

**DISEÑO E IMPLEMENTACIÓN DE UNA RED DE ÁREA LOCAL EN LOS
LABORATORIOS DE ELECTRÓNICA DIGITAL, TELECOMUNICACIONES Y
CONTROL AUTOMÁTICO DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**

ARGEMIRO RAFAEL BERMÚDEZ GUERRERO

MOISÉS BLANCO APARICIO



FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA ELECTRÓNICA

CARTAGENA D.T. Y C.

2005

**DISEÑO E IMPLEMENTACIÓN DE UNA RED DE ÁREA LOCAL EN LOS
LABORATORIOS DE ELECTRÓNICA DIGITAL, TELECOMUNICACIONES Y
CONTROL AUTOMÁTICO DE LA UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**

**ARGEMIRO RAFAEL BERMÚDEZ GUERRERO
MOISÉS BLANCO APARICIO**

**Monografía para optar al título de
Ingeniero Electrónico**

Director:

**Ing. HAROLD GOMEZ
Ingeniero Electrónico**



**FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA ELECTRÓNICA
CARTAGENA D.T. Y C.**

2005

TABLA DE CONTENIDO

	Pág.
INTRODUCCIÓN	
1. MODELO DE REFERENCIA OSI	3
1.1. CAPA FÍSICA	4
1.2. CAPA DE ENLACE DE DATOS	6
1.3. CAPA DE RED	8
1.4. CAPA DE TRANSPORTE	9
1.5. CAPA DE SESIÓN	10
1.6. CAPA DE PRESENTACIÓN	11
1.7. CAPA DE APLICACIÓN	13
2. SUITE DE PROTOCOLOS TCP/IP	14
2.1. COMANDOS TCP/IP	18
2.2. PROTOCOLOS TCP/IP	19
2.3. CÓMO FUNCIONA TCP/IP	20
2.4. LA DIRECCIÓN IP	26
2.5. IPv6	30
3. RED DE ÁREA LOCAL	32
3.1. MÉTODOS DE ACCESO AL MEDIO	32
3.2. MÉTODOS DE TRANSMISIÓN	33
3.3. TOPOLOGÍAS	34

3.4.	EL TRÁFICO	37
3.5.	ETHERNET/802.3	37
3.5.1.	Estructura del protocolo	40
4.	SISTEMAS DE CABLEADO ESTRUCTURADO	44
4.1.	REQUERIMIENTOS PARA LA CONEXIÓN FÍSICA	48
4.2.	ESQUEMA DE COLORES ESTÁNDAR PARA CABLES UTP	55
4.3.	ESTÁNDARES	54
4.4.	ÁREA DE TRABAJO	54
4.5.	CABLEADO HORIZONTAL	55
4.6.	CABLEADO VERTICAL	59
5.	DISEÑO DE LA RED	58
5.1.	DISEÑO SOBRE EL PLANO	61
5.2.	CANTIDADES Y ELEMENTOS	62
6.	COSTOS DE IMPLEMENTACIÓN	60
6.1.	COMPRA DE MATERIALES	60
6.2.	COTIZACIÓN	60
6.2.1.	Mano de obra	60
6.2.2.	Alquiler de herramientas	61
6.2.3.	Otros suministros	61
6.3	COSTOS POR ÁREAS	61
	BIBLIOGRAFÍA	64
	ANEXOS	65

ÍNDICE DE FIGURAS

	Pág.
Figura 1. Estructura de capas del Modelo OSI	3
Figura 2. SASEs y CASEs	13
Figura 3. Arquitectura TCP/IP	17
Figura 4. Formato de cabecera de un datagrama	20
Figura 5. Formato de cabecera de TCP	24
Figura 6. Direcciones IP de Internet	28
Figura 7. Organización de la cabecera IPv6	31
Figura 8. Topología tipo bus	35
Figura 9. Topología tipo anillo	35
Figura 10. Topología tipo estrella	36
Figura 11. Topología bus-estrella	36
Figura 12. Ejemplo de una red ethernet	37
Figura 13. Estructura de trama ethernet	40
Figura 14. Estructura de la dirección de destino	41
Figura 15. Estructura de la dirección fuente	42
Figura 16. Especificaciones de desempeño del panel de parcheo	51
Figura 17. Esquema de colores según T568A o T568B	52
Figura 18. Esquema de colores tipo A	53
Figura 19. Esquema de colores tipo B	54
Figura 20. Plano del área de trabajo	58
Figura 21. Trazado del diseño	58

INTRODUCCIÓN

En el mundo del aprendizaje de hoy, el acceso confiable y eficiente a la información se ha convertido en un elemento importante y determinante en la búsqueda de alcanzar ventajas competitivas sobre otros estudiantes. Así como compañeros de trabajo separados por miles de kilómetros pueden compartir información corporativa instantáneamente, hombres de negocios pueden realizar transacciones millonarias a distancia y al instante, científicos ubicados en diferentes países del mundo trabajan en equipo y logran grandes avances tecnológicos; también se hace indispensable que los estudiantes podamos acceder a información confiable y de alta calidad con fines investigativos, a distancia. En países llamados desarrollados existen grandes avances en tecnologías de la información, el conocimiento es principio y fin de su alto nivel de desarrollo científico, económico y tecnológico. Los diferentes grados de profundización de la investigación nos separan de ellos.

Los estudiantes de Ingeniería Electrónica de nuestra Universidad (Tecnológica de Bolívar), poseemos una gran debilidad: subutilizar los laboratorios de Electrónica Digital, Telecomunicaciones y Control Automático.

El laboratorio de electrónica digital, actualmente cuenta con computadores que no están en red, ni tienen acceso a internet. Además, se hace uso en los mismos, de programas (software) para los cuales no se cuenta con licencia del fabricante. En situación similar se encuentra el laboratorio de control automático. El laboratorio

de telecomunicaciones, no cuenta con computadores, pero en un futuro cercano los podría tener.

Se hace necesario entonces, realizar ingentes esfuerzos para eliminar rápidamente esta debilidad y convertirla en una fortaleza que nos ayude a competir con los mejores.

Una buena forma de eliminar nuestras debilidades es con nuestras propias fortalezas: la gran capacidad y el buen nivel de conocimiento de nosotros los estudiantes para el diseño de redes. Pretendemos que haya una red que integre laboratorios con las facilidades (herramientas) que merecen ellos y sus usuarios, posibilitar el acceso a Internet (fuente de grandes cantidades de información valiosa para el crecimiento y fortalecimiento del conocimiento de los estudiantes), así como a la intranet de la Universidad. De esta manera, la Universidad podrá hacer un importante aprovechamiento de los recursos: una red de computadores dotada con facilidad de acceso tanto a la intranet de la Universidad Tecnológica de Bolívar como a la gran red Internet; además, estas estaciones de trabajo utilizarían el software legal instalado en el servidor de estas. Así mismo, se entregarían puntos de telecomunicaciones (para acceso a dicha red) en el laboratorio de telecomunicaciones; teniendo en cuenta la normatividad del cableado estructurado en dicha red.

1. MODELO DE REFERENCIA OSI

El modelo OSI (Open Systems Interconnection) de telecomunicaciones está basado en una propuesta desarrollada por la organización de estándares internacional (ISO), por lo que también se le conoce como modelo ISO - OSI. Su función es la de definir la forma en que se comunican los sistemas *abiertos* de telecomunicaciones, es decir, los sistemas que se comunican con otros sistemas.

El modelo de referencia consiste en 7 capas. Estas capas se visualizan generalmente como un montón de bloques apilados (stack of blocks), donde solo las capas que tengan otra capa equivalente en el nodo remoto podrán comunicarse.

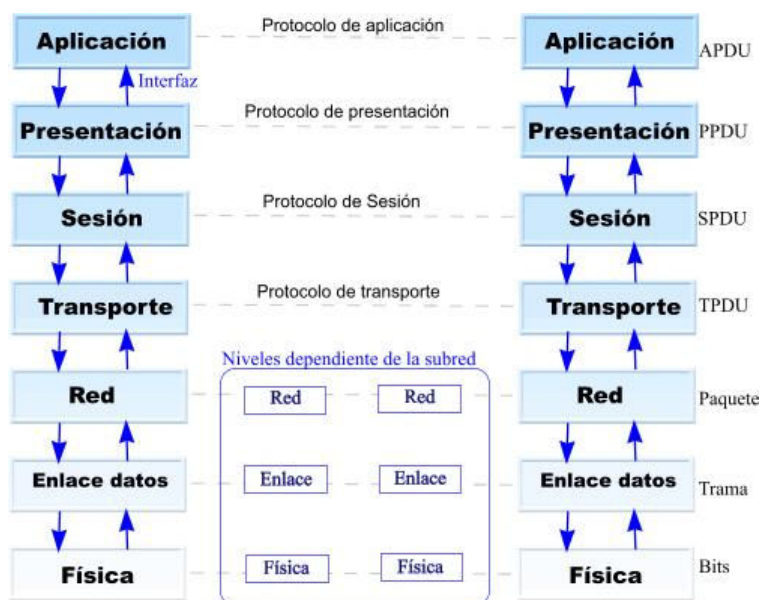


Figura 1. Estructura de capas del Modelo OSI

El protocolo de cada capa solo se interesa por la información de su capa y no por la de las demás, la información se pasa a las capas de abajo hasta que la información llega a la red. En el nodo remoto, la información es entonces pasada hacia arriba hasta que llega a la aplicación correspondiente. Cada capa confía en que las demás harán su trabajo, una capa no se interesa por el funcionamiento de las demás, lo único que es de interés es la forma en como los datos serán pasados hacia arriba o hacia abajo entre las capas.

1.1 CAPA FÍSICA

El nivel físico, o primer nivel del modelo OSI, se preocupa de todos los problemas relacionados con la transmisión de la señal que lleva la información, esta puede ser enviada a través de los medios de transmisión modificando alguna propiedad física del mismo.

Una *señal analógica* representa una onda electromagnética que varía de forma continua. Dependiendo de su espectro, las señales analógicas pueden transmitirse por una amplia variedad de medios (cables como el par trenzado, la fibra óptica, etc.).

Una *señal digital* es una secuencia de pulsos de voltaje que pueden transmitirse por medio de un cable; por ejemplo, un nivel de voltaje positivo constante puede representar el uno binario y un nivel de voltaje negativo puede representar el cero binario.

La transmisión de una señal supone el paso de la misma a través de un determinado medio, pero debido a diferentes fenómenos físicos, la señal que llega al receptor difiere de la emitida por el transmisor. Algunos problemas que afectan la transmisión son: La *atenuación*, la *distorsión*, el *retardo de propagación*, la *diafonía*, paradiafonía y telediafonía, las pérdidas de retorno (RL),

La *atenuación* consiste en el debilitamiento o pérdida de amplitud de la señal recibida frente a la transmitida. A partir de una determinada distancia, la señal recibida es tan débil que no se puede reconocer mensaje alguno. La solución a este problema la encontramos en el uso de repetidores (caso de señales digitales) o amplificadores (señales continuas).

Todas las señales van a tardar un cierto tiempo en recorrer la distancia que separa al emisor del receptor. Además, si en el camino la señal atraviesa determinados circuitos electrónicos, eléctricos, ópticos o de cualquier otra naturaleza, estos pueden añadir un *retardo* adicional.

La *diafonía* (crosstalk) es un fenómeno que todos hemos experimentado en las comunicaciones telefónicas. Consiste en la interferencia de un canal (par) próximo con el nuestro, esto produce una señal que es la suma de la señal transmitida y otra señal externa atenuada que aparece de fondo, generando un ruido mayor que la señal deseada y a su vez un incremento importante en la tasa de errores por bit (BIT ERROR RATE), esto para mencionar el fenómeno de interferencia cercano

llamado NEXT AND CROSSTALK así como el FEXT AND CROSSTALK es el mismo efecto de interferencia pero medido en el extremo lejano.

1.2 CAPA DE ENLACE DE DATOS

El principal propósito de los protocolos de enlace de datos es garantizar que la comunicación entre dos máquinas directamente conectadas está libre de errores. Para conseguir este objetivo, habitualmente se estructura la información a transmitir en pequeños bloques de datos, cada uno de los cuales lleva asociado un código detector de error y un número de secuencia. Dichos bloques se envían de forma secuencial y si uno de ellos sufre un error será reenviado por el transmisor. Se consigue así que un error no implique la retransmisión de todo el mensaje, sino sólo una pequeña parte del mismo.

El nivel de enlace de datos tiene un número de funciones específicas por desarrollar:

- Proporcionar un servicio bien definido al nivel superior (de red).
- Agrupar los bits o caracteres recibidos por el nivel físico en bloques de información, tramas (frames), a los que va asociada información de control para proporcionar los servicios.
- Detectar y solucionar los errores generados en el canal de transmisión.
- Control de flujo, para evitar saturar al receptor.
- Control de diálogo, en canales semi - dúplex será necesario establecer los turnos de transmisión.

El nivel de enlace de datos puede ser diseñado para ofrecer diferentes clases de servicios.

La clase de servicio puede variar de un sistema a otro. Las tres posibilidades más populares son:

- *Servicio sin conexión y sin acuse:* Consiste en hacer que la máquina fuente mande tramas a la máquina destino sin que esta última tenga que reconocerlas. No se establece ninguna conexión (o acuerdo previo) antes de la transmisión de los datos.
- *Servicio sin conexión pero con acuse:* Significa que por cada trama que manda, espera que le llegue un reconocimiento. De esta manera, el emisor sabe si la trama ha llegado satisfactoriamente. Si no llega el reconocimiento correspondiente pasado un tiempo determinado desde la emisión de la trama, el emisor asume que su trama no llegó o llegó dañada y la retransmite.
- *Servicio con conexión:* Con este servicio las máquinas fuente y destino establecen una conexión antes de transmitir los datos. Cada trama que se envía, sobre la conexión establecida, se numera y el nivel de enlace garantiza que cada trama se recibe una sola vez y que se reciben en el orden correcto.

1.3 CAPA DE RED

El nivel de red enruta los paquetes de la fuente al destino final a través de enrutadores intermedios. Tiene que saber la topología de la subred, evitar la congestión, y manejar los casos cuando la fuente y el destino están en redes distintas.

El nivel de red normalmente es la interfaz entre el portador y el cliente. Sus servicios son los servicios de la subred.

- *Sin conexión* (Internet). La subred no es confiable; porta bits y no más. Los hosts tienen que manejar el control de errores. El nivel de red ni garantiza el orden de paquetes ni controla su flujo. Los paquetes tienen que llevar sus direcciones completas de destino.
- *Orientado a la conexión* (sistema telefónico). Los pares en el nivel de red establecen conexiones con características tal como la calidad, el costo, y el ancho de banda. Se entregan los paquetes en orden y sin errores, la comunicación es dúplex, y el control de flujo es automático.

El punto central en este debate es donde ubicar la complejidad. En el servicio orientado a la conexión está en el nivel de red, pero en el servicio sin conexión está en el nivel de transporte. Se representan los dos enfoques en los ejemplos de la Internet y ATM. La estructura interna de la subred es la siguiente:

- *Circuitos virtuales*. Dentro de la subred normalmente se llama una conexión un circuito virtual. En un circuito virtual uno evita la necesidad de elegir una ruta

nueva para cada paquete. Cuando se inicializa la conexión se determina una ruta de la fuente al destino que es usada por todo el tráfico.

- *Datagramas.* Son paquetes que se enrutan independientemente. Los enrutadores tienen solamente las tablas que indican qué línea de salida usar para cada enrutador de destino posible. (Se usan estas tablas en los circuitos virtuales también, durante la inicialización de un circuito.) Cada datagrama tiene la dirección completa del destino (estas pueden ser largas). El establecimiento de las conexiones en el nivel de red o de transporte no requiere ningún trabajo especial de los enrutadores.

1.4 CAPA DE TRANSPORTE

El nivel de transporte es el cuarto nivel en el modelo de referencia OSI y su principal objetivo es garantizar una comunicación fiable y eficiente entre dos computadores, con independencia de los medios empleados para su interconexión.

Para conseguir este objetivo se emplea un protocolo de transporte, que regula el intercambio de información entre extremos. En el nivel de transporte aparece, por primera vez, el concepto de comunicación de extremo a extremo. El protocolo de transporte debe conseguir que sea cual sea el medio de comunicación entre ambos extremos, en particular su fiabilidad (que puede no ser muy buena), se pueda asegurar una comunicación fiable entre los extremos.

Por lo tanto, existe una fuerte dependencia entre el servicio de red y el nivel de transporte, puesto que para que el nivel de transporte proporcione un servicio fiable y eficiente deberá tener en cuenta las características del servicio de red y deberá corregir todas las deficiencias que éste pueda presentar utilizando un protocolo de transporte.

Al igual que sucedía en el nivel de red, el servicio de transporte puede ser orientado a la conexión o sin conexión. Puesto que hemos indicado que uno de los objetivos del nivel de transporte es garantizar la fiabilidad de extremos a extremo, resulta difícil conseguirlo proporcionando un servicio sin conexión.

1.5 CAPA DE SESIÓN

A diferencia de lo que ocurre con los protocolos de aplicación del conjunto TCP/IP, que interactúan directamente con los protocolos de la capa de transporte (UDP y TCP), en el modelo de referencia OSI lo hacen a través de las entidades de protocolo asociadas a dos capas intermedias, de sesión y de presentación.

El propósito principal de la capa de sesión en la pila OSI es minimizar los efectos de los fallos en la red durante una transacción de aplicación. En muchas aplicaciones, una transacción puede ocupar un tiempo considerable y requerir la transferencia de una gran cantidad de datos. Un ejemplo sería una base de datos que contuviera un conjunto de cuentas de clientes o expedientes de empleados y que se transfiriera de un proceso de aplicación servidor a un proceso cliente. Si

ocurre un fallo de la red al final de una transferencia como esta, quizá sea necesario repetir la transferencia completa, o varias transferencias de este tipo.

La característica más importante de la capa de sesión es el intercambio de datos. Una sesión, al igual que una conexión de transporte, sigue un proceso de tres fases: la de establecimiento, la de utilización y la de liberación.

Las primitivas que se le proporcionan a la capa de presentación, para el establecimiento, utilización y liberación de sesiones, son muy parecidas a las proporcionadas a la capa de sesión para el establecimiento, uso y liberación de conexiones de transporte. En muchos casos, todo lo que la entidad de sesión tiene que hacer, cuando primitiva es invocada por el usuario de sesión, es invocar la primitiva de transporte correspondiente para que se pueda así realizar el trabajo. En cualquier caso, y a pesar de estas similitudes, existen importantes diferencias entre el intercambio de datos de sesión y el intercambio de datos de transporte. La más importante de estas diferencias es la forma de liberar las sesiones y las conexiones de transporte.

1.6 CAPA DE PRESENTACIÓN

La capa de presentación trata todos los problemas relacionados con la representación de los datos transmitidos, incluyendo los aspectos de conversión, cifrado y compresión de datos. A diferencia de las cinco capas inferiores, que solamente se ocupan del movimiento ordenado de bits desde el extremo fuente al

extremo destinatario, la capa de presentación se encarga de la preservación del significado de la información transportada.

Cada computador puede tener su propia forma de representación interna de los datos, por lo que es necesario tener acuerdos y conversiones para poder asegurar el entendimiento entre computadores diferentes. Estos datos, a menudo toman la forma de estructuras de datos complejas. El trabajo de la capa de presentación consiste precisamente en codificar los datos estructurados del formato interno utilizado en la máquina transmisora, a un flujo de bits adecuado para la transmisión y, después, decodificarlos para representarlos en el formato del extremo destinatario.

La capa de presentación tiene cuatro funciones principales:

1. Ofrecer a los usuarios una manera de ejecutar las primitivas del servicio de sesión.
2. Proporcionar una manera de especificar estructuras de datos complejas.
3. Administrar el conjunto de estructuras de datos que se requieren normalmente.
4. Transformar los datos entre formas internas y externas

1.7 CAPA DE APLICACIÓN

La capa de aplicación permite a los hosts intercambiar información (estructuras de datos) en su propia sintaxis local. Los programas de usuario (procesadores de texto, e-mail, bases de datos, etc.) requieren servicios de transferencia de información especializados. Estos servicios los ofrecen los Elementos de Servicio Específicos de la Aplicación (SASEs).

Los SASEs usan los servicios ofrecidos por los Elementos de Servicio Comunes a las Aplicaciones (CASEs). Un CASE proporciona servicios de transferencia de la información genéricos que son usados por los diferentes SASEs, tales como establecer una conexión (llamada Asociación) entre SASEs en máquinas distintas.

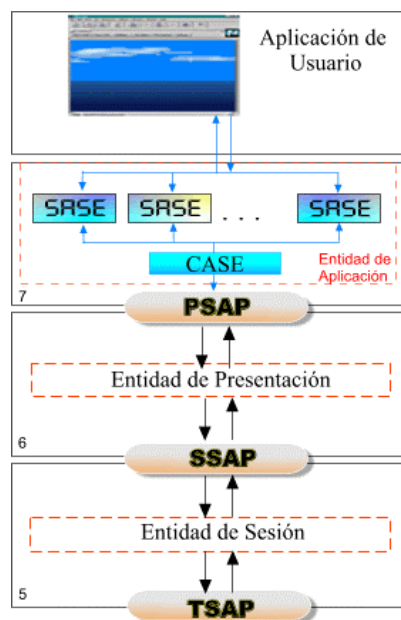


Figura 2. SASEs y CASEs

Un CASE está compuesto por diferentes elementos tales como Elementos de Servicio para Control de Asociación (ACSE), Elementos de Servicio para Operaciones Remotas (ROSE) o elementos de Concordancia (commitment), Concurrencia y Recuperación (CCR).

El ACSE establece la asociación entre SASEs. El ROSE intercambia órdenes y resultados. El CCR descompone la ejecución de operaciones en acciones atómicas y repite las que no se completan satisfactoriamente. La interfaz de usuario adapta las órdenes y respuestas del proceso-aplicación del usuario al SASE. Esta interfaz permite a diferentes programas comerciales trabajar conjuntamente en una red común.

2. SUITE DE PROTOCOLOS TCP/IP

TCP/IP es el protocolo común utilizado por todos los computadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- *Aplicación:* Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- *Transporte:* Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos. La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el software de protocolo de transporte tiene el lado de recepción

enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. La capa de transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel. Para hacer esto, se añade información adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para confirmar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

- *Internet*: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte. La capa Internet maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. La capa Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de enrutamiento para decidir si el datagrama debe procesarse de manera local o debe ser transmitido. Para el caso de los datagramas direccionados hacia la máquina local, el software de la capa de red borra el encabezado del datagrama y selecciona, de entre varios protocolos de transporte, un protocolo con el que manejará el paquete. Por último, la capa Internet envía los mensajes ICMP de error y control necesarios y maneja todos los mensajes ICMP entrantes.

- *Red:* Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc. El software TCP/IP de nivel inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Una interfaz de red puede consistir en un dispositivo controlador (por ejemplo, cuando la red es una red de área local a la que las máquinas están conectadas directamente) o un complejo subsistema que utiliza un protocolo de enlace de datos propios (por ejemplo, cuando la red consiste de conmutadores de paquetes que se comunican con anfitriones utilizando HDLC).
- *Física:* Similar a la capa física del modelo OSI.

FTP, SMTP, TELNET	SNMP, X-WINDOWS, RPC, NFS
TCP	UDP
IP, ICMP, 802.2, X.25	
ETHERNET, IEEE 802.2, X.25	

Figura 3. Arquitectura TCP/IP

TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no

debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de datagrama, y son conjuntos de datos que se envían como mensajes independientes.

2.1 COMANDOS TCP/IP

TCP/IP incluye dos grupos de comandos utilizados para suministrar servicios de red:

- Los comandos remotos BERKELEY
- Los comandos DARPA

Los comandos remotos BERKELEY, que fueron desarrollados en la Universidad Berkeley (California), incluyen órdenes para comunicaciones entre sistemas operativos UNIX, como copia remota de archivos, conexión remota, ejecución de shell remoto, etc. Permiten utilizar recursos con otros hosts, pudiendo tratar distintas redes como si fueran una sola.

Los comandos DARPA incluyen facilidades para emulación de terminales, transferencia de archivos, correo y obtención de información sobre usuarios. Pueden ser utilizadas para comunicación con computadores que ejecutan distintos sistemas operativos.

2.2 PROTOCOLOS TCP/IP

- *FTP* (File Transfer Protocol). Se utiliza para transferencia de archivos.
- *SMTP* (Simple Mail Transfer Protocol). Es una aplicación para el correo electrónico.
- *TELNET*: Permite la conexión a una aplicación remota desde un proceso o terminal.
- *RPC* (Remote Procedure Call). Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- *SNMP* (Simple Network Management Protocol). Se trata de una aplicación para el control de la red.
- *NFS* (Network File System). Permite la utilización de archivos distribuidos por los programas de la red.
- *X-Windows*. Es un protocolo para el manejo de ventanas e interfaces de usuario.

2.3 CÓMO FUNCIONA TCP/IP

IP es sin conexión y está basado en la idea de los datagramas interred, los cuales son transportados transparentemente, pero no siempre con seguridad, desde el hostal fuente hasta el hostal destinatario, quizás recorriendo varias redes mientras viaja.

El protocolo IP trabaja de la siguiente manera; la capa de transporte toma los mensajes y los divide en datagramas, de hasta 64.000 octetos cada uno. Cada datagrama se transmite a través de la red interred, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

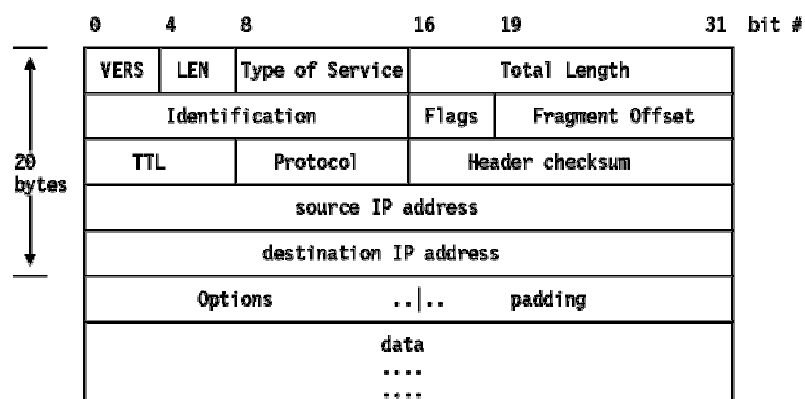


Figura 4. Formato de cabecera de un datagrama

Un datagrama IP consta de una parte de cabecera y una parte de texto. La *cabecera* tiene una parte fija de 20 octetos y una parte opcional de longitud variable. En la figura 4 se muestra el formato de la cabecera. El campo *versión* indica a qué versión del protocolo pertenece cada uno de los datagramas.

Mediante la inclusión de la versión en cada datagrama, no se excluye la posibilidad de modificar los protocolos mientras la red se encuentre en operación.

El campo *opciones* se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información. Esto, básicamente, proporciona un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no está presente en el diseño original. También, para permitir que los experimentadores trabajen con nuevas ideas y para evitar, la asignación de bits de cabecera a información que muy rara vez se necesita.

Debido a que la longitud de la cabecera no es constante, un campo de la cabecera, IHL, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits. El valor mínimo es de 5. El campo *tipo de servicio* le permite al host indicarle a la subred el tipo de servicio que desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Para voz digitalizada, por ejemplo, es más importante la entrega rápida que corregir errores de transmisión. En tanto que, para la transferencia de archivos, resulta más importante tener la transmisión fiable que entrega rápida.

La Longitud total incluye todo lo que se encuentra en el datagrama, tanto la cabecera como los datos. La máxima longitud es de 65.536 octetos (bytes). Tamaño 16 bits.

El campo *identificación* se necesita para permitir que el host destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación. Tamaño 16 bits.

Enseguida viene un bit que no se utiliza, y después dos campos de 1 bit. Las letras DF quieren decir no fragmentar. Esta es una orden para que las pasarelas no fragmenten el datagrama, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente.

Las letras MF significan más fragmentos. Todos los fragmentos, con excepción del último, deberán tener ese bit puesto. Se utiliza como una verificación doble contra el campo de Longitud total, con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

El desplazamiento de fragmento indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8.192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65.536 octetos, que coinciden con el campo *longitud total*. Tamaño 16 bits.

El campo *tiempo de vida (TOS)* es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos. Tamaño 8 bits.

Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitará saber qué hacer con él. El campo *protocolo* indica, a qué proceso de transporte pertenece el datagrama. El TCP es efectivamente una posibilidad, pero en realidad hay muchas más. Tamaño: 8 bits.

El código de redundancia de la cabecera es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del código de redundancia de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida. Tamaño: 16 bit

La *dirección de origen* contiene la dirección del host que envía el paquete. Tamaño: 32 bits.

La *dirección de destino*: Esta dirección es la del host que recibirá la información. Los routers intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bits.

Una entidad de transporte TCP acepta mensajes de longitud arbitrariamente grande procedentes de los procesos de usuario, los separa en pedazos que no excedan de 64.000 octetos y, transmite cada pedazo como si fuera un datagrama separado. La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que TCP deberá utilizar temporizadores y retransmitir los datagramas si es necesario. Los datagramas que consiguen llegar, pueden hacerlo en desorden; y dependerá de TCP el hecho de reensamblarlos en mensajes, con la secuencia correcta.

Cada octeto de datos transmitido por TCP tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecido, desde hace tiempo, en el momento en que los números de secuencia den la vuelta. TCP, sin embargo, sí se ocupa en forma explícita del problema de los duplicados retardados cuando intenta establecer una conexión, utilizando el protocolo de ida-vuelta-ida para este propósito.

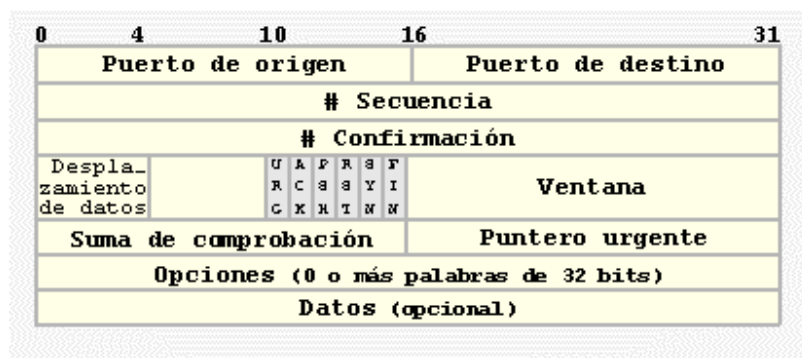


Figura 5. Formato de cabecera de TCP

En la figura 5 se muestra la cabecera que se utiliza en TCP. Los campos *puerto fuente* y *puerto destino* identifican los puntos terminales de la conexión (las direcciones TSAP de acuerdo con la terminología del modelo OSI). Cada host deberá decidir por sí mismo cómo asignar sus puertos.

Los campos *número de secuencia* y *confirmación* en superposición efectúan sus funciones usuales. Estos tienen una longitud de 32 bits, debido a que cada octeto de datos está numerado en TCP.

La *longitud de la cabecera* TCP indica el número de palabras de 32 bits que están contenidas en la cabecera de TCP. Esta información es necesaria porque el campo *opciones* tiene una longitud variable, y por lo tanto la cabecera también.

Después aparecen seis banderas de 1 bit. Si el *puntero* acelerado se está utilizando, entonces URG se coloca a 1. El puntero acelerado se emplea para indicar un desplazamiento en octetos a partir del número de secuencia actual en el que se encuentran datos acelerados. Esta facilidad se brinda en lugar de los mensajes de interrupción. El bit SYN se utiliza para el establecimiento de conexiones. La solicitud de conexión tiene SYN=1 y ACK=0, para indicar que el campo de asentimiento en superposición no se está utilizando. La respuesta a la solicitud de conexión si lleva un asentimiento, por lo que tiene SYN=1 y ACK=1. En esencia, el bit SYN se utiliza para denotar las TPDU CONNECTION REQUEST Y CONNECTION CONFIRM, con el bit ACK utilizado para distinguir entre estas dos posibilidades. El bit FIN se utiliza para liberar la conexión; especifica que el emisor ya no tiene más datos. Después de cerrar una conexión, un proceso puede seguir recibiendo datos indefinidamente. El bit RST se utiliza para reiniciar una conexión que se ha vuelto confusa debido a SYN duplicados y retardados, o a caída de los hostales. El bit EOM indica el Fin del Mensaje.

El control de flujo en TCP se trata mediante el uso de una ventana deslizante de tamaño variable. Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos que se pueden transmitir más allá del octeto asentido por el campo ventana y no cuántas TPDU.

El código de redundancia también se brinda como un factor de seguridad extrema. El algoritmo de código de redundancia consiste en sumar simplemente todos los datos, considerados como palabras de 16 bits, y después tomar el complemento a 1 de la suma.

2.4 LA DIRECCIÓN IP

El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- *Clase A:* Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una

dirección de clase A. Lo normal para las grandes organizaciones es que utilicen una o varias redes de clase B.

- *Clase B:* Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64.516 computadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de computadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de clase B, evitando de esta forma el uso de una de clase A.
- *Clase C:* En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadores en cada red. Estas direcciones permiten un menor número de hosts que las anteriores, aunque son las más numerosas pudiendo existir un gran número de redes de este tipo (más de dos millones).

Tabla de direcciones IP de Internet.					
Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1 .. 126	1 byte	3 byte	126	16.387.064
B	128 .. 191	2 byte	2 byte	16.256	64.516
C	192 .. 223	3 byte	1 byte	2.064.512	254

Figura 6. Direcciones IP de Internet

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos: el número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de host para máquinas que aún no conocen su número de host dentro de la red, o en ambos casos. El número 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera

individual a cada uno. Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al host. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El broadcast es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible.

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (subnets). Como ejemplo podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de dos bytes. En este caso sería posible utilizar el tercer byte para indicar en qué red Ethernet se encuentra un host en concreto. Esta división no tendrá ningún significado para cualquier otro computador que esté conectado a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho más cómodo el acceso que si se tratara de varias direcciones de clase C independientes.

2.5 IPv6

La nueva versión del protocolo IP recibe el nombre de IPv6, aunque es también conocida comúnmente como IPng (Internet Protocol Next Generation). El número de versión de este protocolo es el 6 (que es utilizada en forma mínima) frente a la antigua versión utilizada en forma mayoritaria. Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión antigua no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.)

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bits, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que

supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de bytes como ocurría en la versión 4.

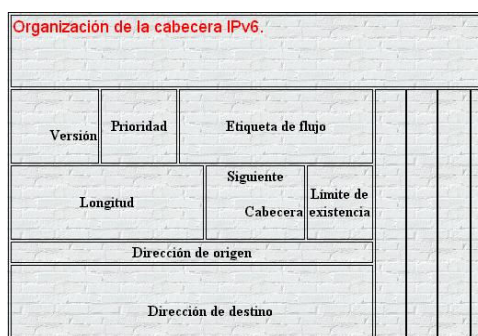


Figura 7. Organización de la cabecera IPv6

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para routing extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

3. RED DE ÁREA LOCAL

Una LAN (Local Area Network) es una red de datos de alta velocidad que cubre un área geográfica relativamente pequeña. Conecta típicamente sitios de trabajo, computadores personales, impresoras, servidores y otros dispositivos. Los usuarios de un computador perteneciente a una LAN reciben muchas ventajas por parte de esta, incluyendo el acceso compartido a los dispositivos, intercambio de información entre los usuarios conectados, y la comunicación entre los usuarios vía correo electrónico, entre otras.

3.1 MÉTODOS DE ACCESO AL MEDIO

La contención de los medios ocurre cuando dos o más dispositivos de la red tienen datos a enviar en el mismo tiempo. Debido a que múltiples dispositivos no pueden hablar en la red simultáneamente, un cierto tipo de método se debe utilizar para permitir acceso de un dispositivo a los medios de la red a la vez. Esto se hace de dos maneras principales: acceso múltiple de portador sensible con detección de colisiones (Carrier Sense Multiple Access Collision Detect CSMA/CD) y token passing. En redes que usan tecnología CSMA/CD tales como las Ethernet, los dispositivos de la red luchan por los medios de la red. Cuando un dispositivo tiene datos a enviar, primero escucha para saber si cualquier otro dispositivo está utilizando actualmente la red. Si no, comienza a enviar sus datos. Después de acabar su transmisión, escucha otra vez para ver si ocurrió una colisión. Una colisión ocurre cuando dos dispositivos envían datos simultáneamente. Cuando

sucede una colisión, cada dispositivo espera una longitud de tiempo al azar antes de volver a enviar sus datos. En la mayoría de los casos, una colisión no ocurrirá otra vez entre los dos dispositivos. Debido a este tipo de contención de la red, cuanto más ocupada una red llega a estar, más colisiones ocurren. Para las redes CSMA/CD, los switches segmentan la red en dominios múltiples de colisión. Esto reduce el número de dispositivos por el segmento de la red que debe luchar por los medios. Creando dominios más pequeños de colisión, el funcionamiento de una red puede ser aumentado perceptiblemente sin requerir cambios de dirección. Las redes CSMA/CD son normalmente half-duplex, significando esto que mientras que un dispositivo envíe información, no puede recibir información en ese mismo momento. Cuando se introducen los switches, la operación full-duplex es posible. Cuando un dispositivo de la red se une directamente al puerto de un switch de la red, los dos dispositivos pueden ser capaces de funcionar en modo full-duplex. De modo full-duplex, el funcionamiento se puede aumentar. Dos dispositivos en una conexión full-duplex pueden enviar datos tan pronto como esta esté lista.

3.2 MÉTODOS DE TRANSMISIÓN

Los métodos de transmisión de una LAN se clasifican en tres: unicast, multicast, y difusión. En cada tipo de transmisión, un solo paquete se envía a uno o más nodos. En una transmisión *unicast*, un solo paquete se envía de la fuente a un destino en una red. Primero, el nodo de la fuente direcciona el paquete usando la dirección del nodo de destinación. El paquete entonces se envía sobre la red, y finalmente, la red pasa el paquete a su destino. Una transmisión *multicast* consiste

en un solo paquete de datos que se copia y se envía a un subconjunto específico de nodos en la red. Primero, el nodo de la fuente direcciona el paquete usando una dirección de multicast. El paquete entonces se envía en la red, que hace las copias del paquete y envía una copia a cada nodo que sea parte de la dirección de multicast. Una transmisión de *difusión* consiste en un solo paquete de datos que se copia y se envía a todos los nodos en la red. En estos tipos de transmisiones, el nodo de la fuente direcciona el paquete usando la dirección de difusión. El paquete entonces se envía a la red, que hace las copias del paquete y envía una copia a cada nodo de la red.

3.3 TOPOLOGÍAS

Las topologías de una LAN definen la manera como se organizan los dispositivos de la red. Cuatro topologías comunes de LAN existen: bus, anillo, estrella y árbol. Estas topologías son arquitecturas lógicas, pero los dispositivos reales no necesitan ser organizados físicamente en estas configuraciones. Las topologías lógicas de bus y anillo, por ejemplo, se organizan comúnmente físicamente como una estrella.

- Una topología de *bus* es una arquitectura lineal de LAN en la cual las transmisiones de estaciones de la red propagan la longitud del medio y es recibida por el resto de las estaciones.

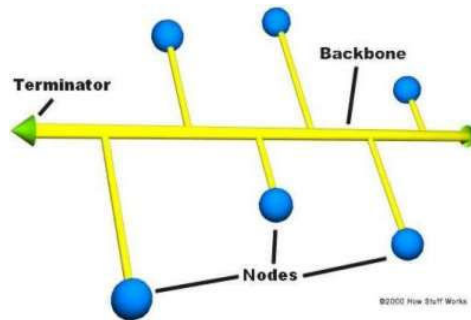


Figura 8. Topología tipo bus

- *Anillo.* Como una red de autobús, los anillos tienen los nodos uno a la derecha del otro. La diferencia es que el extremo de la red se vuelve alrededor al primer nodo, creando un circuito completo.

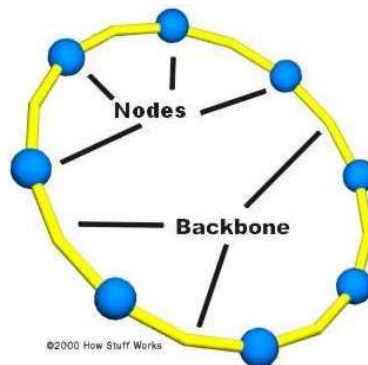


Figura 9. Topología tipo anillo

- *Estrella.* En una red de estrella, cada nodo está conectado con un dispositivo central llamado hub (o a un switch). El switch toma una señal que venga de cualquier nodo y lo reenvía al resto de nodos en la red. Un hub no realiza ningún tipo de filtración o de enrutamiento de datos. Es simplemente una unión de todos los diferentes nodos.

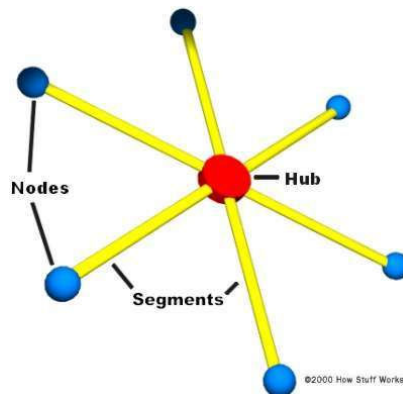


Figura 10. Topología tipo estrella

- *Bus-estrella*. Probablemente la topología más común de las redes de hoy.

Bus-estrella combina los elementos de las topologías de la estrella y de bus para crear un ambiente versátil de la red. Los nodos en áreas particulares están conectados con los switches (que crean las estrellas), y los switches están conectados a lo largo de la espina dorsal de la red (como una red tipo bus). A menudo, las estrellas se jerarquizan dentro de las estrellas.

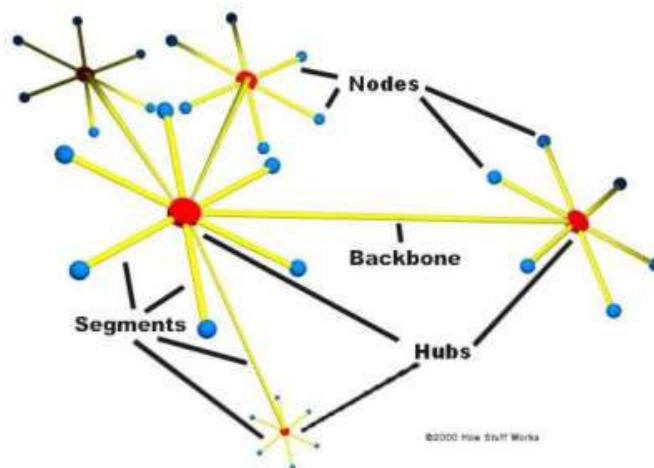


Figura 11. Topología bus-estrella

3.4 EL TRÁFICO

En el tipo más básico de red encontrado hoy, los nodos están conectados simplemente unidos con switches. Cuando una red crece, hay algunos problemas potenciales con esta configuración: *escalabilidad, estado latente, fallos de la red y colisiones*.

La solución es agregar switches como se explicará en la sección de *tecnología ethernet*.

3.5 ETHERNET/802.3

Las tecnologías de red de área local (LAN) conectan muchos dispositivos que están relativamente cerca uno del otro, generalmente en el mismo edificio. En comparación con las WANs, las LANs son más rápidas y más confiables, las continuas mejoras en la tecnología ethernet lo permiten.

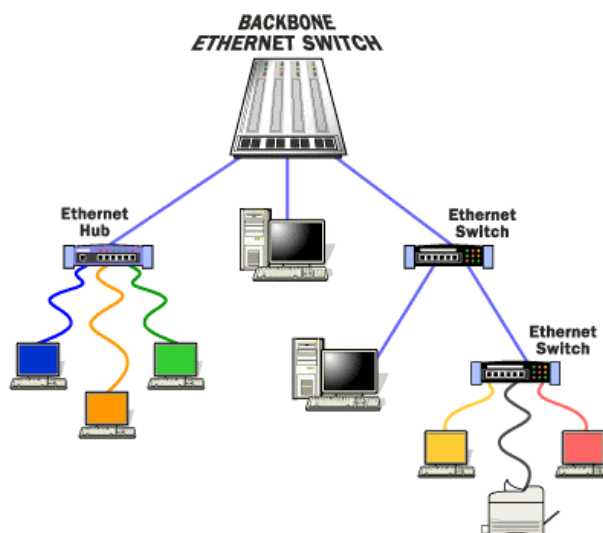


Figura 12. Ejemplo de una red ethernet

Ethernet original describió la comunicación sobre un solo cable compartido por todos los dispositivos en la red. Una vez que un dispositivo se uniera a este cable, tendría la capacidad de comunicarse con cualquier otro dispositivo unido. Esto permite que la red se amplíe para acomodar los nuevos dispositivos sin requerir ninguna modificación a esos dispositivos ya en la red.

Los dispositivos usados comúnmente en LANs basadas en Ethernet, incluyen repetidores (hubs), puentes (bridges), conmutadores (switches) y enrutadores (routers).

Un *repetidor* es un dispositivo de la capa física usado para interconectar los segmentos de los medios de una red extendida. Un repetidor esencialmente permite a una serie de segmentos de cable ser tratados como un solo cable. Los repetidores reciben señales a partir de un segmento de la red, amplifican y retransmiten esas señales a otro segmento de la red. Estas acciones previenen el deterioro de la señal, causada por longitudes de cable largas y por gran cantidad de dispositivos conectados. Los repetidores son incapaces de realizar el proceso de filtración. Además, todas las señales eléctricas, incluyendo disturbios eléctricos y otros errores, se repiten y se amplifican. El número total de los repetidores y de los segmentos de la red que pueden ser conectados es limitado.

Los *puentes* son implementados en redes ethernet para aliviar problemas con la segmentación. Los puentes conectan dos o más segmentos de la red, aumentando el diámetro de la red como lo hace un repetidor, pero los puentes

también ayudan a regular tráfico. Pueden enviar y recibir transmisiones apenas como cualquier otro nodo, pero no funcionan igual que un nodo normal. Una meta del puente es reducir tráfico innecesario en segmentos, hace esto examinando la dirección de destino del bastidor antes de decidir a cómo manejarlo. Los switches son las contrapartes modernas de los puentes, funcionalmente equivalentes pero ofreciendo un segmento dedicado para cada nodo en la red.

Una diferencia vital entre un host y un *switch*, es que todos los nodos conectados al host comparten el ancho de banda entre sí mismos, mientras que un dispositivo conectado con un puerto del switch tiene el ancho de banda completo para sí mismo. En una red completamente switchheada, los switches substituyen todos los hosts de una red Ethernet por un segmento dedicado para cada nodo. Estos segmentos conectan con un switch, que apoya segmentos dedicados múltiples. Puesto que los únicos dispositivos en cada segmento son el switch y el nodo, el switch toma cada transmisión antes de que alcance otro nodo.

Los *enrutadores* son los componentes avanzados de establecimiento de una red que pueden dividir una sola red en dos redes lógicamente separadas. Los enrutadores funcionan basados en protocolos que son independientes de la tecnología específica del establecimiento de una red, como ethernet. Esto permite que los enrutadores interconecten fácilmente varias tecnologías de red, locales y de área amplia, y ha conducido a su despliegue extenso como dispositivos que conectan el mundo como parte del Internet global.

Las redes ethernet modernas utilizan el cableado de par trenzado (twisted pair) o la fibra óptica para conectar estaciones en un patrón radial, pueden funcionar a 10, 100, 1.000 o hasta 10.000 Mbps.

El protocolo Ethernet especifica un sistema de reglas para construir tramas. Hay longitudes mínimas y máximas explícitas para las tramas, y un sistema de pedazos de información requeridos que deben aparecer en el marco. Cada trama debe incluir, por ejemplo, una dirección de destino y una dirección de origen, que identifican al destinatario y al remitente del mensaje. No debe haber entonces dos o más dispositivos de Ethernet con la misma dirección.

3.5.1 Estructura del protocolo



Figura 13. Estructura de trama ethernet

- *Preámbulo* (64 bits)

El paquete comienza con secuencia de 1s y 0s alternados [hasta completar 56 bits (802.3) o 62 bits (Ethernet)] conocido como preámbulo. El preámbulo provee una frecuencia única sobre la red de 5 MHz al comienzo de cada paquete, lo cual permite al receptor bloquear los bits entrantes. El preámbulo es utilizado sólo por el codificador/decodificador Manchester para bloquear la trama de bits recibidos y

permitir la codificación de los datos. El preámbulo recibido en la red no es pasado a través del la MAC (Medium Access Control) hacia el sistema de host. Sin embargo la MAC es responsable para la generación de preámbulos para paquetes transmitidos. La secuencia del preámbulo es seguida por el SFD (Start Frame Delimiter) que corresponde a 10101011 para completar los 8 bits restantes en el paquete 802.3, en el caso del paquete ethernet se agregaran dos bits con dos 1s (11) que corresponde al SYNCH. En ambos casos para completar los 64 bits que tiene el preámbulo.

- *Dirección de destino* (6 bytes)

La dirección destino (DD) es de 48 bits (6 bytes) de tamaño, el cual se transmite primero el bit menos significativo. La DD es utilizada por la MAC receptora, para determinar si el paquete entrante es direccionado a un nodo en particular. Si el nodo receptor detecta una correspondencia entre su dirección y la dirección dentro de la DD, intentará recibir el paquete. Los otros nodos, los cuales no detectan una correspondencia, ignorarán el resto del paquete.

La estructura de la dirección destino es como sigue:



Figura 14. Estructura de la dirección de destino

I/G Dirección Individual/Grupo

0 Dirección individual

1 Dirección de grupo

U/L Dirección Universal/Local

0 Administrada Universalmente

1 Administrada Localmente

▪ *Dirección fuente* (6 bytes)

La dirección fuente (DF) es de 48 bits (6 bytes) de tamaño, el cual se transmite primero el bit menos significativo (en forma canónica). El campo DF es proveído por la MAC transmisora, la cual inserta su propia dirección única en este campo al transmitirse la trama, indicando que fue la estación originadora. Un MAC en el receptor no es requerido para tomar acción basado en el campo DF. Los formatos de direcciones tipo broadcast y multicast son ilegales en el campo DF.

La estructura de la dirección fuente es como sigue:



Figura 15. Estructura de la dirección fuente

0 El primer bit siempre es 0

U/L Dirección Universal/local

0 Administrada Universalmente

1 Administrada Localmente

- *Longitud/Tipo (2 bytes)*

El campo Longitud (802.3)/Tipo (Ethernet) de 2 bytes va seguido del campo DF. La elección de escoger Longitud o tipo es dependiente si la trama es 802.3 o Ethernet. El byte de más alto orden de campo Longitud/Tipo es transmitido primero, con el bit menos significativo de cada byte transmitido primero.

- *Datos (46 - 1500 bytes)*

Este campo contiene los datos (información útil) a ser transferida cuyo tamaño varía de 56 a 1500 bytes.

- *FCS, Frame Check Sequence (4 bytes)*

El campo FCS o secuencia de verificación de tramas contiene el valor del algoritmo CRC (Cyclic Redundancy Check) de 32 bits de la trama completa. El CRC es computado por la estación transmisora sobre la DD, DF, Longitud/Tipo y el campo de Datos y es anexado en los últimos 4 bytes de la trama. El mismo algoritmo CRC es utilizado por la estación transmisora para computar el valor CRC para la trama como es recibida. El valor computado en el receptor es computado con el valor que fue puesto en el campo FCS de la estación transmisora, proveyendo un mecanismo de detección de error en caso de datos corruptos. Los bits del CRC dentro del campo FCS son transmitidos en el orden del bit más significativo al bit menos significativo.

4. SISTEMAS DE CABLEADO ESTRUCTURADO

Antes de la desmonopolización de la Compañía Bell en los Estados Unidos en 1984, los edificios se diseñaban sin tomar en cuenta los servicios de comunicaciones que operarían en ellos. Las aplicaciones emergentes de datos requerían tipos de cableado específicos. Por ejemplo, IBM S/3X operaba en cable twinaxial de 100 y Ethernet en cable coaxial de 50.

Mientras que las compañías de teléfonos locales tenían la oportunidad de colocar su cableado de voz durante la fase de construcción, el personal de datos/computadoras tenía usualmente que instalar su cableado luego de que el espacio estaba ocupado. La infraestructura se alteraba a menudo a costa, y muy a desánimo, del usuario final. Durante este período, el cableado de voz tenía una estructura mínima; una instalación típica de un edificio consistía de cable de par trenzado grado voz, cableado en una topología tipo estrella. El número de pares a cada localidad variaba de 1 a 25 pares. Las longitudes máximas del cable y el número de cross-connects eran determinadas por el proveedor de telefonía o por el fabricante del equipo.

Los primeros cableados de datos, utilizados en la década de los años 60 para conexiones punto a punto entre servidores y terminales, consistían en cable de par trenzado de baja capacitancia para transmisión de señales no balanceadas; que aunque eran suficientes para comunicaciones de baja velocidad, sus limitaciones se hacían evidentes a medida que aumentaban las velocidades de transmisión.

A mediados de los 70's, IBM introdujo procesadores centrales (main-frames) que utilizaban cable coaxial de 93. La introducción del balun, varios años después permitió que el equipo basado en cable coaxial funcionara con cableado de par trenzado grado voz. El balun (palabra derivada de BALanced/UNbalanced) permitió la conversión de una señal de cable coaxial no balanceada en una señal balanceada que podía transmitirse y recibirse sobre cableado de par trenzado grado voz.

A medida que la tecnología Ethernet evolucionó a comienzos de los 80's, proliferó la utilización del cable coaxial de 50. Al crecer la aceptación de Ethernet, los fabricantes líderes tales como Cabletron y Synoptics (Nortel Networks) comenzaron a ofrecer tarjetas de interfaz de red con puertos de toma modular en lugar de conectores coaxiales. Esta tecnología de alta velocidad (10BASE-T) demandó el primer cable de par trenzado grado datos que se clasificó más tarde como UTP Categoría 3.

A mediados de los 80's, IBM desarrolló Token Ring como un competidor de Ethernet, especificando un cable de par trenzado blindado (STP) de 150 de 2 pares. No obstante, a medida que crecía la aceptación del UTP para aplicaciones de datos, éste se utilizó como una alternativa al STP para redes Token Ring de 4 y 16 Mb/s.

Durante este período, los usuarios tenían que elegir entre una gran diversidad de cables (UTP, STP, coaxial, doble coaxial, twinaxial, fibra óptica, etc.) y sus conectores asociados (tomas modulares [jacks], conectores UDC, BNC, twinaxial, DB9, DB15, DB25, ST, SC, FC, etc.). Cuando aparecía un nuevo fabricante o sistema, el cableado antiguo se volvía obsoleto y en lugar de retirar los cables innecesarios, el nuevo cableado se colocaba sobre el antiguo; consecuentemente las canalizaciones para cableado se congestionaban y tenían que instalarse nuevas canalizaciones además del cable.

Para satisfacer la creciente demanda de un cableado de telecomunicaciones para aplicaciones múltiples, varios fabricantes introdujeron sistemas de cableado capaces de soportar las aplicaciones de voz y datos seleccionadas. Pero aún persistía el problema de una gran diversidad de cables de diferentes fabricantes. En algunos casos había compatibilidad, en otros no. Ésta falta de uniformidad urgió a la industria a generar normas que permitieran la compatibilidad entre productos de diversos fabricantes. Para abordar esta necesidad, en 1985 la Asociación de Industrias Electrónicas (EIA [Electronic Industries Alliance]) y la Asociación de la Industria de Telecomunicaciones (TIA [Telecommunications Industry Association]) organizaron comités técnicos para desarrollar un estándar

para cableado de Telecomunicaciones. Estos comités trabajaron durante más de seis años para desarrollar las primeras normas globales sobre cableado, canalizaciones y espacios de telecomunicaciones. Estas normas se han aplicado en muchas naciones y han generado especificaciones adicionales sobre administración, puesta y unido a tierra y categorías universalmente aceptadas para par trenzado balanceado de 100. Dichos comités han estado muy activos como lo evidencian, entre otros, sus más recientes trabajos: adendas de la norma ANSI/TIA/EIA-569-A; normas ANSI/TIA/EIA-568-B.1, 2, 3 y sus respectivas adendas; y la revisión de la norma internacional de cableado genérico ISO/IEC 11801:2002 2ª Edición, la cual actualmente es la base de la gran mayoría de las normas regionales. Los requisitos de la categoría 5e brindan un margen que garantiza el soporte de aplicaciones que utilizan los cuatro pares en forma simultánea para transmisión bidireccional. Los parámetros pendientes de sistemas de cableado de Categoría 6/Clase E y Categoría 7/Clase F se han desarrollado para soportar aplicaciones futuras que demanden anchos de banda por encima de los 100 MHz y mayores márgenes de desempeño a los ofrecidos en la actualidad por la categoría 5e. Aunque las aplicaciones para Categoría 6/Clase E son soportadas tanto por soluciones UTP como ScTP, es interesante notar que el desempeño especificado para la categoría 7/clase F está apuntando a una solución de cableado de par trenzado blindado apantallado (S/FTP).

“Cableado Estructurado” es un término ampliamente utilizado para definir un sistema de cableado genérico de voz, datos e imagen (telecomunicaciones) que soporta un ambiente multiproducto, multifabricante y multimedios. Es una infraestructura de tecnología de la información (IT) que define un diseño de cableado basado en los requisitos del usuario final, permitiendo su implementación aun cuando exista poco o ningún conocimiento del equipo activo o aplicación a instalar. Adaptado tanto a instalaciones de campus como de edificios individuales, el cableado estructurado consta de hasta tres subsistemas que pueden unirse para formar una red completa en una topología tipo estrella.

El concepto estructurado lo definen los siguientes puntos:

- *Solución Longeva:* Cuando se instala un cableado estructurado se convierte en parte del edificio, así como lo es la instalación eléctrica, por tanto este tiene que ser igual de funcional que los demás servicios del edificio. La gran mayoría de los cableados estructurados pueden dar servicio por un periodo de 10 a 15 años, no importando los avances tecnológicos en los equipos de cómputo ni las aplicaciones.
- *Modularidad:* Capacidad de integrar varias tecnologías sobre el mismo cableado voz, datos, video.
- *Fácil Administración:* El cableado estructurado se divide en partes manejables que permiten hacerlo confiable y perfectamente administrable, pudiendo así detectar fallas y repararlas fácilmente.

Una de las ventajas básicas de estos sistemas es que se encuentran regulados mediante estándares, lo que garantiza a los usuarios su disposición para las aplicaciones existentes, independientemente del fabricante de las mismas, siendo soluciones abiertas, fiables y muy seguras. Fundamentalmente las normas TIA/EIA (Asociación de Industrias de las Telecomunicaciones, Asociación de Industrias Electrónicas).

EIA/TIA 568B define entre otras cosas las normas de diseño de los sistemas de cableado, su topología, las distancias, tipo de cables, los conectores, tipos de fibra óptica, etc.

EIA/TIA 569A define los tipos de canalizaciones para ubicar los diferentes tipos de cables ópticos ó de cobre dentro del edificio, los tipos de cajas de inspección, sistemas de cielo falso ó piso falso, etc.

EIA/TIA 942 define los parámetros de diseño, instalación, puesta en marcha de los Centros de Cómputo ó Datacenters.

EIA/ TIA 862 Norma para B.A.S. (Building Automation Services) define todos los lineamientos para automatizar un edificio: Control de Acceso, Sensores, CCTV

(Circuito cerrado de Televisión), Voz, Datos, vídeo, alarmas, control automático de aires acondicionados, control automático de bombas de agua, etc.

EIA/TIA 570 Define los parámetros de instalaciones de cableado de Telecomunicaciones residenciales ó para el hogar.

EIA/TIA 606 define los sistemas de administración, marcación, etiquetado, de todos los sistemas y sub sistemas de cableado estructurado.

EIA/TIA 607 define los requerimientos técnicos para las protecciones eléctricas y los sistemas equipotenciales de tierra para cableados de Telecomunicaciones

4.1 REQUERIMIENTOS PARA LA CONEXIÓN FÍSICA

- *Dispositivo*: cualquier aparato que queremos conectar a la red, este puede ser un teléfono, una computadora, un sensor, una cámara o cualquier otro.

Patch Cord:

Se define como el cordón. Todos los cordones modulares categoría 6 deberán:

- Ser ensamblados en fábrica y su transmisión probada al 100% con un analizador de redes grado laboratorio para un desempeño apropiado a 250 MHz (el fabricante deberá garantizar su compatibilidad para enlaces categoría 6).
- Ser compatible retroactivamente con categorías inferiores.
- Estar equipado con clavijas modulares de 8 posiciones idénticas en cada extremo alambrados en esquema directo en conformidad con las normas.
- Obtener el desempeño requerido sin el uso de componentes de circuito impreso.
- Tener una bota liberadora de tensión moldeada sobre la unión del cable y el conector, disponible en varios colores (negro, blanco, rojo, amarillo, azul y verde) y con un protector para la presilla de la clavija.

- Permitir la colocación de insertos de iconos para una codificación e identificación opcional.
- Usar clavijas modulares que excedan los requisitos de las normas FCC CFR 47 parte 68 subparte F e IEC 60603, y tener un mínimo de 50 micro pulgadas de chapa de oro sobre contactos de níquel.
- Aislantes metálicos en el plug RJ-45 para garantizar la continuidad de las barreras físicas del cable UTP.
- Ser resistente a la corrosión por humedad, temperaturas extremas, y partículas contaminantes.
- Utilizar cable que posea un desempeño de suma de potencias NEXT.
- Estar disponible en longitudes estándar de 3, 5, 7, 10, 15, 20, y 25 ft. con longitudes a medida disponibles bajo pedido.
- Utilizar cable multifilar con un forro redondo y pirotardante.
- Tener una resistencia DC por contacto de $9.38 \Omega / 100 \text{ m}$ como máximo.
- Tener una impedancia de entrada sin promediar de: $100 \Omega \pm 15\%$ de 1 a 100 MHz, $\pm 22\%$ de 100 a 200 MHz y $\pm 32\%$ de 200 a 250 MHz.
- Cumplir o exceder el desempeño eléctrico de la norma ANSI/TIA/EIA-568-B.2-1.
- Deberá tener certificación ETL (Electronic Testing Laboratories). Estar certificado por Underwriters Laboratories (UL).
- *Placa con servicios:* Esta placa contiene las salidas de telecomunicaciones en donde se conectan los dispositivos que estarán ubicados en el área de trabajo. La misma placa puede combinar servicios de voz, datos, video, etc. en cobre ó fibra óptica según sean las necesidades. Para el caso de cobre ésta salida debe soportar conectores tipo RJ 45 de 8 hilos, conectores tipo BNC, Conectores de fibra óptica tipo SC, LC, MT-RJ.

- *Cableado Horizontal:* Se define como el cable que conecta el hardware de conexión
- *Panel de Parcheo:* Es el hardware de conexión horizontal y permite realizar la administración de todos los puntos de voz, datos ó video que convergen en ellos dada la conexión en estrella para cableado horizontal que exige la norma EIA/TIA.

El panel debe cumplir con los siguientes parámetros:

- Deberá estar hecho con aluminio anodizado color negro, en configuraciones de 16, 24, 48, 64 y 96-puertos.
- Deberá acomodar al menos 24 puertos en cada espacio de montaje en bastidor (1rms = 44.5 mm [1.75 in.]).
- Deberá utilizar tecnología TRI-BALANCE con un diseño optimado de balance de pares y respuesta lineal a la diafonía para soportar aplicaciones de hasta 250 MHz.
- Deberá tener conectores por desplazamiento de aislante (IDC) estilo 310 con aislamiento de cuadrante de pares y sistema de acomodo de conductores Pyramid.
- Deberá permitir la terminación de conductores individuales con una herramienta de impacto.
- Deberá ser compatible retroactivamente para permitir que categorías de desempeño inferiores de cables y hardware de conexión puedan operar a su máxima capacidad.
- Cada una de sus tomas modulares deberá tener una cubierta posterior liberadora de tensión con acceso de cable posterior y lateral, el cual podrá ser colocado en el cable antes o después de la terminación.
- En cada toma deberá poder elegir cualquiera de los dos esquemas de alambrado T568A o T568B.

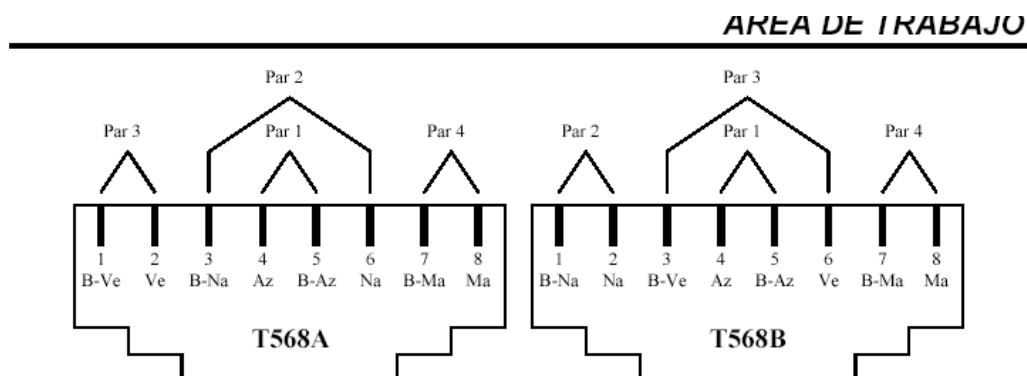
- Deberá tener puertos modulares que cumplan con FCC CFR 47 parte 68 subparte F y con IEC 60603-7 con 50 micro pulgadas de chapa de oro sobre los contactos de níquel.
- Deberá estar totalmente protegido al frente y atrás por una protección física metálica como protección a los circuitos impresos.
- Deberá tener un organizador posterior de cable montable directamente en el panel.
- Deberá tener números de identificación de puertos individuales permanentemente marcados al frente y detrás del panel.
- Deberá estar indicada la categoría de desempeño al frente y en la parte posterior del panel.
- Deberá incluir porta insertos autoadhesivos, portatiras transparente y tiras de designación color blanco. Deberá tener disponibles varias opciones de tiras de designación.
- Deberá tener una certificación Underwriters Laboratories (UL).
- Deberá tener certificación ETL (Electronic Testing Laboratories).
- Deberá cumplir las siguientes especificaciones de desempeño:

Margen sobre la categoría 6 @ 250MHz		
Parámetros	Peor Caso	Típico
Pérdida de Inserción	0.13 dB	0.15 dB
NEXT*	0.75 dB	4.0 dB
FEXT*	2.0 dB	4.9 dB
Pérdida de Retorno	6.5 dB	8.0 dB

* Probado tanto en modo común como en modo diferencial

Figura 16. Especificaciones de desempeño del panel de parcheo

- 4.2 ESQUEMA DE COLORES ESTÁNDAR PARA CABLES UTP



▲ – 6 *Las asignaciones de posiciones en una toma de par trenzado balanceado serán conforme a los esquemas de alambrado T568A o T568B. Se prefiere el esquema de alambrado T568A. El esquema de alambrado T568B puede usarse si es necesario para acomodar ciertos sistemas de cableado de 8 posiciones.*

Los colores indicados se asocian con cable de distribución horizontal. Estas ilustraciones representan la parte frontal de las tomas.

El esquema T568A se elige como esquema recomendado porque su configuración es compatible con una amplia variedad de esquemas de dos pares de aplicaciones existentes de voz y datos. Esta configuración tiene los dos primeros pares en las cuatro posiciones centrales, lo que lo hace apropiado para la mayoría de los sistemas que usaban la antigua configuración USOC de 4, 6 y 8 posiciones.

Δ – 4 *No se recomienda la coexistencia de tomas T568A y T568B en la misma instalación.*

Figura 17. Esquema de colores según T568A o T568B

- *Esquema de colores Tipo A*

En el interior del cable se encuentran 4 pares de hilos como ya lo hemos visto en medio de transmisión, este tipo de cables se encuentran identificados por colores que porta cada una de las puntas de cobre, como se muestra en la siguiente tabla cada color tiene un número de identificación y por lo tanto se crean configuraciones dependiendo del orden de números que tenga cada color.

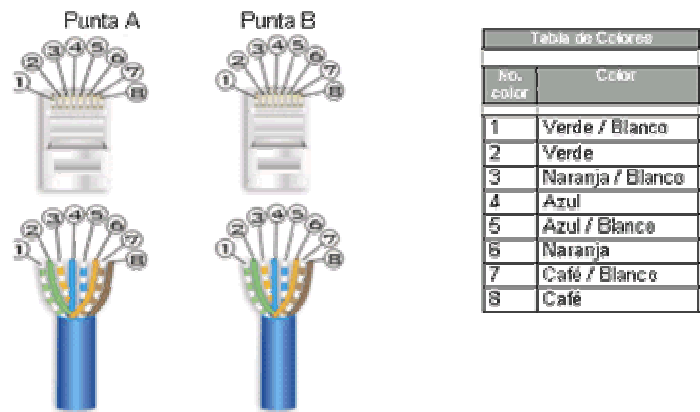


Figura 18. Esquema de colores tipo A

Esta configuración también es llamada Uno a Uno ya que como se muestra en el esquema los números de los colores son consecutivos, del 1 al 8. Con esto decimos que el orden que tenga la Punta A del cable debe ser idéntica a la Punta B.

- *Esquema de colores Tipo B (Estándar EIA/TIA 568B AT&T)*

Esta configuración también es llamada Invertida ya que como se muestra en el esquema los colores no son consecutivos las posiciones de los números son alteradas en algunas posiciones como: la 1 por la 3 y la 2 por la 6. En esta configuración las puntas deben ir idénticas.

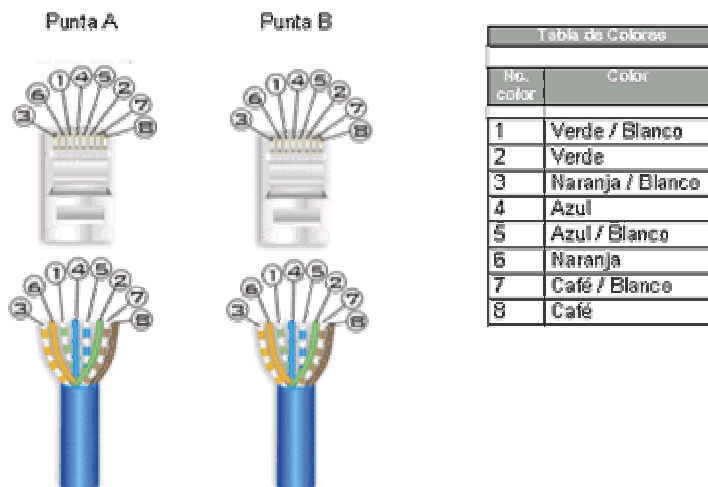


Figura 19. Esquema de colores tipo B

4.3 ESTÁNDARES

Todo el cableado estructurado está regulado por estándares internacionales que se encargan de establecer las normas comunes que deben cumplir todas las instalaciones de este tipo.

SUBSISTEMAS DE CABLEADO ESTRUCTURADO

4.4 ÁREA DE TRABAJO

Se define como la zona donde están los distintos puestos de trabajo de la red. El área de trabajo comprende todo lo que se conecta a partir de la placa de conexiones de salida hasta los propios dispositivos a conectar (computadores e impresoras fundamentalmente). Están también incluidos cualquier filtro, adaptador, etc., que se necesite. Estos irán siempre conectados en el exterior de la salida de telecomunicaciones. Si el cable se utiliza para compartir voz, datos u otros servicios, cada uno de ellos deberá tener un conector que los diferencie en la propia salida de telecomunicaciones.

Salida de Telecomunicaciones

Esta es la interfaz entre el área de trabajo y el cableado horizontal. La caja de salidas de telecomunicaciones constituye también parte del área de trabajo.

Equipos del Área de Trabajo

Dispositivos tales como teléfonos, terminales, computadoras, etc.

Cordones de Equipo

Cordones modulares utilizados para conectar equipo del área de trabajo a la salida de telecomunicaciones.

Adaptadores

Adaptadores y convertidores de medio, tales como los utilizados para transposición de cableado, adaptadores de plug a toma, adaptadores DB25, DB15, DB09, baluns, etc.

4.5 CABLEADO HORIZONTAL

El cableado horizontal se extiende desde la salida de telecomunicaciones del área de trabajo hasta el cross-connect horizontal (HC)/distribuidor de piso (FD) en el cuarto de telecomunicaciones. El cableado horizontal abarca los cables horizontales, la salida de telecomunicaciones y el HC/FD, incluyendo la terminación mecánica y los jumpers o cordones de parcheo localizados en él. El cableado horizontal incluye además, si han sido utilizados, el punto de consolidación y el ensamble de salidas multiusuario de telecomunicaciones (MuTOA). El cableado horizontal no incluye los cordones en el área de trabajo o en el cuarto de telecomunicaciones que conectan directamente al equipo activo.

Desde la salida de telecomunicaciones de cada uno de las áreas de trabajo irá un cable a un punto común de centralización llamado *patch panel* (panel de parcheo).

El panel de parcheo es donde se centraliza todo el cableado del piso del edificio. Es el lugar al que llegan los cables procedentes de cada una de las dependencias donde se han instalado puntos de comunicaciones de la red. Cada salida de telecomunicaciones colocada en el edificio tendrá al otro extremo de su cable una

conexión al panel de parcheo. De esta forma se le podrá dar o quitar servicio a una determinada dependencia simplemente con proporcionarle o no señal en este panel.

Todo el cableado horizontal deberá ir canalizado por conducciones adecuadas. En la mayoría de los casos, se eligen para esta función las llamadas *canaletas* que nos permiten de una forma flexible trazar los recorridos adecuados desde el área de trabajo hasta el panel de parcheo. Es muy conveniente que el panel de parcheo junto con los dispositivos de interconexión centralizada (concentradores, patch cords, routers, fuentes de alimentación, etc.) estén encerrados un *rack* (armario de comunicaciones). De esta forma se aíslan del exterior y por lo tanto de su manipulación accidental. También facilita el mantenimiento al tenerlo todo en un mismo lugar.

La topología usada es en estrella teniendo en cuenta que cada mecanismo de conexión en la salida de telecomunicaciones está conectado a su propio mecanismo de conexión en el panel de parcheo del armario de comunicaciones.

Cada cable horizontal no podrá superar los 90 metros. Además los cables para el parcheo en el armario de comunicaciones no podrán tener más de 5 metros.

4.6 CABLEADO VERTICAL

El backbone se extiende desde el cross-connect principal (MC)/distribuidor de campus (CD) hasta los cross-connects horizontales (HCs)/distribuidores de piso (FDs) e incluye el MC/CD, el o los cross-connects intermedios (ICs)/distribuidores de edificio (BDs), el hardware de conexión dedicado al backbone y los cables que los unen. El backbone incluye además las terminaciones mecánicas y los jumpers y cordones de parcheo usados para conexiones de backbone a backbone. El backbone no incluye cables en los cuartos de telecomunicaciones, cuartos de equipos o acometidas que conectan directamente a equipos activos.

Es el que interconecta los distintos armarios de comunicaciones. Éstos pueden estar situados en plantas o habitaciones distintas de un mismo edificio o incluso en edificios contiguos. En el cableado vertical es usual utilizar fibra óptica o cable UTP.

La topología que se usa es en estrella existiendo un panel de distribución central al que se conectan los paneles de distribución horizontal. Entre ellos puede existir un panel intermedio, pero sólo uno.

En el cableado vertical están incluidos los cables del "backbone", los mecanismos en los paneles principales e intermedios, los patch cords usados para el parcheo, los mecanismos que terminan el cableado vertical en los armarios de distribución horizontal.

5. DISEÑO DE LA RED

5.1 DISEÑO SOBRE EL PLANO

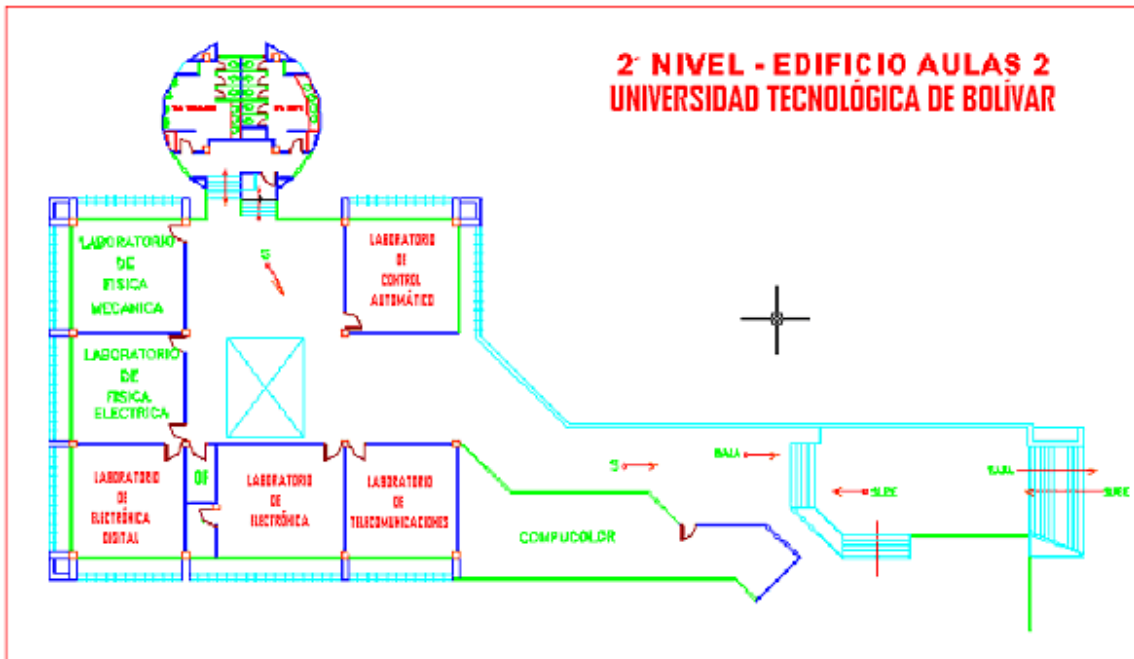


Figura. 20 Plano del área de trabajo

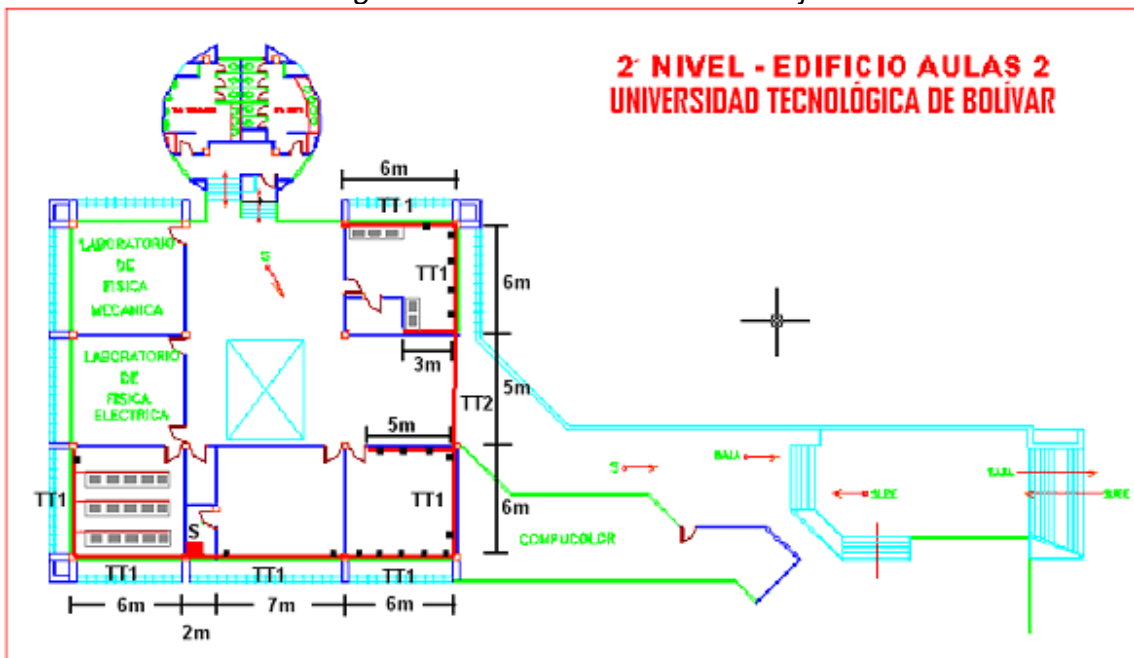


Figura 21. Trazado del diseño

NOTA: El diseño lo realizamos con base en los planos correspondientes proporcionados por la Universidad y con medidas tomadas por nosotros en campo.

S: switch (de 48 puertos) al cual se conectará el cableado

TT1: tendido tipo 1 (canaleta a 40 cm sobre el nivel del piso)

TT2: tendido tipo 2 (canaleta que bordea una viga bajo el techo)

La línea de color rojo representa la ruta del cableado y los pequeños puntos negros representan los puntos de telecomunicaciones. En la red, todo el cableado será UTP de categoría 6, a excepción del utilizado para proveer puntos de telecomunicaciones al laboratorio de control automático, el cual será de tipo STP de igual categoría al resto de la red, para proteger de interferencia generada por motores.

5.2 CANTIDADES Y ELEMENTOS

- Switch Catalyst 2900 de 48 puertos. Cisco systems Ref 2948G-GE-TX
- 80 metros de canaleta tipo DLP. Legrand/Luminex.
- 40 acopladores angulares dobles de cableado universal T568A/B color blanco. Siemon company Ref CT-C6-C6-02
- 40 kit placa frontal alemana, acoplado doble, para un acoplador CT. Incluye placa frontal, anillo de montaje y marco expansor. Siemon company Ref CT-FP-DKIT-02
- 40 cajas para montaje de superficie placa frontal color blanco. Siemon company Ref CT8-BOX-02
- 40 cordones de parcheo modulares MC 6. Siemon company Ref MC6S-03M-02I
- 4 bobinas de 25 acomodadores de gancho y cinturón para cables. Siemon company Ref VCM-25-060-2
- 1 caja de cable blindado redondo sólido (305 m) System 6 ScTP de cuatro pares color gris. Siemon company Ref 9A6X4-E3
- 1 caja de cable redondo sólido (305 m) system 6 UTP de cuatro pares color gris. Siemon company Ref 9C6X4-E3
- 40 conectores (PLUG) RJ45

6. COSTOS DE IMPLEMENTACIÓN

6.1 COMPRA DE MATERIALES

En el complejo mundo del desarrollo tecnológico, las tecnologías emergentes y las mejoras se producen a una velocidad vertiginosa; resulta imperiosamente necesario disponer de un conjunto de cualidades y soporte, que aseguren una acertada toma de decisiones y hagan posible evitar o disminuir al máximo el riesgo de cometer errores en un determinado proyecto.

Es necesario planificar bien. Saber qué materiales y equipos se necesitan y en qué cantidad; estudiar el croquis implementado en el diseño y calcular cuántos metros de cable se necesitan para cada tramo de la red (siempre es bueno calcular algunos metros de más).

6.2 COTIZACIÓN

Presentamos una cotización solicitada a una empresa seria (Melexa S.A. goza de prestigio y reconocimiento por su seriedad en el país), donde se incluyen todos los materiales necesarios para implementar la red (marcas reconocidas y con buen respaldo). Ver Anexos.¹

NOTA: En esta cotización no se incluyen costos por mano de obra, alquiler de herramientas ni material necesario para la identificación de cableado y hardware (marcadores). Estos valores se relacionan a continuación:

6.2.1 MANO DE OBRA

Valor mano de obra	\$ 40.000 por punto instalado
Valor certificación de puntos y de la red.....	\$ 20.000 por cada punto

¹ VER ANEXO COTIZACION

6.2.2 ALQUILER DE HERRAMIENTAS

- Ponchadora de impacto
- Ponchadora de Ratchet profesional
- Taladro de percutor
- Brocas de pared
- Destornilladores
- Probador de Cables LAN RJ 45
- Multitomas

Valor.....\$200.000

6.2.3 OTROS SUMINISTROS

- Marcadores de multidígitos preimpresos
- Libreta de marcadores adhesivos
- Anillos para marcaciones de Cables
- Cintas de amarres
- Bases adhesivas sujeción de cables
- Espiral para cables

Valor.....\$150.000

6.3 COSTOS POR ÁREAS

Se instalaran en total 40 puntos de telecomunicaciones distribuidos de la siguiente manera: 16 puntos en el laboratorio de electrónica digital, 4 puntos en el laboratorio de electrónica (estos no fueron solicitados por la universidad pero consideramos prudente su instalación para su futuro uso), 10 puntos en el laboratorio de telecomunicaciones y 10 más en el laboratorio de control automático. Es un poco complicado desglosar los costos por área, debido a que

no podemos comprar el cable por retazos y para la instalación de un solo salón tendríamos de igual forma que adquirir el switch (que es lo mas costoso) y además la instalación por áreas (salones) implica alquilar las herramientas varias veces y esto incrementa el valor del proyecto. Teniendo en cuenta lo anterior, podríamos dar un **estimado** de lo que costaría la implementación sectorizada del proyecto, dando por sentado que la inversión inicial (primer salón implementado) será la más costosa independientemente de cual sea.

- Laboratorio de electrónica digital

16 Puntos instalados y certificados	\$ 960.000
1 Caja de cable UTP	\$ 245.000
Switch Catalyst*	US\$ 4.071
6 Tramos de canaleta	\$ 190.440
16 Tomas angulares	\$ 580.256
16 Kits de face plates	\$ 85.600
16 Cajas para montaje	\$ 208.000
16 Patch cords	\$ 654.400
16 Plugs RJ45	\$ 15.280
100 Amarres de velcro	\$ 132.000
Alquiler de herramientas y suministros	\$ 350.000
TOTAL	\$ 12.784.276
IVA 16%.....	\$ 2.045.484,16
GRAN TOTAL.....	\$14.829.760,16

* Este valor depende del precio del dólar en el día en que se facture.

- Laboratorio de telecomunicaciones**

10 Puntos instalados y certificados	\$ 600.000
13 Tramos de canaleta	\$ 412.620
10 Tomas angulares	\$ 362.660
10 Kits de face plates	\$ 53.500
10 Cajas para montaje	\$ 130.000
10 Patch cords	\$ 409.000
10 Plugs RJ45	\$ 9.550
TOTAL	\$ 1.997.330
IVA 16%	\$ 316.372,8
GRAN TOTAL	\$ 2.313.702,8

** Este valor solo tiene en cuenta la mano de obra y los elementos requeridos para realizar el montaje, reiteramos que es indispensable la compra de otros elementos y alquiler de herramientas ya relacionados anteriormente.

- Laboratorio de control**

10 Puntos instalados y certificados	\$ 600.000
10 Tramos de canaleta	\$ 317.400
10 Tomas angulares	\$ 362.660
10 Kits de face plates	\$ 53.500
10 Cajas para montaje	\$ 130.000
10 Patch cords	\$ 409.000
10 Plugs RJ45	\$ 9.550
1 Caja de cable UTP	\$ 245.000

TOTAL	\$ 2.168.610
IVA 16%	\$ 346.977,6
GRAN TOTAL	\$ 2.515.587,6

** Este valor solo tiene en cuenta la mano de obra y los elementos requeridos para realizar el montaje, reiteramos que es indispensable la compra de otros elementos y alquiler de herramientas ya relacionados anteriormente.

Tiempo estimado de instalación de la red: dos semanas

BIBLIOGRAFÍA

- www.cisco.com
- www.conocimientosweb.net
- www.eveliux.com
- www.howstuffworks.com
- www.nti.educa.rcanaria.es
- www.neo.icc.ums.es
- www.usuarios.lycos.es
- www.protocols.com
- www.eia.udg.es
- www.ditec.um.es
- www.ieee.com
- END-TO-END Arguments In System Design. J.H. Saltzer, D.P. Reed and D.D. Clark. 1988
- Architectural Principles of the Internet. Brian E. Carpenter 1996
- The Design Philosophy of the DARPA Internet Protocols. 1988
- Computer Networks. Andrew S. Tanenbaum. 4^{ta} Edición 2003. Prentice Hall

Señores.	Universidad Tecnologica de Bolivar
Atte:	ING. ARGEMIRO BERMUDEZ G.
Tel / Fax:	12355436



Cotización Nro: C-18900065
Fecha: ABRIL 11 DE 2005
Responsable: Ing. Carlos H. Rodriguez V.
Teléfono: (57-1) 360 3055
Fax: (57-1) 360 2562
E-mail: crodriguez@melexa.com

Item	Unidad	Referencia	Cant.	Descripción	P/Unit.	P/Total	Entrega
1	Unidad	13LD30038	40	CANALETA PLASTICA DE 10x5 cm, SIN DIVISION, TRAMO DE 2 METROS, MARCA LEGRAND	31.740	1.269.600	INMEDIATA
2	Unidad	19SICTC6C602B	40	TOMA TIPO CT ANGULAR, CATEGORIA 6, COLOR BLANCO, ICONOS ROJOS Y AZULES, MARCA SIEMON	36.266	1.450.640	INMEDIATA
3	Unidad	19SICTFPDKIT02	40	KIT DE FACE PLATE PARA TOMA CT, TIPO ALEMAN, MARCA SIEMON	5.350	214.000	5 SEMANAS
4	Unidad	19SICT8BOX02	40	CAJA PARA MONTAJE EN SUPERFICIE, MARCA SIEMON	13.000	520.000	5 SEMANAS
5	Unidad	19SIMC6S03M02L	40	PATCH CORD STP, CAT 6, 3 METROS, MARCA SIEMON	40.900	1.636.000	5 SEMANAS
6	Unidad	19SIVCM1000601	100	AMARRE VELCRO REUTILIZABEL DE 6 ", COLOR NEGRO, MARCA SIEMON	1.320	132.000	INMEDIATA
7	Unidad	19SC9A5X4E3	1	CABLE STP CATEGORIA 6, CAJA POR 305 MTS, MARCA SIEMON	286.500	286.500	5 SEMANAS
8	Unidad	19SC9C6X4E3	1	CABLE UTP CATEGORIA 6, CAJA POR 305 MTS, MARCA SIEMON	245.000	245.000	INMEDIATA
9	Unidad	19SIP88	40	PLUG RJ45, CAT 5E, MARCA SIEMON	955	38.200	INMEDIATA
10	Unidad	WS-C2948G-GE-TX	1	SWITCH CISCO CATALYST , 48 PORTS 10/100/1.000 MBPS + 4 SFP PORTS	USD\$4.071	9.526.140	6 SEMANAS
Total						14.048.480,00	

Condiciones de Venta:

Validez Oferta

Impuestos

Precio

Forma de Pago

Tiempo Entrega

15 días Calendario

No incluye el IVA

Los precios corresponden a entrega en sus bodegas en Colombia.

Contado. Crédito a 30 días, previa entrega documentación.

Inmediato según item y cantidad

Se otorga el 5% financiero de descuento sin afectar IVA por pago de contado

No retener, somos autorretenedores según resolución 7774 del 8 de agosto de 2002 y grandes contribuyentes