios.

Existen diversos códigos de línea con los que se busca satisfacer necesidades entre el transmisor y receptor como son:

- Sincronización: es necesario determinar cuando empieza y cuando termina el intervalo de un bit para decodificarlo adecuadamente.

- Detección de errores: los códigos deben permitir detectar los errores fácilmente.

- Ancho de banda: debe ser lo más pequeño posible.

- Espectro de la señal: el espectro de la señal debe ser menor que el canal de transmisión para evitar la interferencia intersímbolos. Por esto no es deseable una componente de corriente directa en la codificación, ya que la potencia de la señal es insignificante en frecuencias cercanas a cero, lo que implica que éstas puedan perderse; los componentes de corriente alterna son los más deseables para la transmisión, los cuales se pueden centrar en una portadora a mitad del espectro.

- Costo y complejidad: es importante tener en cuenta el costo de codificación y decodificación de los datos, así como la complejidad del mismo.

Las técnicas de codificación más comunes son la de NRZ, bipolar, bifase y técnicas de scrambling, y se describen a continuación:

NO RETORNO A CERO

Es el camino más común y fácil para transmitir señales digitales usando dos niveles de voltajes diferente para los dígitos binarios, este código se caracteriza porque el nivel de voltaje es constante durante el intervalo de un bit, esto es, no hay transición, un 0 binario se representa con un voltaje positivo constante y un 1 binario por un nivel de voltaje negativo, este código mas tarde se conoció como NRZ (NRZ-L, non return—to-zero-level)

Una variación del NRZ-L es conocido como NRZI (non return to zero, invert on ones) los datos se codifican con la presencia o ausencia de una transición de la señal. Una transición (de alto a bajo o viceversa) representa un

NRZ-No Retorno a Nivel Cero
NRZI-No Retorno a Cero con Inversión a Uno

uno binario, una ausencia de transición indica un cero binario, lo que significa que el voltaje se mantiene en el último nivel de tensión leído.

El NRZI es un ejemplo de un código diferencial. En éste tipo de códigos, la señal se decodifica en base a la polaridad del nivel anterior. El beneficio de éste tipo de esquemas es que es más fácil detectar un transición ocasionada por ruido. En un código NRZ-L todos los unos y ceros pueden ser invertidos, pero en un código NRZI, esto no puede suceder.

Los problemas principales de estos códigos es que una cadena larga de unos o ceros para NRZ-L, o una cadena larga de ceros para NRZI puede ocasionar una pérdida de sincronización, debido a que los niveles de tensión son constantes en un periodo largo de tiempo.

Por su simplicidad, los códigos NRZ comúnmente son usados para grabaciones digitales.

BINARIO MULTINIVEL

Estos códigos utilizan más de dos niveles de señal. Existen dos tipos de códigos binarios multinivel, el bipolar- AMI y el pseudoternario.

En el bipolar-AMI un 0 binario es representado por una ausencia de señal, y un 1 binario es representado por un pulso negativo o positivo alternante. Con este esquema es fácil detectar errores. Si un error aislado, borra o agrega un pulso, causa una violación en las propiedades del código. Otro beneficio de este esquema es que permite una buena sincronización entre el transmisor y receptor cuando se codifican unos, aunque el problema de una cadena larga de ceros persiste.

Las propiedades del código bipolar-AMI son aplicables al código pseudoternario, sólo que en este esquema un 1 binario se representa por una ausencia de señal y un O binario con la transición de pulsos negativos y positivo alternantes. Para éste código una cadena largas de unos será un problema para la sincronización.

BIFASE

Otros código alternativos son los bifase, que solucionan las limitaciones de los NRZ, éstas dos técnicas son la Manchester y la Manchester diferencial.

En el código Manchester, hay una transición a mitad del intervalo de cada bit, un 0 binario se representa por una transición de un nivel alto a un bajo y un 1 binario con una transición de un nivel bajo a alto.

En el código Manchester diferencial, un 0 binario se representa con una transición al principio de cada periodo de bit, y un 1 binario es representado por ausencia de transición al principio de cada periodo de bit.

NRZ-No Retorno a Cero
NRZI-No Retorno a Cero con Inversión a Uno

El inconveniente de estos códigos es que requieren un mayor ancho de banda respecto a los códigos anteriores, sin embargo, presentan ventajas como son:

- Sincronización: debido a la transición durante cada intervalo de bit, el receptor puede sincronizarse.

- Detección de error: La ausencia de una transición esperada puede usarse para detectar errores, aunque el ruido podría invertir ambas señales, antes y después de la transición esperada y causar un error no identificado.

Los códigos bifase son técnicas populares para la transmisión de datos. El más común es el Manchester especificado para el estándar IEEE 802.3 (cable coaxial banda base y par trenzado) en redes bus CSMA/CD. Por otra parte el código Manchester diferencial ha sido especificado para redes en anillo, estándar IEEE 802.5 Token Ring, par trenzado sin apantallar.

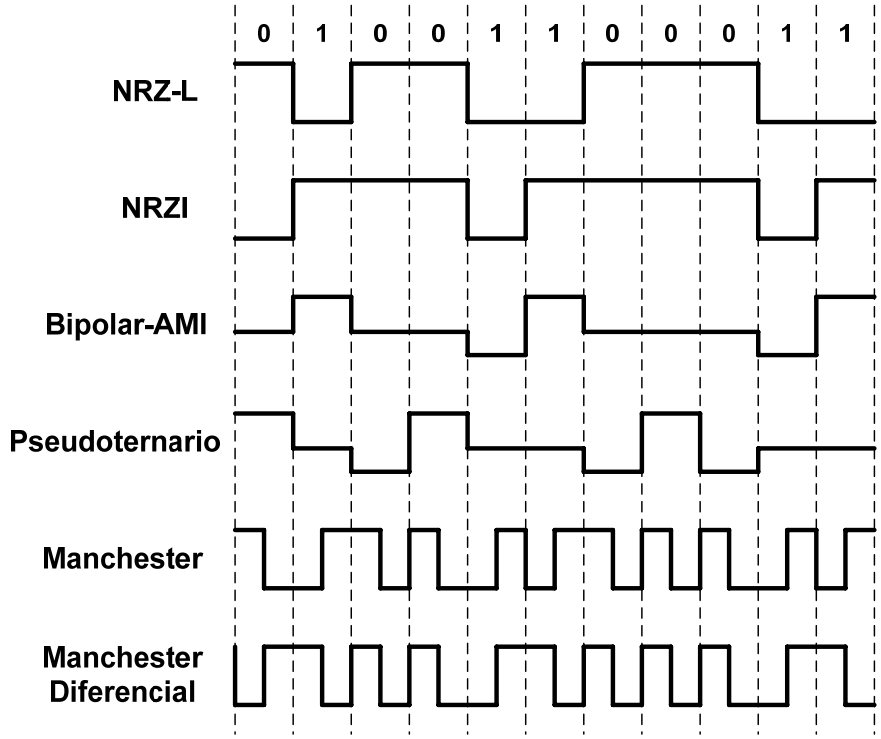


Figura 1.7 Técnicas de Codificación

TÉCNICAS DE SCRAMBLING

Aunque las técnicas bifase son comunes en redes LAN, no han podido ser utilizadas en redes de larga distancia debido a que requieren una lata taza de señalización y da datos que las hace muy costosas para aplicaciones de larga distancia.

CSMA/CD- Acceso múltiple con detección de portadora y detección de colisiones
IEEE- Instituto de Ingenieros Eléctricos-Electrónicos
LAN-Red de Area Local

Las técnicas de scrambling resuelven éstos problemas, se basa en el código bipolar AMI, solucionando el inconveniente de una cadena larga de ceros.

La idea consiste en reemplazar dicha secuencia que ocasiona niveles de voltaje constante por una que provee las suficientes transiciones que ayuden al receptor a sincronizarse. La secuencia resultante es reconocida por el receptor y reemplazada por la secuencia de datos original, el beneficio también radica en que la secuencia original y la resultante son de la misma longitud, lo que implica que no hay un incremento de datos.

Son dos las técnicas de scrambling existentes, en Norte América se usa el bipolar con sustitución de 8 ceros (bipolar with 8 substitution, B8ZS) y en Europa y Japón se usa el bipolar de 3 ceros de alta densidad (hihg-density bipolar 3-zeros, HDB3).

En el esquema B8ZS el 1 binario se representa como en el código bipolar AMI, con nivel positivo y negativo alternante, para el cero binario se codifica de la siguiente manera:

Si aparece un octeto donde todos son ceros, y el pulso de voltaje anterior a dicho octeto fue positivo, éste se codifica como 000+-O-+.

Si aparece un octeto donde todos son ceros, y el pulso de voltaje anterior a dicho octeto fue negativo, éste se codifi.ca como 000-+O+-.

Para el esquema HDB3, el 1 binario se representa como nivel positivo y negativo alternante, y el 0 binario se codifica dependiendo de la polaridad del pulso anterior y si la última violación fue par o impar, esto se ejemplifica en la tabla siguiente:

Polaridad del pulso anterior	Impar	Par
-	000-	+00+
+	00+	-00-

Tabla 1.1Codificación HDB3

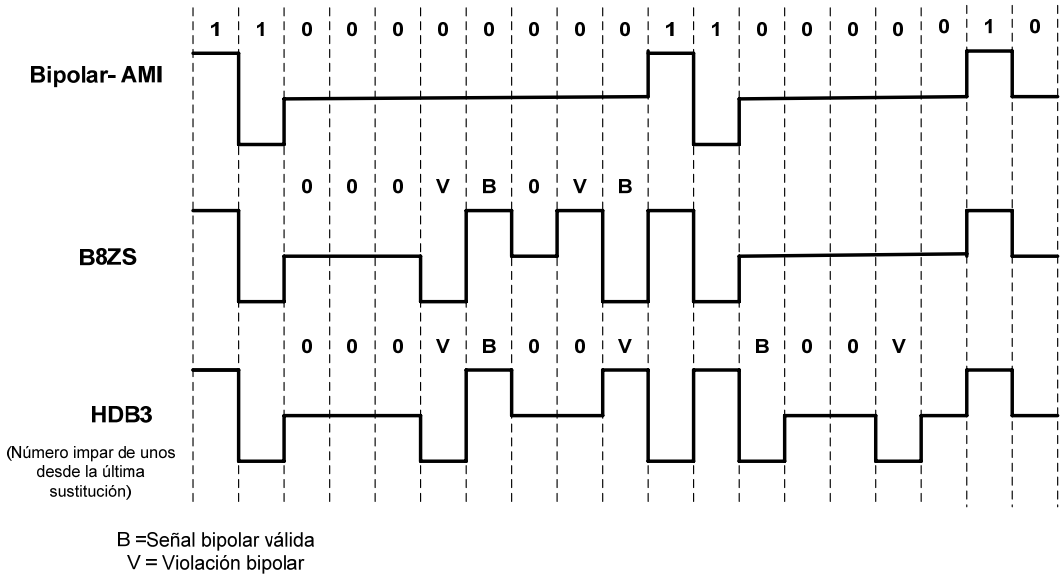


Figura 1.8 Técnicas de Scrambling

1.6.2 CODIFICACION DIGITAL-ANALOGICA (Datos digitales representados por señales analógicas)

Algunas veces, dependiendo de las características del medio, necesitarnos convertir las señales digitales que emiten los ordenadores en señales analógicas que puedan viajar satisfactoriamente por el medio utilizado. La aplicación más común de ésta técnica de codificación la utiliza la red pública telefónica la cual fue diseñada para recibir, transmitir y conmutar datos analógicos, como la voz, en un rango de frecuencias de 300 a 3400 Hz. Debido al surgimiento de las redes y a la facilidades que ellas otorgan, la necesidad de transmitir datos desde los hogares se ha incrementado, es por ello que se codificaron los datos digitales para poder viajar como señales analógicas dentro de la red telefónica. Este tipo de codificación lo permite un dispositivo llamado MODEM, que se encarga de convertir las señales digitales en analógicas y viceversa.

Para convertir las señales digitales en analógicas se debe modular la señal, esto es cambiar algún parámetro de la señal original mediante una frecuencia portadora, dichos parámetros pueden ser la amplitud, frecuencia o fase.

Amplitud: Es el nivel máximo de voltaje de la onda, para la fibra óptica es la mayor intensidad de luz.

Frecuencia: Es el número de veces que se repite un ciclo o una oscilación de la onda en un segundo.

Fase: Es el punto donde comienza el ciclo de la onda y se mide en grados. En la figura 1.9 se ejemplifican los parámetros anteriores.

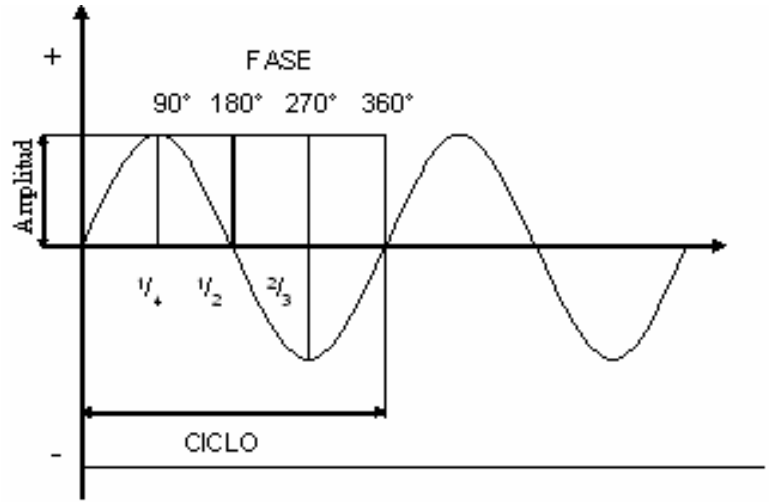


Figura 1.9 Parámetros de una onda

De acuerdo al parámetro modificado de la señal, las técnicas de codificación son:

- Desplazamiento de amplitud (ASK, Amplitud-Shift Keying)
- Desplazamiento de frecuencia (FSK, Frecuency-Shift Keying)
- Desplazamiento de fase (PSK, Phase-Sliift Keying)

ASK

Con ésta técnica los dos valores binarios se representan mediante amplitudes diferentes de portadora.
Un 1 binario se representa con una portadora de amplitud constante y un O binario por ausencia de portadora, esto es, con una amplitud cero.

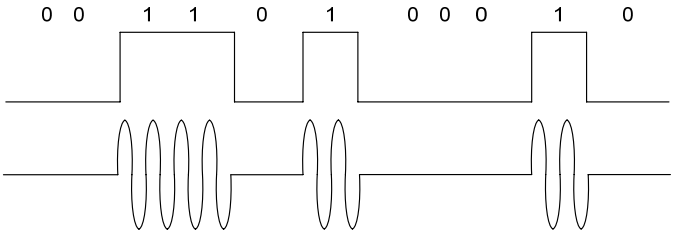


Figura 1.10 Desplazamiento de amplitud

La técnica ASK se utiliza para la transmisión de datos digitales en fibra ópticas, donde uno de los dos estados se representa por un pulso de luz, mientras el otro por una ausencia de luz.

FSK

En FSK los dos valores binarios se representan con dos frecuencias diferentes cercanas a la portadora.

Un 1 binario se representa con una señal de alta frecuencia y un O binario con una señal de baja frecuencia. FSK es menos susceptible a errores en comparación con ASK.

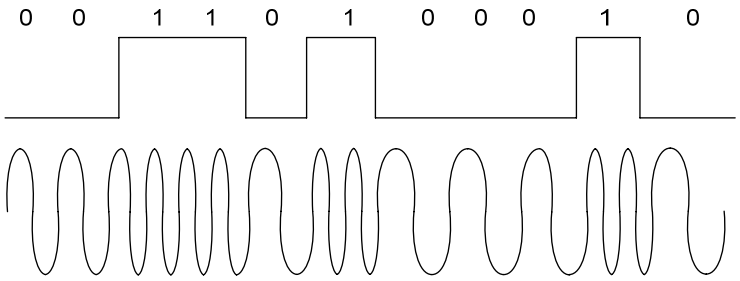


Figura 1.11 Desplazamiento de frecuencia

PSK

En éste esquema los dos valores binarios se representan desplazando la fase de la portadora.

Un 1 binario se representa con una señal cuya fase es opuesta a la fase de la señal que le precede y para un O binario la fase de la señal es la misma que la fase de la señal precedente.

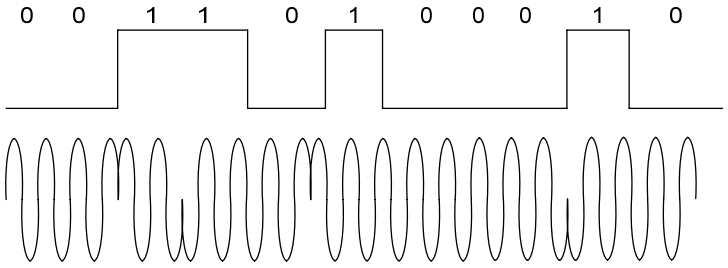


Figura 1.12 Desplazamiento de Fase

1.7 MEDIOS DE COMUNICACIÓN

Un medio de transmisión es un medio físico que transporta información en forma de señales electromagnéticas, éstos permiten interconectar los elementos de la red para llevar a cabo el intercambio de información entre las estaciones de trabajo y los servidores. Los medios de transmisión pueden ser clasificados en guiados y no guiados.

ASK-Modulación por Desplazamiento de Amplitud
FSK-Modulación por Desplazamiento de Frecuencia
PSK-Modulación por Desplazamiento de Fase

En los medios guiados las ondas se transmiten a lo largo de un medio sólido que puede ser un par trenzado (UTP[1]) cable coaxial y fibra óptica; en los medios no guiados, como la atmósfera y el espacio libre, las señales electromagnéticas viajan de manera dispersa, es por ello que en realidad no las guían ya que solo proporcionan un espacio para propagarse.

Las características y calidad de la transmisión de los datos son determinadas por las limitaciones del medio y las características de la señal; para los medios no guiados es más importante conocer el ancho de banda producido por la antena de transmisión que el conocer las limitaciones del medio.

Los puntos principales que hay que considerar en el diseño de un sistema de transmisión son la tasa de datos y la distancia, para determinarlos debemos considerar lo siguiente:

Ancho de banda: se debe considerar el mayor ancho de banda que permita el medio, así como la más alta tasa de datos que se pueda transmitir.

Daños en la transmisión: se considera la atenuación, que es un factor que limita la distancia a la que podemos transmitir.

Interferencia: es un fenómeno que ocasiona que los componentes de una señal se pierdan o distorsionen, esto es causado por bandas de frecuencia cercanas a la usada en la transmisión provocando un traslape en ella, esto aun que es un problema común para los medios no guiados también podemos encontrarlo en los medios guiados, causado por la cercanía de cables.

1.7.1 MEDIOS DE TRANSMISION DE DATOS UTILIZADOS EN REDES

Los medios de transmisión de datos más utilizados para redes de área local son:

A) UTP

CABLE DE PAR TRENZADO

Este cable consiste en pares de hilos de cobre trenzados y recubiertos de una capa aislante externa, el uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. El UTP (unshielded twisted pair) es el medio habitual en telefonía, es barato, fácil de instalar y manipular. Los conectores que se utilizan son los denominados RJ45 y RJ1 1.

Se usan para transmitir tanto señales digitales como analógicas; para señales analógicas, se necesitan amplificadores cada 5 0 6 Km. Para transmisión digital, se requieren repetidores cada 2 o 3 Km.

[1] **UTP**-Cable de Par Trenzado Sin Apantallar

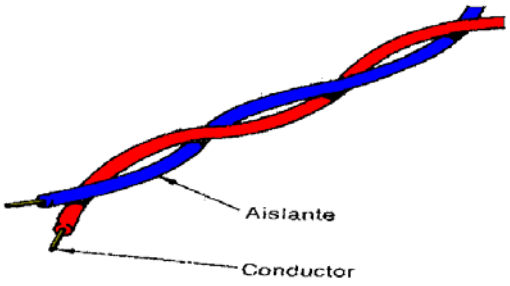


Figura 1.13 Cable de par trenzado

En función de sus características se clasifica en cuatro categorías:

- Categoría 2: Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 4 Mbps.

- Categoría 3: Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 10 Mbps con longitudes de segmento inferiores a 100 metros y una longitud máxima de red de 500 metros. Las trenzas por unidad de distancia son de 7.5 a 10 cm.

- Categoría 4: Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 16 Mbps (actualmente está en desuso).

- Categoría 5: Es un cable de cobre de dos pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 100 Mbps. Las trenzas son del orden de 0.6 a 0.85 cm. (actualmente, al reducirse su coste es el que está siendo más utilizado).

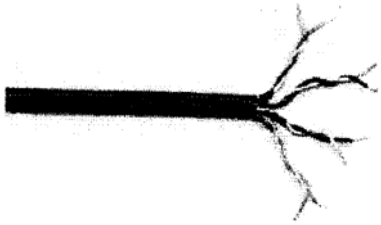


Figura 1.14 Cable de par trenzado nivel 5

B) CABLE COAXIAL

En un cable que consiste en un núcleo de cobre rodeado por material aislante, el cual a su vez esta rodeado por una malla metálica que ayuda a bloquear las interferencias, todo el cable está envuelto en una capa protectora. Tiene un diámetro aproximado de 1.25 cm.

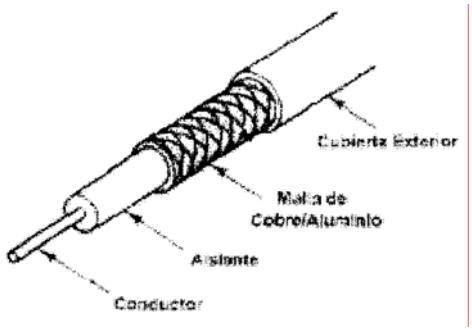


Figura 1.15 Cable Coaxial

La nomenclatura de los cables Ethernet tiene tres partes:

- La primera indica la velocidad en Mbits/seg.
- La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD).
- La tercera los metros de segmento multiplicados por 100.

CABLE	CARACTERISTICAS
10-BASE-5	**Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 500 metros.**
10-BASE-2	**Cable coaxial fino (Ethernet fino). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 185 metros.**
10-BROAD-36	**Cable coaxial Segmentos: máximo de 3600 metros. Velocidad de transmisión: 10 Mb/seg.**
100-BASE-X	**Fast Ethernet. Velocidad de transmisión: 100 Mblseg.**

Tabla 1.2 Tipos de cable coaxial

CABLE COAXIAL DE BANDA BASE

Es un cable de 50 W con una resistencia de 50 para transmisión digital, trasmite una sola señal a una velocidad de transmisión alta.

En función de sus características se clasifica en dos categorías:

- CABLE COAXIAL GRUESO (1OBASE5). Tiene un grosor de 1.27 cm, lleva un conector tipo N, alcanza una velocidad de transmisión de

10 Mbps y una longitud máxima de 500 metros de segmento de red. También se denomina Thiek Ethernet.

- CABLE COAXIAL DELGADO (1 OBASE2). Tiene un grosor de 0.63 cm, lleva un conector tipo BNC, alcanza una velocidad de transmisión de 10 Mbps y una longitud máxima de 200 metros de segmento de red. También se denomina Thin Ethernet.

C) FIBRA OPTICA

Una fibra óptica es un medio de transmisión de luz que consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura.

En la superficie de separación entre el núcleo y la envoltura se produce el fenómeno de reflexión total de la luz, al pasar este de un medio más denso (índice de refracción mayor) a otro menos denso (índice de refracción menor). Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra.

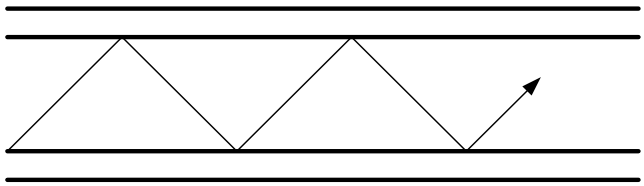


Figura 1.16 Reflexión de la luz en la fibra óptica

Está formado por tres componentes:

Transmisor de energía óptica. Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.

Fibra óptica. Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

Detector de energía óptica. Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para regenerar la señal).

Puede alcanzar velocidades muy altas a grandes distancias sin necesidad de usar repetidores.

Existen dos tipos de fibra óptica:

MULTIMODO: en éste tipo de fibra los rayos que inciden en la frontera con un ángulo mayor al critico se reflejarán internamente, muchos rayos estarán rebotando con ángulos diferentes, diciendo así que cada rayo tiene un modo diferente. Esto conlleva a que cada rayo reflejado tenga una longitud diferente y por tanto diferente tiempo de propagación. Esto hace que los elementos de señalización que se transmitan se dispersen en el tiempo, limitando la velocidad a la que los datos puedan ser correctamente recibidos. Este tipo de fibra es más adecuada para la transmisión a corta distancia. Tiene una circunferencia interna de aproximadamente 9 y circunferencia exterior de aproximadamente 125 µm.

MONOMODO: Cuando el radio del núcleo se reduce, la reflexión total se dará en un número menor de ángulos, la fibra actúa como una guía de onda y la luz se puede propagar solo en línea recta, sin rebotar, obteniéndose un modo único de transmisión. Esta fibra es más cara pero puede transmitir datos a varios Gbps a una distancia de 30 Km., tiene una circunferencia interna de aproximadamente 50 rn y circunferencia exterior de aproximadamente 125 µm.

MULTIMODO DE INDICE GRADUAL: existe un tercer modo de transmisión variando gradualmente el índice de refracción del núcleo. Estas fibras al disponer de un índice de refracción superior en la parte central, hace que los rayos de luz avancen más rápidamente conforme se alejan del eje axial de la fibra. En lugar de describir un zigzag, la luz en el núcleo describe curvas helicoidales debido a la variación gradual del índice de refracción, reduciendo así la distorsión multimodal. El efecto de la mayor velocidad de propagación en la periferia del núcleo se traduce en que aún recorriendo distancias superiores todos los rayos llegan aproximadamente igual en los mismos tiempos.

1.7.2 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 última recibe información analógica que convierte en digital, para ser enviada al computador.

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. Respecto del computador al cual esta conectado, recibe e interpreta comandos de éste (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 módems deben operar con el mismo estándar de comunicación y 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.

1.8 DISPOSITIVOS PARA REDES

Los dispositivos de interconexión de red sirven para facilitar la conexión de redes de área local con otras redes que pueden ser también de área local o de área amplia. Existen varios tipos de dispositivos apropiados para las necesidades de interconexión de la red, estos dispositivos son:

- Gateways
- Bridges
- Router
- Hub
- Switches

1.8.1 GATEWAYS

Las compuertas son dispositivos de hardware y software que permite la comunicación de dos redes que tienen diferentes protocolos. Las compuertas realizan otra función que es la de fragmentar los paquetes de la red para facilitar la comunicación

1.8.2 BRIDGES

Los puentes interconectan redes en el nivel de enlace de datos, éstos pueden leer la dirección fuente en las tramas de datos y la dirección destino, debido a esto, pueden evaluar si la dirección destino indica un nodo de una red remota para enviarlo a dicha red o si la dirección destino reside en la red local para filtrarla, por este funcionamiento los puentes son usados para interconectar dos o más segmentos de red de área local, a los cuales se les denomina segmentos de red o subredes que evitan el tráfico de las misma.

Como los puentes regeneran las tramas y sus formatos, pueden extenderse a distancias ilimitadas utilizando diferentes medios de transmisión, otra característica es que pueden interconectar redes de un mismo protocolo o de diferente. Controla el flujo de datos, maneja error de transmisión, proporciona direccionamiento físico y maneja el acceso al medio.

1.8.3 ROUTER

Un router o encaminador, es un conmutador de paquetes que opera en el nivel de red de OSI. Su función es analizar y encaminar la información, esto es, seleccionar el camino idóneo que debe seguir el paquete, tomando en cuenta factores como, líneas más rápidas, más baratas y menos saturadas.

Permite conectar tanto redes de área local como redes de área extensa, por esta característica se utilizan para conectar redes geográficamente separadas. Proporciona un control de tráfico y funciones de filtrado a nivel de red. Este dispositivo trabaja con direcciones IP.

1.8.4 HUB

Los HUBS trabajan en el nivel fisico de OSI, su propósito es regenerar y retemporizar la señal, también se le denomina repetidor multipuerto porque permiten compartir el uso de una línea entre varios computadores que se conectan en él.

Todos los computadores conectados a los concentradores pueden usar la línea, aunque no de forma simultánea, ni utilizando distintos protocolos, ni distintas velocidades de transmisión. El ancho de banda se divide entre el número de elementos conectados a los puertos del dispositivo.

1.8.5 SWITCHES

Es un dispositivo del nivel de enlace de datos de OSI, los switches toman decisiones basándose en las direcciones MAC haciendo la red más eficiente. Su función principal es conmutar los datos solo hacia el puerto correspondiente al destinatario. La diferencia entre un conmutador y un puente (bridge) es que el puente debe recibir todo el paquete antes de dirigirlo al puerto correspondiente y un conmutador dirige el paquete a su destino una vez recibido el encabezado del paquete (en ella se encuentra la dirección IP del destinatario). Gracias a ello, los conmutadores producen un retraso mínimo en la conmutación (del orden de 40 microsegundos, mientras que el puente supera los 1.000 microsegundos).

De esta manera, utilizando un conmutador se puede dividir una red en varios segmentos y limitar el tráfico al segmento o segmentos a los que pertenece el paquete. Su utilización permite que cada usuario o grupo de usuario tenga su propio segmento dedicado con ancho de banda dedicado.

IP-Protocolo de Internet
MAC-Control de Acceso al Medio
OSI-Interconexión de Sistemas Abiertos

CAPITULO II. ARQUITECTURA DE RED

OBJETIVO PARTICULAR

Conocer y entender el funcionamiento interno de una red, así como, los procedimientos más importantes suscitados en la comunicación.

2.1 ARQUITECTURA

La arquitectura de red es la encargada de determinar las reglas que rigen el diseño y la operación de hardware y software que forman la red, la cual esta determinada por diversos componentes como son:

- El tipo de cableado: aquí podemos encontrar vario tipos de cable como lo son el UTP (en sus diversos niveles), el cable coaxial y la fibra óptica.

- La topología: que pueden ser (como ya se ha mencionado) de estrella, anillo, malla, bus, árbol, ya sea lógica o físicamente.

- El tipo de transmisión: en el que encontramos la transmisión digital o analógica.

- Los protocolos: existen una gran cantidad de protocolos, entre los cuales podemos mencionar, para redes LAN, la ethernet, token ring, FDDI, que determinan como se lleva a cabo la comunicación y los servicios que cada capa provee a la siguiente.

2.2 MODELOS OSI

El modelo OSI (Open Systems Interconnection, Interconexión de Sistemas Abiertos), fue propuesto por la Organización Internacional de Normalización (ISO), la cual es una organización no gubernamental fundada en 1947, que tiene por misión la coordinación del desarrollo y aprobación de estándares a nivel internacional.

El modelo OSI, trata de establecer las bases para la definición de protocolos de comunicación entre sistemas informáticos.

Propone dividir en niveles todas las tareas que se llevan a cabo en una comunicación entre computadoras. Todos los niveles están bien definidos y no interfieren con los demás. De ese modo, si fuera necesario una corrección o modificación en un nivel, no afectará al resto.

FDDI- Interfaz de datos distribuida por fibra
LAN-Red de Area Local
UTP-Cable de Par Trenzado Sin Apantallar

En total se forman siete niveles (los cuatro primeros tienen funciones de comunicación y los tres restantes de proceso). Cada uno de los siete niveles dispone de los protocolos específicos para el control de dicho nivel.

NIVELES MODELO OSI	
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Físico

Tabla 2.1 Niveles del Modelo OSI

2.2.1 DESCRIPICION DEL MODELO OSI

NIVEL FÍSICO

En este nivel se definen las características eléctricas, mecánicas, funcionales y de procedimiento de la red necesaria para establecer y mantener la conexión física, así como las dimensiones físicas de los conectores, los cables y los tipos de señales que van a circular por ellos.

Las características eléctricas relacionan la representación de los bits, la velocidad de transmisión de ellos y la modulación utilizada.

Las características mecánicas relacionan las propiedades físicas de la interfaz con el medio de transmisión, así como la descripción de un conector que une una o más líneas entre los dos extremos (interfaces serie o paralelo).

Relacionadas con el protocolo de comunicación a nivel físico, estarían las características funcionales y de procedimiento. Las primeras indican el significado de cada uno de los circuitos del conector de la interfaz, y la segunda la secuencia de eventos y señales que deben producirse para que la comunicación se lleve a cabo.

Los sistemas de redes locales más habituales definidos en este nivel son: Ethernet, red en anillo con paso de testigo (Token Ring) e interfaz de datos distribuidos por fibra (FDDI, Fiber Distributed Data Interface).

El PDU (Protocol Datagram Unit, Unidad de Datos del Protocolo) del nivel físico es el bit.

NIVEL DE ENLACE DE DATOS

Este nivel tiene como función principal realizar una comunicación virtualmente libre de errores entre entidades de nivel de red, empleando para ello el servicio proporcionado por el nivel físico. De ésta forma se consigue que las entidades de red no tengan que preocuparse de dos de los principales

problemas de la comunicación de datos como son, los errores y la diferencia de velocidad y recursos de los dos sistemas enlazados, ya que las tareas principales del nivel de enlace de datos son:

- Control de errores, cuyo objetivo es verificar que la información sea recibida correctamente mediante métodos de comprobación algorítmica como el CRC o FCS.

- Control de flujo, que consiste en los procedimientos necesarios para que un transmisor rápido no abrume a un receptor lento.

Las normas Ethernet y Token Ring están definidas en este nivel.

La PDU del nivel de enlace es la trama.

NIVEL DE RED

Este nivel se encarga de determinar la ruta que debe seguir un paquete a través de las subredes para alcanzar el destino a partir del origen y controlar la congestión de la subred.

La PDU del nivel de red es el paquete.

Entre los protocolos más utilizados definidos en este nivel se encuentra el Protocolo de Internet (IP, Internet Protocol).

NIVEL DE TRANSPORTE

Asegura la transferencia de la información a pesar de los fallos que pudieran ocurrir en los niveles anteriores, detecta los bloqueos, caídas del sistema y asegura la igualdad entre la velocidad de transmisión y la velocidad de recepción, así como, la búsqueda de rutas alternativas. Su función básica es aceptar datos procedentes del nivel de sesión, encapsularlos en PDUs de nivel de transporte de manera que la información llegue correcta al otro extremo.

La PDU del nivel de transporte es el paquete de transporte.

Entre los protocolos de este nivel más utilizados se encuentran el Protocolo de Control de la Transmisión (TCP, Transmission Control Protocol) de Internet y NetB1OS/NetBEU1 de Microsoft.

NIVEL DE SESIÓN

Organiza las funciones que permiten que dos usuarios se comuniquen a través de la red, algunas funciones son, tareas de seguridad, contraseñas de usuarios y la administración del sistema.

La PDU del nivel de sesión es la transacción o mensajes.

CRC-Verificación por Redundancia Cíclica
PDU-Unidad de Datos del Protocolo

NIVEL DE PRESENTACIÓN

Este nivel tiene como misión fundamental el compatibilizar los sistemas de representación y manipulación de la información de las entidades que se comunican, es decir, traduce la información del formato de la máquina a un formato comprensible por los usuarios (se incluye el control de las impresoras, emulación de terminal y los sistemas de codificación).

NIVEL DE APLICACIÓN

Se encarga del intercambio de información entre los usuarios y el sistema operativo como, la transferencia de archivos, los programas de aplicación y el correo electrónico.

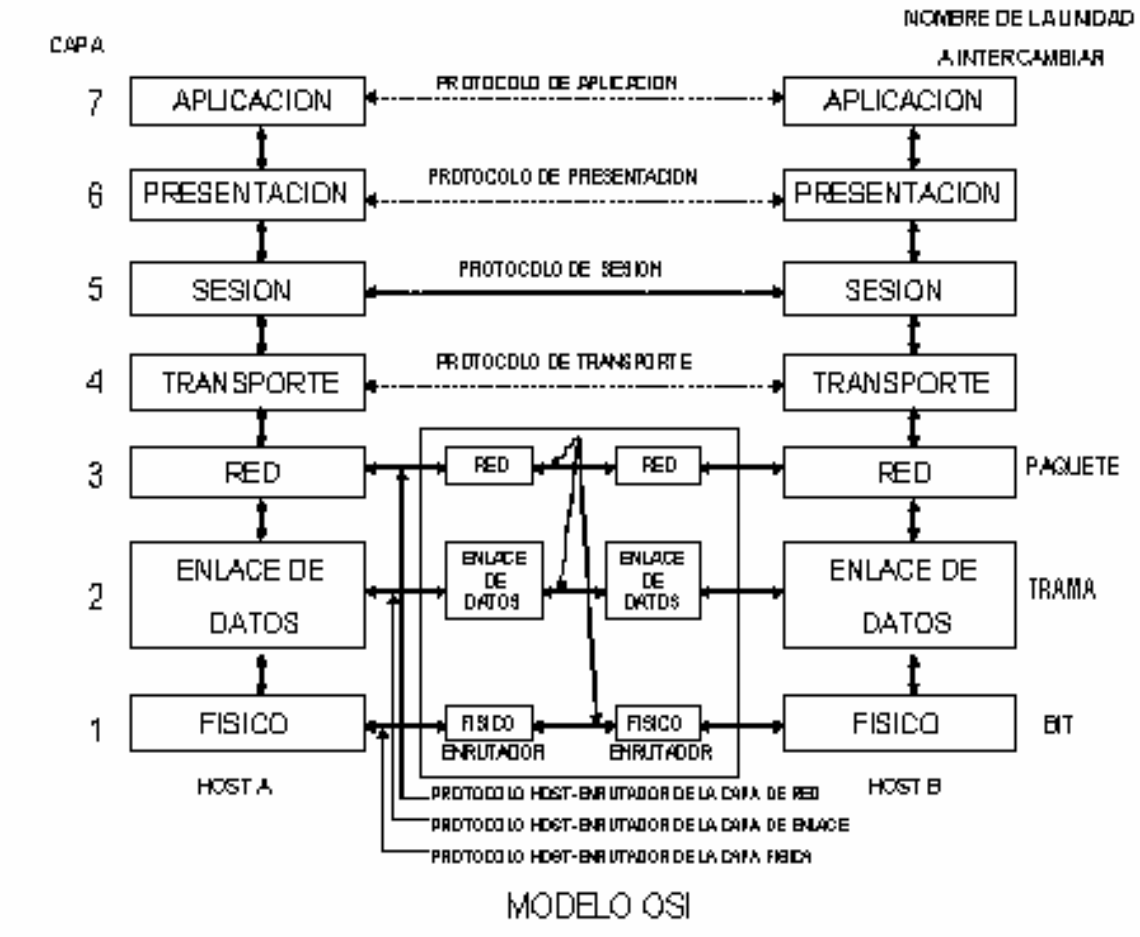


Figura 2.1 Comunicación de niveles

PROCESO DE LA COMUNICACION

El proceso que sigue la información desde que un usuario envía un mensaje hasta que llega a su destino consiste en una bajada a través de todos los niveles (con sus correspondientes protocolos) desde el nivel séptimo hasta llegar al primero. Allí se encontrará en el canal de datos que le dirigirá al

usuario destino y volverá a subir por todos los niveles hasta llegar al último de ellos.

- Los niveles inferiores proporcionan servicios a los niveles superiores.
- Cada nivel dispone de un conjunto de servicios.
- Los servicios están definidos mediante protocolos.
- Los programadores y diseñadores de productos sólo deben preocuparse por los protocolos del nivel en el que trabajan, los servicios proporcionados a los niveles superiores y los servicios proporcionados por los niveles inferiores.

2.3 SERVICIO ORIENTADO A CONEXION Y SIN CONEXIÓN

Un servicio **orientado a conexión** es semejante al modelo telefónico ya que el emisor y el receptor establecen una conexión, la usan y después la liberan. Es un servicio confiable debido a que el receptor acusa cada mensaje recibido, de tal forma que el emisor esta seguro de que éste fue entregado.

En este servicio cada una de las tramas se enumera para asegurar que los paquetes se reciban en el orden en que fueron enviados y con ello controlar el acuse de recibo. Sin embargo el acuse de recibo introduce una sobre carga y retardos que deben evaluarse sobre la aplicación para determinar si vale la pena realizarlo.

Por ejemplo en aplicaciones como el tráfico de voz digitalizada los retrasos que introducen los acuses de recibos son inaceptables, en otras palabras al mantener una conversación es aceptable oír un poco de ruido en la línea o una palabra confusa de vez en cuando que esperar un acuse de recibo.

El procedimiento para establecer la conexión es el siguiente:

El emisor envía al receptor una **petición de llamada** solicitando la conexión lógica, si el receptor acepta la petición envía un paquete de **llamada aceptada** para establecer una ruta, dado que el camino es fijo durante la conexión lógica, éste es similar a un circuito en redes de conmutación de circuitos y se le llama circuito virtual. Además de los datos, cada paquete contiene un identificador de circuito virtual en lugar de una dirección destino. Cada nodo de la ruta preestablecida sabe hacia dónde dirigir los paquetes, no siendo necesaria las decisiones de encaminamiento. Para finalizar, en cualquier momento, las estaciones pueden enviar un paquete **de petición de liberación**. Una estación puede disponer en un instante de tiempo dado de más de un circuito virtual hacia otra estación así como de circuitos virtuales a más de una estación.

Si dos estaciones desean intercambiar datos durante un periodo de tiempo largo, existen ciertas ventajas al utilizar la técnica de circuitos virtuales.

En primer lugar, la red puede ofrecer servicios sobre el circuito virtual, incluyendo orden secuencial y control de errores. El orden secuencial hace referencia al hecho de que, dado que los paquetes siguen la misma ruta, éstos se reciben en el mismo orden en que fueron enviados. El control de errores es un servicio que asegura que los paquetes no sólo se reciben en orden, sino que además son correctos. Por ejemplo, si un paquete en una secuencia del nodo 4 al 6 no llega a este último, o se recibe erróneamente, el nodo 6 puede solicitar al nodo 4 la retransmisión del paquete. Otra ventaja es que los paquetes viajan por la red más rápidamente haciendo uso de circuitos virtuales, ya que no es necesaria una decisión de encaminamiento para cada paquete en cada nodo.

El servicio **orientado a la no conexión** es similar al sistema postal, donde cada carta lleva la dirección completa de destino, las cuales se pueden encaminar en el sistema de manera independiente, así que, si dos mensajes se envían al mismo destino pueden llegar de manera desordenada en comparación de cómo fueron enviados.

El servicio sin conexión se conoce como no confiable ya que no se cuenta con un acuse de recibo, sin embargo, existe una variante de este servicio con acuse de recibo.

- Servicio no orientado a conexión y sin acuse de recibo. Este tipo de servicio es apropiado cuando la tasa de error es muy baja (redes locales fibra óptica) y se deja la misión de comprobar y corregir los datos de de la transmisión a las capas superiores (nivel de red o de transporte).

- Servicio no orientado a conexión con acuse de recibo, se produce un acuse de recibo para cada trama enviada, de esta manera el emisor puede estar seguro de que ha sido recibida. Suele utilizarse en redes con más tasa de error, por ejemplo redes inalámbricas.

El servicio orientado a no conexión también se conoce como datagrama donde no existe la fase de establecimiento de llamada, de esta forma, si una estación desea enviar sólo uno o pocos paquetes, el envío datagrama resultará más rápido, además de que, si se produce congestión en una parte de la red, los datagramas entrantes se pueden encaminar siguiendo rutas lejanas a la zona de congestión lo que no sucede en la técnica de circuitos virtuales, donde los paquetes siguen una ruta predefinida, por lo que es más difícil para la red solucionar la congestión, debido a esto si un nodo falla se perderán todos los circuitos virtuales que atraviesan ese nodo.

La diferencia entre el servicio orientado a conexión y el orientado a no conexión con acuse de recibo es que el primero establece una ruta por la cual viajan todos los paquetes conforme se van enviando y el segundo, los paquetes viajan por distintas rutas llegando de forma desordenada.

2.4 TCP/IP

El modelo TCP/IP surgió en los 80's como una arquitectura generalizada de esquemas no propietarios, a la cual migraron la mayoría de los usuarios que para los años 90 se convirtieron en la totalidad, lo cual originó el crecimiento impresionante de Internet.

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre computadores de cualquier tipo de red o fabricante, respetando los protocolos de cada red individual.

El modelo TCP/IP consta de cuatro niveles funcionales, los cuales se ven en la Tabla 2.2

	OSI
7	APLICACIÓN
6	PRESENTACION
5	SESION
4	TRANSPORTE
3	RED
2	ENLACE DE DATOS
1	FISICO

TCP/IP
APLICACIÓN
TRANSPORTE
RED
INTERFAZ DE RED

Tabla 2.2 OSI VS TCP/IP

NIVEL DE INTERFAZ DE RED

La capa de interfaz de red se encarga de manejar las funciones de hardware y presentar una interfaz estandarizada para la capa de red. TCP/IP no especifica detalles para los protocolos usados en la interfaz de red.

La capa de interfaz de red es responsable de aceptar los mensajes que provienen de la capa de red y prepararlos para su transmisión sobre cualquier tecnología de enlace de datos, así como, circuito físico. Su función es similar a la capa física del modelo OSI.

NIVEL DE RED

Esta capa tiene como función principal permitir que los nodos coloquen paquetes de información en cualquier red y los hagan viajar de manera autónoma.

Los paquetes pueden llegar en un orden diferente de cómo fueron enviados, les corresponde a las capas superiores reacomodarlos, si se desea la entrega ordenada.

La capa de red define un formato de paquete y protocolo oficial llamado IP. El trabajo de la capa de red es entregar paquetes IP a donde fueron

OSI-Interconexión de Sistemas Abiertos
TCP/IP- Protocolo de Control de Transmisión /Protocolo de Internet

enviados. Los procesos más importantes de ésta capa son el ruteo de los paquetes y evitar la congestión. Debido a éstas funciones decimos que la capa de red TCP/IP es similar en funcionalidad a la capa de red OSI.

Los protocolos TCP/IP que operan en esta capa son:

- Protocolo de Internet (IP): es el núcleo de la familia de protocolos TCP/IP que es usado para encaminar los paquetes de un sistema a otro a través de la red.
- Protocolo de Control de Mensajes de Internet (ICMP): su función es reportar los errores que pueden ocurrir durante el enrutamiento de paquetes IP.
- Protocolo de Resolución de Direcciones (ARP): se encarga de convertir las direcciones IP en direcciones físicas de hardware.
- Protocolo de Resolución de Direcciones en Reversa (RARP): permite a los sistemas que no tiene una dirección IP obtenerla, traduciendo la dirección física de hardware a direcciones IP.

EL NIVEL DE TRANSPORTE

Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, TCP (transmission control protocol, protocolo de control de transmisión) es un protocolo confiable orientado a la conexión que permite que una corriente de bytes originada en una máquina se entregue sin errores en cualquier otra máquina de la red. Este protocolo fragmenta la corriente entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred.

En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga del control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo de esta capa, el UDP (user datagram protocol, protocolo de datagrama de usuario), es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa, como las transmisiones de voz o vídeo. La relación entre IP, TCP y UDP se muestra en la figura 2.3.

Los protocolos más importantes de la capa de transporte son:

- Protocolo de datagrama de usuario (UDP): es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo. Se usa para consultas de petición y respuesta de una sola ocasión o en las que la entrega pronta es más importante que la entrega precisa (voz y video).

OSI-Interconexión de sistemas abiertos
TCP/IP- Protocolo de Control de Transmisión /Protocolo de Internet

- Protocolo de Control de Transmisión (TCP): es un protocolo confiable orientado a la conexión que provee un control de secuencia y flujo a la entrega.

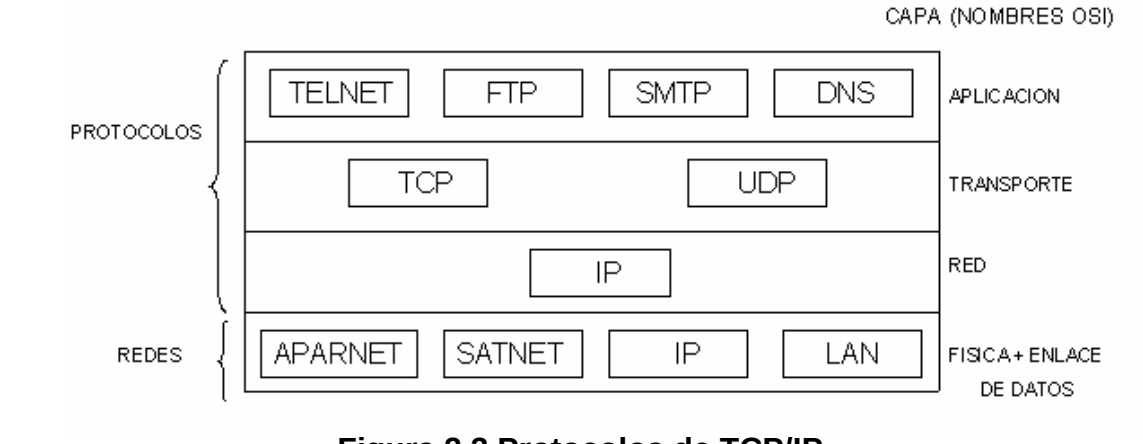


Figura 2.3 Protocolos de TCP/IP

EL NIVEL DE APLICACIÓN

El modelo TCP/IP no tiene capas de sesión ni de presentación. Encima de la capa de transporte está la capa de aplicación, que contiene todos los protocolos de alto nivel que proveen servicios a los usuarios de la red, como login remoto, archivos copiados y compartidos, correo electrónico, servicios de directorio y facilidades de gestión de red.

Entre los protocolos más comunes de ésta capa son:

- PING: es usado para pruebas de conectividad entre dos máquinas de la red.
- TELNET: se utiliza para la conexión remota, mediante la cual el usuario en una terminal o PC se conecta a un computador o dispositivo remoto y trabaja como si estuviese trabajando directamente en él.
- FTP (Protocolo de Transferencia de archivos): se utiliza para enviar archivos de un sistema a otro bajo el control del usuario. FTP puede transmitir datos binarios como datos en código ASCII.
- SMTP (Protocolo Simple de Transferencia de correo): utilizado para la transmisión de mensajes de correo, utiliza las listas de mensajería, la gestión de acuses de recibo y el reenvío de mensajes.
- SNMP (Protocolo Simple de Administración de Red): proporciona las herramientas para administrar y supervisar la red.
- DNS (Sistema de Nombres de Dominio): es un protocolo de resolución de nombres que traduce los nombres de las máquinas a direcciones IP.

PROCESO DE LA COMUNICACIÓN

TCP/IP permite al ordenador enviar datos a través de la subred a otro ordenador o, en caso de que el destino final este en otra subred, a otro dispositivo de encaminamiento. IP se implementa a todos los sistemas finales y dispositivos de encaminamiento, actúa como un portador que llevará bloques de datos desde un ordenador hasta otro, a través de uno o varios dispositivos de encaminamiento. TCP se implementa solo en los sistemas finales; guarda un registro de los bloques de datos para asegurar que todos se entreguen de forma segura a la aplicación apropiada.

Por ejemplo, cuando un usuario A desea enviar una información por el puerto 1 al puerto 2 del usuario B, la aplicación de A pasa el mensaje al TCP con la instrucción de enviarlo al puerto 2 del usuario B. El TCP pasa el mensaje al IP con la única instrucción de enviarlo al computador B, omitiendo la identidad del puerto destino. Por último IP pasa el mensaje a la capa de acceso a la red con la orden de enviarlo al dispositivo de encaminamiento.

Para controlar esta operación se debe transmitir información de control junto con los datos de usuario, cuando el emisor A genera un bloque de datos y lo pasa al TCP, éste puede que divida este bloque en fragmentos pequeños para hacerlos más manejables. A cada uno de estos fragmentos le agrega información de control denominada cabecera TCP, formando un segmento TCP. Esta información de control la utilizará la entidad par TCP en el computador receptor B. En la cabecera se incluyen los siguientes campos:

1. Puerto destino, es la dirección donde se entregan los datos.
2. Numero de secuencia, cada segmento enviado es enumerado secuencialmente para poder ser reordenado en la entidad par.
3. Suma de comprobación, se asigna un código calculado en función del resto del segmento. La entidad receptora realiza el mismo cálculo y lo compara con el código recibido.

Posteriormente TCP pasa cada segmento al IP con la única instrucción de los trasmita a B. Estos segmentos se transmitirán a través de una o varias subredes y serán retransmitidos en uno o más dispositivos de encaminamiento intermedio. IP añade una cabecera de información de control a cada segmento para formar un datagrama IP, en ésta cabecera además de otros campos se incluye la dirección del computador destino.

Finalmente cada datagrama IP se pasa a la capa de acceso a la red para que se envíe a través de la primera subred. La capa de acceso a la red también añade su propia cabecera creando así un paquete o trama.

El paquete se transmite a través de la red al dispositivo de encaminamiento. La cabecera del paquete contiene la información que la red necesita para transferir los datos, entre otros campos la cabecera de red contiene los siguientes:

1. Dirección de la red destino, es la dirección del dispositivo receptor conectado a la red.

2. Funciones solicitadas, el protocolo de acceso a la red puede solicitar funciones como la utilización de prioridades.

En el dispositivo de encaminamiento se elimina la cabecera del paquete y se examina la cabecera IP. El módulo IP del dispositivo de encaminamiento direcciona el paquete a través de la red 2 hacia B, basándose en la dirección destino que contiene la cabecera IP. Para esto se le agrega al datagrama una cabecera de acceso a la red.

Cuando se reciben los datos en B ocurre el proceso inverso, en cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediata superior, hasta que los datos de usuario se almacenen en el proceso destino.

Aunque estos son los pasos más importantes para la transmisión de datos en la arquitectura TCP/IP, ésta no exige que se haga uso de todas las capas, ya que es posible desarrollar aplicaciones que invoquen directamente a los servicios de cualquier capa.

2.5 CAPA DE ENLACE DE DATOS

En la capa de enlace de datos se encuentran las funciones asociadas a los servicios ofrecidos a los usuarios LAN, entre los que encontramos:

- En transmisión, ensamblado de datos en tramas con campos de dirección y detección de errores.
- En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
- Control de acceso al medio de transmisión LAN.
- Interfaz con las capas superiores y control de errores y de flujo.

Para realizar dichas funciones la capa de enlace de datos se divide en dos subcapas, la subcapa MAC, que realiza las tres primeras funciones y la subcapa LLC que se encarga de la cuarta función.

LAN-Red de Area Local
LLC- Control de Enlace Lógico
MAC- Control de Acceso al Medio
TCP/IP- Protocolo de Control de Transmisión /Protocolo de Internet

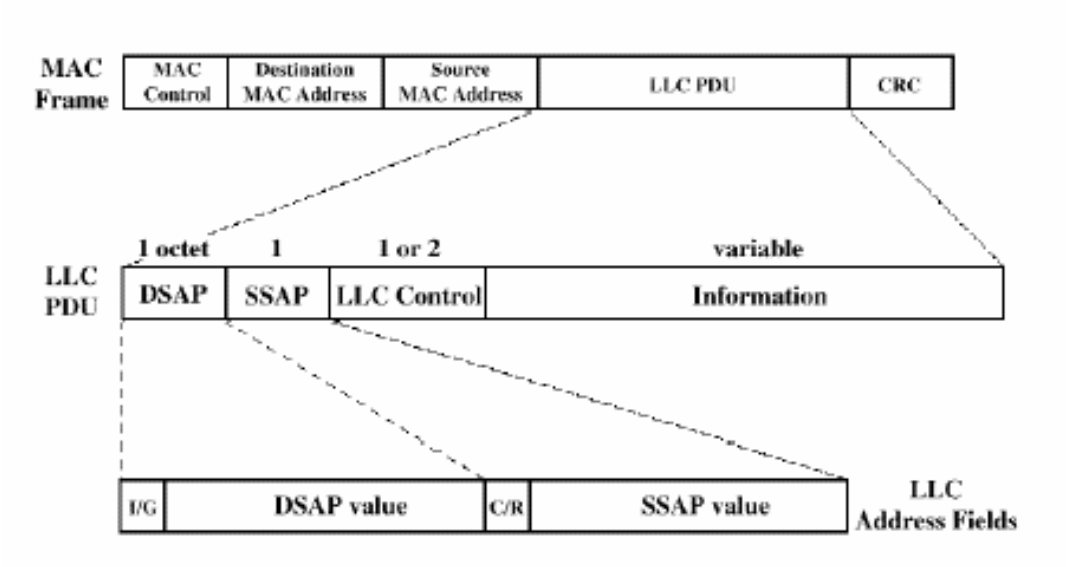


Figura 2.3 Trama de la Capa de Enlace de datos

2.5.1 SUBCAPA MAC

El protocolo MAC[1] es el encargado de controlar el acceso al medio con el objetivo de hacer eficiente el mismo.

Debido a que un conjunto de dispositivos comparten la capacidad de transmisión de la red, debe existir un método que controle el acceso al mismo, de manera que una estación que desee transmitir debe esperar hasta que se le conceda permiso por parte del controlador, en una red descentralizada (ethernet), las estaciones realizan conjuntamente la función de control de acceso al medio para determinar dinámicamente el orden en que transmitirán.

La subcapa MAC recibe un bloque de datos de la subcapa LLC[2], realiza las funciones relacionadas con el acceso al medio y la transmisión de datos, contiene las direcciones de origen y destino, además de ser responsable de la detección de errores y del rechazo de las tramas erróneas.

Cuando una trama MAC es recibida, la estación destino la desensambla, reconoce la dirección MAC destino y determina si debe aceptarla.

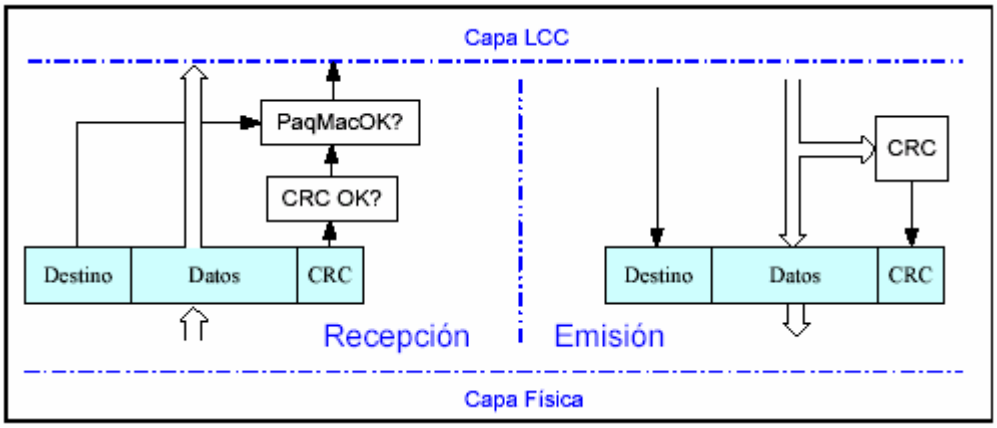


Figura 2.4 Actividad de la capa MAC

[1] **LLC**- Control de Enlace Lógico
[2] **MAC**- Control de Acceso al Medio

La trama MAC[1] difieren ligeramente para los distintos protocolos en uso, sin embargo, tienen un formato similar al de la figura 2.5 y cuentan con lo siguientes campos:

- Control MAC: contiene información de control de protocolo necesaria para el funcionamiento del protocolo MAC, por ejemplo, se podría indicar un nivel de prioridad.
- Dirección MAC destino: punto de conexión física MAC de destino.
- Dirección MAC origen: punto de conexión física MAC de origen.
- LLC[2]: datos LLC de la capa inmediatamente superior.
- CRC[3]: campo de comprobación de redundancia cíclica.

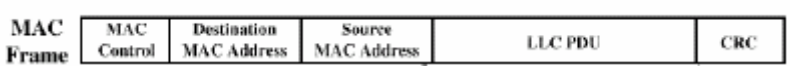


Figura 2.5 Trama MAC

2.5.2 SUBCAPA LLC

Esta subcapa establece y mantiene el enlace entre las computadoras emisora y receptora cuando los datos se desplazan por el entorno físico de la red, también proporciona puntos de acceso al servicio (SAP), que son puntos de referencia a los que otras computadoras que envíen información pueden dirigirse, y utilizar para comunicarse con las capas superiores del conjunto de protocolos dentro de un determinado nodo receptor.

DSAP Y SSAP: Son los puntos de acceso al servicio, destino y origen respectivamente.

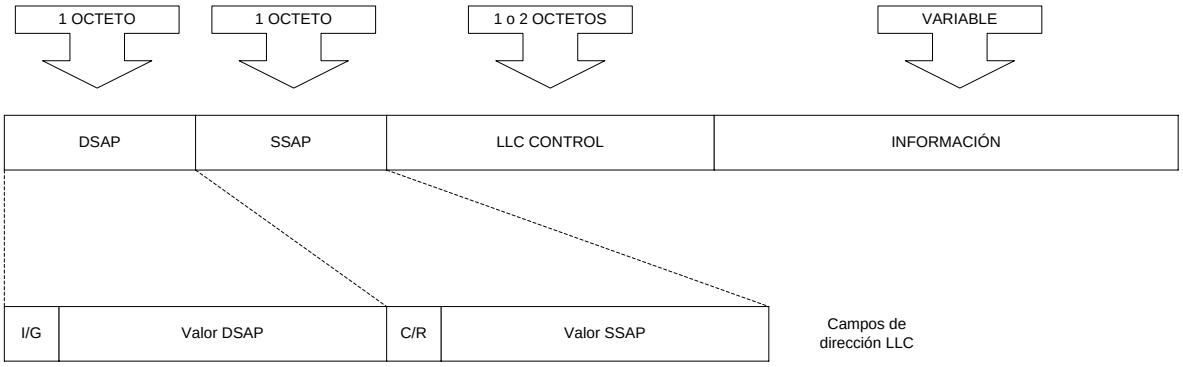


Figura 2.6 Capa LLC

I/G: Individual/Grupo
C/R: Comando/Respuesta

Características específicas

- Debe soportar acceso múltiple, debido a la naturaleza del medio compartido del enlace.

[1] **CRC**-Verificación por Redundancia Cíclica
[2] **MAC**-Control de Acceso al Medio
[3] **LLC**-Control de Enlace Lógico

- Envío a uno o varios de posibles destinos.
- Recepción desde uno de los posibles orígenes.

- La capa MAC le descarga de algunos detalles de acceso al medio.
- Debe soportar algunas funciones del nivel de red

Servicios

- Sin conexión, sin conexión lógica, ni control de flujo ni de errores. Se deja a las capas superiores.
- Orientado a conexión, existe una conexión lógica entre los usuarios del servicio, con control de flujo y de errores.
- Multiplexación, se debe permitir compartir la única conexión con la RAL, entre múltiples puntos de acceso.
- Multicast, Broadcast, aprovecha el medio de transmisión compartido para realizar envíos a múltiples destinos.
- Datagrama
- Circuito Virtual. Soportadas con SAP

La trama LLC Ethernet o SNAP (Sub-Network Access Protocol, Protocolo de Acceso a Subred)

2.6 TECNOLOGIA ETHERNET

Ethernet es una tecnología LAN de conmutación de paquetes inventada por Xerox PARC a principios de los años setenta. Xerox Corporation, Intel Corporation y Digital Equipment Corporation estandarizaron Ethernet en 1978, posteriormente la IEEE la normalizo como IEEE 802.3.

Ethernet se basa en CSMA/CD (Carrier Sense Multiple Access with Collision Detect, Acceso múltiple por Sensado de Portadora con Detección de Colisiones). Es básicamente un método de contienda que trabaja por broadcast, cuando una estación desea transmitir lo hace a todas las estaciones y sólo la estación destino recibe los datos, el resto los descartan.

Este método realiza una evaluación de tráfico, ya que cada estación primero “sensa” el medio físico (escucha) para determinar si otra estación está transmitiendo y en caso de que el medio este siendo utilizado, espera a que se libere y realiza su transmisión. Esto pretende evitar las colisiones aunque no siempre lo consigue. Estas colisiones ocurren debido a que la señal tiene un tiempo de propagación, si otra estación comienza a transmitir habiendo señal en camino, inevitablemente se producirá una colisión. El proceso de ahí en adelante consiste en anular las tramas invalidadas por la colisión, y esperar un tiempo aleatorio tras lo cual se reintenta la transmisión. El método CSMA/CD resulta muy efectivo en medios de poco tráfico, pero por el contrario, en medios con mucha congestión la cantidad de colisiones que se produce reduce notablemente la eficiencia.

IEEE- Instituto de Ingenieros Eléctricos-Electrónicos
LAN-Red de Area Local
LLC-Control de Enlace Lógico
MAC-Control de Acceso al Medio
SAP-Punto de Acceso al Servicio

Ethernet se ha vuelto una tecnología LAN ampliamente usada por muchas compañías, medianas o grandes.

Originalmente el cable coaxial era el único medio de transmisión para Ethernet, el cual tiene aproximadamente ½ pulgada de diámetro y mide hasta 500 m de largo. Se añade una resistencia entre el centro del cable y el blindaje en cada extremo del mismo para prevenir la reflexión de señales eléctricas.

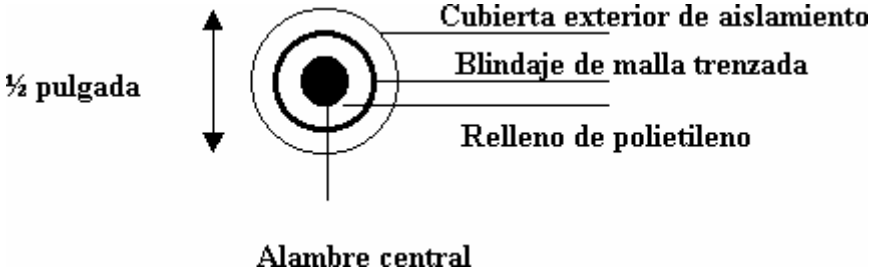


Figura 2.7 Cable Coaxial Ethernet

El cable por sí mismo es completamente pasivo; todos los componentes electrónicos activos que hacen que la red funcione están asociados con las computadoras que se comunican en la red. La conexión entre una computadora y un cable coaxial Ethernet requiere de un dispositivo de hardware llamado transceptor. Físicamente la conexión entre un transceptor y el cable Ethernet requiere de una pequeña perforación a la capa exterior del cable. Los técnicos con frecuencia utilizan el término tap para describir la conexión entre un transceptor Ethernet y el cable. Por lo general, una pequeña aguja de metal montada en el transceptor atraviesa la perforación y proporciona el contacto eléctrico con el centro del cable y el blindaje trenzado.

Cada conexión a una red Ethernet tiene dos componentes electrónicos mayores, un transceptor conectado al centro del cable y al blindaje trenzado del mismo, por medio del cual recibe y envía señales por el cable ether; y una interfaz anfitrión o adaptador anfitrión que se conecta dentro del bus de la computadora a la tarjeta madre con el transceptor.

Un transceptor es una pequeña pieza de hardware que por lo común se encuentra físicamente junto al cable ether. Además del hardware análogo que envía y controla las señales eléctricas en el cable ether, un transceptor contiene circuitería digital que permite la comunicación con una computadora digital. El transceptor, cuando el cable ether está en uso, puede recibir y traducir señales eléctricas analógicas hacia o desde un formato digital en el cable ether. Un cable llamado Attachment Unit Interface (AUI, Interfaz de Unidad de conexión) conecta el transceptor con la tarjeta del adapatador en una computadora anfitrión. Los cables del AUI transportan la potencia eléctrica necesaria para operar el transceptor, las señales de control para su operación y el contenido de los paquetes que se están enviando o recibiendo.

Cada interfaz de anfitrión controla la operación de un transceptor de acuerdo a las instrucciones que recibe del software de la computadora. Para el software del sistema operativo, la interfaz aparece como un dispositivo de entrada/salida que acepta instrucciones de transferencia de datos básicas desde la computadora, controla la transferencia del transceptor e interrumpe el proceso cuando éste ha concluido, finalmente reporta la información de estado. Aun cuando el transceptor es un simple dispositivo de hardware, la interfaz de anfitrión puede ser compleja.

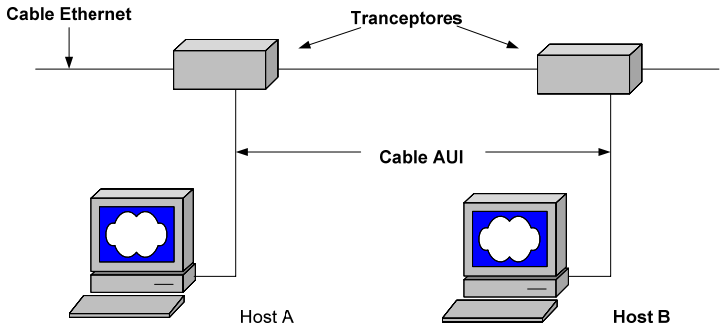


Figura 2.8 Conexión Ethernet

Las diferentes especificaciones de cableado, se encuentran definidas en la norma 802.3.

10Base2 : Tipo bus con coaxial fino

(Thin coaxil). Soporta segmentos de hasta 185 metros y un máximo de 30 nodos por segmento. Es económico pero posee una gran desventaja una apertura o cortocircuito en el cable hace caer a toda la red. Con este cable se reemplazo el costoso transceptor con circuitería digital de alta velocidad especial y proporcionaron una conexión directa desde una computadora hasta el cable ether. De esta forma, en el esquema de cable delgado, una computadora contiene tanto la interfaz de anfitrión como la circuitería necesaria para conectar la computadora con el cable. Los fabricantes de pequeñas computadoras y estaciones de trabajo encontraron el esquema del cable delgado Ethernet especialmente atractivo, debido a que podían integrar el hardware de Ethernet en una sola tarjeta de computadora y hacer las conexiones necesarias de manera directa en la parte posterior de la computadora.

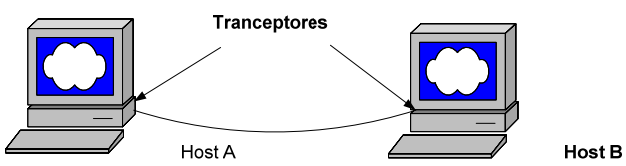


Figura 2.9 Conexión 10Base2

10Base5 : Tipo bus con coaxial grueso

(Thick coaxil). Soporta segmentos de hasta 500 metros y un máximo de 100 nodos por segmento. Requiere de dispositivos de interconexión especiales. Es muy robusto confiable pero su alto costo lo delegan exclusivamente a backbones.

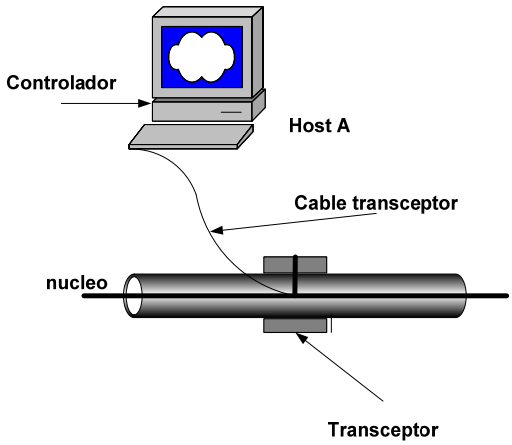


Figura 2.10 Conexión 10Base5

10BaseT : Con cable UTP (Unshielded Twisted Pair)

Con cable telefónico no blindado, partiendo de un hub o switch central lo hace muy versátil y económico. Tiende a reemplazar al coaxial dado que la apertura de un cable no perjudica a toda la red sino solamente a la estación en cuestión.

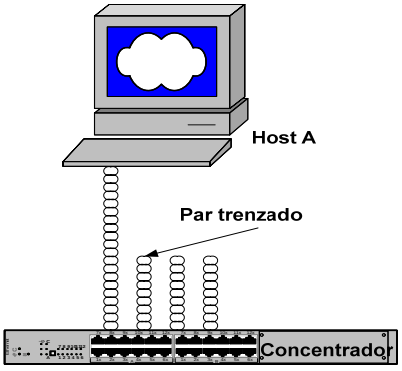


Figura 2.11 Conexión 10BaseT

10 BaseF : Con Fibra óptica.

Maneja distancias de hasta 2000 metros y 1024 nodos por segmento por lo que es ideal para unir edificios o concentradores muy separados.

Cada versión de 802.3 tiene una longitud máxima de cable por segmento. Para permitir redes mayores, se pueden conectar múltiples nodos

mediante repetidores que tienen diferentes configuraciones como se muestra en la siguiente figura.

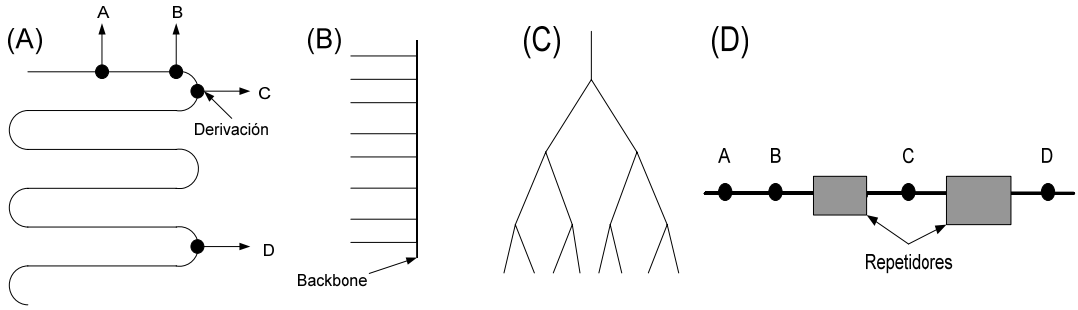


Figura 2.12 Topologías de cableado (A)Lineal, (B)Columnar, (C)Arbol, (D)Segmentado.

2.6.1 PROPIEDADES DE UNA RED ETHERNET

La red Ethernet es una tecnología de bus de difusión de 10 Mbps que se conoce como 'entrega con el mejor esfuerzo' y un control de acceso distribuido. Es un bus debido a que todas las estaciones comparten un sólo canal de comunicación, es de difusión porque todos los transceptores reciben todas las transmisiones. Los transceptores no distinguen las transmisiones, transfieren todos los paquetes del cable a la interfaz anfitrión, la cual selecciona los paquetes que la computadora debe recibir y filtra todos los demás. Las redes Ethernet cuentan con un mecanismo llamado entrega con el mejor esfuerzo debido a que el hardware no proporciona información al emisor acerca de si el paquete ha sido recibido. Por ejemplo, si la máquina de destino es apagada, los paquetes enviados se perderán y el emisor no será notificado.

El control de acceso en las redes Ethernet es distribuido porque, a diferencia de algunas tecnologías de red, Ethernet no tiene la autoridad central para garantizar el acceso. El esquema de acceso de Ethernet es conocido como Carrier Sense Multiple Access with Collision Detect (CSMA/CD) que utiliza una codificación Manchester. Es un CSMA debido a que varias máquinas pueden accesar la red Ethernet de manera simultánea y cada máquina determina si el cable ether está disponible al verificar si está presente una onda portadora. Cuando una interfaz anfitrión tiene un paquete para transmitir verifica el cable ether para comprobar si un mensaje se está transmitiendo. Cuando no se comprueba la presencia de una transmisión, la interfaz de anfitrión comienza a transmitir. Cada transmisión está limitada en duración (dado que hay un tamaño máximo para los paquetes). Además, el hardware debe respetar un tiempo mínimo de inactividad entre transmisiones, esto significa que no se dará el caso de que un par de computadoras que se comuniquen puedan utilizar la red sin que otras máquinas tengan la oportunidad de accederla.

El estándar Ethernet se define en 10 Mbps, lo cual significa que los datos pueden transmitirse por el cable a razón de 10 millones de bits por

segundo. A pesar de que una computadora puede generar datos a la velocidad de la red Ethernet, esta velocidad no es a la que dos computadoras pueden intercambiar datos. La velocidad de la red debe pensarse como una medida de la capacidad del tráfico total de la red. Pensemos en una red como en una carretera que conecta varias ciudades y pensemos en los paquetes como en coches en la carretera. Un ancho de banda alto hace posible transferir cargas de tráfico pesadas, mientras que un ancho de banda bajo significa que la carretera no puede transportar mucho tráfico. Una red Ethernet a 10 Mbps, por ejemplo, puede soportar unas cuantas computadoras que generan cargas pesadas o muchas computadoras que generan cargas ligeras.

2.6.2 DIRECCIONAMIENTO DE ETHERNET

Las redes Ethernet definen un esquema de direccionamiento de 48 bits, cada computadora conectada a estas redes es asignada a un número único de 48 bits conocido como dirección Ethernet. Para asignar una dirección, los fabricantes de hardware adquieren bloques de direcciones Ethernet y las asignan en secuencia conforme fabrican el hardware de interfaz. De esta manera no existen dos unidades de hardware de interfaz que tengan la misma dirección Ethernet.

Por lo general, las direcciones Ethernet se fijan en las máquinas en el hardware de interfaz de anfitrión de forma que se puedan leer. Debido a que el direccionamiento Ethernet se da entre dispositivos de hardware, a estos se les llama direccionamientos o direcciones físicas.

Las direcciones físicas están asociadas con el hardware de interfaz Ethernet, cambiar el hardware de interfaz a una máquina nueva o reemplazar el hardware de interfaz que ha fallado provocará cambios en la dirección física de la máquina.

Conociendo la dirección física Ethernet se pueden hacer cambios con facilidad porque los niveles superiores del software de red están diseñados para adaptarse a estos cambios.

El hardware de interfaz anfitrión examina los paquetes y determina qué paquetes deben enviarse al anfitrión. Debe recordarse que cada interfaz recibe una copia de todos los paquetes aun cuando estén direccionados hacia otras máquinas. La interfaz de anfitrión utiliza el campo de dirección de destino de un paquete como filtro. La interfaz ignora los paquetes que estén direccionados hacia otras máquinas y selecciona sólo los paquetes direccionados hacia él. El mecanismo de direccionamiento y filtrado de hardware es necesario para prevenir que una computadora sea abrumada con la entrada de datos. Aun cuando el procesador central de la computadora podría realizar la verificación, ésta se realiza en la interfaz de anfitrión haciendo que el tráfico en la red sea un proceso menos lento en todas las computadoras.

Una dirección Ethernet de 48 bits puede especificar más que una computadora destino. Una dirección puede ser alguno de los tres tipos siguientes:

- La dirección física de una interfaz de red (dirección de unidifusión).
- La dirección de publidifusión de la red.
- Una dirección de multidifusión

Convencionalmente, la dirección de difusión se reserva para envíos simultáneos a todas las estaciones. Las direcciones de multidifusión proporcionan una forma limitada de difusión en la cual un subconjunto de computadoras en una red acuerda recibir una dirección de multidifusión dada. El conjunto de computadoras participantes se conoce como grupo de multidifusión. Para unirse a un grupo de multidifusión, una computadora debe instruir a la interfaz anfitrión para aceptar las direcciones de multidifusión del grupo. La ventaja de la multidifusión reside en la capacidad para limitar la difusión, todas las computadoras en un grupo de multidifusión pueden ser alcanzadas con un solo paquete de transmisión, pero las computadoras que eligen no participar en un grupo de multidifusión en particular no recibirán los paquetes enviados al grupo.

Para adaptarse al direccionamiento de multidifusión y difusión, el hardware de interfaz Ethernet debe reconocer más que la dirección física. Una interfaz anfitrión por lo general acepta hasta dos clases de paquetes: los enviados a la dirección física de la interfaz (esto es, unidifusión) y los enviados hacia la dirección de difusión de la red. Algunos tipos de interfaz pueden programarse para reconocer direcciones de multidifusión o para alternar entre direcciones físicas. Cuando el sistema operativo comienza a trabajar, éste inicia la interfaz Ethernet, haciendo que se reconozca un conjunto de direcciones. La interfaz entonces examina el campo de direcciones de destino en cada paquete, pasando hacia el anfitrión sólo las transmisiones destinadas a una de las direcciones específicas.

2.6.3 ENCAPSULADO DE DATOS EN UN PAQUETE ETHERNET

La red Ethernet podría pensarse como una conexión de niveles enlazados entre máquinas. De esta manera, la información transmitida podría tener el aspecto de una trama. La trama Ethernet es de una longitud variable pero no es menor a 64 octetos ni rebasa los 1518 octetos (encabezado, datos y CRC). Como en todas las redes de conmutación de paquetes, cada trama Ethernet contiene un campo con la información de la dirección de destino. La figura muestra que la trama Ethernet contiene la dirección física de la fuente y también la dirección física del destino.

Preámbulo	SFD	Destino	Fuente	Tipo	Datos	CRC
8 octetos	1 octeto	6 octetos	6 octetos	2 octetos	64-1500	32

Tabla 2.3 Trama de Ethernet

Además de la información para identificar la fuente y el destino, cada trama transmitida a través de Ethernet contiene un preámbulo, un campo

CRC-Verificación por Redundancia Cíclica

fuente, un campo destino, un campo de tipo, un campo de datos y una Cyclic Redundancy Check (CRC).

- Preámbulo: consiste en 64 bits que alternan ceros y unos para ayudar a la sincronización de los nodos de recepción.

- SFD (START OF FRAME DELIMITER) o Inicio de trama: marca el comienzo de la trama, y esta determinado por el siguiente octeto 10101011.

- Dirección destino: MAC Address del destino compuesto por 6 octetos.

- Dirección origen: MAC Address del origen compuesto también por 6 octetos.

- Tipo: El campo de tipo de trama contiene un entero de 16 bits (2 octetos) que identifica el tipo de datos que se están transfiriendo en la trama, o la longitud de datos LLC. Desde el punto de vista de Internet, el campo de tipo de trama es esencial porque implica que las tramas de Ethernet se auto identifican. Cuando una trama llega a una máquina dada, el sistema operativo utiliza el tipo de trama para determinar que módulo de software de protocolo se utilizará para procesar la trama. La mayor ventaja de que las tramas se auto identifiquen es que éstas permiten que múltiples protocolos se utilicen juntos en una sola máquina y sea posible entremezclar diferentes protocolos en una sola red física sin interferencia. Por ejemplo, uno podría tener un programa de aplicación que utiliza protocolos de Internet, mientras otro utiliza un protocolo experimental local. El sistema operativo utiliza el campo de tipo de una trama entrante para decidir cómo procesar el contenido.

- Datos: Es el campo que contiene la información y tiene una longitud de 64 a 1500 octetos.

- El CRC de 32 bits ayuda a la interfaz a detectar los errores de transmisión: el emisor computa el CRC como una función de los datos de la trama y el receptor computa de nuevo el CRC para verificar que el paquete se ha recibido intacto.

2.7 CAPA TCP

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, es el encargado de dividir el mensaje original en datagramas de menor tamaño, que son más manejables. Los datagramas son dirigidos a través del protocolo IP de forma individual.

TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas, esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

CRC-Verificación por Redundancia Cíclica
LLC-Control de Enlace Lógico
MAC-Control de Acceso al Medio
IP-Protocolo de Internet

La cabecera de un datagrama contiene al menos 160 bit que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. Para evitar todos estos problemas TCP numera los datagramas antes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.

La cabecera TCP debe ser múltiplo de 32 bits, por lo que puede ser necesario añadir un campo de tamaño variable y que contenga ceros al final. El campo de tamaño contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa. Esto permite determinar el lugar donde comienzan los datos.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas señales de confirmación una vez, que se ha recibido y comprobado la información satisfactoriamente. Estas señales se incluyen en el campo apropiado de la cabecera del datagrama (Acknowledgment Number), que tiene un tamaño de 32 bit. Si el servidor no obtiene la señal de confirmación adecuada, transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar. Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información del datagrama llegue con errores a su destino. Para poder detectar cuando sucede esto, se incluye en la cabecera un campo de 16 bit, el cual contiene un valor calculado a partir de la información del datagrama completo (checksum). En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera. Si el valor es distinto significaría que el datagrama es incorrecto, ya que en la cabecera o en la parte de datos del mismo hay algún error.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente. De esta manera el primero empezará por cero, el segundo contendrá un número que será igual al tamaño en bytes de la parte de datos del datagrama anterior, el tercero con la suma de los dos anteriores, y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada uno de los ordenadores

puede procesar los datos que le son enviados. Si esto no se tuviera en cuenta, el ordenador de más potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla. Este inconveniente se soluciona mediante un campo de 16 bit (Windows) en la cabecera TCP, en el cual se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar. Si el valor llega a cero será necesario que el emisor se detenga. A medida que la información es procesada este valor aumenta indicando disponibilidad para continuar la recepción de datos.

Sus características principales son:

- Conexiones fiables, garantizando la integridad de la información, su secuencia correcta y la no pérdida o duplicación
- Adaptación automática al tiempo de tránsito de la red y fiabilidad frente a congestión
- Capacidad de envío de datos urgentes
- Gestión de búfferes en transmisión y recepción
- Posibilidad de esperar conexiones remotas en ciertos canales especificados, denominados "puertos"
- Conexiones 8 bits orientadas al byte, sin distinción alguna de campos, y bidireccionales

En cuanto a los servicios que utilizan este módulo, destacan:

Distribución de las tablas de enrutado

Para que la red en su conjunto ofrezca una imagen homogénea y coherente es necesario que las diferentes pasarelas dispongan de información actualizada sobre su topología. Esto se consigue mediante el intercambio de información de encaminamiento entre los diferentes sistemas, vía los servicios UDP y TCP.

- Protocolo TELNET Este servicio posibilita el acceso en modo terminal a una máquina remota, de forma transparente.
- Protocolo de transferencia de ficheros (FTP) Este protocolo permite el intercambio de ficheros residentes en máquinas distintas, de forma simple, rápida y fiable.
- Protocolo de transferencia de correo electrónico (SMTP)
- Protocolo de transporte hipertexto (HTTP) Esta familia de protocolos son los principales responsables de crecimiento exponencial de Internet, al facilitar considerablemente la búsqueda, el acceso y la gestión de la información esparcida por la red.

TCP-Protocolo de Control de Transmisión
UDP-Protocolo de Datagrama de Usuario

La interfaz de la capa está constituida por procesos y por subrutinas ejecutadas en el contexto del llamante. Su utilización es muy simple.

- PROC_TCP_BC

  Este proceso es el encargado de inicializar este módulo. Debe ser activado con un mensaje "MSG_INIT" o "MSG_QUIT". La activación de este módulo debe ser posterior a la del módulo IP.

- PROC_TCP_SUP

Este es el proceso el que recibe los mensajes de las capas superiores y los gestiona adecuadamente. Los mensajes definidos son:

- MSG_TCP_OPEN

  Este mensaje informa a la capa TCP que se acepta una conexión solicitada por una máquina remota. Los valores de los campos son:

  campo1: Ignorado
  campo2: Identificador de la conexión
  campo3: Ignorado

  El enlace podrá ser utilizado a partir de ese momento. Este mensaje es generado por una capa superior cuando ésta decide aceptar una conexión remota propuesta por el módulo TCP.

- MSG_TCP_CLOSE

  Este mensaje informa a la capa TCP que no hay más información que transmitir a través de una conexión dada. TCP se encarga de que cualquier dato pendiente en los búfferes internos sea correctamente entregado. La conexión sigue abierta para recibir, y no se cerrará hasta que el otro extremo lo decida o enviemos el mensaje definido a continuación. Los valores de los campos son:

  campo1: Ignorado
  campo2: Identificador de la conexión
  campo3: Ignorado

- MSG_TCP_ABORT

  Este mensaje cierra una conexión en ambas direcciones. Cualquier dato en tránsito o en los búfferes internos se perderá. Los parámetros de este mensaje son:

  campo1: Ignorado
  campo2: Identificador de la conexión
  campo3: Ignorado

IP-Protocolo de Internet
TCP-Protocolo de Control de Transmisión

- MSG_MBUF

  A través de este mensaje una capa superior informa al módulo TCP que hay nueva información para transmitir. La capa TCP se hará cargo de la entrega de los datos. Los parámetros del mensaje son:

  campo1: Cadena de MBUFs conteniendo la información que se desea transmitir
  campo2: Identificador de la conexión
  campo3: Puede contener los valores CERO, PUSH o MODO_URGENTE

  Un valor de cero indica que los datos especificados no están sujetos a ningún tratamiento especial. Si su longitud es pequeña la capa TCP puede realizar un almacenamiento temporal en espera de nuevos datos en vez de enviar un segmento de tamaño reducido.

  Si campo3 tiene el valor "PUSH" significa que los datos deben enviarse cuanto antes al otro extremo, y que éste debe entregarlos lo antes posible al proceso responsable. En cuanto a "MODO_URGENTE", supone un "PUSH" implícito (aunque es recomendable incluir la bandera "PUSH" para que sea señalada adecuadamente en el otro extremo) y su objetivo primordial consiste en la resincronización de la transmisión y el intercambio de datos "fuera de banda".

- MSG_TCP_TIMEOUT

  Este mensaje se genera cuando vence el número de reintentos en alguna conexión. Ello puede ser debido a que la red se ha roto, a que la máquina destino se ha caido o bien a que el tiempo de tránsito de los datagramas en la red es demasiado elevado.

  campo1: Indeterminado
  campo2: Identificador de la conexión
  campo3: Indeterminado

  La conexión se cierra de forma automática.

- PROC_TCP_INF

  Este proceso recibe los segmentos TCP y los gestiona adecuadamente. Está diseñado para intercomunicarse con los procesos en los módulos IP e ICMP. Los mensajes que espera recibir son:

  - MSG_ICMP_SOURCE_QUENCH

IP-Protocolo de Internet
ICMP- Protocolo de Control de Mensajes de Internet
TCP-Protocolo de Control de Transmisión

Este mensaje indica a la capa TCP que alguna de sus conexiones transcurre a través de una red muy cargada (congestión) y que debería reducir su tasa de transferencia para aliviarlo. Los parámetros de este mensaje fueron definidos en el módulo ICMP.

- MSG_ICMP_DEST_UNREACHABLE

  Este mensaje informa a la capa TCP que alguna de sus conexiones (o intentos de conexión) no puede alcanzar a la máquina destino. Los parámetros de este mensaje fueron definidos en el módulo ICMP.

- MSG_MBUF

  Este mensaje contiene un segmento TCP recibido por la capa IP. Su formato corresponde al definido en el capítulo dedicado al módulo IP.

En cuanto a los mensajes que transmite, tenemos:

- MSG_TCP_OPEN

  Este mensaje informa a una capa superior que se ha recibido una petición de conexión a uno de sus puertos declarados como "LISTEN". Para que la conexión se establezca la capa superior debe responder con otro "MSG_TCP_OPEN" dirigido a "PROC_TCP_SUP", tal y como se ha visto previamente.

  Este mensaje también se genera cuando somos nosotros los que iniciamos la conexión y la máquina remota lo acepta (ver más adelante).

  El formato de este mensaje es:

  campo1: Cabecera TCP interfaz
  campo2: Identificador de la conexión
  campo3: Indeterminado

  La cabecera TCP interfaz se define como:

```
typedef struct {
  uint16  puerto_remoto;
  uint16  puerto_local;
  uint32  ip_remoto;
  uint32  dummy[4];
} tcp_header;
```

  "puerto_remoto" y "puerto_local" indican los puertos a través de los cuales se ha establecido la conexión. "ip_remoto" contiene la

IP-Protocolo de Internet
ICMP- Protocolo de Control de Mensajes de Internet
TCP-Protocolo de Control de Transmisión

dirección IP de la otra máquina. "dummy" contiene valores indeterminados.

- MSG_TCP_CLOSE

  Este mensaje es generado cuando la máquina remota no desea transmitir más información. Con ello se informa al nivel superior de que no hay más datos pendientes. No obstante nosotros podemos seguir transmitiendo.

  Este mensaje también es generado cuando se aborta una conexión, ya sea en la negociación inicial o bien durante la fase de transferencia. En ese caso cualquier dato que queramos transmitir será ignorado.

  El formato de este mensaje es:

  campo1: Ignorado
  campo2: Identificador de la conexión
  campo3: Ignorado

- MSG_MBUF

  Con este mensaje enviamos a las capas superiores los datos que se van recibiendo. El formato es idéntico al especificado para el proceso "PROC_TCP_SUP". No obstante resulta conveniente realizar algunas matizaciones:

  Dado que tanto los procesos de transmisión como los de recepción TCP incorporan mecanismos de buffering no puede esperarse que cada segmento enviado a este módulo mediante "MSG_MBUF" genere uno y sólo un mensaje "MSG_MBUF" en el receptor. En un momento dado el transmisor puede decidir retrasar el envío de un segmento debido a su escasa longitud, congestión de la red, o al cierre de la ventana de transmisión. Por otra parte, un bloque de información puede suponer el envío de más de un segmento debido al MSS (Maximum Segment Size) negociado al principio de la conexión o la MTU de las redes intermedias. Además el receptor puede decidir concatenar varios segmentos en un sólo "MSG_MBUF" si la red cambia su secuenciamiento, etc.

  La opción "PUSH" tiene como objetivo la entrega cuanto antes de los datos pendientes al proceso destino. No obstante tampoco sirve como delimitador de campos dentro de lo que es la propia secuencia de bytes. El proceso receptor puede no ver el "PUSH" en la misma posición que el transmisor, ni recibirse el mismo número de PUSHs que se transmitieron. De hecho en [RFC1122] se especifica que la bandera "PUSH" no necesita ser transferida al proceso receptor.

IP-Protocolo de Internet
MTU-Unidad de Transferencia Máxima de Datos
TCP-Protocolo de Control de Transmisión

En cuanto a "MODO_URGENTE", tampoco sirve como delimitador claro. Su tarea consiste en conmutar de modo al proceso receptor. Su funcionamiento es inmediato: cuando el transmisor recibe un mensaje "MSG_MBUF" urgente, todos los datos previos todavía no entregados serán marcados como urgentes en el receptor. La utilidad habitual de todo esto consiste en la recuperación de sincronismo entre el transmisor y el receptor. El proceso receptor puede, por ejemplo, ignorar todos los datos marcados como urgentes. Se utiliza una técnica parecida en el protocolo TELNET [RFC854].

Lo único que se garantiza en "MODO_URGENTE" es que los datos que siguen a un mensaje urgente y que no están marcados con ese modo no son recibidos como urgentes en el proceso receptor, siempre y cuando no haya ningún segmento urgente posterior. Esa es la única forma de marcar campos que tiene este protocolo.

UDP

Después de haber analizado un protocolo de IP orientado a la conexión como lo es TCP podemos ahora analizar uno que es no orientado a la conexión como lo es el UDP.

El protocolo UDP (User Datagram Protocol, protocolo de datagrama de usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores, UDP es:

- No orientado a conexión. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino.

- No fiable. Los mensajes UDP se pueden perder o llegar dañados.

UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.

2.7.2 CABECERA TCP

Dos campos incluidos en la cabecera y que son de especial importancia son los números de puerto de origen y puerto de destino. Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo ordenador puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos. El puerto de origen contendrá un número cualquiera que sirva para realizar esta

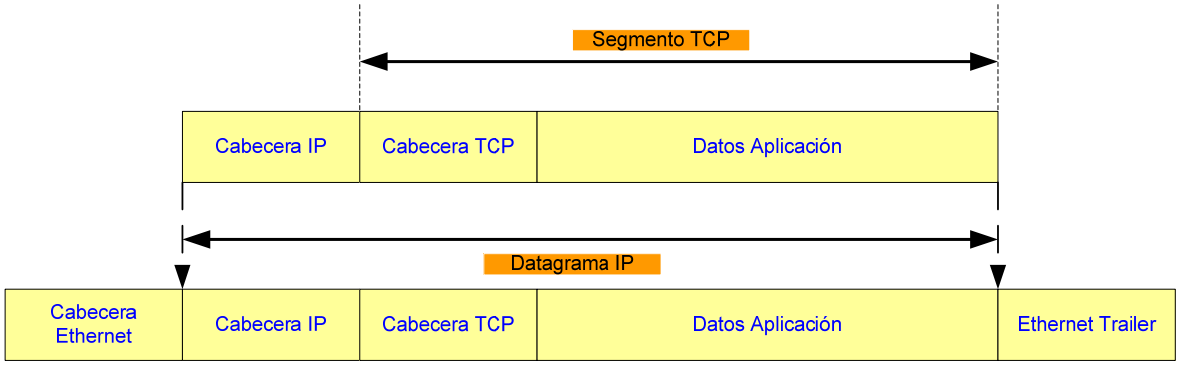
IP-Protocolo de Internet
TCP-Protocolo de Control de Transmisión

distinción. Además, el programa cliente que realiza la petición también se debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor deber tener asignado un número estándar para que pueda ser utilizado por el cliente. (Por ejemplo, en el caso de la transferencia de ficheros FTP el número oficial es el 21). Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

TCP es un protocolo orientado a conexión que proporciona un servicio de transporte fiable de un flujo de bytes entre aplicaciones:

- Orientado a conexión: previo al intercambio de datos los extremos (aplicaciones) tienen que establecer una conexión.
- Fiable: garantiza la entrega ordenada del flujo de bytes entre los extremos de la conexión.
- Flujo de bytes: por la conexión se transmite un flujo de bytes.

Los segmentos TCP se encapsulan en datagramas IP.



FTP-Protocolo de Transferencia de Archivos
IP-Protocolo de Internet
TCP-Protocolo de Control de Transmisión
UDP-Protocolo de Datagrama de Usuario

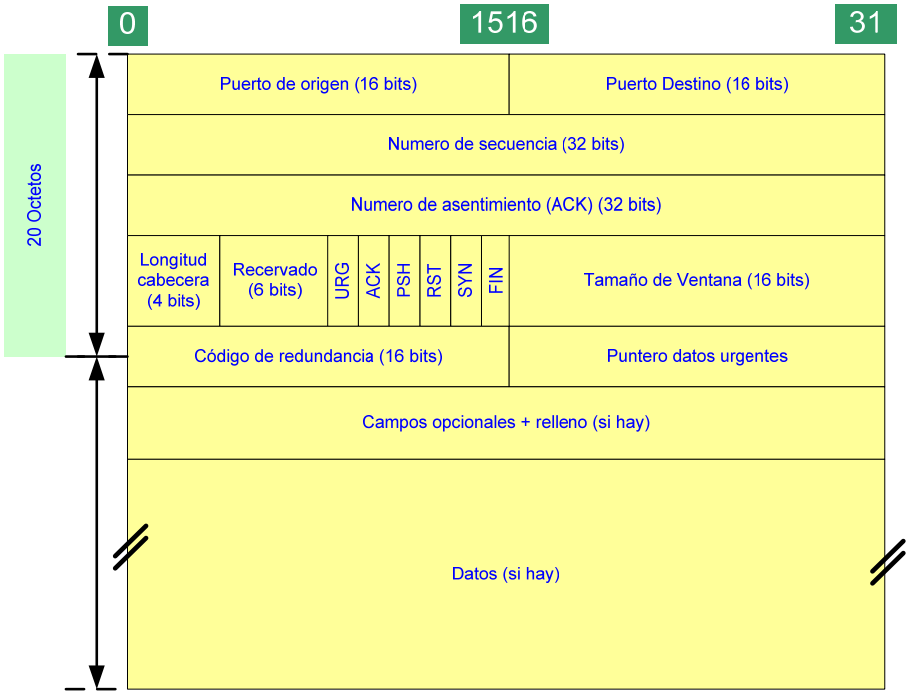


Figura 2.13 Cabecera TCP

Los campos de la cabecera TCP se describen como:

Puertos origen y destino

Indican la conexión lógica entre las dos aplicaciones que se están comunicando (FTP, TELNET, SMTP, etc.).

Identificador único de conexión:

- Par de socket: socket = dirección IP + puerto
- Dirección IP origen, Puerto origen, Dirección IP destino, Puerto destino

Número de secuencia

Posición del primer octeto en el campo de datos en relación con la secuencia original.

- Campo de 32 bits: rango entre 0 y 2^{32}-1.
- Si el flag SYN está activo, este campo contiene el número de secuencia inicial (n) y el primer octeto de datos es el n+1. El flag SYN consume un número de secuencia.
- Servicio full-duplex: cada extremo de la conexión mantiene su número de secuencia de flujo de datos en esa dirección.

FTP-Protocolo de Transferencia de Archivos
IP-Protocolo de Internet
SMTP- Protocolo Simple de Transferencia de correo
TCP-Protocolo de Control de Transmisión

Número de asentimiento (numero de acuse de recibo)

Número de secuencia siguiente al octeto confirmado, indica la posición que ocuparía el próximo octeto que se espera recibir.

- Sólo es válido si está activo el flag ACK.

Longitud cabecera

Número de palabras de 32 bits que componen la cabecera.

- Necesario porque la cabecera es de longitud variable (opciones).
- Campo de 4 bits Ë cabecera TCP limitada a 60 octetos.
- Sin opciones la longitud de la cabecera son 20 octetos.

Reservado

Reservados para uso futuro, deben estar a cero.

Flags

- URG: indica que el campo Puntero Datos Urgentes tiene validez.
- ACK: indica que el campo Número de Asentimiento tiene validez.
- PSH: indica que el segmento requiere envío y entrega inmediata.
- RST: indica aborto de la conexión.
- SYN: sincroniza números de secuencia en el establecimiento de conexión.

Confirmación con ACK

- FIN: indica liberación de conexión.

Tamaño ventana

Indica el número de octetos, adicionales al apuntado por ACK, que está dispuesto aceptar.

- Mecanismo de control de flujo de TCP.
- Anunciado por cada extremo de la conexión.
- Campo de 16 bits: tamaño limitado a 65535 octetos.

Código de redundancia

Campo obligatorio que debe ser calculado por el emisor y verificado por el receptor.

- Incluye todo el segmento TCP, tanto cabecera como datos.

Puntero datos urgentes

Indica el offset (positivo) que debe ser añadido al número de secuencia del segmento para obtener el número de secuencia del último octeto de datos urgentes.

- Sólo es válido si está activo el flag URG.

Campos opcionales

Para incluir opciones.

- Tamaño máximo de datos en un segmento (MSS – Maximun Segment Size):

Mensaje UDP

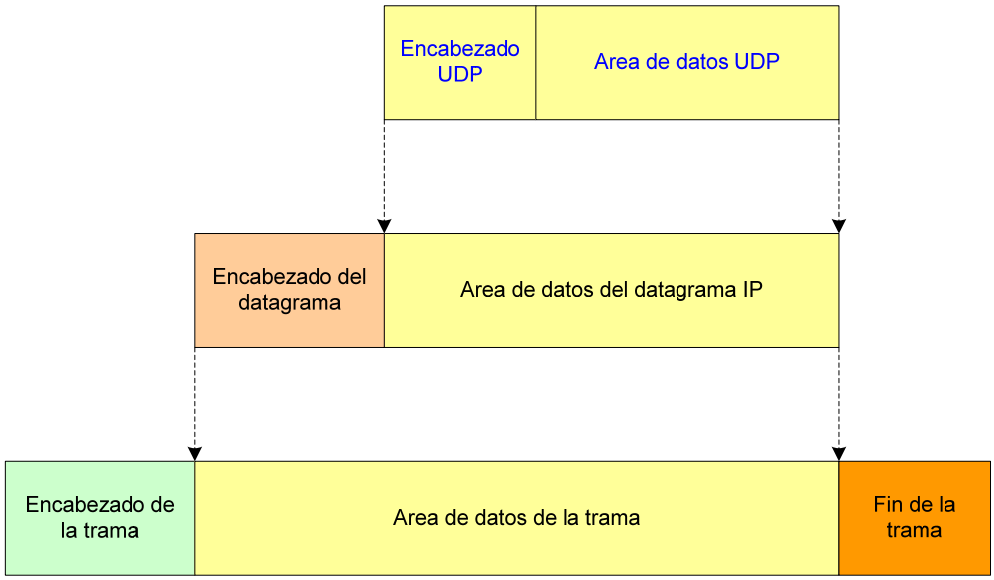


Figura 2.14 Formato Mensaje UDP

TCP-Protocolo de Control de Transmisión
UDP-Protocolo de Datagrama de Usuario

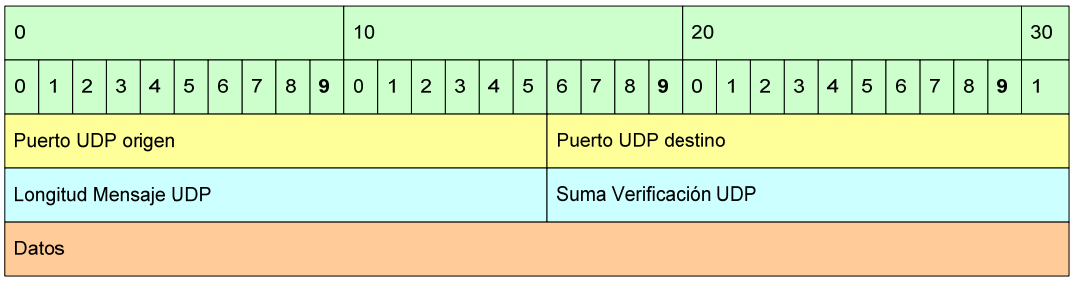


Figura 2.15 Estructura del área de datos UDP.

Descripción de los campos:

Puerto UDP de origen (16 bits, opcional)

Número de puerto de la máquina origen.

Puerto UDP de destino (16 bits)

Número de puerto de la máquina destino.

Longitud del mensaje UDP (16 bits)

Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.

Suma de verificación UDP (16 bits, opcional)

Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.

Datos

Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

2.7.3 NUMERO DE PUERTOS

En las redes que utilizan los protocolos TCP/IP y UDP/IP, cuando un programa cliente necesita de un servicio particular de un servidor, además del tipo de servicio y localización del servidor, debe indicar el puerto por el que se establecerá la conexión. En este sentido, un puerto es un extremo de una conexión lógica. Los puertos se indican por números, y cuando los servicios se refieren a la Web, van incluidos en la sintaxis de la mayoría de las ULRs.

TCP/IP- Protocolo de Control de Transmisión /Protocolo de Internet
UDP/IP- Protocolo de datagrama de usuario/Protocolo de Internet

Para que sea posible utilizar un servicio de un servidor es necesario que el puerto correspondiente del servidor sea el correcto y que esté habilitado.

Coloquialmente diríamos que el servidor debe estar "escuchando" por dicho puerto.

El sistema se comprende mejor considerando que cada paquete de una conexión TCP/IP tiene una cabecera con los siguientes datos:

- Dirección IP de origen (4 bytes)
- Puerto TCP o UDP de origen (2 bytes)
- Dirección IP de destino (4 bytes)
- Puerto TCP o UDP de destino (2 bytes)

La asignación de puertos permite que una máquina pueda establecer simultáneamente diversas conexiones TCP/IP con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección IP, pero van dirigidos a puertos diferentes. También que una máquina pueda establecer simultáneamente diversas comunicaciones TCP/IP con otra utilizando puertos distintos para cada conexión.

Como se ha indicado, los números de puerto se indican mediante una palabra de 2 bytes (16 bits), por lo que el rango de valores es de 216 (0 a 65535) y en principio una aplicación puede utilizar cualquier número dentro del rango.

Sin embargo, con el fin de unificar criterios en cuanto a los puertos que utilizarían las aplicaciones de Internet, la IANA realizó una asignación de los números disponibles en tres categorías:

- Puertos bien conocidos (Well known ports), comprendidos entre 0 y 1023. Estos 1024 (210) puertos pueden ser representados con 10 bits y son reservados para servicios conocidos.
- Puertos registrados (Registered ports). 48127 puertos comprendidos entre 1024 y 49151.
- Puertos dinámicos y privados. Los comprendidos entre los números 49152 y 65535.

En caso de tener que asignar un puerto a una aplicación, si no se elige el correspondiente Well-Known debe seleccionarse un número en el rango 1024 - 65535.

Número de puerto	Descripcón
0	Reservado
1	TCP Servicio de multiplexado de puertos (TCPMUX)
4	No asignado
5	RJE ("Remote Job Entry")

IANA-Agencia de Asignación de Números Internet
TCP/IP- Protocolo de Control de Transmisión /Protocolo de Internet
UDP/IP- Protocolo de datagrama de usuario/Protocolo de Internet

6	No asignado
7	ECHO
18	MSP ("Message Send Protocol")
20	FTP ("File Transfer Protocol") Datos
21	FTP ("File Transfer Protocol") Control
22	SSH Secure Shell Remote Login Protocol
23	Telnet (acceso a terminal remoto)
25	SMTP ("Simple Mail Transfer Protocol")
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	Whois
49	Login Host Protocol (Login) DNS ("Domain Name System")
53	DNS ("Domain Name System")
59	IDENT
69	TFTP ("Trivial File Transfer Protocol, Protocolo Trivial de Transferencia de Archivos ")
70	Servicio Gopher
79	Servicio Finger
80	HTTP ("Hyper Text Transfer Protocol")
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2 ("Post Office Protocol")
110	POP3 ("Post Office Protocol")
113	UDP ("User Datagram Protocol")
115	SFTP ("Simple File Transfer Protocol")
118	Servicios SQL
119	NNTP ("Network News Transfer Protocol")
137	NetBIOS Name Service
139	NetBIOS Datagram Service (Session service)
143	IMAP ("Interim Mail Access Protocol")
150	NetBIOS Session Service
156	SQL Server
161	SNMP ("Simple Network Management Protocol, Protocolo Simple de Administración de Redes ")
162	SNMP trap
179	BGP ("Border Gateway Patrol, Protocolo de entrada de frontera ")
190	GACP ("Gateway Access Control Protocol")
194	IRC ("Internet Relay Chat")
197	DLS ("Directory Location Service")
210	wais (servicio de búsquedas)
389	LDAP ("Lightweight Directory Access Protocol")
396	Novell Netware sobre IP
443	HTTPS ("HyperText Transfer Protocol")
444	SNNP ("Simple Network Paging Protocol")
445	Microsoft-DS
458	Apple QuickTime

513	rlogin Acceso remoto
546	DHCP ("Dynamic Host Configuration Protocol")
547	DHCP Servidor
563	SNEWS
569	MSN
631	UDP ("User Datagram Protocol")
1080	Socks Proxy
Otros Puertos no estándar	
1503	T.120 Utilizado por aplicaciones que comparten aplicaciones
1720	H.323 Utilizado para escuchar llamadas entrantes por aplicaciones como VideoLink_Pro de Smith Micro y Microsoft NetMeeting.
1723	PPTP ("Point-to-Point Tunneling Protocol")
6660-6669	TCP ("Transmission Control Protocol")
8080	Web proxy caching service

Tabla 2.4 Numeración de puertos

2.8 DIRECCIONAMIENTO

IP constituye el protocolo de direccionamiento de la suite de protocolos TCP/IP. Su función esta orientada a proveer direccionamiento en el nivel red e identificación de redes y host. IP es la base para el enrutamiento de los datagramas, otorga una identificación global y única de los elementos de la red. Algunas características del direccionamiento IP son:

Cada máquina con TCP/IP tiene asociado un número de 32 bits al que se llama dirección IP, a la vez la dirección está divida en 4 octetos (grupos de ocho bits), representados por un número decimal de 0 a 255 separados por un punto, (por ejemplo 172.16.25.10.) y que está dividido en dos partes:

Una parte que identifica la dirección de la red (NETID). La cual es asignada por el NIC (Network Information Center), el número de bits que ocupa depende del tamaño de la red y puede ser 8, 16 ó 24.

Una parte que identifica la dirección de la máquina dentro de la red (HOSTID). Las direcciones de los host son asignadas por el administrador de la red.

Una dirección se representa por cuatro valores decimales separados por puntos para que sea más fácil su escritura y memorización.

[0..255] . [0..255] . [0..255] . [0..255]

Cuando se intenta establecer una conexión con otra máquina, no se suele poner la dirección IP de esta, sino que se utiliza un nombre. La máquina se encarga de transformar ese nombre a una dirección IP.

Cuando se quiere conectar con otra máquina que no está en la misma red, se suele utilizar un nombre que es más complejo que las conexiones dentro de la misma red. Dicho nombre consta de dos partes:

- Identificación del usuario@.
- Nombre de la máquina.

El nombre de la máquina se llama dominio, que a su vez puede estar dividido en sub dominios. Lo normal es que un dominio tenga tres subdominios, de los cuales el que esta más a la derecha se denomina subdominio de primer nivel y es el más genérico de todos. Para entender los subdominios se deben mirar de derecha a izquierda. Existen dos tipos de subdominios de primer nivel:

- Dominios de organizaciones

Sub dominio 1er. Nivel Organizaciones	Significado
.com	Comercial
.edu	Educativa
.org	Organización no lucrativa
.gob	Gobierno
.int	Organización internacional
.net	Gestion de redes
.mil	Organización militar

Tabla 2.5 Dominios de Organizaciones

- Dominios geográficos utilizados en el resto del mundo.

Sub dominio 1er. Nivel Geográficos	Significado
at	Austria
au	Australia
ca	Canadá
de	Alemania
es	España
fr	Francia
uk	Reino Unido
mx	México
us	Estados Unidos

Tabla 2.6 Dominios Geográficos

2.8.1 DIRECCION FISICA

El formato de una dirección física o MAC utilizada por los protocolos 802 es el siguiente:

1Byte - 2Byte - 3Byte - 4Byte - 5Byte - 6Byte

Los bytes 1, 2 y 3 pertenecen al identificador OUI (Identificador único de la organización), este identificador es asignado por la IEEE a los fabricantes de hardware o software que soliciten un OUI. Los bytes 4, 5 y 6 son asignados por el fabricante de hardware. La IEEE tiene la responsabilidad de asignar un único OUI. Esto implica que por cada OUI asignado el fabricante puede fabricar hasta 2^24 interfaces de red.

El formato de una dirección física 802 MAC fuente es distinta al formato de una dirección destino. El formato del primer byte de una dirección MAC fuente es el siguiente:

0 1 2 3 4 5 6 7

- Si Bit 1 es igual a 0 implica que la dirección MAC tiene sentido global.
- Si Bit 1 es igual a 1 implica que la dirección MAC tiene sentido local.

En el diseño inicial de protocolo Ethernet no existía el concepto de sentido local. Todas las direcciones en ese momento tenían sentido global únicamente. Cuando el protocolo Ethernet fue standarizado por la IEEE y absorbido por el grupo 802 se tomó la decisión de incorporar el sentido local en una dirección MAC. El sentido local de una dirección MAC permite al administrador de la red asignar los bytes 4, 5 y 6. El sentido global de una dirección MAC es la dirección MAC asignada por el fabricante y no puede ser manipulada por el administrador de la red.

El valor del primer bit (0) es cero para las tramas Ethernet.
El formato del primer byte de una dirección MAC destino es la siguiente:

0 1 2 3 4 5 6 7

- Si Bit 0 es igual a 0 implica que la dirección MAC destino es UNICAST.
- Si Bit 0 es igual a 1 implica que la dirección MAC Destino es MULTICAST.
- Si Bit 1 es igual a 0 implica que la dirección MAC tiene sentido global.
- Si Bit 1 es igual a 1 implica que la dirección MAC tiene sentido local.

Las MAC son direcciones que contienen 4 8bits de longitud y son un componente superior de la Capa de Enlace de Datos (OSI).

Ejemplo: **02-C9-00-P6-01-20**

IEEE- Instituto de Ingenieros Eléctricos-Electrónicos
MAC-Control de Acceso al Medio
OSI-Interconexión de Sistemas Abiertos

2.8.2 DIRECCION LOGICA IP

Las direcciones de IP están formadas por 4 octetos que en su conjunto tienen 32 bits, así que tenemos cuatro campos de 8 bits separados por puntos, cada uno de los campos tiene un valor comprendido entre 00000000 (cero en decimal) y 11111111 (255 en decimal).

Los cuatro octetos componen la dirección de red y de equipo y están en función de la clase de red correspondiente.

Por ejemplo128.2.7.9 es una dirección IP de clase B donde:
128.2 es el número de red y 7.9 es el número de equipo o host.

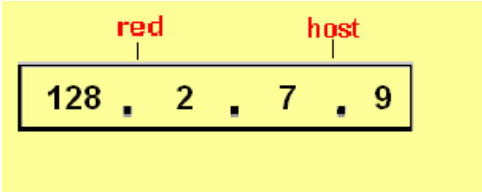


Figura 2.16 Dirección IP

El formato binario para la dirección IP 128.2.7.9 es:

10000000 00000010 00000111 00001001

Las direcciones IP son usadas por el protocolo IP para definir únicamente un host en la red.

A partir de la dirección IP, una red puede determinar si los datos deben ser enviados a través de un router o un gateway hacia el exterior de la red. Si los bytes correspondientes a la red de la dirección IP del host destino son los mismos que los de la dirección de la red actual (enrutado directo), los datos no se pasarán al router, si son diferentes, se les pasaran para que los enrute hacia el exterior de la red. En este caso, el router tendrá que determinar el camino de enrutamiento idóneo en base a la dirección IP de los paquetes y una tabla interna que contiene la información de enrutamiento.

Desde el punto de vista de su accesibilidad podemos clasificar las direcciones IP en:

- **Direcciones IP públicas**: aquellas que son visibles por todos los host conectados a Internet. Para que una máquina sea visible desde Internet debe tener asignada obligatoriamente una dirección IP pública, y no puede haber dos host con la misma dirección IP pública.

- **Direcciones IP privadas**: aquellas que son visibles únicamente por los host de su propia red o de otra red privada interconectada por medio de routers. Los host con direcciones IP privadas no son visibles desde Internet, por lo que si quieren salir a ésta deben hacerlo a través de un router o un proxy que tenga asignada una IP pública. Las direcciones IP privadas se utilizan en redes privadas para interconectar las estaciones de trabajo.

Desde el punto de vista de su perdurabilidad podemos clasificar las direcciones IP en:

- **Direcciones IP estáticas**: aquellas asignadas de forma fija o permanente a un host determinado, por lo que cuando una máquina con este tipo de IP se conecte a la red lo hará siempre con la misma dirección IP. Normalmente son usadas por servidores web, routers o máquinas que deban estar conectadas a la red de forma permanente, y en el caso de direcciones IP públicas estáticas hay que contratarlas, generalmente a un ISP (proveedor de Servicios de Internet). Las conexiones a Internet mediante ADSL son de este tipo.

- **Direcciones IP dinámicas**: aquellas que son asignadas de forma dinámica a los host que desean conectarse a Internet y no tienen una IP fija. Un ejemplo típico de este tipo de direcciones IP es el de una conexión a Internet mediante módem. El ISP dispone de un conjunto de direcciones IP para asignar a sus clientes, de forma que cuando uno de ellos se conecta mediante módem se le asigna una de estas IP, que es válida durante el tiempo que dura la conexión. Cada vez que el usuario se conecte lo hará con una dirección IP distinta.

2.8.3 CLASES DE DIRECCION IP

Son cinco las clases de redes que existen, A,B,C,D y E y se definen en función del numero de computadoras que se van a conectar.

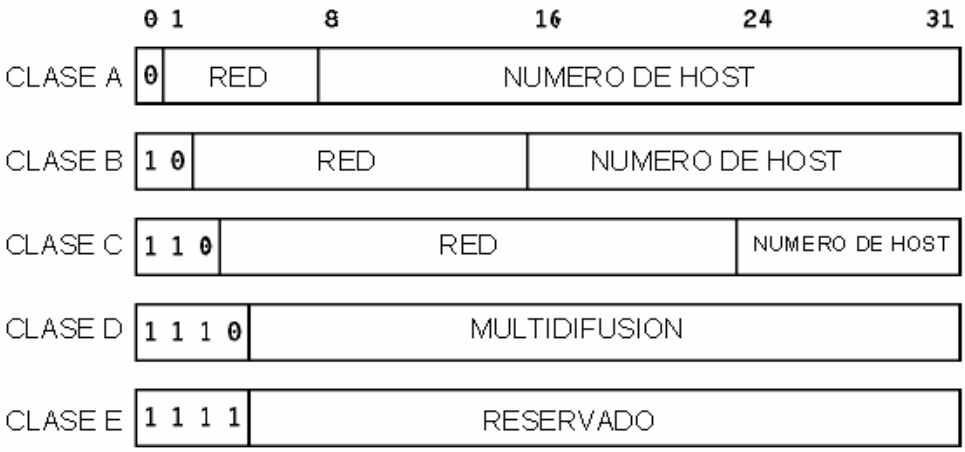


Figura 2.17 Clases de Direcciones IP

ADSL- Línea de Abonado Digital Asimétrica
IP-Protocolo de Internet

- Clase A

Contiene 7 bits para direcciones de red en el cual el primer bit es cero, los demás bits representa direcciones de equipo, esto conlleva a poder conectar únicamente 128 redes, aunque en realidad podemos utilizar 126 ya que la dirección 0 y la 127 están reservadas. Cada una de las 126 redes disponibles pueden contener un numero máximo de1 6 777 216 computadoras aunque al igual que con el numero de redes se reservan las direcciones en donde todos son ceros y todos son unos, teniendo un total de computadoras físicamente conectadas de 16.77.214. Las direcciones de clase A se encuentran comprendidas expresadas de manera decimal entre 0.0.0.0 y 127.255.255.255 y la mascara de subred es 255.0.0.0

- Clase B

Maneja 14 bits para direcciones de red debido a que el valor de los dos primeros bits del primer octetos es siempre 10. Tienen por lo tanto 16 bits para direcciones de equipo, lo que permite un máximo de 16.384 redes cada una con 65.536 computadoras con la misma restricción de no usar las direcciones que contengan todos ceros o todos unos, con lo que pueden tener 65.534 computadoras cada una. Esta clase esta comprendida entre 128.0.0.0 y 191.255.255.255 expresado en decimales y su mascara de subred será de 255.255.0.0.

- Clase C

Contiene 21 bits para direcciones de red ya que el valor del primer octeto es siempre 110 y para direcciones de equipos únicamente tiene 8 bits con lo cual nos permite un máximo de 2.097.152 redes por 256 computadoras. Sus direcciones están comprendidas decimalmente entre 192.0.0.0 y la 223.255.255.255 y su mascara de subred es la 255.255.255.0.

- Clase D

Esta clase esta reservada para direcciones “Multicasting” o multidestino, en la cual se transmite un mensaje de una PC a un grupo específico de computadoras, en esta clase el valor de los primeros cuatro octetos es 1110 y los últimos 28 bits representan los grupos multidestino. Sus direcciones representadas en decimal están comprendidas entre 224.0.0.0 y 239.255.255.255.

- Clase E

Se utiliza con fines de experimentación, esta no se encuentra disponible a usuarios generales. El valor de los primeros cuatro primeros bits del primer octeto es 1111 y, las direcciones en

representación decimal esta comprendidas entre 240.0.0.0. y 255.255.255.255.

clase	primeros bits binarios	primer byte decimal	Identificación de red	identificación de host	número de redes	número de host
A	0	1 - 126	1 byte	3 bytes	126	16.77.214
B	10	128 - 191	2 bytes	2 bytes	16.384	65.534
C	110	192 - 223	3 bytes	1 byte	2.064.512	254

Tabla 2.7 Características de Direcciones IP

2.8.4 MASCARA DE RED

Durante el enrutamiento de la información, TCP/IP tiene que determinar si la información pertenece a una host de la red local o pertenece a uno de una red remota, para esto es necesario enmascarar una parte de la dirección IP para distinguir el ID de red y la ID de host. A esto se le llama mascara de red y es una dirección de 32 bits.

La mascara de red puede estar definida por defecto cuando la red no esta dividida en subredes y se encuentra determinada por la clase de dirección, o definida por el administrador cuando la red esta dividida en segmentos.

La mascara de red definida por la clase de dirección se ven en la tabla siguiente:

Clase	Bits usados por la mascara de red	Valor decimal
Clase A	11111111 00000000 00000000 00000000	255.0.0.0
Clase B	11111111 11111111 00000000 00000000	255.255.0.0
Clase C	11111111 11111111 11111111 00000000	255.255.255.0

Tabla 2.8 Máscaras de red definidas por Clase

En la mascara de red, todos los bits que corresponden a un ID de red están colocados a uno, es decir en decimal, el valor de su octeto es 255 y todos los bits que correspondan al ID de host estarán todos a cero. Si la mascara es 255.255.0.0, los 2 primeros bytes son la parte de red y los 2 últimos son la parte de maquina.

2.8.5 DIRECCIONAMIENTO DE SUBREDES

El administrador de red, cuando trabaja con una red pequeña (pocos host conectados) puede fácilmente configurar el rango de direcciones IP usado, para tener un funcionamiento óptimo del sistema.

Conforme la red va creciendo se hace necesaria una división en partes de la misma debido a que las colisiones aumentan, ocasionando que el rendimiento de la red se ve afectado seriamente. Para resolver este problema se opta por dividir la red en segmentos significativos, de tal forma que mediante switches, que envían las tramas sólo al segmento en el que se encuentra el host destino, limita y controla las colisiones

No obstante al segmentar la red, aumenta el número de host y con ello el número de transmisiones de broadcast llegando a congestionar la red de forma inaceptable, al consumir excesivamente el ancho de banda. Esto se debe porque todos los host están enviando de forma constante peticiones de este tipo: peticiones ARP, envíos RIP, peticiones DNS, etc.

Sin embargo para resolver este problema es preciso dividir la red principal en una serie de subredes, de tal forma que cada una de ellas va a funcionar, a nivel de envío y recepción de paquetes, como una red individual, aunque todas pertenezcan a la misma red principal (mismo dominio). De esta forma, aunque la red en su conjunto tendrá una dirección IP única, a nivel administrativo podemos considerar subredes bien diferenciadas, para tener un control del tráfico de la red y una limitación de las peticiones de broadcast.

Para ejemplificar esto, en el capítulo III vamos a dividir una dirección de red privada en subredes, tomaremos una red de clase B, cuyo procedimiento es aplicable para redes de clase A y C.

2.9 ARP (PROTOCOLO DE RESOLUCION DE DIRECCIONES)

El protocolo ARP (Address Resolution Protocol), se encarga de convertir las direcciones IP en direcciones de la red física.

Esto es, cuando una máquina desea enviar un mensaje a otra, que está conectada a través de una red Ethernet se encuentra con el problema de que la dirección IP de la máquina destino es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que debe encontrar un modo de traducir la dirección IP a la dirección física.

Este protocolo utiliza una tabla denominada Tabla de Direcciones ARP, que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Si la dirección solicitada se encuentra en esta tabla el proceso termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la dirección física de la máquina destino.

Si la dirección buscada no esta en la tabla el protocolo ARP, éste envía un mensaje a toda la red. Cuando un ordenador reconoce su dirección IP envía

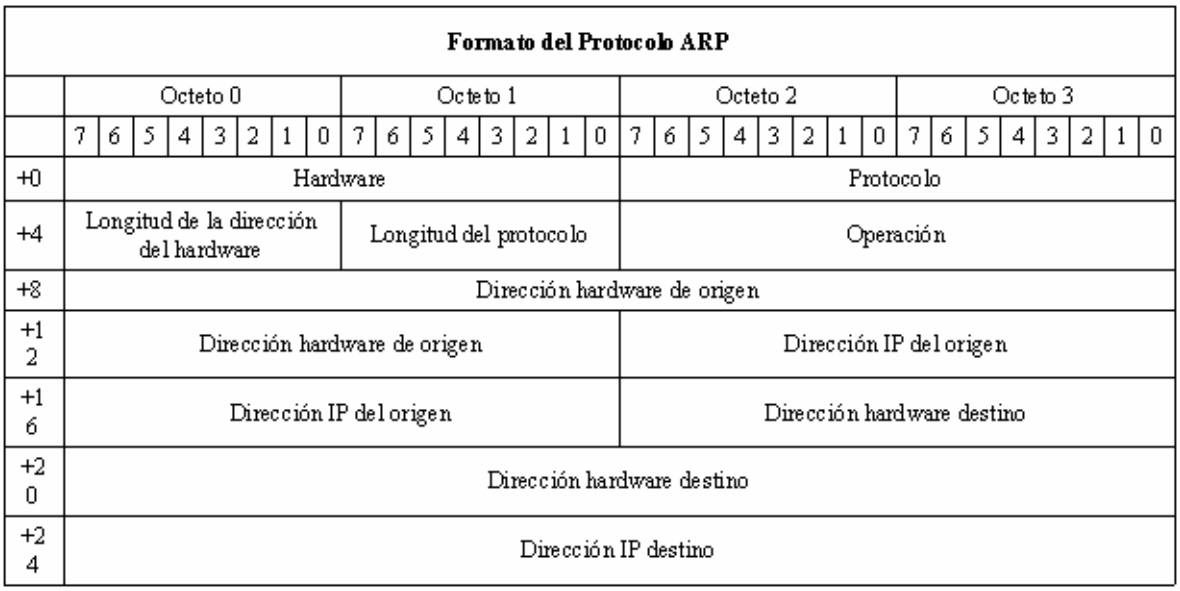
DNS- Sistema de Nombres de Dominio
IP-Protocolo de Internet

un mensaje de respuesta que contiene la dirección física. Cuando la máquina origen recibe este mensaje ya puede establecer la comunicación con la máquina destino, y esta dirección física se guarda en la Tabla de direcciones ARP.

Las tablas ARP reducen el tráfico de la red al evitar preguntas ARP innecesarias.

2.9.1 DISPOSICION DE LOS CAMPOS ARP

El mensaje ARP esta formado por 28 octetos. Los campos que se describen son para una Interfaz Ethernet.



Formato del Protocolo ARP																													
	Octeto 0								Octeto 1								Octeto 2								Octeto 3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
+0	Hardware																Protocolo															
+4	Longitud de la dirección del hardware								Longitud del protocolo								Operación															
+8	Dirección hardware de origen																															
+12	Dirección hardware de origen																Dirección IP del origen															
+16	Dirección IP del origen																Dirección hardware destino															
+20	Dirección hardware destino																															
+24	Dirección IP destino																															

Figura 2.18 Disposición de los campos ARP

Tipo de Hardware

El campo Hardware indica el tipo de interfaz. Por Ejemplo, el valor de una red Ethernet es 1.

Protocolo

Identifica el protocolo usado. Por ejemplo el valor de la interfaz Ethernet es 0800 hex.

Longitud de la dirección Hardware

Especifica la longitud (en bytes) de la dirección de hardware del paquete El valor para Ethernet es 6, lo que proporciona 48 bits para una dirección Ethernet (12 semi-octetos)

Longitud del Protocolo

Este campo se usa para definir la longitud de la dirección de red. Para una red IP es 4 bytes.

Operación

Especifica el código de la operación. La solicitud ARP tiene valor 1, y la respuesta ARP tiene valor 2.

Dirección Hardware del Origen

Contiene las direcciones físicas del computador fuente.
La dirección Hardware de Origen (para Ethernet) esta formada por octetos que representan una dirección Ethernet de 48 bits, o un numero.

Dirección IP de Origen

La dirección IP de Origen puede ser una dirección de clase A, B o C.

Dirección Hardware de Destino

Este campo esta formado igual que el campo Dirección Hardware de Origen.

Dirección IP de Destino

Este campo es igual que el campo Dirección IP de Origen

2.9.2 PROXY ARP

La función de Proxy ARP es la de encaminar paquetes de una máquina que se ubica en una determinada subred hacia una máquina ubicada en una subred diferente, dentro de la misma red IP, a través de un router.

Para ello cuando un el host A quiere enviar un datagrama IP al host B, primero ha de determinar la dirección de red física del host B usando ARP.
Como A no puede diferenciar entre las redes físicas, su algoritmo de encaminamiento IP piensa que el host B está en su misma red local y envía un broadcast de petición ARP. El host B no lo recibe, pero sí el "router" R. R entiende de subredes, es decir, ejecuta la versión de subred del algoritmo de encaminamiento y será capaz de ver que el destino de la petición ARP (en el campo de dirección de protocolo de destino) está localizado en otra red física.

ARP-Protocolo de Resolución de Direcciones
IP-Protocolo de Internet

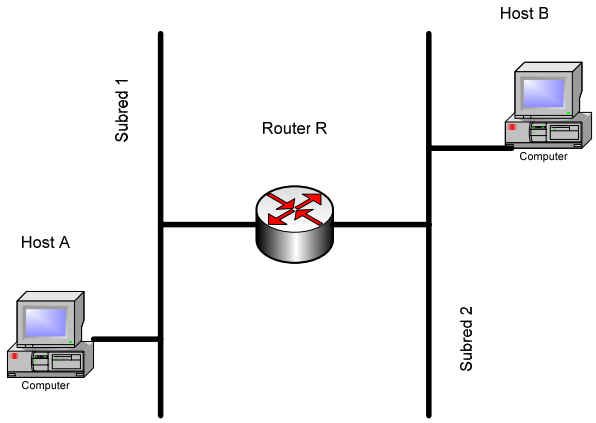


Figura 2.19 Funcionamiento básico de Proxy ARP

Cuando el host A quiere enviar un datagrama IP al host B, primero ha de determinar la dirección de red física del host B usando ARP.

Como A no puede diferenciar entre las redes físicas, su algoritmo de encaminamiento IP piensa que el host B está en su misma red local y envía un broadcast de petición ARP. El host B no lo recibe, pero sí el router.

R ejecuta la versión de subred del algoritmo de encaminamiento y es capaz de ver que el destino de la petición ARP (en el campo de dirección de protocolo destino) está localizado en otra red física.

Si las tablas de encaminamiento de R especifican que el siguiente salto a otra red se produce a través de un dispositivo diferente, replicará al ARP como si fuera el host B, diciendo que la dirección de B es la del mismo router.

El host A recibe esta respuesta ARP, la introduce en su caché y envía los paquetes dirigidos a B, a través del router R, que los retransmitirá a la subred adecuada.

El resultado es una subred transparente:

- Los host normales (como A y B) desconocen de subredes, por lo que usan el algoritmo de encaminamiento clásico.
- Los router entre subredes:
  - Utilizan el algoritmo IP para subredes.
  - Usan un módulo ARP modificado, que puede responder en nombre de otros hosts.

2.10 RARP (PROTOCOLO DE RESOLUCION DE DIRECCIONES EN REVERSA)

Para ayudar a un nodo a descubrir su propia dirección de IP se diseñó una variante del ARP llamado ARP inverso (RARP - reverse ARP).

ARP-Protocolo de Resolución de Direcciones
IP-Protocolo de Internet

El objetivo era que lo usasen las estaciones de trabajo sin disco y otros dispositivos que necesitasen obtener configuración de red de un servidor de red.

La estación que usa el protocolo RARP difunde una petición en la que indica su dirección física y solicita su dirección de IP. Un servidor de la red, que contiene una tabla de traducción entre direcciones físicas y direcciones IP responde a la petición, enviando la dirección que le corresponde.

RARP es el encargado de traducir direcciones físicas en direcciones IP.

Host	Dirección física	Dirección IP
A	A3.BB.05.17.29.D0	194.18.133.5
R	A3.BB.05.33.12.99	194.18.133.1

TABLA 2.9 Direcciones Físicas/IP

RARP ha sido superado por el protocolo BOOTP y su versión mejorada, el Protocolo de configuración dinámica de host (DHCP - Dynamic Host Configuration Protocol).

2.11 IP (DATAGRAMA DEL PROTOCOLO DE INTERNET)

El principal protocolo que opera en la Capa de Internet es el protocolo IP (Internet Protocol), encargado de identificar cada uno de los paquetes que pasan por la capa y de seleccionar la mejor ruta posible entre los host que desean comunicarse.

IP proporciona un servicio de de distribución de paquetes caracterizado por:

- Transmisión de datos en datagramas (paquetes IP).
- No está orientado a la conexión, lo que significa que los paquetes que circulan entre los host son tratados de forma independiente, lo cual origina que cada uno pueda seguir una trayectoria diferente en su viaje hasta el host destino.
- No es confiable, ya que no implementa mecanismos de verificación de entrega de paquetes, lo que no garantiza una entrega de los mismos, ni la entrega en secuencia, ni la entrega única. Esto queda en manos del protocolo TCP de la capa superior.
- No implementa corrección de errores ni control de congestión.
- Puede fragmentar los paquetes, si es necesario.
- Direcciona los paquetes mediante direcciones lógicas IP de 32 bits (IP v4).
- Sólo verifica la integridad del paquete en sí, no los datos que contiene.

RARP- Protocolo de Resolución de Direcciones En Reversa
TCP-Protocolo de Control de Tramsmisión

Así que sus funciones principales son el direccionamiento de los paquetes y la administración del proceso de fragmentación y desfragmentación de los mismos. Para el direccionamiento de los paquetes, el protocolo IP examina la topología de la red para determinar la mejor ruta de envío.

A pesar de estas características, que parecen dar a entender que es un protocolo poco fiable, IP es fundamental para poder intercomunicar diferentes redes, hasta tal punto que constituye el pilar sobre el que se ha construido Internet. Para dar confiabilidad al sistema se usan tanto los protocolos de las capas superiores como los de la Capa de Enlace de Datos, encargandose IP tan sólo del enrutamiento de paquetes entre los host que se comunican.

2.11.1 ENCABEZADO DEL IP

El esquema de envío de IP es similar al que se emplea en la capa Acceso a red. En esta última se envían Tramas formadas por un Encabezado y los Datos. En el Encabezado se incluye la dirección física del origen y del destino.

En el caso de IP se envían Datagramas, estos también incluyen un Encabezado y Datos, pero las direcciones empleadas son Direcciones IP.

Encabezado	Datos

El encabezado IP esta compuesto de 32 bits, los campos que más nos interesan son: versión, tipo de servicio, banderas, tiempo de vida, desplazamiento y protocolo.

2.11.2 DESCRIPCION DE LOS CAMPOS EN EL DATAGRAMA IP

Formato del Datagrama IP

Los Datagramas IP están formados por Palabras de 32 bits. Cada Datagrama tiene un mínimo de cinco palabras y un máximo de quince.

<table>
<tr><td>Versión</td><td>Cabecera</td><td>Tipo de Servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificación</td><td>Banderas</td><td>Desp. De Fragmento</td></tr>
<tr><td colspan="2">TTL</td><td>Protocolo</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="5">Dirección IP de la Fuente</td></tr>
<tr><td colspan="5">Dirección IP del Destino</td></tr>
<tr><td colspan="4">Opciones IP (Opcional)</td><td>Relleno</td></tr>
<tr><td colspan="5">DATOS</td></tr>
</table>

Figura 2.20 Formato del Datagrama IP

IP-Protocolo de Internet
TTL -Tiempo de Vida

Versión (4 bits)

Versión del protocolo IP (4 bits). Este campo hace posible la transición entre diferentes versiones del protocolo IP, ejecutando cada máquina la mayor versión que soporte.

Cabecera (4 bits)

Longitud del encabezado IP en palabras de 32 bits, necesario ya que la cabecera de un datagrama no es constante. El valor mínimo de este campo es 5, y el valor máximo 15, lo que limita la cabecera a 600 bytes.

Tipo de Servicio (8 bits),

Tipo de servicio que establece la Prioridad del datagrama (3 bits), Procesamiento con Retardos cortos (Delay-1 bit), la solicitud de Alto Desempeño (Throughput-1 bit) y la soliccitud de mínima probabilidad de pérdida (Reliability-1 bit).

Su estructura es:

Prioridad	D	T	R	Sin Uso

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes. Los tipos D, T y R solicitan un tipo de transporte dado: D = Procesamiento con retardos cortos, T = Alto Desempeño y R = Alta confiabilidad. Nótese que estos bits son solo "sugerencias", no es obligatorio para la red cumplirlo.

Longitud Total (16 bits)

Indica la Longitud total del datagrama IP. La longitud máxima es de 65.635 bytes.

El tamaño para un Datagrama debe ser tal que permita la encapsulación, esto es, enviar un Datagrama completo en una trama física. El problema está en que el Datagrama debe transitar por diferentes redes físicas, con diferentes tecnologías y diferentes capacidades de transferencia. A la capacidad máxima de transferencia de datos de una red física se le llama MTU (el MTU de ethernet es 1500 bytes por trama). Cuando un Datagrama pasa de una red a otra con un MTU menor a su tamaño es necesaria la fragmentación. A las diferentes partes de un Datagrama se les llama fragmento*.* Al proceso de reconstrucción del Datagrama a partir de sus fragmentos se le llama Reensamblado de fragmentos.

El control de la fragmentación de un Datagrama IP se realiza con los campos de la segunda palabra de su cabecera.

IP-Protocolo de Internet
MTU-Unidada de Transferencia Máxima de Datos

Identificación (16 bits)

Número de 16 bits que identifica al Datagrama, permite implementar números de secuencias, además de reconocer los diferentes fragmentos de un mismo Datagrama, pues todos ellos comparten este numero.

Banderas (3 bits).

Un campo de tres bits donde el primero está reservado. El segundo, llamado bit de No Fragmentación significa:

- 0 = Puede fragmentarse el Datagrama
- 1 = No puede fragmentarse el Datagrama, generalmente porque el host destino es incapaz de juntar los fragmentos. Si este flag está activado y el datagrama llega a una red que precisa la fragmentación, el datagrama será desechado.

El tercer bit es llamado Más – Fragmentos y significa:

- 0 = Unico fragmento o Ultimo fragmento,
- 1 = Aun hay más fragmentos.

Cuando hay un 0 en Más fragmentos, debe evaluarse el campo desplazamiento De Fragmento: si este es cero, el Datagrama no esta fragmentado, si es diferente de cero, el Datagrama es un último fragmento.

Desplazamiento De Fragmento (13 bits)

Indica la ubicación del datagrama actual en uno fragmentado, medido en unidades de 64 bits. Si el paquete no está fragmentado, este campo tiene un valor cero.

TTL (8 bits).

Tiempo de espera, que puede estar un datagrama en la red antes de su destrucción, acción necesaria para que un datagrama no entregado no vague indefinidamente por la red. Generalmente se implementa mediante la métrica de contador de saltos (número de routers que puede atravesar el datagrama antes de su destrucción).

Protocolo (8 bits)

Especifica que protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos de Datagrama IP. Algunos valores posibles son: 1 = ICMP, 6 = TCP, 17 = UDP, 88 = IGRP (Protocolo de Enrutamiento de Pasarela Interior de CISCO).

ICMP- Protocolo de Control de Mensajes de Internet
IP-Protocolo de Internet
TCP-Protocolo de Control de Transmisión
TTL-Tiempo de Vida
UDP-Protocolo de Datagrama de Usuario

Checksum (16 bits)

Es un campo de Suma de comprobación de la cabecera del datagrama, para la comprobación de errores. El útil para detectar errores generados por palabras de memoria erróneas en uno de los routers que atraviesa en datagrama.

Dirección IP de la Fuente/Destino

Direcciones IP de origen (32 bits) y destino (32 bits) del datagrama.

Opciones IP

Existen hasta 40 bytes extra en la cabecera del Datagrama IP que pueden llevar una o más opciones. Su uso es bastante raro.

- Uso de Ruta Estricta (Camino Obligatorio)
- Ruta de Origen Desconectada (Nodos Obligatorios)
- Crear registro de Ruta
- Marcas de Tiempo
- Seguridad Básica del Departamento de Defensa
- Seguridad Extendida del Departamento de Defensa

Relleno

Bits necesarios para asegurar que la longitud del datagrama sea múltiplo de 32 bits.

Datos

Segmento TCP/UDP de la Capa de Transporte.

2.11.3 FINALIDAD DEL DATAGRAMA

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en secuencias incorrectas o fragmentados intencionadamente para permitir que un nodo con un buffer limitado pueda tomarlo. Es la responsabilidad del protocolo TCP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones éstos son recibidos por la maquina origen.

Debido a todas estas características la finalidad de un datagrama es la de autocontener independientemente y transportar la información suficiente para ser encaminada desde su ordenador origen a su ordenador destino sin tener que depender de que se haya producido anteriormente tráfico alguno entre ambos y la red de transporte.

IP-Protocolo de Internet
TCP-Protocolo de Control de Transmisión

2.12 ICMP (PROTOCOLO DE INTERNET MENSAJES DE ERROR Y CONTROL)

El Protocolo IP utiliza el protocolo de mensajes de control Internet (ICMP, Internet Control Message Protocol) para informar de los errores que pueden ocurrir durante el enrutamiento de paquetes IP.

El protocolo ICMP utiliza el soporte básico de IP como si se tratara de un protocolo de nivel superior. Sin embargo, ICMP es realmente una parte integral del protocolo IP, y debe ser implementado por todo módulo IP.

Los mensajes ICMP son enviados en varias situaciones:

- Cuando un datagrama no puede alcanzar su destino
- Cuando un enrutador no dispone de capacidad de almacenamiento temporal para reenviar un paquete IP
- Cuando el enrutador puede dirigir al computador para enviar el tráfico por una ruta más corta.

El propósito de estos mensajes de control no es hacer a IP fiable, sino suministrar información sobre los problemas en el entorno de comunicación.

Los mensajes ICMP se envían usando la cabecera IP básica. El primer octeto de la parte de datos del datagrama es el campo de tipo ICMP; el valor de este campo determina el formato del resto de los datos. Los campos etiquetados como "no usado" están reservados para posteriores extensiones y deben ser cero al ser enviados, y los receptores no deberán usar estos campos (excepto para incluirlos en la suma de control).

2.12.2 FORMATO DE LOS MENSAJES ICMP

Aunque cada tipo de mensaje tiene su propio formato, todos ellos comparten los primeros tres campos: TIPO (8 bits), CODIGO (8 bits) y CHECKSUM (16 bits).

TIPO	CODIGO	CHECKSUM

El campo TIPO identifica al tipo de mensaje ICMP y determina su formato. Puede tener alguno de estos valores:

- 0: Respuesta de Eco (Echo Replay)
- 3: Destino Inaccesible (Host Unreachable)
- 4: Disminución del tráfico desde el origen (Source Quench)
- 5: Redireccionar (Redirect)
- 8 : Solicitud de Eco (Echo Request)
- 11 : Tiempo Excedido (Time Exceeded)
- 12 : Problema de Parámetros (Parameter Problem)

- 13 : Marca de tiempo (Timestamp)
- 14 : Respuesta de marca de tiempo (Timestamp Reply)
- 17 : Solicitud de información (Information Request)
- 18 : Respuesta de información (Information Reply)

Mensajes Solicitud de Eco y Respuesta al Eco

Este es el tipo de mensaje que envía la maquina cuando se emplea el comando ping. Solicitud de Eco pide a la maquina destino que responda con una Respuesta de Eco con un numero de secuencia apropiado.

TIPO (8 o 0)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Datos Opcionales		

Mensaje Destino Inaccesible

Es el mensaje empleado para reportar que no es posible entregar un Datagrama. El campo CODIGO describe mejor el problema:

- 0 : Red Inaccesible
- 1 : Host Inaccesible
- 2: Protocolo Inaccesible
- 3: Puerto Inaccesible
- 4: Necesita Fragmentación
- 5: Falla en la Ruta de Origen
- 6: Red de Destino Desconocida
- 7: Host Destino Desconocido
- 8: Host de Origen Aislado
- 9: Comunicación con Red Destino Administrativamente Prohibida
- 10: Comunicación con Host Destino Administrativamente Prohibida
- 11: Red Inaccesible por el tipo de servicio
- 12: Host Inaccesible por el tipo de servicio

TIPO (3)	CODIGO (0...12)	CHECKSUM
NO – USADO (debe ser cero)		
Encabezado IP + Primeros 8 bytes de Datos IP		

Los errores de red inaccesible por lo general implican fallas de enrutamiento. Debido a que el mensaje ICMP contiene la cabecera del Datagrama que lo produjo (en el campo de datos), el origen sabrá cual es el destino inaccesible.

ICMP- Protocolo de Control de Mensajes de Internet
IP-Protocolo de Internet

Mensaje De Disminución Del Tráfico Desde El Origen

Debido a que IP funciona sin conexión, un Router no puede reservar memoria o recursos de comunicación antes de recibir los Datagramas. En consecuencia los Routers pueden verse repentinamente saturados por el trafico. A esta situación se le llama congestión.

El congestionamiento se da por que un Host de alta velocidad genera Datagramas mas rápido de lo que el Router puede manejar o porque muchos Host envían Datagrama a la misma dirección al mismo tiempo.

Cuando los datagramas llegan mas rápido de lo que un router puede manejarlos, este los coloca en un buffer. Si los datagramas son parte de una ráfaga pequeña, esto soluciona el problema, pero si continúan llegando datagramas se saturan los buffers y el router debe descartar los nuevos datagramas. Es entonces cuando el router genera un mensaje ICMP de disminución del tráfico desde el origen solicitando a este reducir la tasa de envío de datagramas. No existe un mensaje ICMP para revertir esta solicitud, en general poco después de bajar la tasa de envío, los hosts la aumentan progresivamente hasta recibir otro mensaje de disminución del tráfico desde el origen

TIPO (4)	CODIGO (0)	CHECKSUM
NO - UTILIZADO (debe ser cero)		
Encabezado IP + 8 primeros bytes de Datos IP		

Mensaje Redireccionar

Se asume que los Routers conocen rutas correctas. Los Host comienzan con información mínima de enrutamiento y aprenden nuevas rutas de los Routers. En caso de que un Host utilice una ruta no optima, el Router que lo detecta envía un mensaje ICMP Redireccionar solicitándole que actualice su tabla de enrutamiento IP.

TIPO (5)	CODIGO (0...3)	CHECKSUM
Dirección IP del Router		
Encabezado de IP + 8 primeros bytes de Datos IP		

Mensaje Tiempo Excedido

Debido a que los Routers solo deciden sobre el próximo "Salto" usando tablas locales, errores en esas tablas pueden generar "ciclos de enrutamiento" para algún destino. Esto provoca que los Datagramas sean descartados por vencimiento de su TTL. Siempre que un Router descarte un Datagrama ya

ICMP- Protocolo de Control de Mensajes de Internet
IP-Protocolo de Internet
TTL -Tiempo de Vida

sea por vencimiento de TTL o por vencimiento del Tiempo de Reensamblado, envía un mensaje de Tiempo Excedido a la fuente.

TIPO (11)	CODIGO (0 o 1)	CHECKSUM
NO – UTILIZADO (debe ser cero)		
Encabezado de IP + 8 primeros bytes de Datos IP		

CODIGO = 0: Descartado por vencimiento de TTL
CODIGO = 1: Descartado por vencimiento de Tiempo de Reensamblado.

Mensaje Problema de Parámetros

Cuando un Router o un Host encuentran un problema que no ha sido cubierto con los mensajes ICMP anteriores, envía este mensaje.

TIPO (12)	CODIGO (0 o 1)	CHECKSUM
Indicador	NO – Utilizado (debe ser cero)	
Encabezado de IP + 8 primeros bytes de Datos IP		

El campo indicador apunta al campo dentro del encabezado IP que generó el problema.

Mensaje Solicitud de Marca deTiempo y Respuesta de Marca de Tiempo

Una técnica sencilla provista por TCP/IP para sincronizar relojes emplea ICMP para obtener la hora de la otra maquina. Una maquina envía a otra una solicitud de Marca de tiempo, solicitándole que informe su valor actual para la hora del día. La otra maquina envía una respuesta de marca de tiempo con esa información.

TIPO (13 o 14)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Timestamp Origen		
Timestamp al Recibir		
Timestamp al Transmitir		

Mensaje Solicitud de Información y Respuesta de Información

Para aprender la mascara de subred utilizada por la red local, una maquina puede enviar un mensaje ICMP Solicitud Información de Mascara de

ICMP- Protocolo de Control de Mensajes de Internet
TTL -Tiempo de Vida
TCP/IP-Protocolo de Control de Transmisión/Protocolo de Internet

Subred a un Router y esperar su Respuesta. Si la maquina no conoce la dirección del Router, puede enviar este mensaje por difusión.

TIPO (17 o 18)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Mascara de Subred		

2.12.3 PRUEBAS DE ACCESIBILIDAD Y DESTINO (PING)

El comando PING es una orden específica de petición a un servidor o estación de trabajo para conocer el estado de su conexión.

También muestra determinadas estadísticas sobre el estado de la conexión establecida.

La forma de escribir este comando es:

PING <opción> <dirección IP>

Si en vez de una dirección IP indica un nombre de equipo, deberá encontrarse en el archivo HOSTS local o en el servidor DNS.

OPCIÓN	SIGNIFICADO
a	Resuelve las direcciones IP en nombres de equipos.
f	Envía un indicador para que las puertas de enlace no fragmenten el paquete.
i <número>	Espera respuesta del equipo el tiempo dado.
j <equipos>	Encamina los paquetes mediante la lista de equipos indicada (el número máximo de equipos que se pueden indicar es 9). Los equipos consecutivos pueden separarse por puertas de enlace intermedias.
k cequipos>	Encamina los paquetes mediante la lista de equipos indicada (el número máximo de equipos que se pueden indicar es 9). Los equipos consecutivos no pueden separarse por puertas de enlace intermedias.
l <número>	Pone el número de bytes de datos al indicado.
n <número>	Hace los reintentos de comunicación el número indicado de veces y se para.
r<número>	Registra el camino del paquete de salida y el paquete de vuelta en el apartado “Enrutamiento de registro” (<número> ha de estar entre 1 y 9).
s <número>	Indica la marca de hora para el número de saltos indicado.
T	Envía continuamente la señal al equipo, esperando cada vez la respuesta. Para salir de la orden, pulse [Ctrl] + [C].
v <servicio>	Manda la señal con el tipo de servicio indicado.
w <tiempo>	Especifica el intervalo de tiempo de espera en milisegundos.

Tabla 2.10 Opciones del comando PING

DNS-Sistema de Nombres de Dominio
IP-Protocolo de Internet

2.13 DETERMINACION DE RUTAS IP

Enrutar es el proceso de selección de un camino para el envío de paquetes. La computadora que hace esto es llamada Router.

En general se puede dividir el enrutamiento en Entrega Directa y Entrega Indirecta. La Entrega Directa es la transmisión de un Datagrama de una maquina a otra dentro de la misma red física. La Entrega Indirecta ocurre cuando el destino no esta en la red local, lo que obliga al Host a enviar el Datagrama a algún Router intermedio. Es necesario el uso de mascaras de subred para saber si el Host destino de un Datagrama esta o no dentro de la misma red física.

Encaminamiento con Salto al Siguiente.

La forma más común de enrutamiento requiere el uso de una Tabla de Enrutamiento IP, presente tanto en los Host como en los Routers. Estas tablas no pueden tener información sobre cada posible destino, de hecho, esto no es deseable. En ves de ello se aprovecha el esquema de direcionamiento IP para ocultar detalles acerca de los Host individuales, además, las tablas no contienen rutas completas, sino solo la dirección del siguiente paso en esa ruta.

En general una tabla de encaminamiento IP tiene pares (Destino, Router), donde destino es la dirección IP de un destino particular y Router la dirección del siguiente Router en el camino hacia destino. Nótese que Router debe ser accesible directamente desde la maquina actual.

Este tipo de encaminamiento trae varias consecuencias, llamada consecuencia directa de su naturaleza estática:

- Todo tráfico hacia una red particular toma el mismo camino, desaprovechando caminos alternativos y el tipo de tráfico.
- Solo el Router con conexión directa al destino sabe si este existe o esta activo.
- Es necesario que los Routers cooperen para hacer posible la comunicación bidireccional.

Manejo de Datagramas Entrantes.

Cuando un Datagrama llega a un Host, el software de red lo entrega a IP. IP verifica la dirección de destino y si esta concuerda con la de la maquina local, entonces acepta el Datagrama y lo entrega a las capas superiores. De no coincidir la dirección de destino, el Datagrama es descartado.

Por otra parte, un Router que reciba un Datagrama compara la dirección de destino con la suya propia. Si coinciden, el Datagrama pasa a las capas

superiores, sino, se le aplica el algoritmo de encaminamiento y se reenvía el Datagrama.

Direccionamiento sin Clase

Empleando Mascaras de subred, se lograba convertir una única red (generalmente una Clase B) en múltiples redes lógicas interconectadas y administradas por la organización propietaria. El problema se presenta cuando el crecimiento explosivo de las redes locales produce el fenómeno ROADS (Running Out of Address Space), que consiste simplemente en el agotamiento del espacio de direcciones útil, causado por la gran demanda de las direcciones Clase B, de las cuales solo hay 16.384, mientras que las Clases C permanecían sin asignar.

Para enfrentar este problema se desarrollo el esquema de Direcciones sin Clase, que consiste en asignar a una misma organización un bloque continuo de direcciones de Clase C. De esta manera, una organización que requiera conectar a Internet un numero moderado de Hosts (digamos 3.800) puede recibir un bloque de 16 redes continuas de Clase C (por ejemplo, de la red Clase C 199.40.72.0 a la 199.40.87.0), con lo cual dispone de 4.096 direcciones IP validas para administrar.

CIDR Enrutamiento Inter Dominio Sin Clases (Classless Inter Domain Routing)

El esquema de direcciones sin clase genera el problema de aumentar la información que debe incluirse en las tablas de enrutamiento. En el caso del ejemplo, se tendría que incluir 16 nuevas entradas en cada tabla de enrutamiento de cada Host y Router. CIDR resuelve el problema al incluir en las tablas información acerca del tamaño de los bloques y el numero de bloques, así, en las tablas de enrutamiento IP e tienen pares (Destino, Router), donde destino no es una dirección de Host o Red tradicional, sino que incluye información acerca del numero de redes que incluye el bloque (en nuestro ejemplo, 16) y el tamaño de cada una de esas redes (en el ejemplo, son Clases C, 256 direcciones cada una).

El Direccionamiento sin clase modifica la estructura de una dirección IP, de esta manera:

Prefijo de Red	Identificador de Host

Así, CIDR debe incluir en las tablas de enrutamiento cual es la primera red que compone el bloque, cuantos bits se emplean como Prefijo de Red y la mascara de subred que se emplea. En nuestro ejemplo, las tablas de enrutamiento IP contendrían esta información:
199.40.72.0/20 255.255.240.0

Refiriéndose a un bloque que se inicia con la red 199.40.72.0 y que tiene 20 bits en el prefijo de red. La mascara 255.255.240.0

(11111111.11111111.11110000.00000000) nos indica que se están usando 4 bits extra (los que se han resaltado) para identificar a las redes que componen al bloque. Nótese que cuatro bits permites agrupar precisamente 16 redes Clase C.

Un aspecto importante que hay que subrayar es que en ningún momento cambia el algoritmo básico de enrutamiento IP, lo que cambia es el contenido de las tablas. Además, las nuevas tablas contienen información resumida, por lo que buscar una dirección destino en la tabla se hace de otra manera, pero el algoritmo permanece inalterado.

El problema de buscar direcciones de destino en una tabla, consiste en que cualquier dirección cuya mascara de destino tenga menos bits, incluye a la que tiene mas bits. Es decir, una mascara de subred como 255.255.0.0 (11111111.11111111.00000000.00000000, de 16 bits de prefijo de red) incluye dentro de si a la mascaras de subred 255.255.128.0 (11111111.11111111.10000000.00000000, 17 bits de prefijo de red) y esta a su ves incluye a la mascara 255.255.192.0 (11111111.11111111.11000000.00000000) y en general, entre menos bits tiene el prefijo de red, mas direcciones Host abarca. Por esta razón cuando se explora la tabla de enrutamiento IP en busca de una dirección de destino, se hace una búsqueda que inicia con las mascaras de más bits y termina en la de menos bits. Es decir, se inicia con mascaras como 255.255.255.255 (todo en uno) y se continua con la 255.255.255.254 (31 unos y un cero) y así sucesivamente. Esto quiere decir que tendrían que hacerse 32 recorridos secuenciales a la tabla, lo cual es muy ineficiente en cuanto a tiempo, pues además de ser un procedimiento demorado se sabe ya que direcciones normales de Clase B (255.255.0.0) requieren 16 barridos a la tabla, además, hacen falta 32 barridos para notar que no hay una entrada en la tabla para esas direcciónes. Por esta razón se emplean otros métodos para hacer estas búsquedas en las tablas de enrutamiento IP. Un esquema muy popular emplea un Arbol Binario, en el cual cada bit representa una nueva rama en el árbol. Así, en nuestro ejemplo podrían dividirse las direcciones asignadas a la organización (4.096) en subredes de esta forma: dos subredes de 1.024 direcciones cada una, tres de 512 y dos de 256 direcciones. Así el árbol resultante será como lo muestra la siguiente imagen:

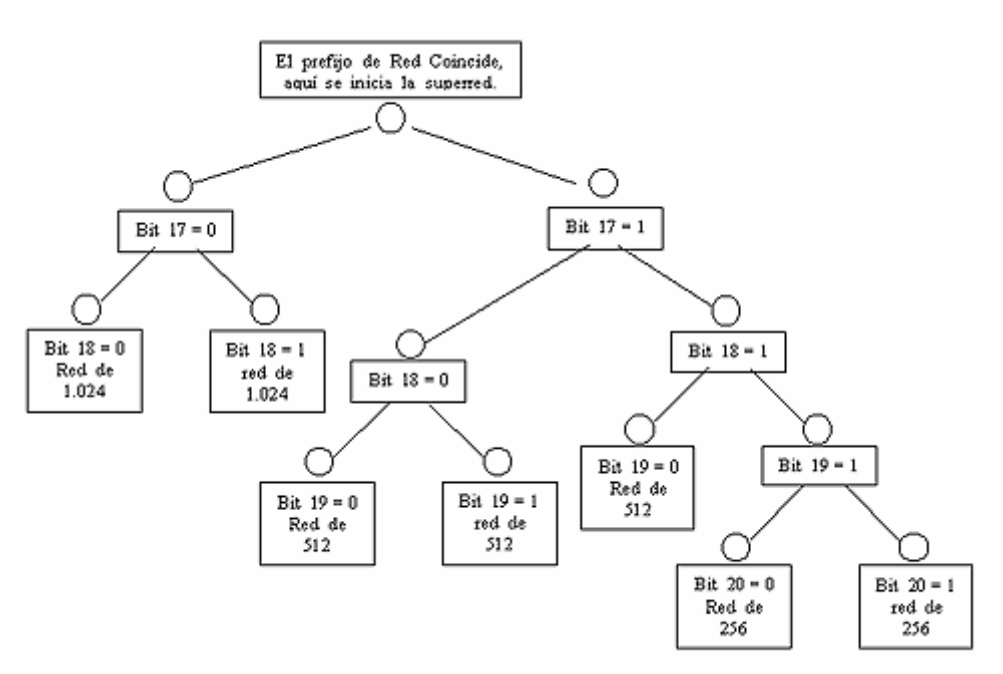


Figura 2.21 Esquema de árbol

CAPITULO III. DISEÑO DE LA RED

OBJETIVO PARTICULAR

Diseñar la infraestructura de una red con los parámetros necesarios para su funcionamiento.

3.1 DISEÑO DE LA RED LAN

La infraestructura de la red LAN para la Secundaria se basa en la interconexión de tres edificios (A, B y C donde encontramos la Dirección, servicios escolares, laboratorios, salones de clase y laboratorios de computo distribuidos en ellos) mediante los switches 3com (modelo 2226) en dos de éstos y un switch 2016 para el tercero, utilizando una conexión inalámbrica.

El núcleo de la red será un router cisco (modelo 1721), el cual realiza las funciones de control de flujo, tráfico y direccionamiento, las interfaces hacia este router desde los switches son a través de un access point para los edificios ya especificados. Siguiendo la conexión del router 1721 hacia internet tenemos una gateway proporcionada por nuestro ISP Prodigy Infinitum de TELMEX (512 Mb).

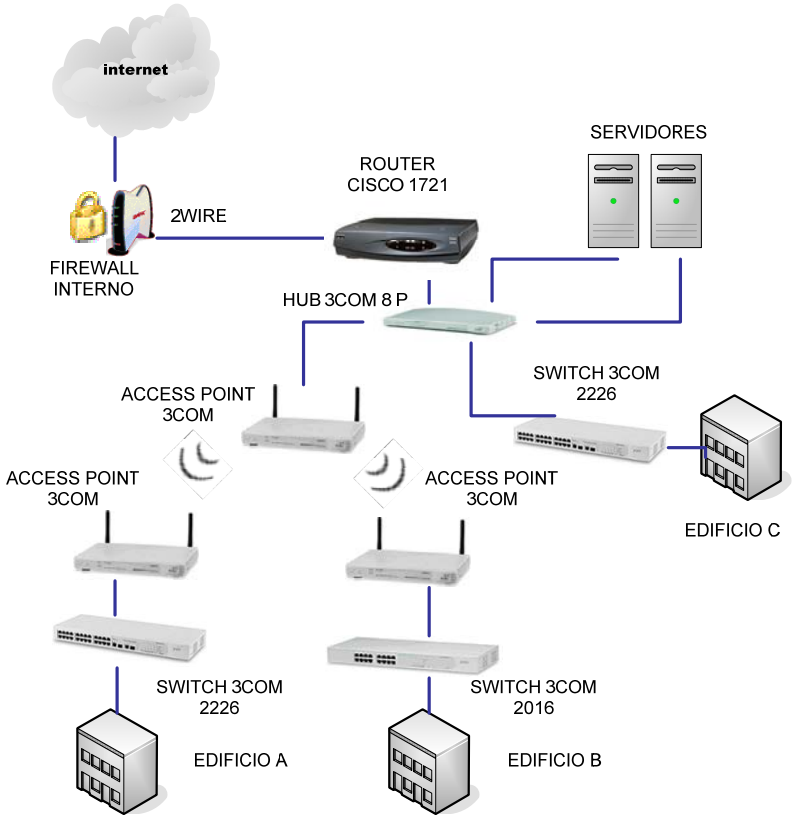


Figura 3.1 Conexión de la red

ISP-Proveedor de Servicios de Internet
LAN-Red de Area Local

El diseño de la red conlleva definir el número de subredes que se requieren, tomando en cuenta la proyección a futuro, lo que implica realizar un cálculo en el cual podamos visualizar en números los alcances de los equipos a conectar.

Este cálculo se hace a partir de la elección de tipo de red a conectar y la dirección IP elegida, además del número de subredes y los equipos terminales que se podrán conectar a ella.

En nuestro diseño hemos elegido la dirección IP de clase B, 160.26.0.0, con 6 subredes de proyección a futuro y cerca de 30 equipos por subred.

Una dirección IP tiene 32 bits, en una red de clase B se usan 16 para nombra la red y los siguientes 16 forman el nombre del host. Para poder nombrar las subredes se toman bits del tercer octeto, por lo que disminuye la cantidad de computadoras que se pueden conectar.

Para obtener las direcciones de las subredes nos basamos en la siguiente tabla, la cual simplifica el trabajo y nos permite construir de forma rápida las direcciones IP. Esta tabla es de doble entrada, en la fila superior encontramos el número de bits que se pueden tomar del tercer octeto para nombrar las direcciones de subred. La fila correspondiente a incrementos indica el valor decimal del bit dentro del octeto. La fila de la mascara de subred nos indica el valor decimal, el cual depende del número de bits que se toman del tercer octeto. Por ultimo tenemos la fila de número de subredes en la cual seleccionaremos el número que mas convenga para la construcción de nuestra red.

NUMERO DE BITS								
INCREMENTOS								
MASCARA DE SUBRED								
Nº DE SUBREDES								

La fila que corresponde al “Número de bits” se llena con la cantidad de bits que pueden ser tomados de un octeto para nombrar la subred, se enumeran de izquierda a derecha en forma consecutiva como se muestra en la tabla.

NUMERO DE BITS	1	2	3	4	5	6	7	8
INCREMENTOS								
MASCARA DE SUBRED								
Nº DE SUBREDES								

La siguiente fila llamada incrementos se llena con la formula 2^n en donde n toma los valores de 0 a 7 y los resultados se colocan de derecha a izquierda como a continuación se muestra.

NUMERO DE BITS	1	2	3	4	5	6	7	8
INCREMENTOS	128	64	32	16	8	4	2	1
MASCARA DE SUBRED								
Nº DE SUBREDES								

La fila que corresponde a las direcciones de mascara de subred se llena de derecha a izquierda tomado el valor de la celda inmediata superior que corresponde a la fila de incrementos mas el valor de la celda anterior en la línea de mascara de subred. Ejemplo para la columna que corresponde a 2 bits tenemos que se toma el valor de 64 más el anterior que es 128 el cual nos arroja un resultado de 192.

NUMERO DE BITS	1	2	3	4	5	6	7	8
INCREMENTOS	128	64	32	16	8	4	2	1
MASCARA DE SUBRED	128	192	224	240	248	252	254	255
Nº DE SUBREDES								

La fila que corresponde a número de subredes se llena de izquierda a derecha con la formula 2^n-2

NUMERO DE BITS	1	2	3	4	5	6	7	8
INCREMENTOS	128	64	32	16	8	4	2	1
MASCARA DE SUBRED	128	192	224	240	248	252	254	255
Nº DE SUBREDES	0	2	6	14	30	62	126	254

El resultado del calculo para la dirección IP 160.26.0.0 con 6 subredes, es una mascara de subred de 255.255.224.0 donde observamos que hay una diferencia con respecto a la mascara básica de clase B que es 255.255.0.0, esta mascara de subred también se puede denotar como 160.16.0.0/19 donde 19 nos indica el número de bits con los que nombramos la red. Con los 13 bits restantes de la dirección de IP podemos calcular el número de computadoras que se pueden conectar a cada segmento de la red.

2^n-2 donde n tomara el valor de 13

con lo que tenemos:

2^{13}-2= 16 384 computadoras.

Para conocer los nombres de las subredes tomamos en cuenta de la tabla la fila de incrementos donde se observa que para formar las 6 subredes tenemos un incremento de 32.

Dirección de red	Dirección de inicio	Dirección final	Dirección de difusión
160.26.32.0	160.26.32.1	160.26.63.254	160.26.63.255
160.26.64.0	160.26.64.1	160.26.95.254	160.26.95.255
160.26.96.0	160.26.96.1	160.26.127.254	160.26.127.255
160.26.128.0	160.26.128.1	160.26.159.254	160.26.159.255
160.26.160.0	160.26.160.1	160.26.191.254	160.26.191.255
160.26.192.0	160.26.192.1	160.26.223.254	160.26.223.255
160.26.224.0	160.26.224.1	160.26.255.254	160.26.254.255

Para concluir el cálculo decimos que la dirección IP de la red debe ser la misma que utiliza la interfaz ethernet del router (160.26.0.0), que es la misma del switch que se utiliza como central o conector multipuesto de los switches de las subredes y de los servidores.

La dirección IP de la interfaz serial (que nos conecta hacia internet) será la proporcionada por nuestro ISP.

Así tenemos:

Servidor de Archivos y directorio activo: 160.26.0.1
Servidor de Antivirus e Intranet: 160.26.0.2
Edificio A: 160.26.32.0
Edificio B: 160.26.64.0
Edificio B: 160.26.96.0

3.2 DESCRIPCION DEL LUGAR

La secundaria cuenta con tres edificios, el edificio a y b miden 9m de ancho por 29m de largo y 7.5 m de altura. El edificio c mide 9m de ancho por 35 m de largo y 7.5m de altura. La distancia entre el edificio b y el c es de 25 m, del edificio b al a hay 20 m y la separación del edificio a al c es de 35 m.

ISP-Proveedor de Servicios de Internet
IP-Protocolo de Internet

PERSPECTIVA SUPERIOR DE LA SECUNDARIA 425

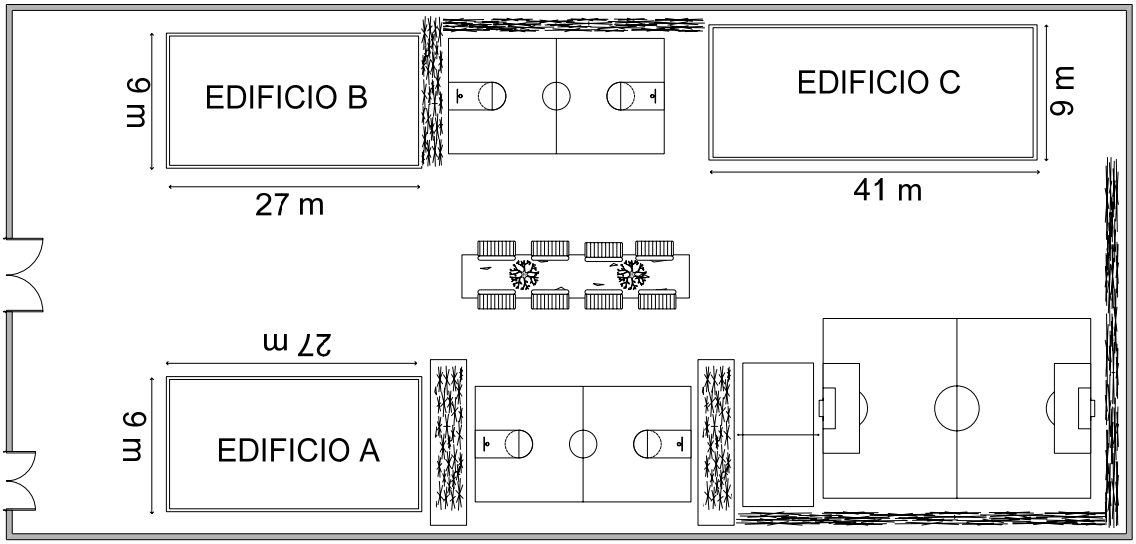


Figura 3.2 PERSPECTIVA SUPERIOR DEL LUGAR

3.2.1 EDIFICIO A

- En la planta baja encontramos la dirección, la supervisión, una bodega y los baños.
- En el primer piso encontramos el salón de orientación, el salón de cómputo 1, el audiovisual y el salón de primero 5.
- En el segundo piso tenemos el salón de primero 1, 2, 3, 4.

3.2.2 EDIFICIO B

- En la planta baja están los baños de los profesores, la cooperativa, el salón de maestros y el salón de segundo 1.
- En el primer piso están los salones de segundo 1, 2, 3, 4.
- En el segundo piso están los salones de tercero 1, 2, 3, 4.

Todos los salones de los edificio A y B miden 8m de ancho por 6m de largo y 2.5m de alto.

3.2.3 EDIFICIO C

- En la planta baja están los laboratorios 1 y 2 donde se imparten Física y química, además del salón de danza.
- En el primero piso el salón de dibujo técnico, el de corte y confección, así como el de estructuras metálicas.
- En el segundo piso el taller de electricidad, el salón de taquimecanografía y el de cómputo 2.

Los salones de este edificio miden 8m de ancho por 10m de largo y 2.5m de alto. Más 3m de bodega y 2m de escaleras.

Las áreas que nosotros identificamos como de oportunidad son los salones de clases, el audiovisual, orientación, dirección, supervisión, sala de maestros, laboratorios, electricidad y cómputo.

3.3 SERVIDORES Y NODOS

SWITCH EDIFICIO A			
GRUPO DE TRABAJO ”EDIFICIO A”			
NOMBRE DE USUARIO	IDENTIFICACIÓN	DIRECCIÓN IP	PUERTO
Director	Director_1	160.26.32.1	2
Secretaria 1	Secretaria1_2	160.26.32.2	3
Secretaria 2	Secretaria2_3	160.26.32.3	4
Secretaria 3	Secretaria3_4	160.26.32.4	5
Supervisión	Supervisión_5	160.26.32.5	6
Orientación	Orientación_6	160.26.32.6	7
Computo A	ComputoA_8	160.26.32.8	8
	HUB		9 SWITCH
ComputoA1	ComputoA1_9	160.26.32.9	1
ComputoA2	ComputoA2_10	160.26.32.10	2
ComputoA3	ComputoA3_11	160.26.32.11	3
ComputoA4	ComputoA4_12	160.26.32.12	4
ComputoA5	ComputoA5_13	160.26.32.13	5
ComputoA6	ComputoA6_14	160.26.32.14	6
ComputoA7	ComputoA7_15	160.26.32.15	7
ComputoA8	ComputoA8_16	160.26.32.16	8
ComputoA9	ComputoA9_17	160.26.32.17	9
ComputoA10	ComputoA10_18	160.26.32.18	10
ComputoA11	ComputoA11_19	160.26.32.19	11
ComputoA12	ComputoA12_20	160.26.32.20	12
ComputoA13	ComputoA13_21	160.26.32.21	13
Profesor A	Profesor A_22	160.26.32.22	14
SWITCH			
Audiovisual	Audiovisual_22	160.26.32.23	10
Salón primero 1	Sprimero1_23	160.26.32.24	11
Salón primero 2	Sprimero2_24	160.26.32.25	12
Salón primero 3	Sprimero3_25	160.26.32.26	13
Salón primero 4	Sprimero4_26	160.26.32.27	14
Salón primero 5	Sprimero5_27	160.26.32.28	15

Tabla 3.1 Direcciones de los equipos del edificio A

SWITCH EDIFICIO B			
GRUPO DE TRABAJO ”EDIFICIO B”			
NOMBRE DE USUARIO	IDENTIFICACIÓN	DIRECCIÓN IP	PUERTO
Sala de maestros	Salamaestros_1	160.26.64.1	2
Salón Segundo 1	Ssegundo1_2	160.26.64.2	3
Salón Segundo 2	Ssegundo2_3	160.26.64.3	4
Salón Segundo 3	Ssegundo3_4	160.26.64.4	5
Salón Segundo 4	Ssegundo4_5	160.26.64.5	6
Salón Segundo 5	Ssegundo5_6	160.26.64.6	7
Salón Tercero 1	Stercero1_7	160.26.64.7	8
Salón Tercero 2	Stercero2_8	160.26.64.8	9
Salón Tercero 3	Stercero3_9	160.26.64.9	10
Salón Tercero 4	Stercero4_10	160.26.64.10	11

Tabla 3.2 Direcciones de los equipos del edificio B

SWITCH EDIFICIO C			
GRUPO DE TRABAJO ”EDIFICIO C”			
NOMBRE DE USUARIO	IDENTIFICACIÓN	DIRECCIÓN IP	PUERTO
Laboratorio 1	Lab1_1	160.26.96.1	2
Laboratorio 2	Lab2_2	160.26.96.2	3
Electricidad	Electricidad_3	160.26.96.3	4
Cómputo C	ComputoC_4	160.26.96.4	5
Cómputo C1	ComputoC1_5	160.26.96.5	6
Cómputo C2	ComputoC2_6	160.26.96.6	7
Cómputo C3	ComputoC3_7	160.26.96.7	8
Cómputo C4	ComputoC4_8	160.26.96.8	9
Cómputo C5	ComputoC5_9	160.26.96.9	10
Cómputo C6	ComputoC6_10	160.26.96.10	11
Cómputo C7	ComputoC7_11	160.26.96.11	12
Cómputo C8	ComputoC8_12	160.26.96.12	13
Cómputo C9	ComputoC9_13	160.26.96.13	14
Cómputo C10	ComputoC10_14	160.26.96.14	15
Cómputo C11	ComputoC11_15	160.26.96.15	16
Cómputo C12	ComputoC12_16	160.26.96.16	17
Cómputo C13	ComputoC13_17	160.26.96.17	18
Cómputo C14	ComputoC14_18	160.26.96.18	19

Tabla 3.3 Direcciones de los equipos del edificio C

3.4 DISPOSITIVOS DE INTERCONEXION

Los dispositivos de interconexión que usaremos en nuestro diseño son:

Un router que va a controlar el flujo de información y tráfico de la red, switches que van a funcionar como controladores del flujo de la información en las subredes, además de ser el punto de interconexión entre el servidor y éstas. Una gateway que será la puerta de entrada y salida de los usuarios hacia internet. Los hubs serán dispositivos multipuerto para la conexión de varios equipos hacia un nodo central. Para proteger el acceso desde internet utilizaremos un programa firewall en cada computadora. Y para la conexión inalámbrica un access point.

Los equipos de interconexión generalmente se concentran en un solo lugar llamado site.

El SITE es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones.

El site además de contener el cableado necesario para la conexión de los equipos, también debe tener un estándar de colocación y protección de los mismos, a éste le denominamos RACK.

Rack (O Soporte Metálico)

Es una estructura de metal muy resistente, generalmente de forma cuadrada de aproximadamente 2 o 3 mts de alto por 1 mt de ancho, en donde se colocan los equipos regeneradores de señal y los Patch-Panels, estos son ajustados al Rack sobre sus orificios laterales mediante tornillos.

Los Patch Panels son estructuras metálicas con placas de circuitos que permiten la interconexión entre equipos. Un Patch-Panel posee una determinada cantidad de puertos (RJ-45End-Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas. En estos conectores es donde se ponchan las cerdas de los cables provenientes de las rosetas u otros Patch-Panels. La idea del Patch-Panel además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan los equipos de una red.

En la figura 3.3apreciamos el SITE de nuestra red ubicada en el edifio C, planta baja, donde tenemos el router, el hub multipuerto del router (debido a que éste solo cuenta con dos puertos ethernet), los servidores y el access point, así como la ventilación y el voltaje necesario.

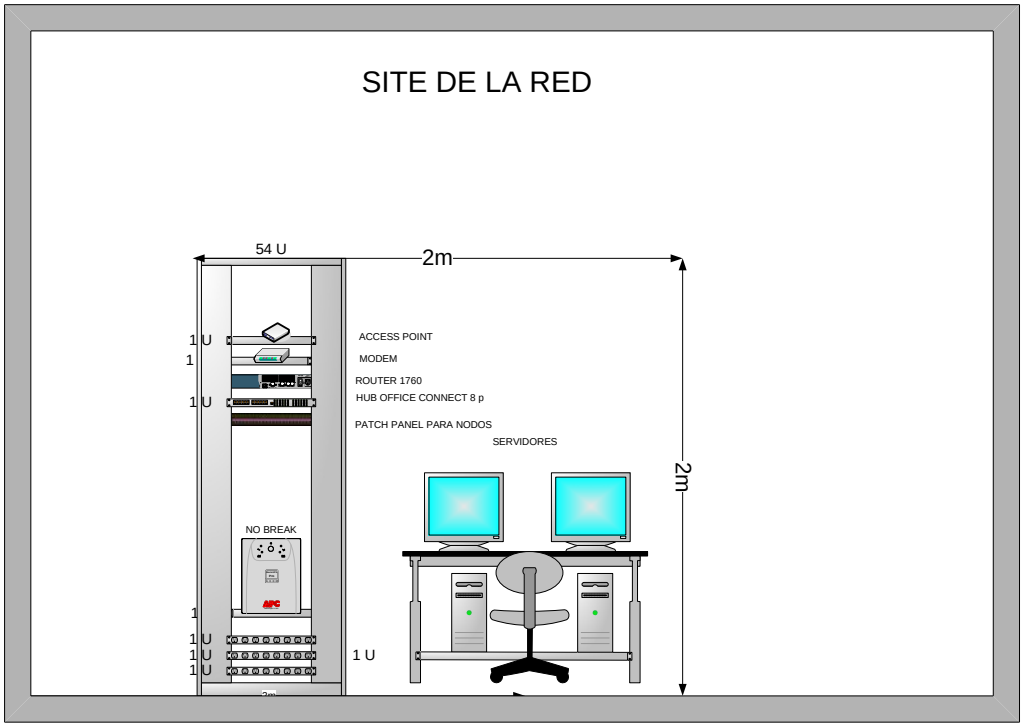


Figura 3.3 Site de la Escuela 425

3.4.1 ROUTER

La Serie de Routers de acceso Cisco 1700 es un producto modular para el acceso a Internet, Intranet y Extranet que esta diseñada para ofrecer soluciones integrales a pequeñas y medianas empresas, permitiendo una gran flexibilidad para adaptarse al continuo cambio de los requerimientos y al crecimiento de las tecnologías WAN.

La familia de Routers CISCO 1700 permiten integrar tarjetas de interfaz WAN soportando una gran variedad de tecnologías WAN (RDSI, xDSL, Serie Sínc/Asinc para líneas dedicadas, Frame Relay, X.25 y SMDS), ofrece las mejores características del sector, entre las que se incluyen una sólida calidad de servicio (QoS), seguridad en la red, cifrado y firewall, y ofrecen nuevos módulos de red que proporcionan redes de contenido y servicios de VPN mejorados que satisfacen las necesidades empresariales de las delegaciones y oficinas pequeñas. Estos routers ya pueden ofrecer también otros elementos integrados, como la telefonía por IP, el correo de voz y la operadora automatizada, lo que permite a los clientes instalar en su oficina un solo dispositivo para cubrir todas las necesidades de la empresa, lo que simplifica la gestión, el mantenimiento y el manejo, reduciendo así el coste total de propiedad.

IP-Protocolo de Internet
RDSI-Red Digital de Servicios Integrados
SMDS- Servicio de Conmutación de Datos de varios Megabits
VPN-Red Privada Virtual
WAN-Redes de Area Amplia
xDSL-Línea de Abonado Digital

Para nuestro diseño el router de la marca cisco serie 1721 fue el que más cubrió nuestras necesidades de operabilidad y disponibilidad de manejo de información.

Las características que ofrece éste router son:

- Amplia gama de opciones de acceso WAN, que incluyen la conexión DSL y ADSL.
- Un procesador RISC que soporta un alto funcionamiento de ruteo, encriptación y servicios de banda ancha.
- Administración del ancho de banda.
- Priorización de tráfico y calidad de servicio.
- Soporta el estándar IEEE 802.1Q (Ruteo de LAN´s virtuales).
- Acceso por VPN con firewall.
- Soporta los estándares de seguridad IPSec, and DES and 3DES.
- Detección automática de velocidad
- Negociación duplex automética
- Flexibilidad: Soporta protocolos de ruteo como, OSPF, EIGRP, HSRP y DHCP.
- Servicios: Incluye un Firewall dinámico, VPN, DSU (560 64 Kbps) e así como, administración remota y SMNP.
- Seguridad: Firewall Cisco IOS, VPN IPsec (DES6 and 3DES7) y encriptación para E1/T1 usando un módulo opcional de VPN.
- Voz: Telefonía sobre IP, soporta ADSL, además de trabajar con la infraestructura existente como los faxs.

DATOS TECNICOS

- Software: Cisco IOS
- Conectividad: Interfaces - 1 puerto Ethernet 10Base-T/100Base-TX - RJ-45, 1 puerto auxiliar RJ45 y 1puerto de consola RJ-4.
- Memoria: Flash Memory - 16 MB (instalada) / 64 MB (max), RAM de 32 MB (installada) / 96 MB (max)
- Stándares IEEE 802.3, IEEE 802.3U, IEEE 802.1Q
- Indicadores de estado de los puertos, actividad de enlace, energía.
- Modo de comunicación Full-duplex
- Protocolos de red, TCP/IP, IPX/SPX, AppleTalk, L2TP, PPP
- Tasa de transferencia de datos 100 Mbps
- Protocolos de conmutación, Frame Relay, ATM, Ethernet
- Protocolo de enlace de datos, Ethernet, Fast Ethernet

ADSL- Línea de Abonado Digital Asimétrica
ATM-Modo de Transferencia Asíncrono
DES- Estándar de Encriptación de Datos
DHCP- Protocolo de configuración dinámica de servidores
DSL- Línea de abonado digital
IEEE- Instituto de Ingenieros Eléctricos-Electrónicos
IP-Protocolo de Internet
LAN-Red de Area Local
OSPF- Primero la ruta libre más corta
PPP-Protocolo Punto a Punto
SNMP- Protocolo Simple de Administración de Redes
VPN-Red Privada Virtual
WAN -Redes de Area Amplia

Figura 3.4 Router 1721

Para nuestro diseño por el momento solo nos interesa el erutamiento, el control de tráfico y la seguridad.

CONFIGURACION

La configuración de un router se basa únicamente en activar las interfaces y configurar los parámetros de software para los protocolos encaminados y de encaminamiento.

Existen varias formas de configurar un router, una de ellas es utilizando directamente la consola o bien cargando un archivo de configuración ubicado en un servidor TFTP (protocolo trivial de transporte de archivos) dentro de la red, también se puede configurar a través de una estación de trabajo que ejecute un software especial para gestión de redes como por ejemplo el cisco Works, o bien trabajando en un programa basado en gráficos como lo es config maker de cisco.

Para realizar la configuración del router iniciaremos con la habilitación de la consola, la cual se llevará a cabo a través de la interfaz Ethernet-LPT figura 3.5, del router y la PC respectivamente.

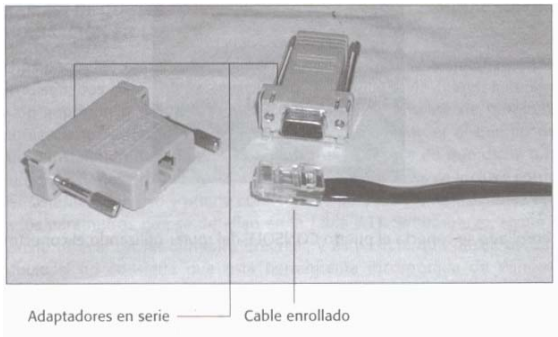


Figura 3.5 Cable de conexión Router-PC

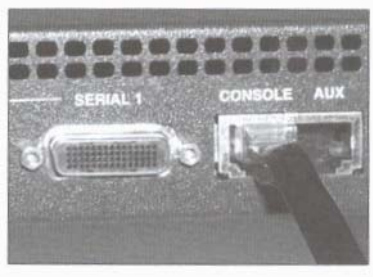


Figura 3.6 Puerto de la consola del router

Teniendo la interfaz entre el router y la PC se utiliza un software de emulación terminal como lo es Hyper Terminal.

Para ello necesitamos abrir el programa que viene integrado cualquier sistema operativo windows.

Ya abierta la ventana de descripción de la conexión nos disponemos a dar un nombre a ésta, en este caso utilizaremos el nombre de router2800 y se elegirá un icono para guardar el perfil de conexión, posteriormente al aceptar los datos anteriores aparece una ventana donde se describe los datos del contacto, en ella se selecciona como medio de conexión COM 1, con ello procede la configuración del puerto como se ilustra en las figuras 3.7 y 3.8.

Figura 3.7 Hyperterminal

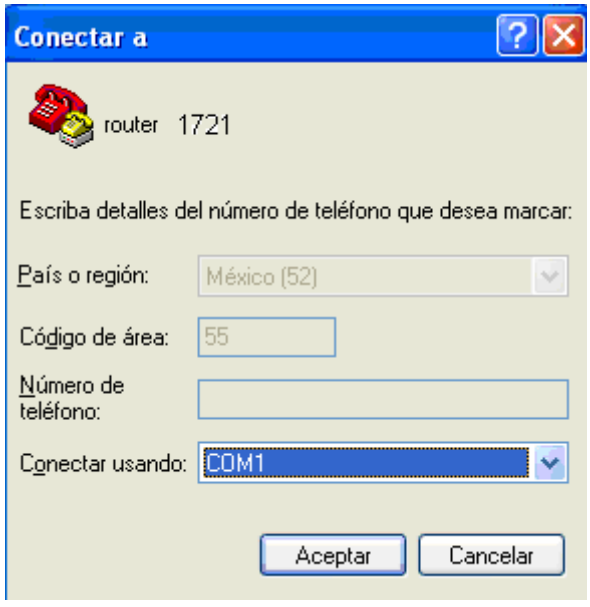


Figura 3.8 Configuración del puerto de Hyperterminal

Establecida la comunicación entre el router y la PC nos dispondremos a utilizar el programa de SETUP en el cual definiremos el nombre de host para el router, contraseñas y puertos.

PASO 1. Se seleccionará la opción yes cuando los mensajes de encendido hayan terminado.

Mensajes de encendido

From the Cisco IOS CLI, enter the **setup** command in privileged EXEC mode:
Router> **enable**
Password: **<password>**
Router# **setup**
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
If your router reloads and does not already have a configuration file, you are prompted to enter the setup command facility:

Would you like to enter the initial configuration dialog? [yes/no]:

PASO 2. Para continuar con la configuración de gestión básica seleccionaremos nuevamente Yes a la pregunta que nos aparece en la parte final de los siguientes mensajes

Mensajes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: **yes**

PASO 3. En este paso nos dispondremos a nombrar el host para el router, en pantalla observaremos lo siguiente:

Configuring global parameters:
Enter host name [Router]: **SECCUNDARIA1721**

PASO 4. Escribiremos la contraseña de activación la cual se encontrará cifrada por el sistema. Esta contraseña nos permite entrar al modo privilegiado para visualizar y cambiar la configuración del router.

The enable secret is a password used to protect access to

privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.

Enter enable secret: ***********

PASO 5. Escribimos una contraseña de activación diferente a la contraseña secreta de activación, esta contraseña no esta cifrada con lo cual puede verse al visualizarse la configuración. Con esta contraseña solo podemos tener acceso a los comandos no destructivos que permiten examinar algunos parámetros de la configuración sin hacer cambio alguno.

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: *******

PASO 6. En este paso se solicita al usuario introducir una contraseña de terminal virtual que evita un acceso no autenticado al router mediante puertos que no sean de la consola.

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: *******

PASO 7. Se configuran el router mediante preguntas de sistema de manera más adecuada para nuestra red.

Configure SNMP Network Management? [yes]:
Community string [public]:

Aparece en pantalla el resumen de las interfaces disponibles.

Nota. El número de interfaces depende del tipo de plataforma del router modular de cisco y de los módulos y tarjetas de interfaces instalados.

```
Current interface summary

Controller Timeslots D-Channel Configurable modes Status
T1 0/0     24        23        pri/channelized    Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Prol
FastEthernet0/0            unassigned      NO  unset  up                    up
FastEthernet0/1            unassigned      NO  unset  up                    dow
```

Figura 3.9 Interfaces del Router

PASO 8. Posteriormente se debe seleccionar una de las interfaces disponibles para conectar el router con la red de gestión

Enter interface name used to connect to the management network from the above interface summary: **fastethernet0/0**

PASO 9. Después de seleccionar la interfaz a utilizar responderemos a las solicitudes siguientes que representan las características de nuestra red.

Configuring interface FastEthernet0/0:
Use the 100 Base-TX (RJ-45) connector? [yes]: **yes**
Operate in full-duplex mode? [no]: **no**
Configure IP on this interface? [yes]: **yes**
IP address for this interface: **160.26.0.0**
Subnet mask for this interface [255.255.0.0] : **255.255.224.0**
Class B network is 160.26.0.0, 19 subnet bits; mask is /19

PASO 10. Se mostrará la siguiente información**.**

The following configuration command script was created:
hostname **SECUNDARIA1721**
enable secret 5 1D5P6$PYx41/lQIASK.HcSbfO5q1
enable password ***********
line vty 0 4
password *******
snmp-server community public
!
no ip routing
!
interface FastEthernet0/0
no shutdown
media-type 100BaseX
half-duplex
ip address 160.26.0.0 255.255.224.0
!
interface FastEthernet0/1
shutdown
no ip address
!
end

PASO 11. Responder a las solicitudes siguientes y se mostrará un pequeño menú con opciones del 0 al 2, en la cual con el número 2 se salvrá la coniguración.

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: **2**
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started! **RETURN**
The user prompt is displayed:
SECUNDARIA1760>

3.4.2 SWITCHES DE SUBRED

El **3Com® Baseline Switch 2226** es uno de los switches que vamos a utilizar, el cual nos ofrece un switching a velocidad de cable de Capa 2 suficiente para redes pequeñas a medianas que no requieren de capacidades de administración. El switch incluye 24 puertos de switching 10/100 y dos puertos con funcionalidad dual para conexiones Gigabit de cobre o fibra. Se puede escoger entre funcionamiento de alta velocidad 10/100/1000 para redes troncales o servidores fijos sobre cobre, o SFPs (Small Form-Factor Plug-in) con módulos de transceptores 1000BASE-LX ó -SX para conexiones a servidores o redes
troncales de fibra.

Las características que ofrece el dispositivo son:

- Avanzadas funciones de switching tales como el establecimiento de prioridades de tráfico IEEE 802.1p con filas de servicio en dos Clases de Servicio (CoS) aseguran que las aplicaciones en tiempo real, tales como audio y vídeo, lleven prioridad para funcionar de forma más efectiva, y permiten que el switch opere en ambientes de redes grandes.

- Los puertos de MDI/MDIX automático identifican y se adaptan al tipo de cable de Ethernet, eliminando los errores de cableado más comunes y simplificando su instalación. Los puertos con capacidades de auto-detección detectan y se ajustan a la velocidad del dispositivo conectado para optimizar el rendimiento de la red.

- El switch está diseñado para operar como switch solo o montado en un rack,

- LEDs fáciles de leer en el panel frontal proveen una sinopsis del estado e información sobre la red para simplificar los diagnósticos y resolver problemas.

- Su configuración pre-programada asegura que el switch funcione al sacarlo de su caja, sin necesidad de configuración o software de administración

DATOS TECNICOS

- **Puertos:** 24 puertos 10BASE-T/100BASE-TX y 2 puertos con funcionalidad dual para ranuras 10BASE-T/100BASE-TX/1000BASE-T ó SFP. Auto MDI/MDIX en todos los puertos.

- **Interfaz de medios:** RJ-45

- **Funciones de switching Ethernet :** Switching a velocidad de cable de Capa 2 sin bloqueo; re-envíos Store-and-forward; auto-negociación bi-direccional y de una sola vía; establecimiento de prioridades de tráfico 802.1p (prioridad de filas)
- Direcciones MAC que se soportan: 4,000

CONFIGURACION

El Switch Viene Pre-programado, no necesite configuración.

Figura 3.10 3Com® Baseline Switch 2226

El **Switch 3Com® SuperStack® 3 Baseline 10/100 de 16** puertos es un switch sin bloqueo y sin necesidad de administración diseñado para oficinas pequeñas a medianas.

Las características que ofrece el dispositivo son:

- Auto-negociación que ajusta la velocidad del puerto con la del dispositivo de comunicación. Cualquiera de los 16 puertos del switch pueden ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de banda, o Fast Ethernet 100BASE-TX para usuarios de potencia con conexiones de red más nuevas.

- El establecimiento integrado de prioridades IEEE 802.1p con dos filas de prioridades facilita la administración del tráfico en redes de empresas más grandes.
- Se puede instalar en rack o apilarse para maximizar el espacio disponible.

DATOS TECNICOS

- Puertos: 16 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración MDI/MDIX
- Interfaces para medios: RJ-45
- Funciones de switching Ethernet: Velocidad total sin bloqueo en todos los puertos Ethernet, auto-negociación y control de flujo bidireccional / semi-dúplex, establecimiento de prioridades de tráfico, 802.1p
- Direcciones MAC que se soportan: 4,000

IEEE- Instituto de Ingenieros Eléctricos-Electrónicos
MAC-Control de Acceso al Medio

CONFIGURACION

No se necesita configuración o software de administración

Figura 3.11 3Com® Baseline Switch 2016

3.4.3 HUB OFFICE CONNECT DUAL SPEED

El HUB que vamos a utilizar es un 3com OfficeConnect Dual Speed de 16 Puertos 10/100Mbps 'autosensing que detectan automáticamente la velocidad del dispositivo incorporado, para optimizar el rendimiento de la red. Es un dispositivo plug and play ya que necesita configuración, se adapta fácilmente a la red, puede transmitir de manera half-duplex o full-duplex. Los conectores son Rj45.

Figura 3.12 HUB

3.4.4 ACCESS POINT

El access point es un punto de acceso inalámbrico que nos permite ahorrar el cableado externo y ahorrar costos de instalación del mismo que además nos permite tener una red de Alta velocidad Alto Rendimiento para las Oficinas Más Pequeñas.

Con el 3Com OfficeConnect Wireless 11g Access Point, los usuarios pueden acceder a los recursos de red, a Internet, y al e-mail a velocidades de hasta 54 Mbps y a una distancia de hasta 100 metros que resulta ideal para pequeñas oficinas que trabajan con aplicaciones de audio, vídeo y multimedia exigentes. Al utilizar el estándar 802.11g el espectro radio de 2,4 GHz, el punto de acceso 11g es compatible hacia atrás con los productos 802.11b.

El 3Com OfficeConnect Wireless 11g Access Point soporta portátiles, PCs, y otros dispositivos de cliente inalámbricos 802.11g y 802.11b.

Características

El punto de acceso es asequible y fácil de instalar. Ofrece características de rendimiento y de resistencia a fallos que seleccionan automáticamente el mejor canal y velocidad de conexión, por lo que las conexiones permanecen claras y abiertas. Utiliza también encriptación avanzada WAP (Wireless

Protected Access, Acceso protegido a redes Inalámbricas) de 256 bits, así como encriptación WEP (Wireless Encryption Protocol, Protocolo de encriptación Inalámbrico) por clave compartida de 40/64 y 128 bits para ayudar a proteger los datos en la LAN inalámbrica.

La encriptación avanzada WAP de 256 bits ayuda a proporcionar una máxima seguridad inalámbrica, mientras que la encriptación WEP por clave compartida de 40/64 y 128 bits ayuda a proteger la privacidad de los clientes inalámbricos heredados.

Soportar velocidades de transmisión de hasta 54 Mbps para usuarios 802.11g, y hasta de 11 Mbps para usuarios 802.11b, a distancias de hasta 100 metros (328 pies)

La función Clear Channel Select (selección de canal libre) escoge automáticamente el canal de radio con el menor tráfico para unas conexiones sin problemas.

La función Dynamic Rate Shifting (cambio dinámico de velocidad) adapta automáticamente la mejor velocidad de conexión para responder a situaciones cambiantes físicas y de interferencia.

La administración basada en Web con una interfaz de navegador familiar le permite configurar y administrar dispositivos de red desde cualquier lugar

La certificación Wi-Fi ayuda a garantizar la interoperabilidad con productos de otros vendedores.

ESPECIFICACIONES

- Velocidades de Datos: 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11b: 11, 5,5, 2, 1 Mbps.
- Alcance Operativo : Máx. en interiores:100 metros (328 pies); Máx. en exteriores: 457 metros (1.499 pies)
- Protocolo de Acceso a Medios: CSMA/CA
- Puertos físicos: LAN: 1 puerto Ethernet 10/100 Mbps
- Seguridad: Encriptación WPA de 256 bits
- Encriptación WEP por clave compartida de 40/64 y 128 bits
- Indicadores LED: Potencia; estado de puertos de LAN - enlace, velocidad y actividad; estado de puertos de WLAN - enlace, actividad; Alerta/diagnósticos

Figura 3.13 ACCESS POINT

CONFIGURACION

Rápida y fácil instalación con el programa Access Point Discovery que identifica y configura automáticamente los dispositivos de red, normalmente sin configuración manual.

3.4.5 ROUTER-GATEWAY

El MODEM 2wire, es el Router que Telmex esta distribuyendo para su servicio de Infinitum inalámbrico, la principal ventaja de este dispositivo es que cuenta con 3 interfaces de acceso, inalámbrico (WiFi), Ethernet y USB, por lo cual es la opción mas sencilla de poder compartir nuestra conexión a internet a todas las pc´s de nuestra LAN.

Conexión del MODEM al router:

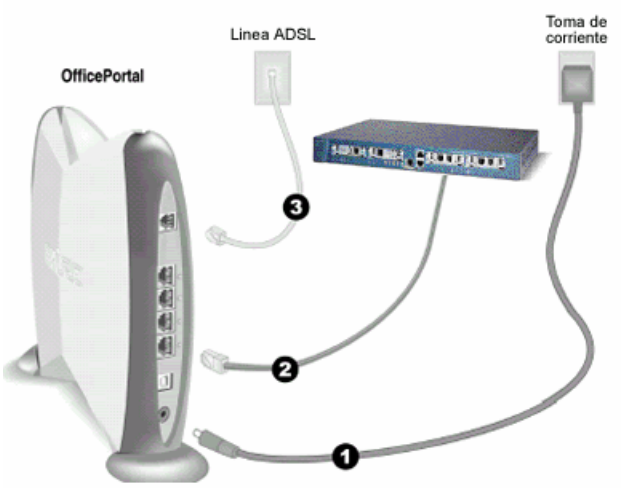


Figura 3.14 Conexión física de 2wire

Status de los Led's del 2wire:

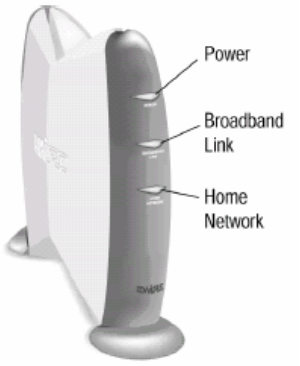


Figura 3.15 Estatus de los leds del MODEM

Led de Power	Estado
Apagada	El home Portal no esta recibiendo energia
Verde parpadeante	El Home Portal esta encendiendo

Verde Sólido	Encendido y en funcionamiento normal
Rojo Sólido	Error de sistema
Led de Broadband Link	Estado
Apagado	No hay señal ADSL el router no esta conectado a una línea ADSL
Naranja parpadeante	EL router esta intentando establecer una conexión ADSL
Rojo sólido	El router no ha conseguido sincronizar con la central (No hay conexión ADSL)
Naranja Sólido	El router ha establecido una conexión ADSL pero aun no hay conexión con el ISP (falta lanzar la conexión y validación)
Verde parpadeante	El router esta tratando de validar claves y establecer una conexión
Verde sólido	El router ha establecido la conexión
Led de Local Network	Estado
Apagado	No hay ninguna computadora conectada al router.
Encendido	Existe por lo menos una computadora conectada al router ya sea por tarjeta ethernet, wireless o USB

Tabla 3.4 Estatus de los leds del 2wire

CONFIGURACION

Para la configuración del MODEM 2wire debemos seguir los siguientes pasos:

El primero abrimos nuestro navegador (ya sea Internet Explorer, netscape navigator o como en nuestro caso Opera) y vamos a la dirección IP 172.16.0.1, con la cual nos mostrara la siguiente pagina, en ella seleccionaremos el menú de Broadband link tal y como se muestra en la figura.

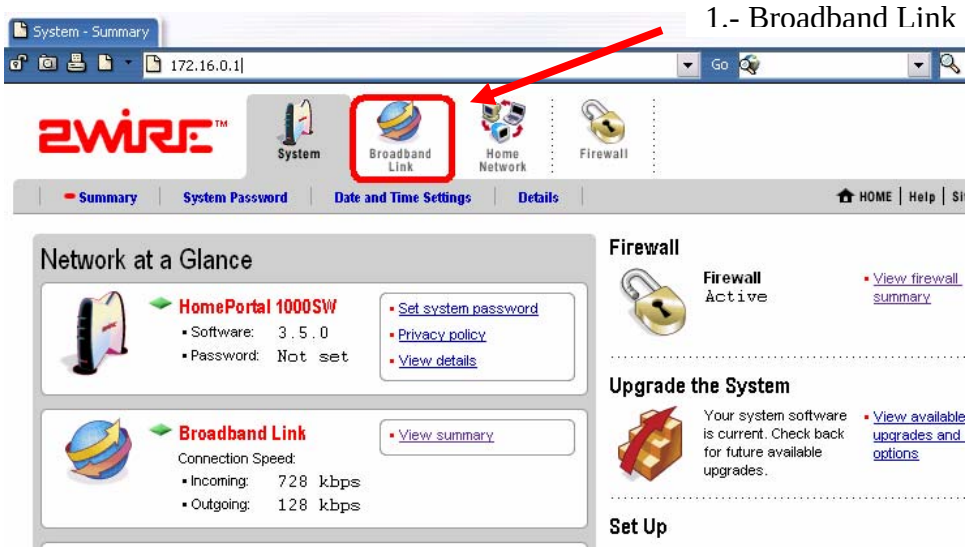


Figura 3.16 Pagina de configuración 2wire

ADSL- Línea de Abonado Digital Asimétrica
IP-Protocolo de Internet

El menú Broadband link nos mostrara la siguiente pantalla, en la cual seleccionaremos Advanced Settings

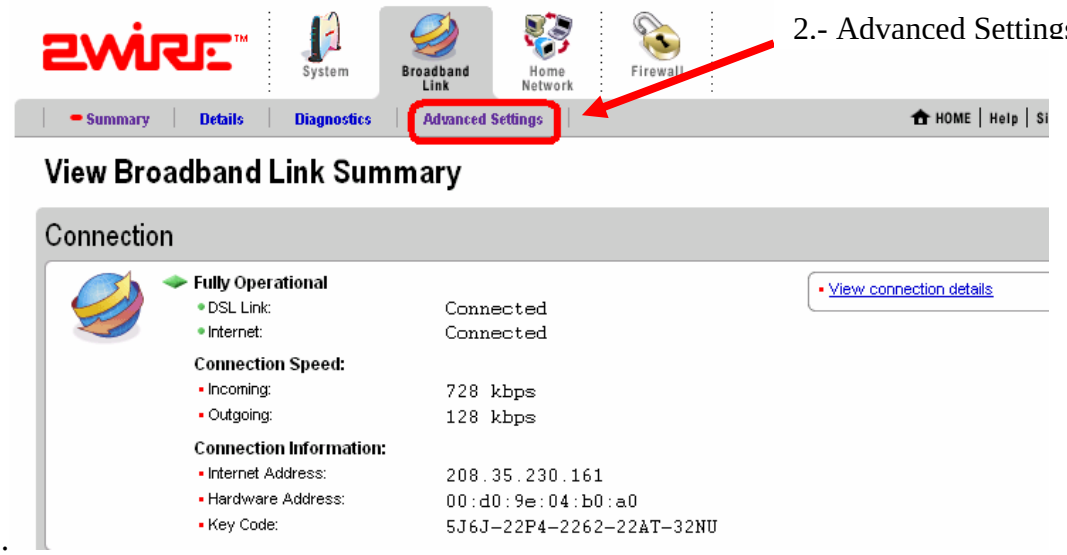
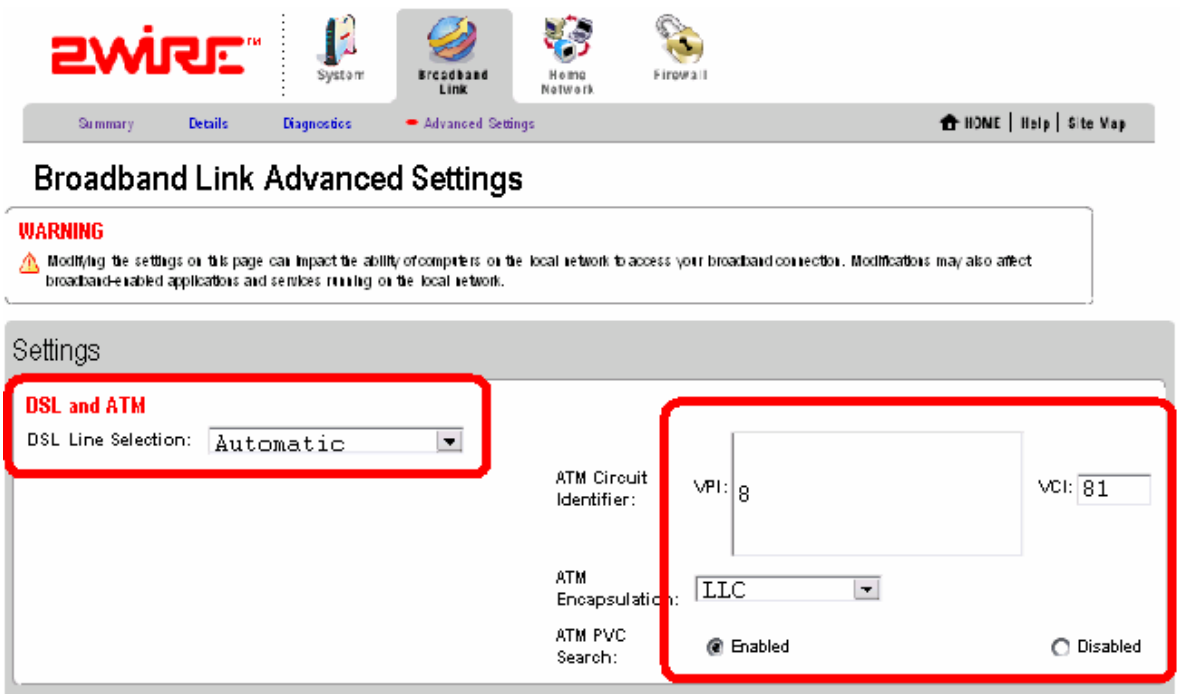


Figura 3.17 Pagina de configuración (Menu Broadband Link)

Dentro del menú de de Advanced Settings configuraremos la red del MODEM de la siguiente manera, los espacios en blanco deben de quedarse asi:



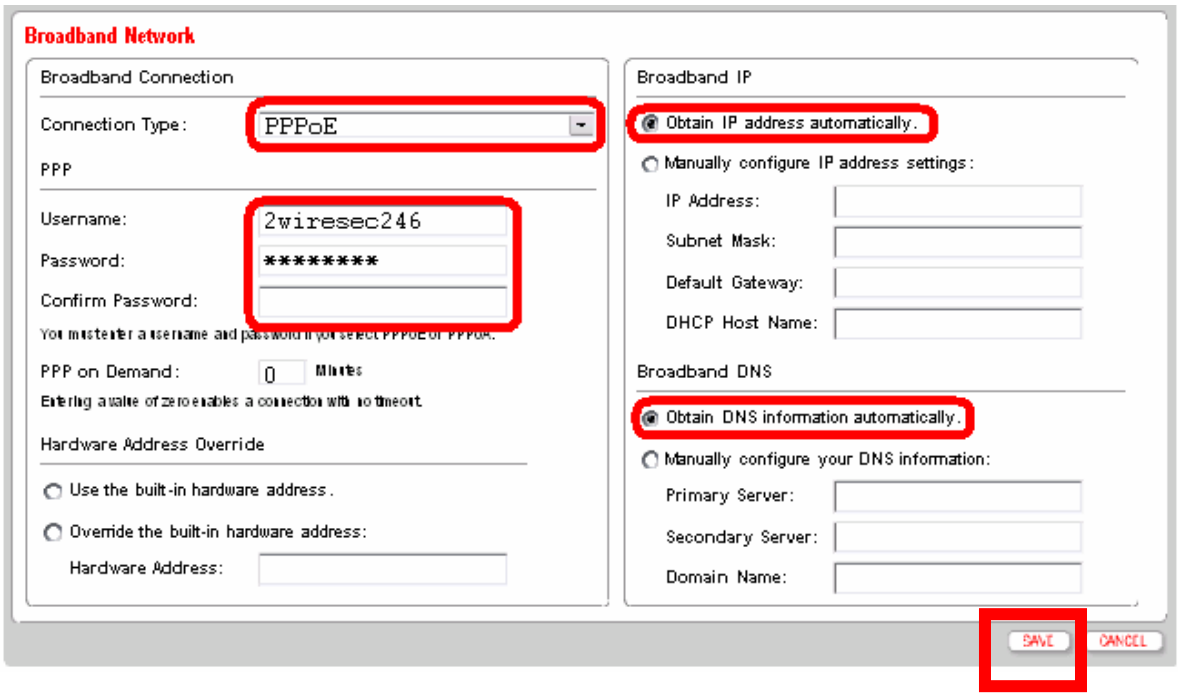


Figura 3.18 Pagina de configuración (Broadband Link / Advanced settings)

Después solo damos clic en Save y nuestra conexión esta lista.

La última pantalla que nos mostrara la página de configuración es la siguiente, en la cual tenemos que poner especial cuidado en la información de Connetion ya que esta nos dirá si el MODEM se encuentra totalmente conectado.

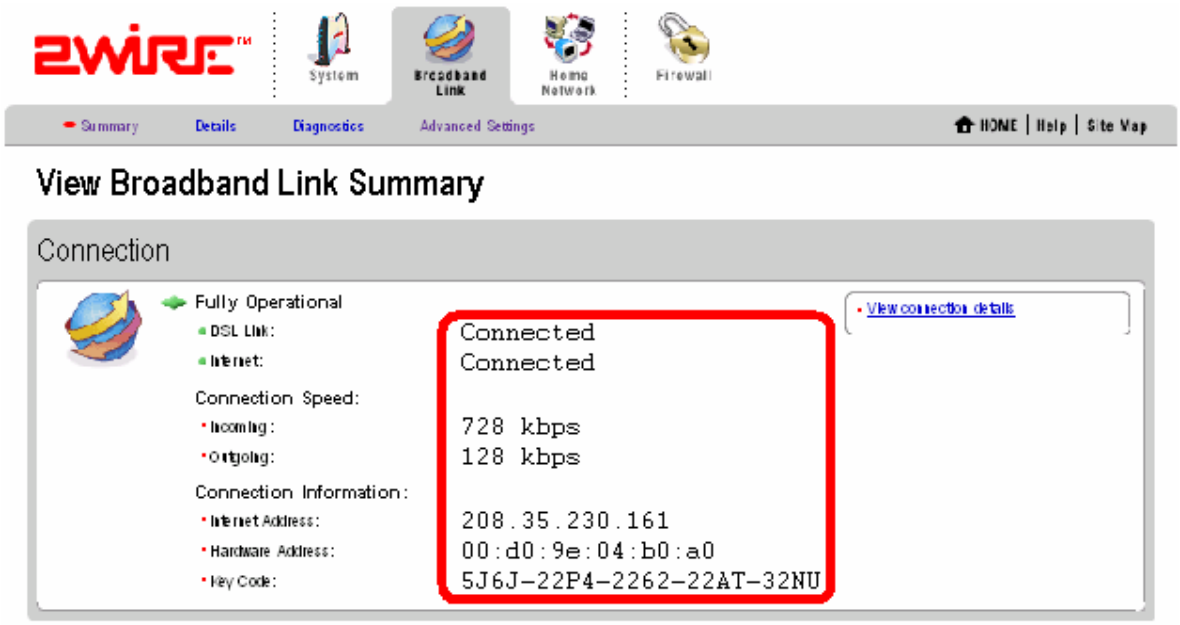


Figura 3.19 Pagina de configuración 2wire (Estado de la conexión)

CONFIGURACION DE FIREWALL

En la pagina principal del 2wire seleccionamos el menú de Firewall, en la cual seleccionaremos las aplicaciones que tienen acceso a Internet y cuales no.

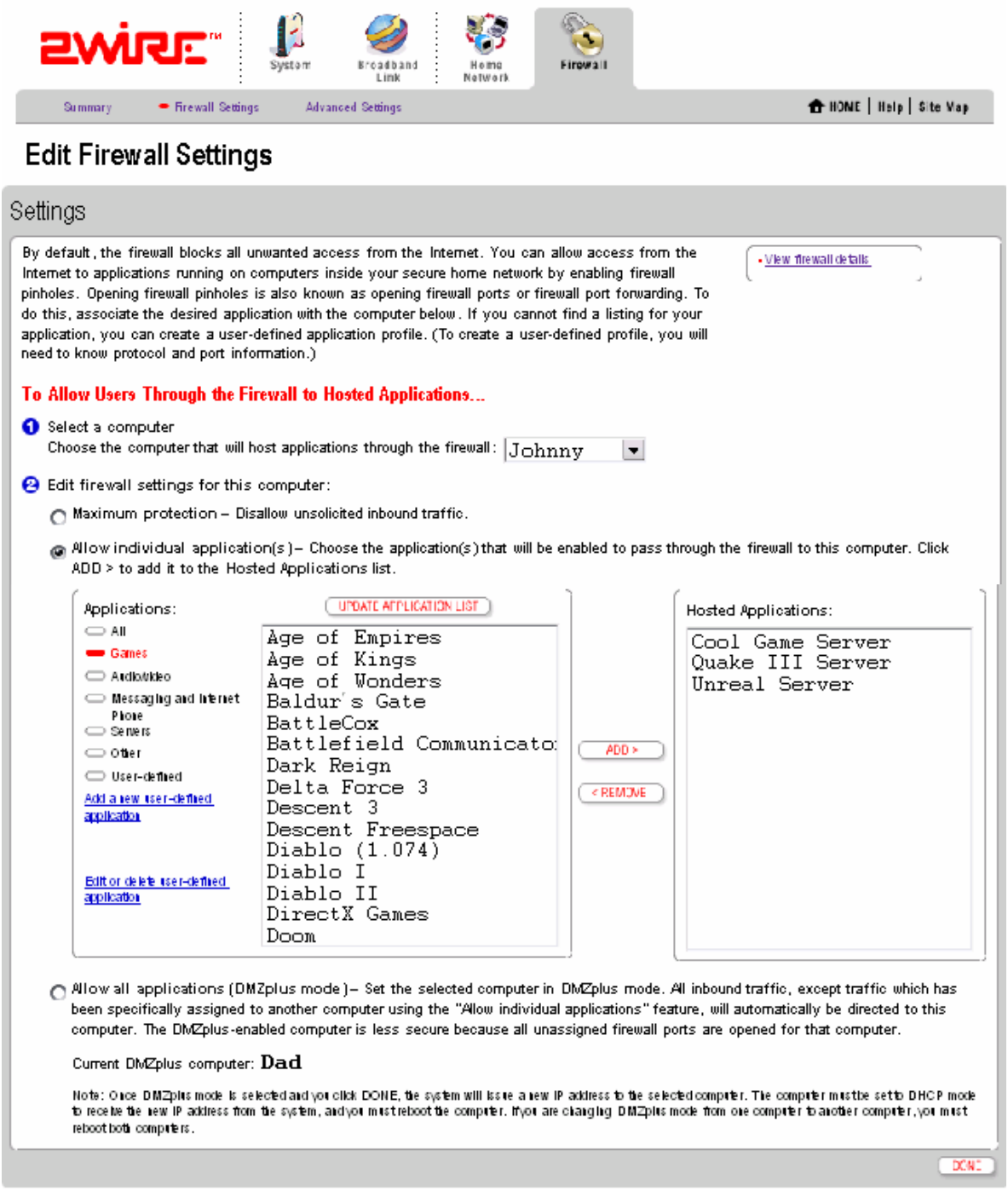


Figura 3.20 Pagina de configuración 2wire (Firewall)

Este impedirá la conexión de un equipo externo a nuestra red hacia una PC hospedada en la red de la secundaria.

3.5 MEDIOS DE TRANSMISION

Los parámetros necesarios para obtener un cable de conexión tienen su propia especificación fijados por la norma hasta una frecuencia de 100 Mhz en todos sus pares.

Los parámetros eléctricos que se miden son:

- Atenuación en función de la frecuencia (db)
- Impedancia característica del cable (Ohms)
- Acoplamiento del punto mas cercano (NEXT- db)
- Relación entre Atenuación y Crostalk (ACR- db)
- Capacitancia (pf/m)
- Resistencia en DC (Ohms/m)
- Velocidad de propagación nominal (% en relación C)

Distancias permitidas:

- El total de distancia especificado por norma es de 99 metros.
- El límite para el cableado fijo es 90 m.
- El limite para los parches de cable en el panel de parcheo es 6 m. y el limite para los parches de cable en la conexión del terminal es de 3 m.

3.5.1 UTP

El cable de par trenzado sin apantallar UTP esta formado de 4 pares (8 hilos en total), que no dispone de protección contra las interferencias externas, por lo que solo es adecuado para entornos relativamente libres de perturbaciones.

Los pares están numerados (de 1 a 4), y tienen colores estándar, aunque los fabricantes pueden elegir la disposición particular en la conexión, sin embargo, la norma TIA/EIA 568-A específica dos modalidades, la T568A y T568B, de las cuales la T568B es probablemente la más extendida.

T568A			
NUMERO DE PIN	COLOR 1ª OPCION		DESIGNACION
PAR 1	4	AZUL	R1
	5	BLANCO/AZUL	T1
PAR 2	3	BLANCO/NARANJA	T2
	6	NARANJA	R2
PAR 3	1	BLANCO/VERDE	T3
	2	VERDE	R3
PAR 4	7	BLANCO/CAFÉ	T4
	8	CAFE	R4

Tabla 3.5 Asignación de pines T568A

T568B			
NUMERO DE PIN	COLOR 1ª OPCION		DESIGNACION
PAR 1	4	AZUL	R1
	5	BLANCO/AZUL	T1
PAR 2	1	BLANCO/NARANJA	T2
	2	NARANJA	R2
PAR 3	3	BLANCO/VERDE	T3
	6	VERDE	R3
PAR 4	7	BLANCO/CAFÉ	T4
	8	CAFE	R4

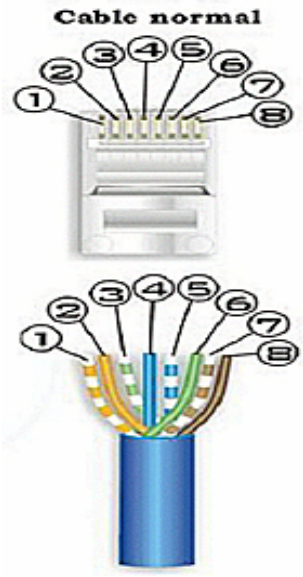


Tabla 3.6 Asignación de pines T568B

Las designaciones T y R significan Tip y Ring, denominaciones que vienen de los primeros tiempos del teléfono. En la actualidad se refieren a los cables positivos (Tip) y negativos (Ring) de cada par.

Los cables de par trenzado son más económicos que los coaxiales y admiten más velocidad de transmisión, sin embargo la señal se atenúa antes que en los coaxiales, por lo que deben instalarse repetidores y concentradores (hubs). Para garantizar un mínimo de fiabilidad los cables UTP no deben estar destrenzados ni aún en distancias cortas. Por la misma razón, los cables de conductores paralelos (cable plano) no deben ser utilizados en redes.

En las nuevas instalaciones UTP deben utilizarse todos los pares, porque a diferencia de Ethernet y Token-Ring, que utilizan un par para transmitir y otro para recibir, algunos de los nuevos protocolos transmiten sobre múltiples pares.

En las conexiones 10 Base-T solo se utilizan los pares 2 y 3, pero es recomendable conectar los 4 pares, los cuales pueden servir para una posterior actualización a 100Base-T4, además, a pesar que las conexiones con menos cables trabajan bien, es mas estable mantener todos los cables conectados. No obstante, debe verificarse la integridad de la conexión en el lado del hub y en el lado de la tarjeta Ethernet.

El conector RJ-45 (ISO 8877) es el macho; la hembra, denominada Jack, se monta en la NIC ("Network Interface Card") del DTE, en una toma de pared ("Patch panels") que se montan sobre un bastidor ("Rack").

El tipo de cableado de UTP puede ser recto o cruzado dependiendo de las necesidades de la conexión. Este cableado asegura en ambos casos que las líneas de Transmisión (Tx) de un aparato se comunican con las líneas de Recepción (Rx) del otro aparato.

DTE-Equipo Terminal de Datos
UTP-Cable de par trenzado Sin Apantallar

Cable recto Pin a pin

Son los cables que conectan un concentrador con un nodo de red (Hub⇔Nodo); los hilos están ponchados para a par al RJ-45 en ambos extremos, es decir, los pares de colores están conectados en las mismas posiciones en ambos extremos. La razón es que el hub realiza internamente el cruce de señal.

Cable cruzado cross-over

Son cables que conectan dos concentradores o dos transceptores entre si, o incluso dos tarjetas (Nodo⇔Nodo), cuya distancia no supere los 10 m. El par 2 (pines 1 y 2) y el par 3 (pines 3 y 6) están cruzados Como regla general, el cable cruzado se utiliza para conectar elementos del mismo tipo o similares, por ejemplo, dos DTE conectado a una LAN, dos concentradores (Hubs), dos conmutadores (Switchs) o dos enrutadores (Routers).

Se deben tener muy claros los siguientes conceptos respecto al uso de uno y otro tipo de cable:

El cable cruzado ("cross-over") solo debe ser utilizado cuando PC es conectado directamente a otro PC, sin que exista ningún elemento adicional (hubs, routers, etc). En realidad, puesto que la mayoría de las redes utilizan al menos un concentrador, el cable cruzado solo se utiliza en circunstancias excepcionales, por ejemplo realización de pruebas cuando se desea comprender la complejidad de la red y se conectan dos PCs directamente.

Los dispositivos Ethernet no pueden detectar un cable cruzado utilizado de forma inadecuada; este tipo de cables encienden los LEDs de actividad en los adaptadores, concentradores y Switches. La única forma de saber el tipo de cable (cruzado o recto) es mediante un multimetro.

Para las tarjetas de 10 Mb en el conector 1 se utiliza la configuración T568A y en el conector 2 la configuración T568B, cruzando solo dos pares.

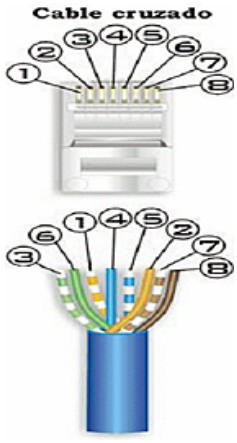


Figura 3.21 Cable cruzado

Para las tarjetas 10/100 la configuración es la siguiente:

DTE-Equipo Terminal de Datos
LAN-Red de Area Local

Conector1	Color del cable	Conector2
PIN 1	BLANCO/NARANJA	PIN 3
PIN 2	NARANJA	PIN 6
PIN 3	BLANCO/VERDE	PIN 1
PIN 4	AZUL	PIN 7
PIN 5	BLANCO/AZUL	PIN 8
PIN 6	VERDE	PIN 2
PIN 7	BLANCO/MARRÓN	PIN 4
PIN 8	MARRÓN	PIN 5

Tabla 3.7 Asignación de Pines crossover

3.5.2 CABLEADO ESTRUCTURADO

Es un sistema de cableado capaz de integrar tanto los servicios de voz, datos y vídeo, como los sistemas de control y automatización de un edificio bajo una plataforma estandarizada y abierta que nos ayuda a controlar los procesos y sistemas de administración de un edificio.

Backbone

Es la corrida principal del cable que parte del punto principal de distribución y se interconecta con todas las salidas de telecomunicaciones. El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical en trepisos en edificios de varios pisos. Además, incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. Tiene una topología de estrella jerárquica aunque también suelen utilizarse las topologías de bus o de anillo, tiene como máximo dos niveles de jerarquía, para evitar degradación de la señal.

El cableado estructurado se hará a través de canaletas a nivel de piso como se aprecia en la figura 3.22 para el edificio A, 3.23 para el edificio B y 3.24 para el edificio C. Así también se puede apreciar la ubicación de los nodos (rosetas) y la ruta que seguirá el cable desde el switch a cada nodo, conociendo así la longitud de cable necesaria para conectar los equipos.

CABLEADO DEL EDIFICIO A

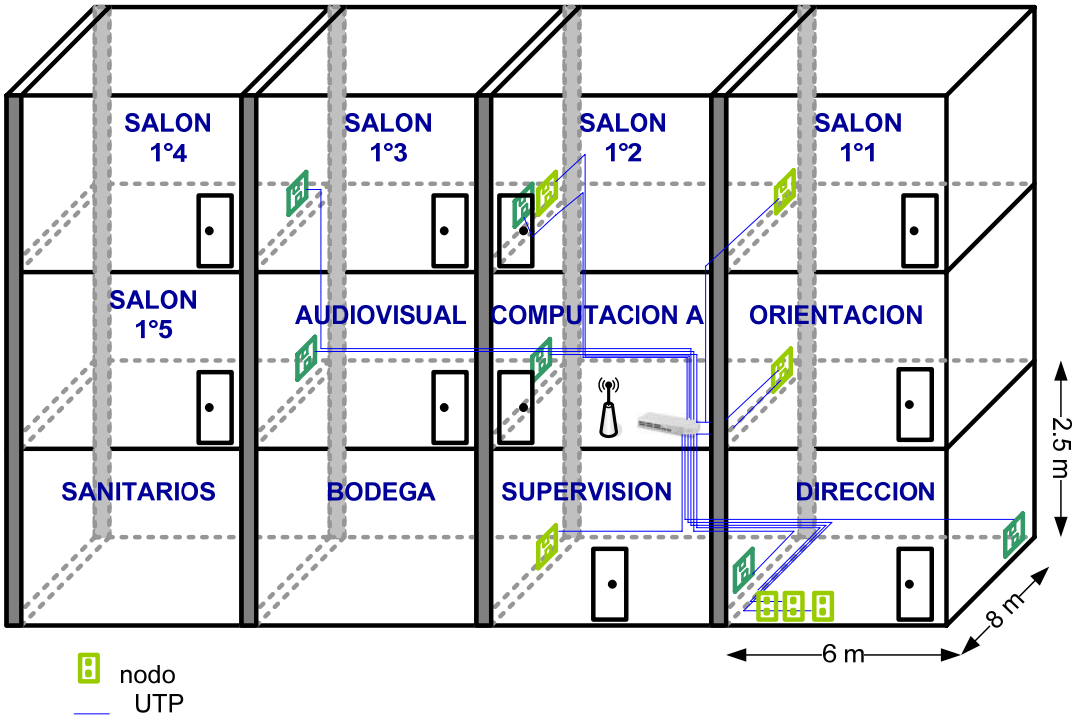


Figura 3.22 Cableado Estructurado Para El Edificio A

CABLEADO DEL EDIFICIO B

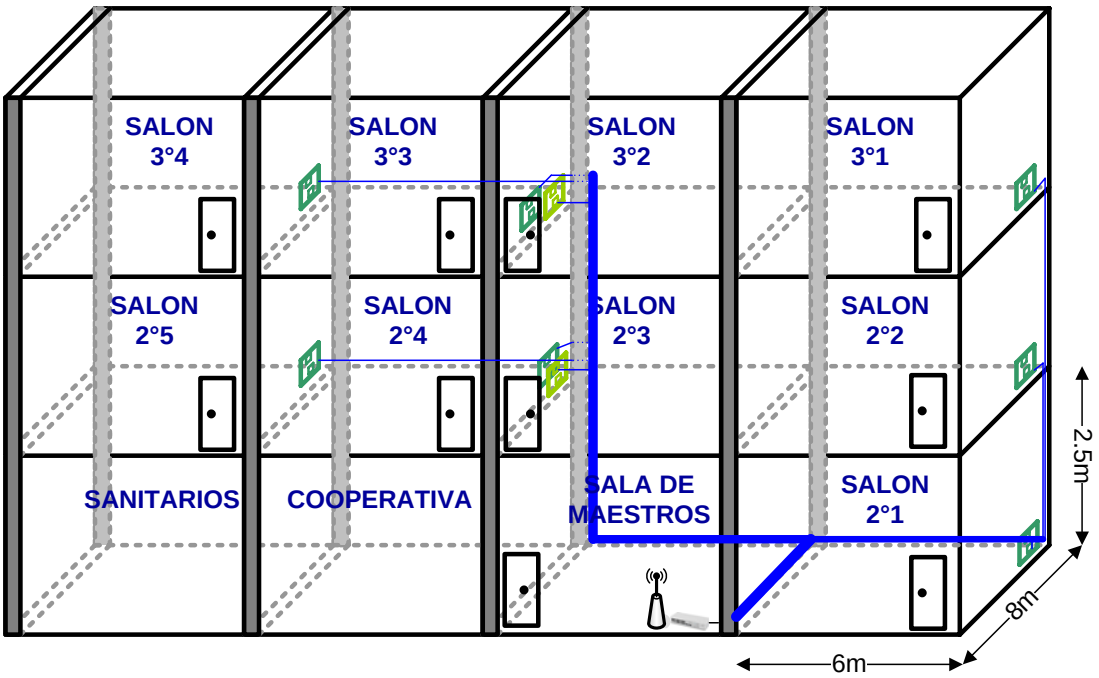


Figura 3.23 Cableado Estructurado Para El Edificio C

CABLEADO DEL EDIFICIO C

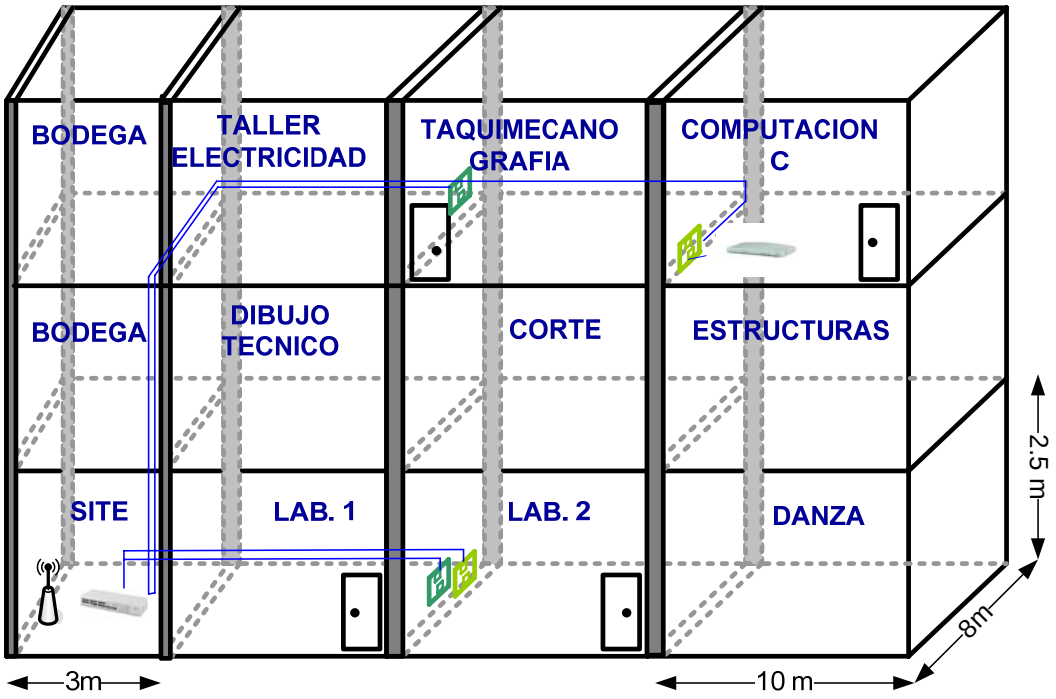


Figura 3.24 Cableado Estructurado Para El Edificio B

La longitud total de cable por edificio se muestra en las siguientes tablas.

UBICACIÓN	COMPUTADORA	LONGITUD DE CABLE (mts)
Salon De Computacion Edificio A	PROFESOR A	5
Salon De Computacion Edificio A	ComputoA1	6
Salon De Computacion Edificio A	ComputoA2	7
Salon De Computacion Edificio A	ComputoA3	8
Salon De Computacion Edificio A	ComputoA4	9
Salon De Computacion Edificio A	ComputoA5	11
Salon De Computacion Edificio A	ComputoA6	12
Salon De Computacion Edificio A	ComputoA7	13
Salon De Computacion Edificio A	ComputoA8	14
Salon De Computacion Edificio A	ComputoA9	16
Salon De Computacion Edificio A	ComputoA10	17
Salon De Computacion Edificio A	ComputoA11	18
Salon De Computacion Edificio A	ComputoA12	19
Salon De Computacion Edificio A	ComputoA13	20
SALON DE ORIENTACION	Orientación	13
SALON DE AUDIOVISIAL	Audiovisual	18
SALON 1°5	Sprimero5	26
SALON 1°4	Sprimero4	29
SALON 1°3	Sprimero3	19
SALON 1°2	Sprimero2	18.5
SALON 1°1	Sprimero1	12.5
SUPERVISION	Supervision	12
Secretaria 1	Secretaria1	13
Secretaria 2	Secretaria2	13.5
Secretaria 3	Secretaria 3	14

TOTAL	**363.5**

Tabla 3.8 Longitud de cable para el edificio A

UBICACIÓN	COMPUTADORA	LONGITUD DE CABLE (mts)
LABORATORIO 1	Lab1	17
LABORATORIO 2	Lab2	19.5
ELECTRICIDAD	Electricidad	16
COMPUTACION C	ComputoC	32
Salón De Computación Edificio C	ComputoC1	6
Salón De Computación Edificio C	ComputoC2	7
Salón De Computación Edificio C	ComputoC3	8
Salón De Computación Edificio C	ComputoC4	9
Salón De Computación Edificio C	ComputoC5	11
Salón De Computación Edificio C	ComputoC6	12
Salón De Computación Edificio C	ComputoC7	13
Salón De Computación Edificio C	ComputoC8	14
Salón De Computación Edificio C	ComputoC9	16
Salón De Computación Edificio C	ComputoC10	17
Salón De Computación Edificio C	ComputoC11	18
Salón De Computación Edificio C	ComputoC12	19
Salón De Computación Edificio C	ComputoC13	20
	TOTAL	**254.5**

Tabla 3.9 Longitud de cable para el edificio C

UBICACIÓN	COMPUTADORA	LONGITUD DE CABLE (mts)
Sala de maestros	Salamaestros_1	2
Salón Segundo 1	Ssegundo1_2	16.5
Salón Segundo 2	Ssegundo2_3	19.5
Salón Segundo 3	Ssegundo3_4	22.5
Salón Segundo 4	Ssegundo4_5	18.5
Salón Segundo 5	Ssegundo5_6	19
Salón Tercero 1	Stercero1_7	25.5
Salón Tercero 2	Stercero2_8	21
Salón Tercero 3	Stercero3_9	21.5
Salón Tercero 4	Stercero4_10	28
	TOTAL	**194**

Tabla 3.10 Longitud de cable para el edificio B

Distribución de nodos del salón de computación edificio A

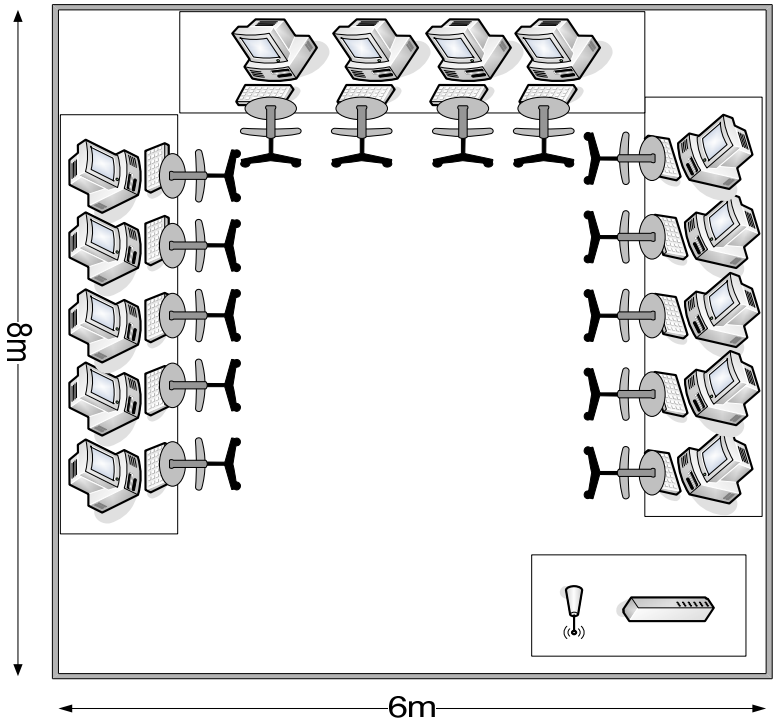


Figura 3.25 Salón de Computación A

Distribución de nodos del salón de computación edificio B

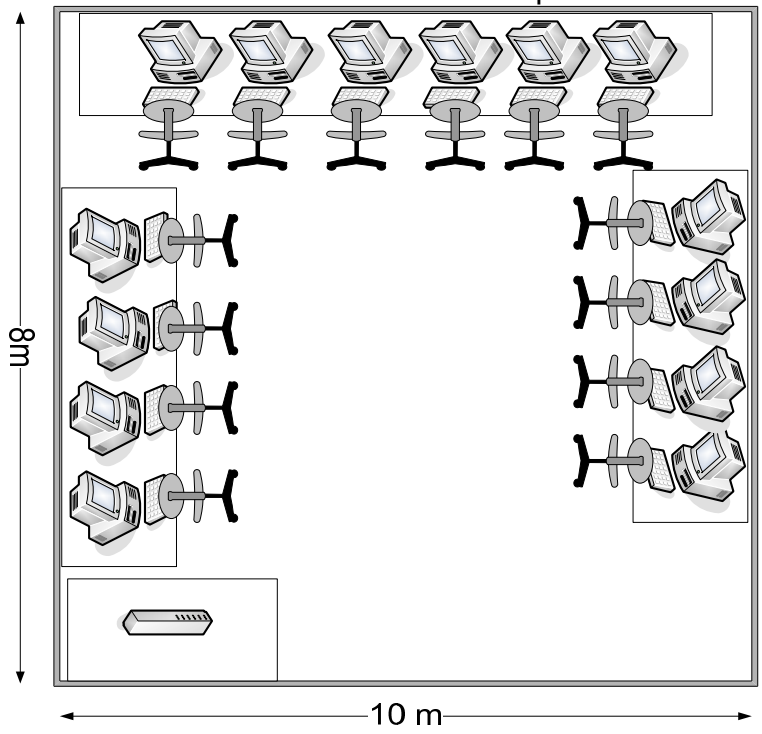


Figura 3.26 Salón de Computación C

3.6 TARJETAS DE RED

Las tarjetas de red que instalaremos en los equipos de cómputo son Tarjetas NIC PCI 10/100 con un procesador 3XP que se encarga de atender las

tareas relacionadas con el tráfico de red (suma de comprobación), liberando al sistema de dicho trabajo para que se ocupe de las aplicaciones principales. Con esto se logra un mejor rendimiento de red y del sistema.

La tarjeta NIC se comunica con equipos de conmutación para optimizar la transferencia de datos, reduciendo la perdida de paquetes y las retransmisiones.

Figura 3.27 Tarjeta NIC

Estas tarjetas son para las PC´s en cableado interno. Para atender la comunicación externa con los edificios, se utilizarán tarjetas inalámbricas para la comunicación.

3.7 SERVIDORES

Para el funcionamiento óptimo de nuestra red, nosotros hemos considerado la existencia de 4 servidores.

- **Servidor de archivos**: el cual va almacenar la información necesaria del personal y alumnos que integran la escuela. Además de la biblioteca virtual y los temarios de las materias. Así mismo contendrá el directorio activo y el dominio que son necesarios para mantener la seguridad de nuestra red, permitiendo que solo personas que estén incluidas en el dominio puedan ingresar a una computadora. Además de administrar los recursos compartidos de la red. El directorio activo es el servicio de directorio incorporado al sistema operativo que almacena información acerca de objetos de la red y facilita la búsqueda y utilización de esa información por parte de los usuarios.

  Cuenta con las siguientes características:

  - Incorpora un directorio que es un almacén de datos para guardar información acerca de los recursos compartidos (llamados también objetos)

- Incorpora reglas básicas que definen las clases de objetos y los atributos contenidos en el directorio. Los atributos se definen independientemente de las clases. Cada atributo solo se define una vez y se puede utilizar múltiples clases. Las clases también conocidas como clases de objetos describen los posibles objetos del directorio que se pueden crear: Cada clase es una colección de atributos. Al crear un objeto los atributos almacenan la información que describe al objeto.

- Define un catalogo global que contiene la información acerca de cada uno de los objetos del directorio que permite a los usuarios y administradores encontrar información del directorio con independencia del dominio del directorio que realmente contiene los datos

- Incorpora índices y consultas, para que los usuarios o las aplicaciones de red puedan publicar y encontrar los objetos y sus propiedades

- Para establecer una tolerancia a los fallos, proporciona un servicio de replicación que distribuye los datos del directorio por toda la red. Para ello, todos los controladores de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio de sus dominios y cualquier cambio en los datos del directorio se replica en todos los controladores de dominio del dominio

- Integración con el subsistema de seguridad para asegurar el proceso de inicio de sesión en la red, así como, control de acceso tanto de las consultas de datos del directorio, como de las modificaciones de los datos.

- El directorio activo esta contenido en las unidades organizativas, en estas se pueden colocar usuarios, grupos, equipos y otras unidades organizativas.

- **Servidor Web**, va a otorgar la página de intranet por donde los profesores y alumnos van a ingresar cuando necesiten extraer información de temarios y biblioteca. Así mismo contendrá el antivirus que nos proveerá sus actualizaciones.

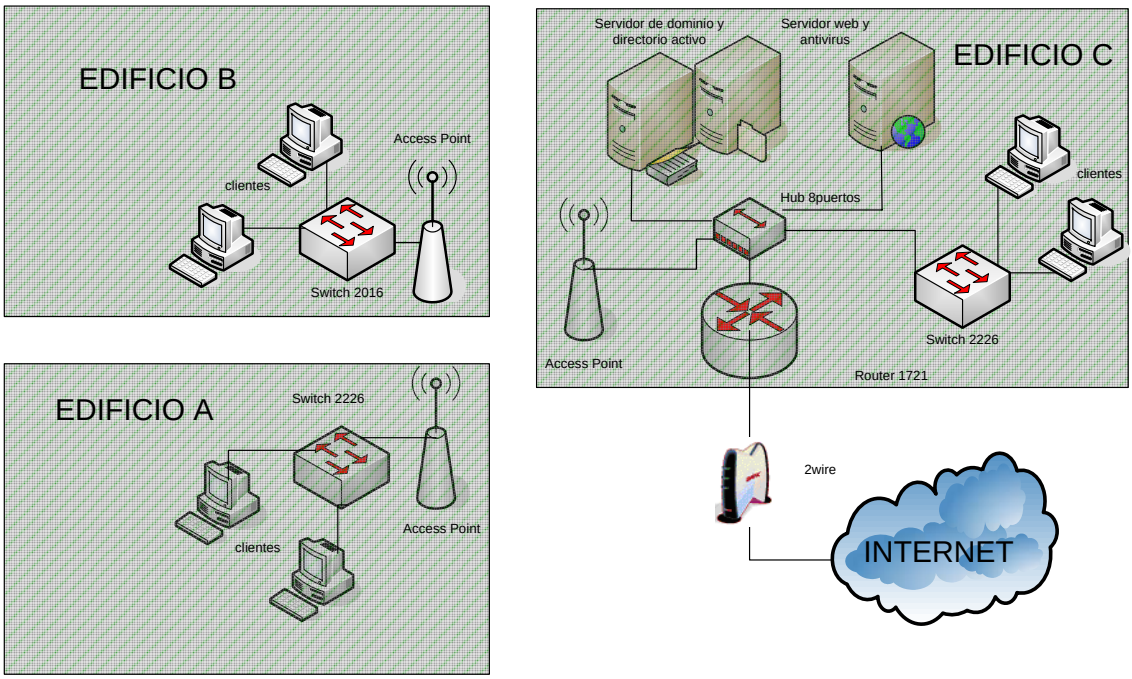


Figura 3.28 Diagrama a bloques de la ESCUELA SEC 425

3.8 SOFTWARE

3.8.1 WINDOWS 2003 SERVER Y XP

Escogimos Windows 2003 server como sistema operativo en todos los servidores, debido a las herramientas que ofrece en cuanto a la administración de la red, tales como dominio, directorio activo, correo, compatibilidad con SQL y una interfaz amigable para el administrador, además de un mejor control de seguridad.

El sistema operativo para las PC´s, será Windows XP, con sus respectivas actualizaciones, esto es porque ofrece una mayor seguridad para competición de recursos y logeo de usuarios, así también, es compatible con la mayoría del software que se utilizan en el mercado.

El mantenimiento y actualizaciones de los recursos que nos ofrecen los sistemas operativos basados en Windows son amplios y compatibles con el hardware y software que se utilizan en aplicaciones de red.

3.8.2 PAQUETERIA

Dentro de los múltiples programas que se pueden utilizar para desarrollo de trabajos en las PC´s de nuestra red se instalará Office XP para la captura de de informes y creación de presentaciones.

3.8.3 APLICACIONES

- ENCARTA: donde encontraremos la biblioteca virtual.

3.9 COMPAÑÍA ISP

Telmex nos proporcionara una velocidad de conexión de 512 Mb de los cuales tenemos para nuestro Upload 256 y para el Download 512 debido a que el tipo de conexión es ADSL (Línea de Abonado digital asíncrona).

CAPITULO IV. COSTO-BENEFICIO

OBJETIVO PARTICULAR

Conocer el costo de implementación de la red diseñada, plantear los beneficios que se van a obtener y determinar si es viable la implementación.

4.1 COSTO DE HARDWARE

Como hardware nosotros consideramos todo dispositivo físico y tangible que hace posible el flujo de información a través de la red, así también, estamos considerando los objetos físicos que nos ayudan a interconectar los dispositivos y proteger el flujo de datos.

4.1.1 DISPOSITIVO DE INTERCONEXION

DISPOSITIVOS	PRECIO p/u	PIEZAS	PRECIO TOTAL
Router Cisco 1721	**$15,575.98**	**1**	**$15,575.98**
3Com® Baseline Switch 2226	**$ 1,758.59**	**2**	**$ 3,517.18**
3Com® Baseline Switch 2016	**$ 1,283.46**	**1**	**$ 1,283.46**
3Com OfficeConnect Wireless 11g	**$ 743.65**	**3**	**$ 2,230.95**
Hub office connect dual speed 8P	**$850.00**	**1**	**$850.00**
Hub office connect dual speed 16P	**$1,300.00**	**1**	**$1,300.00**
		TOTAL	**$24,757.57**

Tabla 4.1 Cotización de dispositivos de interconexión

Actualmente la secundaria solo cuenta con el 2WIRE para la salida a internet, solamente un salón tiene este beneficio, con la implementación de los dispositivos de la tabla 4.1 se tendrá la posibilidad de conectar los tres edificios del plantel para que todos tengan acceso a internet e información en línea.

4.1.2 MEDIOS DE TRANSMISION

CABLE	PRECIO MT	MTS	PRECIO TOTAL
UTP[1] NIVEL 5	**$3.00**	**812**	**$2,436**

Tabla 4.2 Cotización de cableado

La cantidad de cable total considera el cableado interno de los tres edificios y el cableado del rack, es el total considerado para todo la conexión necesaria.

[1] **UTP**-Cable de Par Trenzado Sin Apantallar

4.1.3 SERVIDOR

El servidor que nosotros creemos convenientes para las aplicaciones que se van a desarrollar es un HP ProLiant ML110 G2 ideal para pequeñas redes, provee una plataforma de gran alcance que otorga todas las características relevantes de un servidor en un paquete fácil de utilizar. Es fácil de escalar dependiendo de las necesidades de la red.

Figura 4.1 HP ProLiant ML110 G2

PROCESADOR

Procesador Intel® Pentium® 4 3.40GHz/800MHz con tecnología HyperThreading bus de 800 MHz

MEMORIA CACHE

Integrada 1024-KB nivel 2 ECC

MEMORIA RAM

512 MB PC3200 DDR 400

DISCO DURO

5 disco duros 80GB SATA 1.5Gb 7200rpm

TARJETA DE RED

Intel 82541PI PCI Gigabit NIC 10/100/1000

CONTROLADOR DE ALMACENAMIENTO

Integrados 4 puertos Serial ATA con controlador RAID

MONITOR

Monitor SyncMaster 551v 15", Dot Pitch 0.28 COLOR, RESOLUCION MAXIMA 1024x768@75 Hz

QUEMADOR

HP DVD+RW 16X Drive

COMPONENTES	PRECIO p/u	PIEZAS	PRECIO TOTAL
CPU SERVDIROR	**$16,267.9**	**1**	**16,267.9**
MONITOR (15")	**$1,000.00**	**1**	**$1,000.00**
TECLADO (MULTIMEDIA)	**$120.00**	**1**	**$120.00**
MOUSE (OPTICO)	**$100.00**	**1**	**$100.00**
		TOTAL	**$**17,487.90

Tabla 4.3 Cotización del Servidor

Se considera un servidor físico para soportar la operación diaria con un raid 1 que es un espejo del disco duro principal. Este servidor aloja el directorio activo, la web y los archivos. El servidor trae cargado el sistema operativo Windows 2000.

4.1.4 PC´S

Las 28 PC´s de los centros de cómputo con las que cuenta la escuela tienen las siguientes características:

- Procesador Pentium III
- Memoria RAM de 128 Mb
- Disco Duro de 20 Gb
- Monitor de 15"
- Teclado, Mouse y bocinas.
- Lector de CD

Estas características en las PC´s son suficientes para soportar la demanda de las aplicaciones que van a utilizar en los centros de cómputo.

Solo se van a actualizar las computadoras de las secretarias y el Director. Así como cotizar las pc´s que hacen falta para la red.

El kit de actualización ofrece:

- Gabinete ATX con fuente de poder y ventilador
- Motherboard, incluye sonido, video, fax, red y puertos usb
- Procesador AMD Sempron 2200
- Memoria RAM de 256 Mb

Las computadoras ya tienen monitor, teclado y Mouse, lector de cd, el disco duro que tienen es de 20 Gb.

COMPONENTES	PRECIO p/u	PIEZAS	PRECIO TOTAL
KIT DE ACTUALIZACIÓN	**$ 2,199.00**	**4**	**$ 8,796**
		TOTAL	**$ 8,796**

Tabla 4.4 Cotización de Kit de Actualización para PC´s

Las computadoras que se van a adquirir tiene las siguientes características:

- Memoria RAM de 256 Mb
- Gabinete ATX con fuente de poder y ventilador.
- Procesador AMD Sempron 2200
- 128Mb de memoria
- disco duro de 40gb
- unidad cd rom
- Motherboard incluye sonido video fax red
- puertos USB
- Monitor de 15”
- Floppy 1.44 Mb
- Teclado multimedia
- Mouse óptico
- bocinas

La adquisición de equipo nuevo conforma a las áreas de orientación, supervisión, sala de maestros, audiovisual y todos los salones de 1°, 2° y 3°, así como los laboratorios y electricidad. En total son 21 PC´s.

COMPONENTES	PRECIO p/u	PIEZAS	PRECIO TOTAL
COMPUTADORAS	**$3,900.00**	**21**	**$81,900.00**
		TOTAL	**$81,900.00**

Tabla 4.5 Cotización de PC´s

4.1.5 PERIFERICOS

Los periféricos cotizados son necesarios para la protección de los dispositivos y para el cableado estructurado.

ACCESORIO	PRECIO p/u	PIEZAS	PRECIO TOTAL
RACK (usado)	**$1,000.000**	**1**	**$1,000.000**
PANEL DE PARCHEO (usado)		**1**	
BANDEJAS (usado)		**1**	
REGULADORES	**$150.00**	**4**	**$600.00**
NO BREAK 1000 VA, 600 WATTS, P/60 MINUTOS	**$2,600.000**	**1**	**$2,600.000**
PLUGS RJ45 (100 PIEZAS)	**$ 0.600**	**200**	**$120.00**
ROSETA	**$4.200**	**60**	**$252.00**
CANALETAS (2M)	**$21.000**	**406**	**$8,526.00**

ESTUCHE CON SURTIDO DE 300 CINCHOS DE COLORES	**$48.000**	**1**	**$48.00**
		TOTAL	**$13,146.00**

Tabla 4.6 Cotización de Periféricos

4.2 COSTO DE SOFTWARE

El Software es toda aplicación que se va a instalar en el servidor o en los clientes y que es necesaria para la operación normal de la red y para otorgar las herramientas de trabajo.

SOFTWARE	PRECIO p/licencias	licencias	PRECIO TOTAL
WINDOWS XP HOME EDITION	**$1,052.73**	**1**	**$1,052.73**
OFFICE XP	**$3,539.98**	**1**	**$3,539.98**
ENCARTA BIBLIOTECA	**$700.00**	**1**	**$700.00**
NORTON	**$608.00**	**1**	**$608.00**
		TOTAL	**$5,900.71**

Tabla 4.7 Cotización de Software

4.3 COSTO TOTAL DE IMPLEMENTACION

COMPONENTE	PRECIO
HARDWARE	**$148,523.47**
SOFTWARE	**$5,900.71**
COSTO TOTAL	**$154,424.18**

Tabla 4.8 Costo total de implementación

La cotización anterior abarca el diseño completo de la red, así como el funcionamiento óptimo de la misma y de las herramientas que posibilitan alcanzar los objetivos del diseño. Sin embargo existen muchas posibilidades de bajar el costo real del mismo.

Nosotros hemos pensado en la donación de equipos por parte de algunas empresas lo cual significaría reducir el costo.

Para hacer la petición de una donación se necesita seguir el siguiente procedimiento:

06/enero/2005

Hoy en día, las donaciones de computadoras a Instituciones de Educación Básica permiten a profesores y alumnos hacer uso de las herramientas de formación más actualizadas. En el pasado, la correcta administración de los recursos tecnológicos donados ha resultado una tarea confusa, ardua y en muchas ocasiones, difícil.

Ahora la Alianza por la Educación de Kimat México es un punto de unión para que la educación en México se convierta en sinónimo de oportunidad, estableciendo un programa que permite actualizar y administrar con eficiencia el hardware de las computadoras que las escuelas primarias y secundarias han recibido mediante donaciones.

Renueva y Aprende otorga la documentación de la licencia del Sistema Operativo Windows original y los CDs de instalación correspondientes (sin costo) para dichos equipos de cómputo. A través de este programa se ofrecen las ediciones Windows 98, Windows 2000 y Windows XP para equipos Pentium III o anteriores, de modo que las escuelas puedan seleccionar la versión que se adapte mejor a la funcionalidad y a las características técnicas del equipo que ellos requieren.

Las escuelas deberán suscribirse, sin costo al programa, mediante el llenado de un formulario, que les será entregado a través del trabajador de Kimat México que les haya hecho la propuesta e invitación al programa. Cabe mencionar que de ser seleccionado se tiene un status de espera de alrededor de año y medio.

Son elegibles para participar en Renueva y Aprende las Instituciones de Educación Básica (escuelas públicas o privadas, autoridades locales de educación, sistemas y distritos educativos) que impartan clases de enseñanza primaria y secundaria.

REQUISITOS

Para mantener la actualización de los equipos Kimat México se reserva el derecho de cancelación del proyecto si el nivel académico general de la institución decae con relación al manejado cuando se realizo la solicitud.

- El promedio mínimo para ser una institución elegible es de 9 global.
- Kimat México se reserva el derecho de evaluar a un grupo de estudiantes de dicha institución para corroborar el nivel académico.

Además de plantear cursos para los estudiantes a través del ciclo escolar y en vacaciones de cambio de ciclo.

- Las escuelas pueden presentar solicitudes para registrar su solicitud una sola vez y en cualquier momento, durante el año calendario. Las licencias proporcionadas mediante Renueva y Aprende son perpetuas.

RESTRICCION

La escuela deberá conservar la propiedad de los equipos a los que se ha concedido licencia mediante este programa, y no podrá transferir licencias de Sistemas Operativos Windows a los alumnos ni a organizaciones externas.

Con el Programa Renueva y Aprende, podremos unir más puntos en favor de la educación en México. Por ser una empresa socialmente responsable con actividad en México, Kimat México reconoce la importancia de participar en causas que beneficien a la sociedad.
Director General Lic. Gerardo Anzures
Kimat México

Con esta alternativa el costo se reduce a:

COMPONENTE	PRECIO
HARDWARE	**$66,623.47**
SOFTWARE	**$4,847.98**
COSTO TOTAL	**$71,471.45**

Tabla 4.9 Reducción de Costos

El beneficio obtenido al implementar la red lo encontramos:

A nivel alumno:

Internet
Clases dinámicas e ilustrativas para ejemplicar mejor el conocimiento
Acceso a una biblioteca virtual que les permita consultar los temas que deseen, aclarar dudas o buscar tareas.

A nivel Profesor
Les da la posibilidad de tener un temario bien estructurado
Obtener la información que deseen sobre los temas que imparte de manera que conozcan más al respecto y puedan transmitir más conocimientos
Ilustrar las clases de materias pesadas como son física, química, historia, geografía y laboratorios, para que los alumnos se interesen más por ello y no se fastidien.
Organización de la información que manejan acerca de los alumnos, al tenerla en línea facilita el control y la búsqueda de la misma.
Acceso a cursos en línea que se imparten por la red.

A nivel Dirección

Digitalizar la documentación de los alumnos para que se tenga un control, organización y seguridad de los mismos.

Asegurar la calidad de la clases y la productividad de los profesores al llevar un temario en línea que se deba cumplir, llevando un control sobre los temas que se impartieron y los que no.

Acceso a Internet por medio de los cuales puedan hacer los pagos en línea y a lo mejor recibir por el mismo medio.

Nosotros estamos conscientes que la inversión es fuerte, sin embargo, toda implementación tecnológica cuesta, pero los beneficios obtenidos los vemos en una agilización de información, fácil acceso y manejo de datos y la posibilidad de que todos tengamos acceso a los nuevos conocimientos.

CONCLUSION

Al concluir el diseño de la red para la escuela secundaria, encontramos que los beneficios para cada uno de los niveles que la conforman, se convirtieron en valores de superación ya que al contar con estas nuevas herramientas tanto los alumnos como los profesores y miembros administrativos pueden encontrar puntos de interés y desarrollo para su vida diaria ya que la información se encuentra al alcance y de forma eficiente y sencilla pueden culminar su trabajo con mayor rapidez y con menos papeleo.

Para los alumnos resulta mas atractivo contar con nuevas herramientas de trabajo y de enseñanza ya que en ocasiones a pesar de que el sistema tradicional nos trae mucho conocimiento, el interés por el equipo de computo y las formas de comunicación que se tienen hoy en día hacen que los adolescentes encuentren en la red la mejor forma de desarrollar sus aptitudes de investigación y de conocimiento, ya que al tener un ambiente controlado para únicamente tener acceso a paginas de valor científico produce la conciencia de que una herramienta tan poderosa como lo es Internet puede utilizarse con fines de desarrollo y no solo de diversión, lucro y pornografía que son los males mas grandes que aquejan nuestros monitores cuando intentamos buscar hasta el mas mínimo concepto.

Este proyecto hace algunos años, por el precio de los equipos, sonaría descabellado, pero hoy en día gracias a los planes de financiamiento y a los planes de donación de algunas empresas es posible crear laboratorios de trabaja en los mismos salones de clase, y con ello despertar el interés y la imaginación de los adolescentes, inculcándoles, valores de desarrollo.

Nuestro proyecto comenzó siendo solo un proyecto para la culminación de nuestros estudio profesionales, pero con el tiempo se a convertido en un interés por desarrollar redes de confianza que permitan a los alumnos no solo de secundaria sino también a los de primaria, navegar en redes escolares que tengan la rapidez, información y seguridad, que otras no tienen, a un bajo costo.

Por ultimo hemos comprendido que el desarrollo de las redes a través de los años nos permiten ahora contar con las herramientas necesarias para ofrecer como ingenieros un apoyo para la solución de problemas y necesidades de nuestra comunidad, integrando los conocimientos de nuestro desarrollo estudiantil y laboral.

Estamos consientes que en un futuro inmediato nuestra red necesitara de actualizaciones y hasta de modificaciones, ya que los continuos desarrollos de equipo nos dejan pensar que las comunicaciones inalámbricas y dispositivos portables como Palm´s, hacen posible que los empleados administrativos y profesores tengan siempre cerca su información para la actualización de los conocimientos que trasmiten tanto como de los suyos para la administración de sus propios recursos.

GLOSARIO DE TERMINOS

ACCESS POINT. Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles para su centralización o para su enrutamiento.

ADSL(Asymmetric Digital Subscriber Line). Línea de Abonado Digital Asimétrica que consiste en una línea digital de alta velocidad, apoyada en el par trenzado de cobre que lleva la línea telefónica convencional o línea de abonado en donde la velocidad de bajada y la de subida no son simétricas, es decir que normalmente permiten una mayor velocidad de bajada que de subida.
ALGORITMO. Regla o proceso bien definido para resolver un problema. En redes, los algoritmos se utilizan comúnmente para determinar la mejor ruta para el tráfico desde un origen particular hasta un destino particular.

AMPLIFICADOR. Dispositivo que produce un incremento significativo en el alcance de la señal de las WLAN. Consta de un receptor de bajo ruido pre-amplificado y un amplificador lineal de salida de radio frecuencia (RF).

AMPLITUD DE BANDA. Especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ANCHO DE BANDA. Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. El término se utiliza también para describir la medida de capacidad de transmisión de un medio o protocolo de red datos.

APPLETALK. Serie de protocolos de comunicaciones diseñada por Apple Computer. Existen dos fases actualmente. La Fase 1, la versión anterior, soporta una red física simple que puede tener solamente un número de red y estar en una zona. La Fase 2, la versión más reciente, soporta redes lógicas múltiples en una red física simple, y permite a las redes estar en más de una zona.

ARP (Address Resolution Protocol). Protocolo de Resolución de Direcciones de la suite de protocolos TCP/IP que convierte las direcciones lógicas IP en direcciones físicas MAC para el uso de Ethernet.

ARP PROXY. Protocolo de resolución de direcciones proxy. Variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un router) envía una respuesta ARP en nombre de un nodo extremo al host solicitante. ARP proxy puede disminuir el uso del ancho de banda en enlaces WAN de baja velocidad.

ASK (Amplitud-Shift Keying). Técnica donde los dos valores binarios se representan mediante amplitudes diferentes de portadora. Un 1 binario se representa con una portadora de amplitud constante y un O binario por ausencia de portadora.

ASCII (American Standard Code for Information Interchange). Código Americano Estándar para el intercambio de Información que consta de 7 bits más 1bit de paridad.

ATENUACION. Es la pérdida de potencia sufrida por la señal (acústica, eléctrica u óptica) al transitar por cualquier medio de transmisión.

ATM (Asynchronous Tranfer Mode). Modo de Transferencia Asíncrono, protocolo de transmisión de conmutación de paquetes a través de celdas de tamaño fijo de 53 bytes mediantes el uso de canales virtuales y trayectos virtuales.

AUI (Attachment Unit Interface). Interfaz de unidad de conexión. Interfaz IEEE 802.3 entre una MAU y una NIC (network interface card). El término AUI también se puede referir al puerto del panel posterior con el cual se podría conectar un cable AUI,

B8ZS (bipolar with 8 substitution). Bipolar con sustitución de 8 ceros, un método norteamericano de codificación usado en el sistema del T-portador que permite 64kbps completo por segundo por el canal, en el cual el 1 binario se representa con nivel positivo y negativo alternante, y para 8 ceros continuos de señal se codifica de la siguiente manera, si aparece un octeto donde todos son ceros, y el pulso de voltaje anterior a dicho octeto fue positivo, éste se codifica como 000+-O-+. Si aparece un octeto donde todos son ceros, y el pulso de voltaje anterior a dicho octeto fue negativo, éste se codifi.ca como 000-+O+-.

BACKBONE. La parte de una red que actúa como ruta primaria para el tráfico que sale y llega de otras redes con mayor frecuencia.

BANDA ANCHA. Volumen de información que puede circular por un medio físico de comunicación de datos, capacidad de conexión. A mayor capacidad mayor velocidad. Se mide en **hertz** o ***bps*** (bits por segundo)

BANDA BASE. Característica de una tecnología de red donde se utiliza sólo una frecuencia portadora. Ethernet es un ejemplo de red de banda base. También llamada banda estrecha.

BASE DE DATOS. Conjunto de información para varios usuarios. Suele admitir la selección de acceso aleatorio y múltiples vistas o niveles de abstracción de los datos subyacentes.

BGP (Border Gateway Protocol). Protocolo de entrada de frontera, mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un router que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca.

BIT. Dígito del sistema binario de numeración, es la unidad más pequeña de información y la unidad base en comunicaciones.

BIT DE PARIDAD. Bit adicional que acompaña a cada grupo de un código, de tal forma que el número de unos que se transmite siempre sea par o impar.

BOOTP. Protocolo de inicio del sistema operativo Permite a una estación de trabajo descubrir su dirección IP, una dirección IP de un servidor BootP en una red, o un archivo de configuración cargado en el arranque de un dispositivo.

BRIDGES. Véase Puente

BROADCAST. Difusiones que se producen cuando una fuente envía datos a todos los dispositivos de una red. En la tecnología Ethernet el broadcast se realiza enviando tramas con dirección MAC de destino FF.FF.FF.FF.FF.FF. En el protocolo IP se realiza enviando datos a una dirección de difusión, aquella dirección IP que tiene todos los bytes de host configurados en 255. Cuando se envían datos a esta dirección de difusión IP éstos son recibidos por todos los nodos.

BUFFER. Es una ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada.

BYTE. Conjunto de bits continuos mínimos que hacen posible, un direccionamiento de información en un sistema computarizado. Está formado por 8 bits.

CABLE COAXIAL. Cable que consta de un conductor cilíndrico exterior hueco que envuelve a un único alambre conductor interno. En las LANs se utilizan normalmente dos tipos de cable coaxial, cable de 50 ohms que se utiliza para la señalización digital, y cable de 75 ohms que se utiliza para la señal analógica y la señalización digital de alta velocidad.

CATV. Un sistema de televisión comunitaria, servida por cable y conectada a una antena (o grupo de antenas) común.

CIDR (Classless Inter Domain Routing). Enrutamiento Inter Dominio Sin Clases, es un método de direccionamiento IP, en donde no importan las clases. Lo que importa es el prefijo

CODIFICACION. Consiste en transformar la formulación de un mensaje mediante una serie de reglas dispuestas según un plan metódico y sistemático. Al conjunto de estas reglas metódicas que definen la codificación se les denomina código.

CODIFICACION BIFASE. Técnicas de Codificación en las cuales los valores binarios se representan por transiciones de nivel positivo a negativo y viceversa.

CODIFICACION CRIPTOGRAFICA. Técnicas que connsisten en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje, mediante algoritmos de cifrado.

CODIFICACION DIFERENCIAL. Técnica de codificación digital por la cual un valor binario es denotado por un cambio de señal en lugar de un nivel de señal en particular.

CODIGO BIPOLAR AMI. Técnica de codificación en la cual un 0 binario es representado por una ausencia de señal, y un 1 binario es representado por un pulso negativo o positivo alternante

CODIGO MANCHESTER. Técnica de coficación en la cual hay una transición a mitad del intervalo de cada bit, un 0 binario se representa por una transición de un nivel alto a un bajo y un 1 binario con una transición de un nivel bajo a alto.

CODIGO MANCHESTER DIFERENCIAL. Técnica de Codificación en la cual un 0 binario se representa con una transición al principio de cada periodo de bit, y un 1 binario es representado por ausencia de transición al principio de cada periodo de bit.

CODIGO PSEUDOTERNARIO. Técnica de Codificación en la cual esquema un 1 binario se representa por una ausencia de señal y un O binario con la transición de pulsos negativos y positivo alternantes.

CONCENTRADOR. Véase Hub.

CONECTOR BNC. (Bayonet Neil-Concelman, o a veces British Naval Connector) Se usa para la interconexión de equipos y/o dispositivos en redes locales 10BASE2 Ethernet con cable coaxial

CONECTOR N. Conector coaxial más utilizado para conectar las antenas a los nodos wireless, ya que su coste es asequible, pierde poca señal y es perfecto para conectarlo a cable con poca perdida de señal.

CONMUTACION DE CIRCUITOS. Establecen a través de la red, un camino físico continuo entre las dos estaciones que se quieren comunicar, como si fuera una línea punto a punto. Hasta que no se ha establecido ese camino no se inicia la transmisión.

CONMUTACION DE PAQUETES. La transmisión se realiza subdividiendo la información en paquetes, que viajan a través de distintos caminos físicos.

CORRIENTE ALTERNA. Es la corriente eléctrica que cambia repetidamente de polaridad, esto es, su voltaje instantáneo va cambiando en el tiempo desde 0 a un máximo positivo, vuelve a cero y sucesivamente

CORRIENTE DIRECTA. Es la corriente que tiene un único sentido de circulación. Es la producida por las pilas y por los adaptadores AC-DC.

CoS (Class of Service). La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se

agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.

CRC (Cyclic Redundancy Checksum). Verificación por redundancia cíclica, es un Código detección de errores muy utilizado, que calculan un número binario, llamado CRC, a partir de los bits a proteger. En el destino, se repite el cálculo para ver si coincide o no con el CRC.

CSMA/CD (Carrier Sense Multiple Access with Collision Detect) Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso al medio en el cual los dispositivos listos para transmitir datos primero verifican el canal en busca de una portadora. Si no se detecta ninguna portadora por un lapso especificado, un dispositivo puede transmitir. Si dos dispositivos transmiten a la vez, tiene lugar una colisión y ésta es detectada por todos los dispositivos que entran en colisión. En consecuencia, la colisión demora las retransmisiones desde dichos dispositivos por un lapso al azar. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

DATAGRAMA. Agrupamiento lógico de información enviada como una unidad de capa de red por un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información en la Internet. Los términos frame, mensaje, paquete, y segmento también se utilizan para describir los agrupamientos lógicos de información en las diferentes capas del modelo de referencia OSI y en varios círculos de tecnología.

DATOS DIGITALES. Son datos que se caracterizan por tener un espectro discreto y finito, formado por dos estados binarios (unos y ceros).

DATOS ANALOGICOS. Son datos que se caracterizan por tener un espectro continuo y un intervalo infinito de valores.

DECODIFICACION. Es el proceso inverso a la codificación que consiste en descifrar el mensaje mediante el uso del mismo código con el cual fue codificado.

DEMODULAR. Proceso de retornar una señal modulada a su forma original. Los módems realizan la demodulación, tomando una señal análogica y retornándola a su forma original (digital).

DES (Data Encryption Standard). Estándar de Encriptación de Datos, es desde 1977 de uso obligatorio en el cifrado de informaciones gubernamentales no clasificadas, desarrollado por IBM como una variación de un criptosistema anterior, Lucifer, y posteriormente, tras algunas comprobaciones llevadas a cabo por la NSA estadounidense, pasó a transformarse en el que hoy conocemos como DES, es un sistema de clave privada tanto de cifrado como de descifrado; posee una clave de entrada con una longitud de 64 *bits*, produciendo una salida también de 64 bits, con una clave de 56 *bits* (el octavo bit de cada byte es de paridad), llamada clave externa, en la que reside toda la seguridad del criptosistema ya que el algoritmo es de dominio público.

DHCP (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de servidores en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP.

DIAFONIA. Denominada en inglés Crosstalk, se presenta cuando parte de las señales presentes en uno de ellos, considerado perturbador, aparece en el otro, considerado perturbado.La diafonía, en el caso de cables de pares trenzados se presenta generalmente debido a acoplamientos magnéticos entre los elementos que componen los circuitos perturbador y perturbado o como consecuencia de desequilibrios de admitancia entre los hilos de ambos circuitos. La diafonía se mide como la atenuación existente entre el circuito perturbador y el perturbado, por lo que también se denomina atenuación de diafonía.

DIRECCION IP. Dirección de 32 bits asignada a los hosts que utilizan TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D, o E) y se escribe en forma de 4 octetos separados con puntos (formato decimal con punto). Cada dirección consiste en un número de red, un número opcional de subred, y un número de host.

DIRECCION MAC. Dirección de la capa de enlace de datos estandarizada, necesaria para cada puerto o dispositivo conectado a una LAN. Otros dispositivos en la red utilizan estas direcciones para localizar puertos específicos en la red, y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen una longitud de 6 bytes y son controladas por IEEE. También conocidas como dirección de hardware, dirección de capa MAC, o dirección física.

DIRECTORIO ACTIVO. Es el nombre utilizado por Microsoft para referirse a su implementación del protocolo LDAP en los servidores.

DISCO DURO. Es un conjunto de discos magnéticos metálicos, empaquetados al vacío en una carcasa también metálica (generalmente de aluminio o magnesio, pero en cualquier caso de un metal no magnetizable) y que gracias a las enormes velocidades de giro (se puede hablar de hasta 10.000 revoluciones por minuto) son capaces de almacenar una gran cantidad de datos.

DISPOSITIVOS DE INTERCONEXION DE RED. Son dispositivos que sirven para facilitar la conexión de redes de área local con otras redes que pueden ser también de área local o de área amplia. Algunos de ellos son Gateways,Bridges,Router…

DNS (Domain Name System). Sistema de Nombres de Dominio utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DSU. Dispositivo utilizado en la transmisión digital que adapta la interfaz física en un dispositivo DTE a una facilidad de transmisión tal como T1 o E1. DSU es también responsable por funciones tales como la temporización de la señal.

DTE (Data Termial Equipment). Equipo terminal de datos, dispositivo en el extremo usuario de una interfaz de usuario a red que sirve como origen de datos, destino, o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza en forma típica señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como computadoras, traductores de protocolo y multiplexores.

DOMINIO. Grupo de equipos y dispositivos de una red que se agrupan con reglas y procedimientos comunes. En Internet, una parte del árbol de jerarquía de nombres que se refiere a los agrupamientos generales de redes basadas en tipo de organización o geografía.

DSAP (Destiny Service Acces Point). Punto de Acceso al Servicio Destino, es la dirección individual o grupal para las direcciones de capa superiores de la pila de protocolos de red.

E1. Sistema de transmisión digital de área amplia, utilizado predominantemente en Europa, que transporta datos a una velocidad de 2,048 Mbps.

EIGRP. Es un protocolo de enrutamiento híbrido que ofrece lo mejor de los algoritmos de vector-distancia y del estado de enlace. Se considera un protocolo de enrutamiento avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

ENCRIPTACION. La aplicación a los datos de un algoritmo específico para alterar la presentación de los datos al hacerlos incomprensibles para los terceros que no estén autorizados a ver la información.

ENRUTADOR. Véase Router

ENRUTAMIENTO. Proceso que consiste en encontrar la ruta hasta el host de destino. El enrutamiento es muy complejo en las redes de grandes dimensiones debido a los diversos destinos intermedios potenciales que un paquete debe atravesar antes de llegar a su host de destino.

ESTANDAR. Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc...

EXTRANET. Es una red privada virtual resultante de la interconexión de dos o más intranets que utiliza Internet como medio de transporte de la información entre sus nodos.

ETCD (Equipment Terminal Circuit Data). Un Equipo terminal del circuito de datos es todo dispositivo que participa en la comunicación entre dos dispositivos pero que no es receptor final ni emisor original de los datos que forman parte de esa comunicación.

ETHERNET. Estándar IEEE 802.3 más común para redes LAN que admite velocidades de transferencia de datos de Mpbs, compatibles con velocidades de 10, 100 ó 1000 Mbps y que utiliza la técnica CSMA/CD para controlar el acceso al medio.

FASE. La fase de una onda expresa la posicion relativa de un monte o valle de esta onda, con respecto a otra onda

FAST ETHERNET. Ethernet a velocidades de 100 Mbps.

FCS. Véase CRC

FDDI (Fiber Distributed Data Interface). Interfaz de datos distribuida por fibra. Norma LAN, definida por ANSI X3T9.5, que especifica una red de token-passing de 100-Mbps que utiliza un cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble para dar redundancia.

FIBRA MULTIMODO. Tipo de fibra óptica en la cual los rayos que inciden en la frontera con un ángulo mayor al crítico se reflejarán internamente, muchos rayos estarán rebotando con ángulos diferentes, diciendo así que cada rayo tiene un modo diferente

FIBRA MULTIMODO DE INDICE GRADUAL. Tipo de fibra óptica que varía gradualmente el índice de refracción, al disponer de un índice de refracción superior en la parte central, hace que los rayos de luz avancen más rápidamente conforme se alejan del eje axial de la fibra. En lugar de describir un zigzag, la luz en el núcleo describe curvas helicoidales debido a la variación gradual del índice de refracción, reduciendo así la distorsión multimodal.

FIBRA MONOMODO. Tipo de fibra óptica donde el radio del núcleo es reducido, de manera que la reflexión total se da en un número menor de ángulos, ocasionando que la fibra actúe como una guía de onda y la luz pueda propagarse solo en línea recta, sin rebotar, obteniéndose un modo único de transmisión

FIBRA OPTICA. Medio físico capaz de conducir una transmisión de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más costoso, pero no es susceptible a la interferencia electromagnética, y es capaz de mayores velocidades de datos. Llamado a veces fibra óptica.

FICHEROS. Un archivo o fichero informático es una entidad lógica compuesta por una secuencia finita de bytes, almacenada en un sistema de archivos ubicada en la memoria secundaria de un ordenador. Los archivos son agrupados en directorios dentro del sistema de archivos y son identificados por un nombre de archivo. El nombre forma la identificación única en relación a los otros archivos en el mismo directorio.

FIREWALL. Router o servidor de acceso, diseñados como un buffer entre cualquier red pública y red privada conectadas. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

FOTODIODO. Es un semiconductor construido con una unión PN, sensible a la incidencia de la luz visible o infrarroja. Para que su funcionamiento sea correcto se polariza inversamente, con lo que se producirá una cierta circulación de corriente cuando sea excitado por la luz.

FOTON. Cantidad mínima de energía de la luz u otra radiación electromagnética.

FRAGMENTO. Parte de un paquete más grande que ha sido dividido en unidades más pequeñas.

FRAGMENTACIÓN. Proceso de dividir un paquete en unidades más pequeñas cuando se transmite por un medio de red que no puede soportar el tamaño original del paquete.

FRAME RELAY. Protocolo de la capa de enlace de datos conmutados, de norma industrial, que administra varios circuitos virtuales utilizando una encapsulación HDLC entre dispositivos conectados. Frame Relay es más eficaz que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FRECUENCIA. Es el número de veces que se repite un ciclo o una oscilación de la onda en un segundo.

FSK (Frecuency-Shift Keying). Técina en la cual los dos valores binarios se representan con dos frecuencias diferentes cercanas a la portadora. Un 1 binario se representa con una señal de alta frecuencia y un O binario con una señal de baja frecuencia.

FTP (File Transfer Protocol). Protocolo de Transferencia de archivos de la suite de TCP/IP del nivel de aplicación utilizado para transferir archivos entre nodos de red.

FULL DUPLEX. Capacidad para la transmisión simultánea de datos entre una estación transmisora y una estación receptora.

GATEWAYS. Caja electrónica o un dispositivo de red lógico que interconecta redes incompatibles o dispositivos al realizar la conversión del protocolo.

HDB3 (Hihg-Density Bipolar 3-zeros). Técnica de Codificación, Bipolar de 3 ceros de Alta Densidad, en la cual el 1 binario se representa como nivel positivo y negativo alternante y una cadena de 3 ceros se reemplaza codificando dependiendo de la polaridad del pulso anterior y si la última violación fue par o impar.

HALF-DUPLEX. Capacidad de transmisión de datos solamente en una dirección a la vez, entre una estación de envío y una estación de recepción.

HARDWARE. Es el nombre que se le da a todo aquel componente físico que puede ser conectado al CPU.

HDLC (High-Level Data Link Control).Control de enlace de datos de alto nivel. Protocolo de la capa de enlace de datos, orientado a bit y síncrono desarrollado por ISO. Proveniente de SDLC, HDLC especifica un método de encapsulación de datos sobre enlaces en serie síncronos que utilizan caracteres de frame y checksums

HOST. Sistema de computación en una red. Similar al término nodo excepto que el host usualmente implica un sistema de computación, mientras que un nodo generalmente se aplica a cualquier sistema en red, incluyendo los servidores de acceso y routers.

HOSTID. Identificador de dirección de máquina.

HSRP (Hot Standby Router Protocol). Es un protocolo de redundancia para redes IP que permite la detección y recuperación automática ante la caida del router activo. HSRP funciona entre los routers que hagan de primario y backup, y por medio de ese protocolo ambos routers comparten la misma dirección Mac e IP (la configurada en el default gateway de los PCs), de tal modo que la caída del router principal es totalmente transparente para los PCs. El protocolo HSRP permite balanceo de carga en cuanto a las tareas de routing inter-VLAN (cada router puede estar activo para una VLAN y en modo standby para otra cuyo router activo sea el otro componente del par redundante) de forma que los rendimientos de ambos routers pueden sumarse para calcular el rendimiento global de la solución.

HTTP (HyperText Transfer Protocol). Protocolo de transferencia de hipertexto que transmite documentos HTML entre servidores y clientes de internet.

HTTPS. Versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.

HUB. Repetidor Ethernet multipuerto, algunas veces denominado como concentrador, que permite compartir el uso de una línea entre varios computadores que se conectan en él, su propósito es regenerar y retemporizar la señal.

HYPER TERMINAL. Es un programa que puede utilizarse para conectar con otros equipos, sitios telnet de Internet, servicios de boletines electrónicos, servicios en línea y equipos host con un módem o un cable de módem nulo.

IANA. Es el acrónimo de Internet Assigned Number Authority. La Agencia de Asignación de Números Internet era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN

ICMP (Internet Control Messages Protocol).Protocolo de Control de Mensajes de Internet, es uno de los protocolos centrales de la suite de protocolos de Internet. Es usado principalmente por los Sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible ó que un router ó host no puede ser localizado.

IEEE (Institute Electric-Electronic Engineer).Instituto de Ingenieros Eléctricos-Electrónicos que desarrolla estándares de comunicación y redes.

IEEE 802.1p. Estándar que Prioriza el tráfico de red en la subcapa de vínculo de datos/MAC.

IEEE 802.11b. Trabaja en la frecuencia de los 2,4 GHz, con 13 canales disponibles y posibilita velocidades de 11 Mbps en su primera versión y 22 Mbps en su edición Plus.

IEEE 802.11g. Protocolo de comunicación inalámbrica aprobado en abril de 2003 que faculta a operar a 54 Mbps en la frecuencia de los 2,4 Ghz.

IEEE 802.1Q. Define el funcionamiento de los puentes VLAN que permite definir, hacer funcionar y administrar VLAN dentro de las infraestructuras de LAN con puente

IEEE 802.3. Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT, y 10Broad36. Las variaciones físicas de Fast Ethernet incluyen 100BaseT, 100BaseT4, y 100BaseX.

IEEE 802.3U. Define el método de acceso al medio CSMA/CD y las especificaciones de capa física para 100BASE-TX y 100BASE-FX Fast Ethernet.

ICMP (Internet Control Message Protocol). Protocolo de mensajes de control en Internet. Protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP.

IEFT (Internet Engineering Task Force). Grupo de Trabajo en Ingeniería de Internet es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986.

IGRP (Interior Gateway Router Protocol). Protocolo de Enrutamiento de Pasarela Interior que llama a cada router para enviar toda o parte de su tabla de ruteo en un mensaje de actualización debutas a intervalos regulares a cada uno de sus routers cercanos.

IMAP (Internet Mail Access Protocol). Protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una vez configurada la cuenta IMAP, puede especificar las carpetas que desea mostrar y las que desea ocultar, esta característica lo hace diferente del protocolo POP.

IMPEDANCIA. La impedancia es la oposición que presenta un circuito al paso de la corriente alterna.

INDICE DE REFRACCION. Es el número adimensional que expresa la relación existente entre la velocidad de la luz en el aire y la velocidad de la luz en un medio más denso.

INFRARROJO. La radiación infrarroja o radiación térmica es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas. Consecuentemente, tiene menor frecuencia que la luz visible y mayor que las microondas. El nombre de infrarrojo, que significa por debajo del rojo, proviene de que fue observada por primera vez al dividir la luz solar en diferentes colores por medio de un prisma que separaba la luz en su espectro verticalmente de manera que el rojo era el que estaba mas abajo y el violeta el mas arriba

INTERFERENCIA. Es cualquier proceso que altera, modifica o destruye una señal durante su trayecto en el canal existente entre el emisor y el receptor.

INTERNET. Término utilizado para referirse a la mayor internetwork global que conecta a decenas de miles de redes de todo el mundo y que tiene una cultura que apunta básicamente a la investigación y a la estandarización basándose en el uso en la vida real.

INTRANET. Es una red de Área Local (LAN) privada empresarial o educativa que proporciona herramientas vía Internet las cuales tienen como función principal proveer lógica de negocios para aplicaciones de captura, reportes, consultas, etc. con el fin de auxiliar la producción de dichos grupos de trabajo; es también un importante medio de difusión de información interna a nivel de grupo de trabajo.

IP (Protocol Internet). Protocolo de Internet que especifica el formato de los paquetes y su método de direccionamiento, IP direcciona los paquetes y los reenvía al puerto correcto.

IPv4. Es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implemento extensamente, y forma la base de

Internet. IPv4 usa direcciones de 32 bits, limitándola a 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).

IPv6. Es la versión 6 del Protocolo de Internet (Internet Protocol), un estándar del nivel de red encargado de dirigir y encaminar los paquetes a través de una red. IPv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (3,4 x 10^{38} ó 340 sextillones) direcciones
IPSec (Internet Protocol security). Protocolo de Seguridad de Internet que es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente fue desarrollado para usarse con el nuevo estandar IPv6, aunque posteriormente se adaptó a IPv4.

IPX (Internetwork Packet eXchange). Intercambio de paquetes interred, Protocolo de nivel de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

IRC (Internet Relay Chat). Es un protocolo de comunicación en tiempo real basado en texto, el cual permite debates en grupo y/o privado, el cual se desarrolla en canales de chat que generalmente comienzan con el carácter # o &, este último sólo es utilizado en canales locales del servidor. Es un sistema de charlas muy popular actualmente y ampliamente utilizado por personas de todo el mundo.

ISO (International Organization for Standardization). Organización internacional para la normalización que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a red. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de red.

ISP (Internet Service Provider). Proveedor de Servicios de Internet, empresa dedicada a conectar a Internet la línea telefónica de los usuarios, redes distintas e independientes, ambas.

L2F (Layer 2 Forwarding) fue diseñado para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas.

L2TP (Layer 2 Tunneling Protocol) fue diseñado para corregir las deficiencias de los protocolos protocolos PPTP y L2Fy establecerse como un estándar aprobado por el IETF. L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

LAN (Local Area Network). Red de área local de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos,

terminales y otros dispositivos en un único edificio u otra área geográficamente limitada

LAN VIRTUAL. Véase VLAN.

LASER. Dispositivo de amplificación de luz por emisión estimulada de radiación. Los láseres son aparatos que amplifican la luz y producen haces de luz coherente; su frecuencia va desde el infrarrojo hasta los rayos X.

LDAP (Lightweight Directory Access Protocol). Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet.

LLC. Control de enlace lógico. La más alta de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa LLC maneja el control de errores, el control de flujo, el entramado y el direccionamiento de subcapa MAC. El protocolo LLC que más prevalece es IEEE 802.2, que incluye tanto la variante sin conexión como la orientada a conexión.

LOGIN. Identificación de usuario y contraseña para acceder a otro ordenador.

MAINFRAMES. Los mainframes son grandes, rápidos y caros sistemas que son capaces de controlar cientos de usuarios simultáneamente, así como cientos de dispositivos de entrada y salida.

MAN (Metropolitan Area Network). Red de área metropolitana que abarca un área metropolitana. En general, una MAN abarca un área geográfica más vasta que una LAN, pero cubre un área geográfica más pequeña que una WAN.

MAC. Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos, por ejemplo, si se utilizará token passing o contención.

MASCARA DE SUBRED. Se utiliza para enmascarar toda o parte de la dirección IP que se utiliza en una dirección de subred.

MASCARA DE RED. Se utiliza para enmascarar una parte de la dirección IP para distinguir el ID de red y la ID de host

MDI. Interfaz dependiente de los soportes. Cable utilizado para las estaciones finales.

MDIX. Interfaz dependiente de los soportes con cable cruzado (MDIX) que se utiliza con los concentradores y conmutadores.

MEDIO DE TRANSMISION. Son el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos y pueden ser dos tipos de medios, guiados y no guiados

MEDIOS GUIADOS. Son aquellos que utilizan unos componentes físicos y sólidos para la transmisión de datos. También conocidos como medios de transmisión por cable.

MEDIOS NO GUIADOS. Los medios no guiados o sin cable utilizan el espacio para la transmisión de datos.

MEMORIA CACHE. La memoria caché se utiliza para mantener una copia en su disco duro de las páginas de Internet visitadas recientemente. Esta funcionalidad reduce el tiempo de carga de las páginas que usted visita con mayor frecuencia.

MEMORIA RAM. Se trata de una memoria de semiconductor en la que se puede tanto leer como escribir. Es una memoria volátil, es decir, pierde su contenido al desconectar la energía eléctrica. Se utiliza normalmente como memoria temporal para almacenar resultados intermedios y datos similares no permanentes.

MICROONDAS. Son ondas de radio de alta frecuencia y por consiguiente de longitud de onda muy corta tienen muchas aplicaciones, radio y televisión, radares, meteorología, comunicaciones vía satélite, medición de distancias, investigación de las propiedades de la materia o cocinado de alimentos.

MODEM. Modulador-desmodulador. Dispositivo que convierte señales digitales y análogas. En el punto de origen, un módem convierte señales digitales a una forma apropiada para la transmisión por facilidades de comunicación análogas. En el punto de destino, las señales análogas se recuperan a su forma digital. Los módem permiten la transmisión de datos por líneas telefónicas de grado voz.

MODULACION. Engloba el conjunto de técnicas para transportar información sobre una onda portadora, típicamente una onda senoidal. Estas técnicas permiten un mejor aprovechamiento del canal de comunicación lo que permitirá transmitir más información simultánea y/o proteger la información de posibles interferencias y ruidos.

MOTHER BOARD. Es un circuito integrado con varios microchips y diferentes tipos de ranuras y conectores. En ella se conectan todos los componentes del computador incluyendo el procesador.

MTU (Maximum Transfer Unit). Unidad Máxima de Transferencia de datos, es un término informático que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.

MULTICAST. Transmite copias de un único paquete a varios puertos.

MULTIMETRO. También denominado polímetro, es un instrumento electrónico de medida que combina varias funciones en una sola unidad. Las más comunes son las de voltímetro, amperímetro y ohmetro.

MULTIPLEXACION. Técnica que permite la transmisión de varias señales lógicas simultáneamente a lo largo de un único canal físico.

MULTIPLEXACIÓN POR DIVISIÓN DE FRECUENCIA (FDM), es un tipo de multiplexación utilizada generalmente en sistemas de transmisión analógicos. Mediante este procedimiento, el ancho de banda total del medio de transmisión es dividido en porciones, asignando cada una de estas fracciones a un canal.

NetB1OS/NetBEU1. Protocolo de red originalmente creado para redes locales de computadoras IBM PC. NetBIOS engloba un conjunto de protocolos de nivel de sesión, que proveen 3 tipos de servicios, servicio de nombres, servicio de paquetes y servicio de sesión.

NETID. Es el Identificador de dirección de red.

NIC (Network Interface Card). Tarjetas de Interfaz de Red, es un dispositivo electrónico que permite a un ordenador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom etc). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, etc.), pero, actualmente el más común es del tipo Ethernet utilizando un interfaz o conector RJ45.

NNTP (Network News Transfer Protocol). Protocolo de transferencia de noticias basado en tiras de textos envíados sobre canales TCP de 7 bit ASCII . Es usado para subir y bajar así como para transferir artículos entre servidores.

NODO. Punto final de conexión de red o unión común para varias líneas de red. Los nodos pueden ser, procesadores, controladoras o estaciones de trabajo

NRZ (non return to-zero). Código sin retorno a cero. Las señales NRZ mantienen niveles de tensión constantes, sin transiciones de señal (sin retorno a un nivel de tensión cero) durante un intervalo de bit.

NRZ-I (non return to zero, invert on ones). Código sin retorno a cero invertido. Las señales NRZ mantienen niveles de tensión constantes, sin transiciones de señal (sin retorno a un nivel de tensión cero), pero interpretan la presencia de datos al comenzar un intervalo de bit como una transición de señal, y la falta de datos como una falta de transición.

MULTICAST. Paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.

NODO. Punto final de una conexión de red, o unión común a dos o más líneas en una red. Los nodos pueden ser procesadores, controladores, o estaciones de trabajo. Los nodos, que pueden variar según su capacidad de enrutamiento y otras capacidades funcionales, pueden estar interconectados por enlaces, y servir como puntos de control en la red. El término nodo se emplea a veces de

modo genérico para indicar cualquier entidad que puede tener acceso a una red, y es utilizado a menudo en forma intercambiable con dispositivo.

OCTETO. Se describe como la unidad básica de almacenamiento de información, generalmente equivalente a ocho bits, pero el tamaño del byte depende del código de información en el que se defina.

ONDA ELECTROMAGNETICA. Son aquellas ondas que no necesitan un medio material para propagarse. Incluyen, entre otras, la luz visible y las ondas de radio, televisión y telefonía. Todas se propagan en el vacío a una velocidad constante, muy alta (300 0000 km/s) pero no infinita. Las ondas electromagnéticas se propagan mediante una oscilación de campos eléctricos y magnéticos. Los campos electromagnéticos al "excitar" los electrones de nuestra retina, nos comunican con el exterior y permiten que nuestro cerebro "construya" el escenario del mundo en que estamos.

ORDENADOR. También llamado computadora, es un sistema digital con tecnología microelectrónica capaz de procesar información a partir de un grupo de instrucciones denominado programa. La estructura básica de una computadora incluye microprocesador (CPU), memoria y dispositivos de entrada/salida (E/S), junto a los buses que permiten la comunicación entre ellos.

OSI (Open Systems Interconnection). Interconexión de sistemas abiertos. Programa de estandarización internacional creado por ISO e ITU-T para desarrollar normas para red de datos que faciliten la interoperabilidad entre equipos de diversos fabricantes.

OSPF (Open Shortest Path First). Significa "primero la ruta libre más corta", este protocolo de pasarella interior en realidad usa varios criterios para determinar cuál es la mejor ruta hacia un destino. Entre estos criterios se incluyen las métricas de costo, que influyen en elementos tales como velocidad, tráfico, confiabilidad y seguridad de la ruta.

OUI. Identificador único de la organización, es un término que refiere a un número 24-bit asignado incluyendo a una compañía u organización para el uso en varios productos del hardware, de Ethernet de interfaz de la red tarjetas y los adaptadores del autobús del anfitrión del canal de la fibra. Para el uso de Ethernet, el OUI se combina con un número interno-asignado 24-bit para formar un MAC ADDRESS.

PAQUETE. Agrupamiento lógico de información que incluye un encabezado que contiene información de control y datos del usuario.

PATCH-PANELS. Un conjunto de pins y puertos que pueden ser montados en un bastidor o ménsula de pared en el armario de cableado. Los patch panels actúan como tableros de conmutación que conectan los cables de las estaciones de trabajo unos con otros y con el exterior.

PDU (Protocol Datagram Unit). Unidad de datos de protocolo, Unidad de datos especificada en un protocolo de capas que consta de información de control de protocolo y datos de usuarios de la capa.

PING. Protocolo que permite descubrir si una estación está activa.

POLARIDAD. Se refiere a los polos positivos y negativos que utiliza la corriente continua, esto es, los aparatos de corriente continua no suelen incorporar protecciones frente a un eventual cambio de polaridad, lo que puede acarrear daños irreversibles en el aparato. Para evitarlo, y dado que la causa del problema es la colocación inadecuada de las baterías, es común que los aparatos incorporen un diagrama que muestre cómo deben colocarse. Así mismo, los contactos se distinguen empleándose, convencionalmente, un muelle metálico para el polo negativo y una placa para el polo positivo.
POP3 (Post Office Protocol). Tercera versión del protocolo diseñado para la gestión, el acceso y la transferencia de mensajes de correo electrónico entre dos máquinas, habitualmente un servidor y una máquina de usuario.Los servidores POP3 permiten tener acceso a una sola bandeja de entrada a diferencia de los servidores IMAP, que proporcionan acceso a múltiples carpetas en los servidores.
PORTADORA. Onda principal en la que la amplitud o la frecuencia se sujeta por una modulación para el seguimiento de las variaciones de una señal audio o vídeo o de otra oscilación.

PPTP(Point-to-Point Tunneling Protocol). Es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

PPP. Protocolo punto a punto. Un sucesor de SLIP, PPP brinda conexiones router a router y host a red sobre circuitos síncronos y asíncronos.

PROXY ARP. Veáse ARP proxy

PSK (Phase-Sliift Keying). Técnica en la cual los dos valores binarios se representan desplazando la fase de la portadora. Un 1 binario se representa con una señal cuya fase es opuesta a la fase de la señal que le precede y para un O binario la fase de la señal es la mirna que la fase de la señal precedente.

PROCESADOR. Onda principal en la que la amplitud o la frecuencia se sujeta por una modulación para el seguimiento de las variaciones de una señal audio o vídeo o de otra oscilación.

PROTOCOLO. Conjunto de reglas que rige cómo los dispositivos intercambian información a través de las redes.

PUENTE. Dispositivo que conecta dos redes. Los puentes son específicos del hardware, aunque son independientes del protocolo. Los puentes funcionan en los niveles de la capa 1 y de la capa

PUERTO. Los puertos físicos proporcionan componentes de conexión que permiten a los microprocesadores comunicarse con los equipos periféricos.

QoS. Calidad de servicio que permite a los administradores de red decidir qué tráfico de red se reenvía y cómo se reenvía en función de las prioridades, tipos de aplicación y direcciones de origen y destino.

RACK. Es un gabinete metálico donde se colocan los dispositivos de red para tener un mayor control y orden.

RADIOFRECUENCIA. Se aplica a la porción del espectro electromagnético en el que se pueden generar ondas electromagnéticas aplicando corriente alterna a una antena.

RADIUS (Remote Authentication Dial-In User Service) Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISPs). Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

RAL. Redes de Area Local Inalámbricas.

RAM DINAMICA (DRAM). Tipo de memoria de semicounductor que almacena datos como cargas en capacitares que necesitan regenerarse de manera periódica.

RAM ESTATICA (SRAM). RAM de semiconductor que guarda información en celdas formadas por slip-flops y que no necesita de un refresco periódico.

RARP(Reverse Address Resolution Protocol). Protocolo de Resolución de Direcciones en Reversa asigna direcciones físicas MAC a direcciones lógicas IP.

RDSI. Red Digital de Servicios Integrados, es una red que procede de lar evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

RJ. Conector tipo ficha registrado. Conectores estándar normalmente empleados para conectar las líneas telefónicas. Los conectores RJ se utilizan actualmente para las conexiones telefónicas y 10BaseT como así también para otros tipos de conexiones de red. RJ-11, RJ-12, y RJ-45 son algunos de los tipos de conectores RJ más difundidos.

RJ-45. Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorias 4, 5, 5e y 6).

ROUTERS. Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los routers envían paquetes de una red a otra en base a la información de capa de red.

SAP (Service Access Point). Puntos de acceso al Servicio, interfaz física a través de los cuales los niveles de orden más bajo en el modelo OSI proveen servicios a los de mayor orden

SEÑAL ANALOGICA. Se dice que una señal es analógica cuando las magnitudes de la misma se representan mediante variables continuas; esto es, análogas a las magnitudes que dan lugar a la generación de esta señal.

SEÑAL DIGITAL. Se dice que una señal es digital cuando las magnitudes de la misma se representan mediante valores discretos en lugar de variables continuas.

SEÑALIZACION. Proceso que consiste en enviar una señal de transmisión sobre un medio físico a los fines de la comunicación.

SERVICIO ORIENTADO A CONEXIÓN. Es un servicio semejante al modelo telefónico ya que el emisor y el receptor establecen una conexión, la usan y después la liberan. Es un servicio confiable debido a que el receptor acusa cada mensaje recibido, de tal forma que el emisor esta seguro de que éste fue entregado.

SERVICIO ORIENTADO A NO CONEXIÓN. Es un servicio similar al sistema postal, donde cada carta lleva la dirección completa de destino, las cuales se pueden encaminar en el sistema de manera independiente, así que, si dos mensajes se envían al mismo destino pueden llegar de manera desordenada en comparación de cómo fueron enviados.

SERVIDOR. Equipo central que proporciona servicios a otros equipos de una red. Entre los servicios se incluyen el almacenamiento de archivos y el acceso a aplicaciones.

SFTP (Simple File Transfer Protocol). Es un protocolo que permite establecer conexiónes seguras para transferencia de archivos. A diferencia de FTP, SFTP facilita un canal de datos encriptado.

SINCRONIZACION. Establecimiento de un intervalo de tiempo constante entre cada evento.

SMDS (Switched Multi-megabit Data Service), servicio de conmutación de datos de varios megabits, es una red WAN pública, que extiende los servicios de las redes LAN y MAN. Su objetivo primordial es el de proporcionar conectividad para MAN's, subredes FDDI, y redes LAN privadas, de modo que compartir los datos sea tan fácil como realizar una llamada telefónica, y soportando tanto datos como voz y vídeo.

SNMP (Simple Network Manage Protocol). Protocolo Simple de Administración de Redes que Gestiona las LAN. El software basado en SNMP se comunica con los dispositivos que disponen de agentes SNMP incorporados. Los agentes SNMP recopilan información de la actividad de la red y del estado del dispositivo y la envían de vuelta a una estación de trabajo.

SMTP (Simple Mail Transfer Protocol/Protocolo Simple de Transferencia de correo) Protocolo de la suite TCP/IP del nivel de aplicación que permite la transferencia de correo electrónico Acrónimo

SNAP (Sub-Network Access Protocol), Protocolo de Acceso a la Subred de Internet que opera entre una entidad de red de la subred y una entidad de red en el sistema extremo. SNAP especifica un método estándar de encapsulación de datagramas IP y mensajes ARP por las redes IEEE. La entidad SNAP del sistema extremo utiliza estos servicios de la subred y realiza tres funciones clave: transferencia de datos, gestión de conexión y selección de QOS.

SOCKET. Estructura de software que opera como punto extremo de comunicaciones dentro de un dispositivo de red.

SOFTWARE. Es el nombre que se le da a todo aquel componente que forma parte de una computadora de manera logica

SQL (Structured Query Lenguaje). El Lenguaje de consultas estructurado es una herramienta para organizar, gestionar y recuperar datos almacenados en una base de datos informática. Es un lenguaje informático que se puede utilizar para interaccionar con una base de datos y más concretamente con un tipo especifico llamado base de datos relacional.

SSAP (Source Service Acces Point). Punto de acceso al servicio origen, SAP del nodo de la red designado en el campo origen de un paquete.

SSH (Secure Shell Remote Login Protocol). Shell seguro que Inicia una sesión en un equipo remoto a través de una red, ejecuta comandos y transfiere archivos de un equipo a otro.

SUBCAPA. Es una capa dentro de otra capa.

SUBDOMINIOS. Es un dominio dentro de un dominio. Esto quiere decir: por ejemplo, dominio igarcom.com subdominio secure.igarcom.com; aquí podemos ver que secure es un dominio dentro del dominio igarcom.com. De estos subdominios puede tener ilimitados y no necesitan ser registrados. El control lo realizará mediante el panel de control que IGARCOM pone a su disposición al contratar el servicio.

SUBRED. Son redes segmentadas arbitrariamente por un administrador de red para brindar una estructura de enrutamiento multinivel, jerárquico, protegiendo a la subred de la complejidad del direccionamiento de las redes conectadas. Las subredes comparten un componente de dirección común

SWITCH. Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de datos del modelo OSI.

T1. Facilidad de portadora de WAN digital. T1 transmite datos formateados en DS1 a 1,544 Mbps por la red de conmutación telefónica, mediante una codificación AMI o B8ZS.

TARJETAS DE RED. Véase NIC.

TCP (Transmission Control Protocol). Protocolo de Control de la Transmisión de la capa de transporte encargado de dividir el mensaje original en datagramas de menor tamaño, que son más manejables.

TCP/IP. Protocolo de control de transmisiones. Permite a dos sistemas principales comunicarse e intercambiar corrientes de datos. El TCP garantiza la entrega de los paquetes y que éstos se transmitan y reciban en el orden en que se envían.

TFTP (Trivial File Transfer Protocol). Protocolo trivial de transferencia de archivos que utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

TELNET Protocolo de la suite TCP/IP del nivel de Aplicación de emulación de terminal. Permite a los usuarios del sistema iniciar una sesión y utilizar los recursos de redes remotas.

TERMINAL. Dispositivo simple donde se pueden ingresar o recuperar datos de una red. En general, las terminales tienen un monitor y un teclado, pero no tienen procesador ni unidad de disco local.

TOKEN. Frame (trama) que contiene información de control. La posesión de token permite a un dispositivo de red transmitir datos por la red.

TOKEN RING. LAN token passing desarrollada y soportada por IBM. Token Ring corre a 4 ó 16 Mbps por una topología de anillo. Similar a IEEE 802.5.

TOPOLOGIA. Disposición física de nodos y medios de red dentro de una estructura de red empresarial.

TOPOLOGIA ANILLO. Conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

TOPOLOGIA ARBOL. Topología LAN similar a la topología de bus, excepto que las redes en árbol pueden contener ramificaciones con múltiples nodos. Las transmisiones desde una estación se propagan a lo largo del medio, y son recibidas por todas las otras estaciones.

TOPOLOGIA BUS. Usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

TOPOLOGIA ESTRELLA. Conecta todos los cables con un punto central de conexión.

TOPOLOGIA ESTRELLA EXTENDIDA. Conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

ESTRELLA JERÁRQUICA. Similar a una estrella extendida. pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

TOPOLOGIA FISICA. Define la disposición real de los cables o medios, la manera en como están conectados los equipos físicamente.

TOPOLOGIA LOGICA. Define la forma en que los hosts acceden a los medios para enviar datos.

TOPOLOGIA MALLA. Cada host tiene sus propias conexiones con los demás hosts

TRAMA. Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

TRANSCEPTOR. Es un dispositivo que realiza, dentro de una misma caja o chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones. Dado que determinados elementos se utilizan tanto para la transmisión como para la recepción, la comunicación que provee un transceptor solo puede ser semiduplex, lo que significa que pueden enviarse señales entre dos terminales en ambos sentidos, pero no simultáneamente

TTL (Time To Live). Tiempo de existencia, Campo en un encabezado IP que indica el tiempo que se considera válido un paquete .

UDP (User Datagram Protocol). Protocolo de Datagrama de Usuario del nivel de transporte no orientado a la conexión. Transmite paquetes pero no garantiza su entrega.

URL (Universal Resource Locutor). Localizador universal de recursos. Esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y demás servicios a través de un explorador WWW.

UTP (unshielded twisted pair). Par trenzado sin blindaje. Medio de cables de cuatro pares utilizado en varias redes. UTP no requiere de un espacio fijo entre conexiones que sí es necesario con las conexiones de tipo coaxial. Hay cinco tipos de cableados UTP de uso común: cableado de categoría 1, cableado de categoría 2, cableado de categoría 3, cableado de categoría 4, y cableado de categoría 5.

VLAN. Redes de área local virtual. Subgrupos lógicos de una red de área local (LAN) creados utilizando software en lugar de una definición de solución de hardware.

VPN. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WAN (Wide Area Network). Red de área amplia de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

WAP (Wireless Protected Access). Protocolo de aplicación de tecnología inalámbrica que posibilita el acceso a páginas web especialmente diseñadas para este lenguaje y está disponible en versiones 1.1 y 2.0.
WEP (Wireless Encryption Protocol). Proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red.

X.25. Estándar ITU-T que define cómo se mantienen las conexiones entre DTE y DCE para el acceso a terminales remotas y las comunicaciones entre computadores en PDNs. X.25 especifica LAPB, un protocolo de capa de enlace de datos, y PLP, un protocolo de capa de red. Frame Relay ha reemplazado en cierta medida a X.25.

xDSL. DSL(Digital Subscriber Line). Línea de abonado digital es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica local: ADSL, ADSL2, ADSL2+ SDSL, IDSL, HDSL y VDSL.Tienen en común que utilizan el par trenzado de hilos de cobre convencionales de las líneas telefónicas para la transmisión de datos a gran velocidad.

BIBLIOGRAFIA

ROUTER CISCO
JOE HABRAKEN
PEARSON EDUCATION

LOCAL AREA NETWORK
JAMES MARTIN
PRENTICE HALL

REDES DE COMPUTADORAS
ANDREW. S. TANENBAUM
PEARSON EDUCATION

COMUNICACIONES Y REDES DE COMPUTADORAS
WILLIAM STALLING
PRENTICE HALL

WWW.CISCO.COM
WWW.3COM.COM