

**DISEÑO DE UNA RED DE COMPUTADORES PARA LA CORPORACIÓN
UNIVERSITARIA DE LA COSTA**

**DAGOBERTO DE LA HOZ ACUÑA
CESAR AUGUSTO URIBE MANZUR
SHELLY MARIA VASQUEZ MEDINA**

**CORPORACION UNIVERSITARIA DE LA COSTA
FACULTAD DE INGENIERIA ELECTRONICA
BARRANQUILLA**

2003

**DISEÑO DE UNA RED DE COMPUTADORES PARA LA CORPORACION
UNIVERSITARIA DE LA COSTA**

**DAGOBERTO DE LA HOZ ACUÑA
CESAR AUGUSTO URIBE MANZUR
SHELLY MARIA VASQUEZ MEDINA**

Proyecto de investigación como requisito para optar el título de
Ingeniero Electrónico

Director
RICARDO TAFFUR

**CORPORACION UNIVERSITARIA DE LA COSTA
FACULTAD DE INGENIERIA ELECTRONICA
BARRANQUILLA
2003**

Nota de aceptación

Presidente del jurado

Jurado

Jurado

Barranquilla, Julio de 2003

Le doy gracias a Dios por darme la vida para poder realizar esta tesis , a mis padres por brindarme su apoyo, a toda mi familia por darme animo para terminar esta carrera, a mis compañeros por brindarnos su colaboración y a Shelly y Cesar por sacar adelante esta tesis.

Dagoberto De la hoz Acuña

Le doy gracias al Dios grande y poderoso que me ha permitido realizar una de mis principales metas.

Gracias también a mis padres y a mi familia, por apoyarme y por empujarme para culminar esta etapa de mi vida y a todos aquellos que colocaron una semilla en este tiempo de estudiante para que yo saliera adelante.

Cesar Uribe Manzúr

Agradezco mucho a Dios, por ubicarme en el lugar indicado con las personas indicadas y por guiar cada paso de mi vida.

A mi familia por todo su apoyo; a mis amigos por ser mi segunda familia y ayudarme a superar mis momentos difíciles.

A mis compañeros de tesis y grandes amigos Dago y Cesar, por su tenacidad y cariño.

Con especial orgullo agradezco y dedico este triunfo a mi mamá Maryluz Medina, quien aunque siempre estuvo lejos, nunca estuvo ausente y a mis dos lindos hermanos Demmys e Ivan, por ser la luz que ilumina mi vida.

Shelly Vásquez Medina

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Ricardo Taffur, Ingeniero Electrónico y Director de Programa de la Facultad de Ingeniería Electrónica, por su atención y colaboración.

José Torres, Ingeniero Electrónico y Asesor Técnico, por su paciencia, y por brindarnos los recursos y conocimientos necesarios para el diseño e implementación de este proyecto.

Horacio Varona, Ingeniero Electrónico y Docente de la Corporación Universitaria de la Costa, por sus grandes aportes y por apoyarnos en las decisiones finales, que conllevaron a la eficiencia de este diseño.

Alfonso Marino, Ingeniero Electrónico y Asesor Técnico, por sus valiosas orientaciones en el desarrollo del diseño, correspondiente a este trabajo de grado.

Leonardo Chica, Ingeniero Electrónico y Docente de la Corporación Universitaria de la Costa, por sus grandes ideas que gracias a ellas se pudo realizar un buen diseño para este proyecto.

Carlos Lizarazo, Ingeniero de sistemas, por su dedicación en la elaboración de la presentación, para la sustentación de nuestro proyecto.

Pedro Camargo, Ingeniero Electrónico, por brindarnos los elementos necesarios para la configuración de la red, y los software incluyentes.

RESUMEN

Diseñar una LAN, incluye una gran responsabilidad y un estudio detallado de lo que se requiere, por parte de quien realiza esta tarea, con el fin lograr un mayor rendimiento en los medios de transmisión y en los equipos a utilizar para la optimización de los procesos; la idea básica tiende a crear una autopista de información, con un soporte lo suficientemente robusto, como para tolerar todo el tráfico de información y la gran transferencia de datos que se presenten; asimismo contar con la ventaja de poder crear diversas conexiones lógicas entre los equipos, pues aunque estos estarán conectados físicamente, no quiere decir que tengan que comunicarse, porque las interacciones entre PC's realmente se establece mediante conexiones lógicas.

Son muchas las herramientas que facilitan al hombre el manejo del recurso informativo, así como el acceso a éste. Una de estas herramientas, que permite utilizar el recurso de la información de manera más eficiente rápida y confiable, la constituyen las redes de computadoras, las cuales aparecen enmarcadas dentro del vertiginoso avance tecnológico, que ha caracterizado a las últimas décadas del presente siglo.

Una red es un conjunto de computadoras o dispositivos de procesamiento conectadas entre sí, de forma lógica y física con la finalidad de optimizar sus recursos y emular el proceso de un sistema de cómputo único.

Palabras Clave: Red de computadores, Redes de información, Acceso a la información, Computadoras

ABSTRACT

To design a LAN, includes a big responsibility and a detailed study of what needs from itself, on the part of whom it realizes this task, with the end to achieve a major yield in the means of transmission and in the teams to be used for the optimization of the processes; the basic idea tends to create an information freeway, with a support the sufficiently robust thing, as to tolerate all the traffic of information and the big transference of information that appear; also to be provided with the advantage of being able to create diverse logical connections between the teams, so although these will be connected physically, does not mean that they have to communicate, because the interactions between PC's really settles by means of logical connections.

There is great the hardware that facilitate to the man the handling of the informative resource, as well as the access to this one. One of this hardware, which allows to use the resource of the information of a more efficient rapid and reliable way, is constituted by the networks of computers, which turn out to be framed inside the vertiginous technological progress, which it has characterized to the last decades of the present century.

A network is a set of computers or devices of prosecution connected between themselves, of logical and physical form for the purpose of optimizing its resources and emulating the process of a system of the only calculation.

Key words: Network of computers, Networks of information, Access to information, Computers.

CONTENIDO

	Pág.
CAPITULO 1. DISEÑO DE UNA RED DE COMPUTADORES PARA LA CORPORACION UNIVERSITARIA DE LA COSTA	
1.1. INTRODUCCION.....	23
1.2. PLANTEAMIENTO DEL PROBLEMA.....	24
1.3. JUSTIFICACION.....	26
1.4. OBJETIVOS.....	27
1.4.1 OBJETIVO GENERAL.....	27
1.4.2 OBJETIVOS ESPECÍFICOS.....	27
CAPÍTULO 2. REDES	
2.1 CONCEPTO DE REDES.....	28
2.2 CRITERIOS DE REDES.....	29
2.3 APLICACIONES.....	30
2.4 PROTOCOLOS.....	32
2.5 ESTÁNDARES.....	32
2.6 ORGANIZACIONES DE ESTANDARIZACIÓN.....	33
2.6.1 Comités de creación de estándares.....	33
CAPÍTULO 3. CONCEPTOS BASICOS	
3.1 CONFIGURACIÓN DE LA LÍNEA.....	37
3.1.1 Punto a punto.....	37
3.1.2 Multipunto.....	38
3.2 TOPOLOGÍAS.....	38
3.2.1 Malla.....	39
3.2.2 Estrella.....	40
3.2.3 Árbol.....	41

3.2.4 Bus	42
3.2.5 Anillo	43
3.2.6 Topologías híbridas	45
3.3 MODOS DE TRANSMISIÓN.....	45
3.3.1 Símplex	45
3.3.2 Semidúplex.	46
3.3.3 Full-dúplex.....	46
3.4 Clases De Redes	47
3.4.1 Red de área local (LAN)	47
3.4.2 Redes de área metropolitana (MAN)	48
3.4.3 Red de área amplia (WAN)	49
3.5 EL MODELO OSI	50
3.5.1 Niveles del modelo OSI	50
3.5.1.1 Nivel físico	50
3.5.1.2 Nivel de enlace de datos	51
3.5.1.3 Nivel de red	52
3.5.1.4 Nivel de transporte	53
3.5.1.5 Nivel de sesión	54
3.5.1.6 Nivel de presentación	55
3.5.1.7 Nivel de aplicación	56

CAPÍTULO 4. REDES DE AREA LOCAL (LAN)

4.1 PROYECTO 802	57
4.1.1 IEEE 802.1	58
4.1.2 LLC	58
4.1.3 MAC	58
4.1.4 Unidad de datos del protocolo (PDU)	58
4.1.4.1 DSAP y SSAP	59
4.1.4.2 Control	59

4.2 ETHERNET	59
4.2.1 Método de acceso: CSMA/CD	60
4.2.2 Direccionamiento	61
4.2.3 Formato de trama	62
4.2.4 Implementación	63
4.2.4.1 10BASE-T: Ethernet de par trenzado	63
4.3 OTRAS REDES ETHERNET	65
4.3.1 Ethernet conmutada	65
4.3.2 Fast Ethernet	66
4.3.2.1 100Base-TX.	68
4.3.3 Gigabit Ethernet	68
4.4 INTRANET	69
4.4.1 Compartición de recursos en la Intranet.	69
4.5 MEDIOS DE TRANSMISION	70
4.5.1 Medios guiados	71
4.5.1.1 Cable coaxial	71
4.5.1.1.1 Tipos de cable coaxial	72
4.5.1.1.1.1 Thick (grueso)	72
4.5.1.1.1.2 Thick (fino)	73
4.5.1.2 Par trenzado	73
4.5.1.2.1 Tipos de cable de par trenzado	75
4.5.1.2.1.1 Cable no blindado (UTP)	75
4.5.1.2.1.2 Cable blindado (STP)	77
4.5.1.3 Fibra óptica	77
4.5.1.3.1 Tipos de fibra óptica	80
4.5.1.3.1.1 Fibras multimodo de índice escalonado	80
4.5.1.3.1.2 Fibras multimodo de índice de gradiente gradual	81
4.5.1.3.1.3 Fibras monomodo	82
4.5.1.3.2 Elementos básicos de un sistema de fibra óptica	83
4.5.1.3.3 Sistemas de conexión	84

4.5.1.4 Aplicaciones	85
4.5.1.5 Comparación entre los diferentes medios de transmisión	85
4.5.1.6 Rendimiento de cables según su ancho de banda	86
4.5.2 Medios de transmisión no guiados	86
4.5.2.1 Comunicaciones vía satélite	86
4.5.2.2 Microondas	89
4.5.2.3 Luz infrarroja	90

CAPÍTULO 5. EQUIPOS DE RED

5.1 EQUIPOS ACTIVOS	92
5.1.1 Tarjeta de red o adaptador	92
5.1.2 Hub o concentrador	97
5.1.2.1 Clases de hubs	99
5.1.2.1.1 Hubs activos	99
5.1.2.1.2 Hubs pasivos	99
5.1.2.2 Funcionamiento	99
5.1.3 Switch	101
5.1.3.1 Funcionamiento	102
5.1.4 Puentes o bridges	105
5.1.5 Ruteador o Router	107
5.1.6 Gateways o pasarelas	110
5.1.7 DTU	111
5.1.8 Grupos de trabajo	111
5.1.8.1 Opción #1: Solución con ruteador	112
5.1.8.2 Opción #2: Solución con switch	113
5.2 EQUIPOS PASIVOS	114
5.2.1 Armarios y gabinetes	114
5.2.2 Racks	115
5.2.3 Patch-panel	116
5.2.4 Bandejas	117

5.2.5 Organizador de cables	117
5.2.6 Patch-cords	117
5.2.7 Patch-cord para fibra óptica	118
5.2.8 Canaletas	118

CAPÍTULO 6. CABLEADO ESTRUCTURADO

6.1 EVOLUCIÓN DE LOS SISTEMAS DE CABLEADO	119
6.2 CONSIDERACIONES	122
6.3 DEFINICIÓN	123
6.4 CARACTERÍSTICAS	124
6.5 SUBSISTEMAS DE CABLEADO ESTRUCTURADO	124
6.5.1 Subsistema de administración	125
6.5.1.1 Armarios repartidores	126
6.5.2 Subsistema Horizontal	127
6.5.2.1 Cableado horizontal.	128
6.5.2.2 Área de trabajo	129
6.5.3 Subsistema vertical	130
6.6 EJEMPLO DE UN CABLEADO ESTRUCTURADO TÍPICO	134

CAPÍTULO 7. PROTOCOLO TCP/IP

7.1 DEFINICIÓN DE PROTOCOLO TCP/IP	132
7.1.1 TCP/IP e Internet	132
7.1.2 TCP/IP y OSI	133
7.1.3 Encapsulado	133
7.2 NIVEL DE RED	134
7.2.1 Protocolo IP	134
7.2.1.1 Datagramas	135
7.3 DIRECCIONAMIENTO	136
7.3.1 Clases de redes	137
7.3.2 Nodos con más de una dirección.	138

7.3.2.1 Ejemplo de interconexión entre tres redes	138
7.4 SUBREDES	139
7.4.1 Tres niveles de jerarquía	141
7.4.2 Enmascaramiento	141
7.4.3 Direcciones IP especiales y reservadas	143
7.5 OTROS PROTOCOLOS EN EL NIVEL DE RED	144
7.5.1 Protocolo de resolución de direcciones (ARP)	144
7.5.2 Protocolo de resolución inversa de direcciones (RARP)	145
7.5.3 Protocolo de mensajes de control de Internet (ICMP)	146
7.5.4 Protocolo de mensajes de grupos de Internet (IGMP)	146
7.6 NIVEL DE TRANSPORTE	147
7.6.1 Protocolo de datagramas de usuario (UDP)	148
7.6.2 Protocolo de control de transmisión (TCP)	149
7.6.2.1 El segmento de TCP	151

CAPÍTULO 8. PROCESO DE TRABAJO

8.1 DISEÑO Y PLANIFICACIÓN DE LA RED	154
8.1.1 Segmentar la Universidad	154
8.1.2 Levantamiento de la red actual	155
8.1.2.1 Bloque1 Piso1	156
8.1.2.2 Bloque1 Piso2	159
8.1.2.3 Bloque2 Piso4	159
8.1.2.4 Bloque3 Piso2	160
8.1.2.5 Bloque3 Piso3	160
8.1.2.6 Bloque5 Piso2	161
8.1.2.7 Bloque32 años, Piso2	161
8.1.3 Modelo de red de área local para cada dependencia	162
8.1.4 Interconectar las redes que operan en la CUC	165
8.1.4.1 Descripción del diseño	166
8.1.4.2 Ventajas del diseño	168

8.1.4.3 Recomendaciones	168
8.1.4.4 Especificaciones generales de diseño	169
8.1.4.4.1 Cuarto de Telecomunicaciones	169
8.1.4.4.2 Topología de la red	170
8.1.4.4.3 Protocolo de bajo nivel	170
8.1.4.4.4 Sistemas Operativos	171
8.1.4.4.5 Protocolos de comunicación	171
8.1.4.4.6 Elección de los elementos pasivos	172
8.1.4.4.7 Elección de los elementos activos	176
8.2 IMPLEMENTACIÓN	178
8.3 MONTAJE DE LA RED	179
8.3.1 Colocación de canaletas	179
8.3.2 Fijación de los puntos de red y el patch-panel	180
8.3.3 Cableado	180
8.3.4 Conexión de los puntos de red	181
8.3.5 Desconexión	182
8.3.6 Conexionado del patch-panel	183
8.3.7 Construcción de los patch-cord	183
8.3.8 Cable cruzado (Crossover)	184
8.3.9 Verificación del cableado	185
8.3.10 Conexionado del switch	186
8.4 CONFIGURACIÓN	186
8.5. MANTENIMIENTO DEL CABLEADO DE UNA RED INFORMÁTICA	189
9. GLOSARIO	190
10. CRONOGRAMA DE ACTIVIDADES	194
11. CONCLUSION	195
BIBLIOGRAFIA	197
ANEXOS	198

LISTA DE TABLAS

	Pág.
Tabla 4.1 Normas del proyecto 802	57
Tabla 4.2 Comparación entre Modelo OSI y el Modelo IEEE	57
Tabla 4.3 Comparación entre las implementaciones de Ethernet Gigabit	69
Tabla 4.4 Características de la nomenclatura de los cables Ethernet	72
Tabla 4.5 Comparación entre los diferentes medios de transmisión	85
Tabla 7.1 Tabla de direccionamiento	139
Tabla 7.2 Máscara de subred	142
Tabla 7.3 Direcciones IP reservadas	143
Tabla 7.4 Rango de direcciones IP reservadas	144
Tabla 8.1. Crossover	184

LISTA DE FIGURAS

	Pág.
Figura 2.1 Redes.....	28
Figura 3.1. Configuración de una línea punto a punto	37
Figura 3.2. Configuración de línea multipunto	38
Figura 3.3 Malla.....	40
Figura 3.4 Topología en estrella	41
Figura 3.5 Topología en árbol	41
Figura 3.6 Topología bus.....	42
Figura 3.7 Topología en anillo.....	44
Figura 3.8 Topología híbrida	45
Figura 3.9 Símplex.....	46
Figura 3.10 Semidúplex.....	46
Figura 3.11 Full-Dúplex	47
Figura 3.12 LAN	48
Figura 3.13 MAN	49
Figura 3.14 WAN	50
Figura 4.1 Formato PDU	59
Figura 4.2 IEEE 802.3	60
Figura 4.3 Colisión en CSMA/CD	61
Figura 4.4 Trama MAC 802.3	62
Figura 4.5 Conexión 10BASE-T	64

Figura 4.6 Topología 10BASE-T	65
Figura 4.7 Una Ethernet que usa un conmutador	66
Figura 4.8 Cable coaxial	71
Figura 4.9 Composición del cable coaxial	71
Figura 4.10 Cable de par trenzado	75
Figura 4.11 Fibra óptica	77
Figura 4.12 Estructura de una Fibra Multimodo de Índice Escalonado	81
Figura 4.13 Estructura de una Fibra Multimodo de Índice de Gradiente Gradual	82
Figura 4.14 Estructura de Fibra Monomodo	83
Figura 4.15 Elementos básicos de un sistema de fibra óptica	84
Figura 4.16 Rendimiento de cables según ancho de banda	86
Figura 4.17 Red de datos AT&T con satélite y ordenador central	89
Figura 4.18 Antena de Microondas	90
Figura 4.19 Luz infrarroja	91
Figura 5.1 Tarjetas de red	92
Figura 5.2 Hub físico	97
Figura 5.3 Conexiones entre hubs	98
Figura 5.4 Conexiones entre hubs con conector BNC	98
Figura 5.5 Hub activo	99
Figura 5.6 Funcionamiento del hub	100
Figura 5.7 Switch	101
Figura 5.8 Switch de 24 puertos	101

Figura 5.9 Switch comercial	102
Figura 5.10 Funcionamiento del switch	102
Figura 5.11 Filtrado	103
Figura 5.12 Conexiones entre switch	105
Figura 5.13 conexión de dos LANs por medio de un puente	105
Figura 5.14 Segmentos de red antes del puente	106
Figura 5.15 Segmentos de red después del puente	106
Figura 5.16 Puentes para redes inalámbricos	107
Figura 5.17 Router	107
Figura 5.18 Router en el modelo OSI	108
Figura 5.19 Grupos de trabajo	112
Figura 5.20 Solución con ruteador	112
Figura 5.21 Solución con switch	113
Figura 5.22 Armario	114
Figura 5.23 Armario y gabinete	115
Figura 5.24 Racks	115
Figura 5.25 Patch-panel	116
Figura 5.26 Patch-panel con cableado	116
Figura 5.27 Bandejas	117
Figura 5.28 Organizador de cable	117
Figura 5.29 Patch-cord	117
Figura 5.30 Patch-cord para fibra óptica	118
Figura 5.31 Canaletas	118

Figura 6.1 Cableado estructurado	119
Figura 6.2 Esquema de la evolución en los sistemas de cableado	121
Figura 6.3 Distribución de los subsistemas de cableado estructurado	125
Figura 6.4 Estructura jerárquica de los repartidores	127
Figura 6.5 Cableado horizontal	128
Figura 6.6 Distancias permitidas entre los diferentes puntos de conexión	129
Figura 6.7 Tomas de red	129
Figura 6.8 Distancia requerida desde el toma hasta el PC	130
Figura 6.9 Mecanismos de conexión entre los paneles principales e intermedios	130
Figura 6.10 Cableado estructurado típico	131
Figura 7.1 Una internet de acuerdo a TCP/IP	133
Figura 7.2 TCP/IP y el modelo OSI	134
Figura 7.3 Datagrama IP	136
Figura 7.4 Dirección Internet	137
Figura 7.5 Clases de direcciones IP	138
Figura 7.6 Ejemplo de interconexión de redes	139
Figura 7.7 Una red con dos niveles de jerarquía sin subredes	140
Figura 7.8 Una red con tres niveles de jerarquía (subredes)	140
Figura 7.9 Dirección de una red con y sin subredes	141
Fig. 7.10. A.R.P	145
Figura 7.11 Direcciones de puertos	147
Figura 7.12 Formato de un datagrama UDP	149
Figura 7.13 Formato del segmento TCP	150

Figura 8.1 Estructura lógica de las actuales redes CUC	156
Figura 8.2 Mecanismo de conexión	163
Figura 8.3 Interconexión entre switches	165
Figura. 8.4. Estructura lógica de la LAN CUC	166
Figura 8.5. Cable UTP cat5e	172
Figura 8.6. Estándar T568A	173
Figura 8.7. Sistema de cableado	174
Figura 8.8. Patch-panel de 24 puertos	174
Figura 8.9. Patch-plug	175
Figura 8.10. Conectores RJ45	175
Figura 8.11. Canaleta de dos cavidades	176
Figura 8.12. Router	176
Figura 8.13. Switch maestro	177
Figura 8.14. Switches esclavos	177
Figura 8.15. Mecanismo de Conexión	181
Figura 8.16. Ponchadora de impacto	182
Figura 8.17. Conexión del Patch-Panel	183
Figura 8.18. Ponchadora	184
Figura 8.19. Comprobador de cables	185
Figura 8.20. Figura Verificación del cableado	185

LISTA DE ANEXOS

	Pág.
Anexo 1. Planos CUC	199
Anexo 2. Esquema de la red del laboratorio de Automatismo	212

1.1. INTRODUCCION

Actualmente, el manejo de la información de modo eficiente constituye una de las principales preocupaciones dentro de cualquier organización, sea esta de origen público o privado, por lo que se hace necesario manejarla y emplearla con mucho criterio, pues de ello depende, en gran medida, el éxito o fracaso del manejo de la misma.

Son muchas las herramientas que facilitan al hombre el manejo del recurso informativo, así como el acceso a éste. Una de estas herramientas, que permite utilizar el recurso de la información de manera más eficiente rápida y confiable, la constituyen las redes de computadoras, las cuales aparecen enmarcadas dentro del vertiginoso avance tecnológico, que ha caracterizado a las últimas décadas del presente siglo.

Una red es un conjunto de computadoras o dispositivos de procesamiento conectadas entre sí, de forma lógica y física con la finalidad de optimizar sus recursos y emular el proceso de un sistema de cómputo único.

Las universidades, deben garantizar a sus integrantes el acceso a la información con fines eminentemente investigativos, por lo que no podían permanecer ajenas al uso de ésta herramienta. Más concretamente, la Corporación Universitaria de la Costa, lo ha entendido así, y ha adquirido desde hace varios años una gran variedad y cantidad de computadoras y equipos de comunicaciones para satisfacer sus propias necesidades.

1.2. PLANTEAMIENTO DEL PROBLEMA

Hace algún tiempo, se viene poniendo en práctica la filosofía de los recursos compartidos, así como el uso de Internet. Esta modalidad ha permitido dar conexión de red entre la red de Admisiones, los departamentos del núcleo, tales como: la Facultad de Derecho, Ingeniería, Contaduría, Arquitectura y Análisis, entre otras, ubicados en distintos bloques de la Corporación.

Sin embargo, todavía existen dentro de la Corporación, dependencias que, aún cuando lo requieren, no están conectadas a esta red. Un ejemplo de ello lo constituyen las oficinas de Bienestar, Biblioteca y las Facultades de Psicología y Tecnología en Telecomunicaciones, las cuales no están conectadas con la red de Admisiones y Registros, ni a ninguna red externa. Esta, es una de las razones que motivan a crear un diseño de Red para la Corporación Universitaria de la Costa.

Los siguientes aspectos son variables por considerar:

- a. Hacer el estudio de la red actual en la Corporación y con base en él, considerar las condiciones de trabajo.
- b. Analizar el plano del edificio para poder esquematizar el diseño del cableado.
- c. Identificar los lugares del edificio, donde se requieren puntos de interconexión.
- d. Hacer las conexiones entre los computadores de las diferentes dependencias, para que todas, puedan interactuar entre sí.

- e. Crear una autopista de transmisión basada en fibra óptica, para que se puedan integrar varios programas, en esta oportunidad y en futuras aplicaciones.
- f. Considerar la posibilidad de establecer un nodo de servicio de Internet para los estudiantes, a precio más económico que el ofrecido por el comercio.

1.3. JUSTIFICACION

La Corporación Unicosta, es una entidad educativa, que consta de varios bloques, donde funcionan distintas dependencias de carácter administrativo y académico, entre estas dependencias debe existir cierta interconexión. Pero muchas de estas dependencias no cuentan con el acceso a redes de comunicación, lo cual le dificulta notoriamente al personal adscrito, aprovechar el recurso informativo que podrían proveerle otras redes, limitándose de esta manera la actividad investigativa del personal, así como la comunicación directa de éstas con otras redes, ubicadas dentro del mismo ámbito universitario, inclusive dentro del mismo edificio. Por ello, el diseño de una red interna de comunicación en la Corporación Universitaria de la Costa surge como una solución a la necesidad de resolver este inconveniente, pues este proyecto, permite definir un cableado estructurado que básicamente, trata de unir varias redes pequeñas, conformadas por cada bloque en una misma red, que sería una autopista de comunicación, con el fin que cada dependencia pueda tener acceso directo a otras dependencias en caso de necesitar la información que ellas contengan, de una forma rápida y confiable, bajo todas las normas de seguridad pertinentes.

Además con esta tendencia de comunicación la Corporación tendrá la oportunidad de actualizarse en lo que a sistema de redes se refiere; si se tiene en cuenta que muchas de las carreras que aquí se cursan, tienen orientaciones tecnológicas y es de muy buena imagen contar con un sistema que además de ser necesario y moderno representa una nueva alternativa para ayudar al desarrollo integral de las redes del entorno universitario.

1.4. OBJETIVOS

1.4.1 OBJETIVO GENERAL

Diseñar una Red para que las diferentes dependencias de la Corporación, tengan acceso a las redes tanto internas como externas.

1.4.2 OBJETIVOS ESPECÍFICOS

- ✓ Diseñar un sistema de cableado estructurado para la red general de computadores sobre la que trabajará todo el edificio

- ✓ Determinar los dispositivos de interconexión que serán necesarios, para el diseño de la red.

- ✓ Crear una autopista de información que soporte las condiciones iniciales de conexión propuestas para la transferencia de información, y que a su vez pueda sobrellevar futuras aplicaciones.
- ✓ Diseñar e instalar una Red de Computadores, para el Laboratorio de Automatismos, perteneciente a la Facultad de Ingenierías de la Corporación Universitaria de la Costa

2. REDES

2.1 CONCEPTO DE REDES

Una red es un sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota (de voz, vídeo, datos, etc.) y facilitar el intercambio de información entre usuarios con intereses comunes.

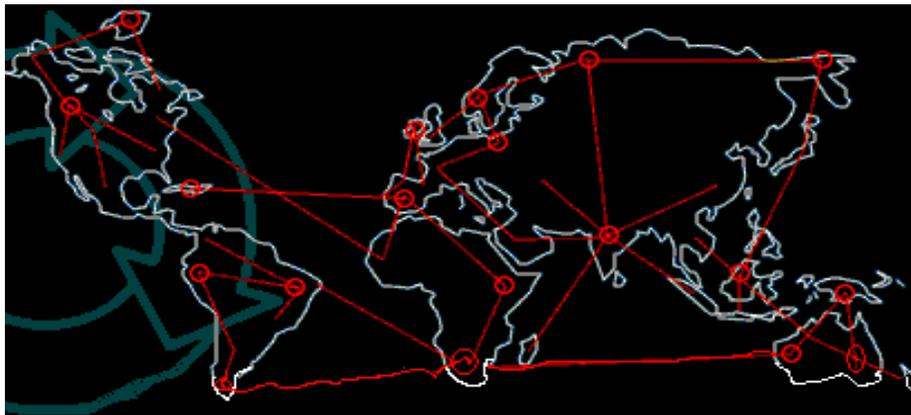


Figura 2.1 Redes

Esta formada por un conjunto de dispositivos (denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red.

La más simple de las redes conecta dos computadoras, permitiéndoles compartir archivos e impresos. Una red mucho más compleja conecta todas las computadoras de una empresa o compañía en el mundo.

2.2 CRITERIOS DE REDES

Para que sea considerada efectiva y eficiente, una red debe satisfacer un cierto número de criterios. Los más importantes son las prestaciones, la fiabilidad y la seguridad.

a. **Prestaciones.** Las prestaciones se pueden medir de muchas formas, incluyendo el tiempo de tránsito y el tiempo de respuesta. El tiempo de tránsito es la cantidad de tiempo necesario para que un mensaje viaje de un dispositivo a otro. El tiempo de respuesta es el tiempo transcurrido entre una petición y una respuesta. Las prestaciones de una red dependen de un cierto número de factores, incluyendo el número de usuarios, el tipo de medio de transmisión, las capacidades de los dispositivos hardware conectado y la eficiencia del software.

- b. **Fiabilidad.** Además de tener en cuenta la exactitud de la entrega, la fiabilidad de la red se mide por la frecuencia de fallo, el tiempo que le cuesta al enlace recuperarse del fallo y la robustez de la red dentro de la catástrofe.
- c. **Seguridad.** Los aspectos de seguridad de la red incluyen proteger los datos contra accesos no autorizados y contra los virus.
 - ✓ **Accesos de autorizados.** Para que una red sea útil, los datos sensibles deben estar protegidos frente a acceso no autorizados. La protección puede llevarse a cabo un cierto número de niveles. En el nivel más bajo están los códigos y contraseñas de identificación de los usuarios. A un nivel más alto se encuentran las técnicas de cifrado. Con estos mecanismos, los datos se alteran de forma sistemática de forma que si son interceptados por un usuario no autorizado sean ininteligibles.
 - ✓ **Virus.** Debido a que la red es accesible desde muchos puntos, puede ser susceptible de sufrir ataques de virus de computadoras. Un virus es un código que se ha introducido en la red ilícitamente y que genera daños al sistema. Una buena red está protegida ante ataques de virus mediante mecanismos de software y hardware diseñados específicamente para ese propósito.

2.3 APLICACIONES

Algunas de las aplicaciones de las redes en distintos campos son las siguientes:

- a. **Marketing y ventas.** Las redes de computadoras se usan extensivamente en las organizaciones de marketing y de ventas. Los profesionales del marketing las usan para recolectar, intercambiar y analizar relacionados con las necesidades y con los ciclos de desarrollo de productos.

- b. **Servicios financieros.** Los servicios financieros actuales son totalmente dependiente de las redes de computadoras. Las aplicaciones incluyen búsqueda de historia de créditos, intercambio de moneda extranjera y servicios de investigación y transferencia electrónica de fondos, las cuales permiten a un usuario transferir dinero sin ir a un banco.

- c. **Fabricación.** Las redes de computadoras se usan actualmente en muchos ámbitos de la fabricación, incluyendo el proceso de fabricación en sí mismo.

- d. **Mensajería electrónica.** Probablemente, la aplicación de las redes más extendida es el correo electrónico (e-mail).

- e. **Servicios de directorios.** Los servicios de directorios permiten almacenar listas de archivos en una en una localización centralizada para acelerar las operaciones de búsqueda a nivel mundial.

- f. **Servicios de información.** Los servicios de información de la red incluyen boletines y bancos de datos. Un servidor Web que ofrezca especificaciones técnicas para un producto nuevo es un servicio de información.

- g. **Intercambio electrónico de datos (EDI).** El EDI permite la transmisión de información comercial.
- h. **Teleconferencia.** La teleconferencia permite llevar a cabo conferencias sin que los participantes estén en el mismo lugar. Las aplicaciones incluyen conferencias sencillas de texto, conferencias de voz y videoconferencias.
- i. **Teléfono celular.** En el pasado, dos socios que quisieran utilizar los servicios de la compañía telefónica tenían que estar enlazados por una conexión física fija. Las redes celulares actuales hacen posible mantener conexiones con teléfonos móviles incluso mientras se está viajando a largas distancias.
- j. **Televisión por cable.** Los servicios futuros a proporcionar por la red de televisión por cable pueden incluir video bajo demanda, así como la misma información, financiera y servicios de comunicación actualmente proporcionados por las compañías telefónicas y las redes de computadoras.

2.4 PROTOCOLOS

En las redes de computadoras, la comunicación se lleva a cabo entre distintas entidades de distintos sistemas. Una entidad es cualquier cosa capaz de enviar o recibir información. Algunos ejemplos incluyen programas de aplicación, paquetes de transferencia de archivos, navegadores, sistemas de gestión de bases de datos y software de correo electrónico. Un sistema es un objeto físico que contiene una o más entidades. Algunos ejemplos incluyen las computadoras y los terminales. Pero no basta con que dos entidades se envíen flujos de bits entre sí para que se entiendan. Para que exista comunicación, las entidades deben estar de acuerdo en un protocolo. Un protocolo es un conjunto de reglas que gobiernan la comunicación de datos. Un protocolo define qué se comunica, cómo se comunica y cuándo se comunica. Los elementos claves de un protocolo son su sintaxis, su semántica y temporización.

2.5 ESTÁNDARES

Con la existencia de tantos factores a sincronizar, es necesario llevar a cabo un gran trabajo de coordinación entre los nodos de una red si se quiere que haya algún tipo de comunicación, independientemente de que sea exacta y eficiente. Un estándar proporciona un modelo de desarrollo que hace posible que un producto funcione adecuadamente con otros sin tener en cuenta quien lo ha fabricado.

Los estándares son esenciales para crear y mantener un mercado abierto y competitivo entre los fabricantes de los equipos y para garantizar la interoperabilidad nacional e internacional de los datos, la tecnología y los procesos de telecomunicaciones.

El pragmatismo actual y la presión de los consumidores ha forzado a la industria a reconocer la necesidad de modelos generales y hay un acuerdo global de lo que deben ser estos modelos. La inteligencia y la previsión de los diseñadores parecen ser tales que los estándares que están siendo adoptados actualmente facilitaran mas que retrasaran el desarrollo técnico

2.6 ORGANIZACIONES DE ESTANDARIZACIÓN

Los estándares son desarrollados mediante la cooperación entre comités de creación de estándares, foros y agencias reguladoras de los gobiernos.

2.6.1 Comités de creación de estándares. Aunque hay muchas organizaciones que se dedican a la definición y establecimiento de estándares para datos y comunicaciones, en Norteamérica se confía fundamentalmente en aquellos publicados por los siguientes:

ISO: The International Standards Organization (ISO; también denominado como Organización Internacional para la Estandarización) es un organismo multinacional cuyos miembros provienen fundamentalmente de los comités de creación de estándares de varios gobiernos a lo largo del mundo. Creado en 1947, el ISO es una organización totalmente voluntaria dedicada a acuerdos mundiales sobre estándares internacionales. Con un número de miembros que actualmente incluyen cuerpos representativos de 82 naciones industrializadas, su objetivo es facilitar el intercambio internacional de productos y servicios, proporcionando modelos de compatibilidad, mejoras de calidad, mejoras de productividad y precios más baratos. El ISO es activo en el desarrollo de la cooperación en los ámbitos científicos, tecnológicos y de las actividades económicas. De interés primordial para este libro son los esfuerzos de ISO en el campo de la

tecnología de la información, que han resultado en la creación del modelo de Interconexión de Sistemas Abiertos (OSI) para redes de comunicaciones. Los Estados Unidos están representados en el ISO por el ANSI.

ITU-T: A principios de la década de los 70, un cierto número de países estaba definiendo estándares nacionales para telecomunicaciones, pero a pesar de ello seguían habiendo muy poca compatibilidad internacional. Las Naciones Unidas respondieron a este problema, formando como parte de su Unión Internacional de Telecomunicaciones (ITU), un comité, denominado comité consultivo para la telefonía y la telegrafía internacional. Este comité estaba dedicado al desarrollo y establecimiento de estándares para telecomunicaciones en general y para la telefonía y los sistemas de datos en particular. El primero de marzo de 1993, el nombre de éste comité se cambió a Unión Internacional de Telecomunicaciones- Sector de Estándares de Telecomunicaciones (ITU-T).

La ITU-T, está dividida en grupos de estudio, cada uno de los cuales se dedica a aspectos distintos de la industria. Los comités nacionales (como ANSI en los Estados Unidos y el CEPT en Europa) envían propuestas a éstos grupos de estudio. Si los grupos de estudio están de acuerdo la propuesta es ratificada y se convierte en una parte de los estándares de la ITU-T, que se emiten cada 4 años. Los estándares mejor conocidos de la ITU-T son las series V (V.32, V.33, V.42) que definen la transmisión de datos a través de líneas telefónicas; la serie X (X.25, X.400 y X.500) que definen la transmisión de datos a través de redes digitales públicas; correo electrónico, servicios de directorios y la RDSI, que incluyen partes de las otras series y definen la emergente red digital internacional.

Los productos actuales incluyen una ampliación de RDSI llamada RDSI de banda ancha, conocido popularmente como la autopista de la información.

ANSI: A pesar de su nombre, el Instituto Nacional Americano para la estandarización ANSI es una corporación completamente privada sin ánimo de lucro que no tiene ninguna relación con el gobierno federal de los estados Unidos. Sin embargo todas las actividades de ANSI están orientadas hacia el desarrollo de los Estados Unidos, y sus ciudadanos tienen una importancia primordial. Los objetivos expresados por ANSI incluyen servir como una institución de coordinación nacional para la estandarización voluntaria dentro de los Estados Unidos, persiguiendo que la adopción de los estándares permita hacer avanzar la economía de los Estados Unidos y asegurar la participación y la protección del interés público. Los temas actuales de discusión incluyen planificación e ingeniería de interconexión de redes; servicios, señalización y arquitectura RDSI; y jerarquía óptica (SONET).

IEEE: El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) es la mayor sociedad profesional de ingeniería del mundo. De ámbito internacional, sus objetivos son el desarrollo de la teoría, la creatividad y la cantidad de los productos de la ingeniería, la electrónica y la radio, así como otras ramas relacionadas de la ingeniería. Como uno de sus objetivos principales, el IEEE prevé el desarrollo y adopción de estándares internacionales para la computación y comunicación. El IEEE tiene un comité especial para las redes LAN, del cual se ha sugerido el proyecto 802 (por ejemplo, los estándares 802.3, 802.4 y 802.5).

EIA: En la línea de ANSI, la Asociación de Industrias Electrónicas (EIA) es una organización sin ánimo de lucro que dedicada a la promoción de aspectos de la fabricación electrónica. Sus objetivos incluyen el despertar el interés de la educación pública y hacer esfuerzos para el desarrollo de los estándares. En el campo de la tecnología de la información, la EIA ha hecho contribuciones significativas mediante la definición de interfases de conexión física y de especificaciones de señalización eléctrica para la comunicación de datos. En particular, el EIA-232-D, EIA-449 y EIA-530, que definen la transmisión serie entre dos dispositivos digitales (por ejemplo, computadora a módem)

3. CONCEPTOS BASICOS

3.1 CONFIGURACIÓN DE LA LÍNEA

La configuración de la línea se refiere a la forma en que dos o más dispositivos que se conectan a un enlace. Un enlace es el medio de comunicación física que transfiere los datos de un dispositivo a otro. A efectos de visualización es sencillo imaginar cualquier enlace como una línea que se dibuja entre dos puntos. Para que haya comunicación, dos dispositivos deben estar conectados de alguna forma al mismo enlace simultáneamente. Hay dos configuraciones de línea posibles: punto a punto y multipunto.

3.1.1 Punto a punto. Una configuración de línea punto a punto proporciona un enlace dedicado entre dos dispositivos. Toda la capacidad del canal se reserva para transmisión entre ambos dispositivos. La mayoría de las configuraciones punto a punto usan cables para conectar los extremos, pero también son posibles otras opciones, como las microondas o los satélites de enlace.

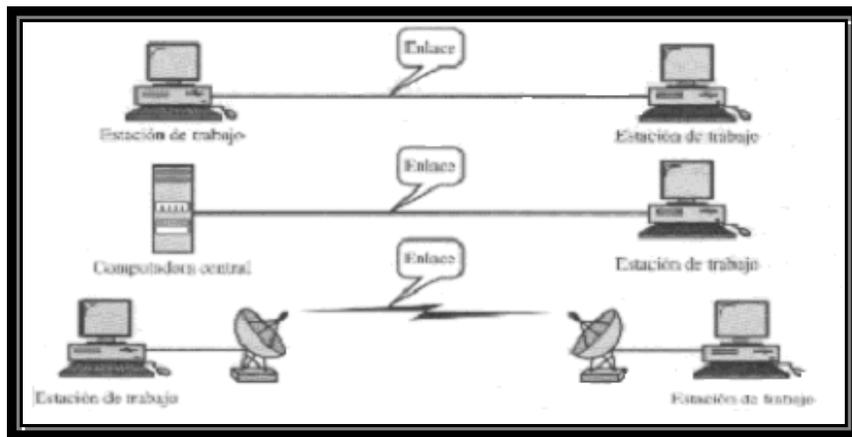


Figura 3.1. Configuración de una línea punto a punto

Cuando se cambian los canales de la TV con control remoto mediante mando a distancia por infrarrojos, se establecen conexiones de punto a punto entre el mando a distancia y el sistema de control de televisión.

3.1.2 Multipunto. La configuración de línea multipunto es una conexión en la que varios dispositivos comparten el mismo enlace.

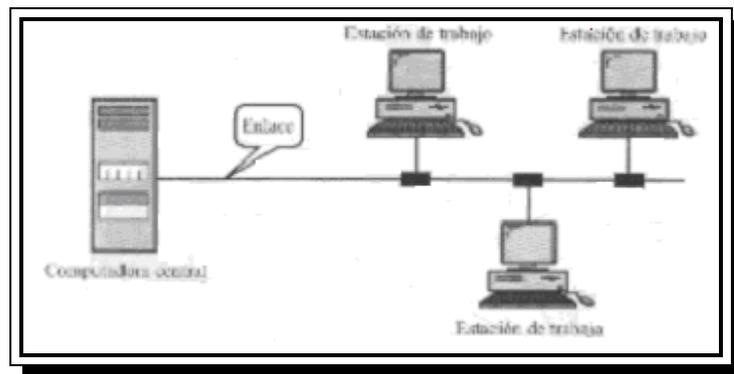


Figura 3.2. Configuración de línea multipunto

En un entorno multipunto, la capacidad del canal es compartida en el espacio o en el tiempo. Si varios dispositivos pueden usar el enlace de forma simultánea, se dice que hay una configuración de línea compartida espacialmente. Si los usuarios deben compartir la línea por turnos, se dice que se trata de una configuración de línea de tiempo compartido.

3.2 TOPOLOGÍAS

El termino de topología se refiere a la forma en que esta diseñada la red, bien físicamente o lógicamente. Dos o más dispositivos se conectan a un enlace; dos o más enlaces forman una topología.

La topología de una red es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre si (habitualmente denominados nodos). Hay cinco posibles tecnologías básicas: malla, estrella, árbol, bus y anillo. Estas cinco clases describen como están interconectados los dispositivos de una red, lo que no indica su posición física. Por ejemplo, que exista una topología en estrella no significa que todas las computadoras de la red deban estar situadas físicamente en forma de estrella alrededor de un concentrador. Una cuestión a considerar al elegir una topología es el estado relativo de los dispositivos a enlazar. Hay dos relaciones posibles: igual a igual o paritaria, donde todos los dispositivos comparten el enlace paritariamente, y primario-secundario, donde un dispositivo controla el tráfico y los otros deben transmitir a través de él.

3.2.1 Malla. En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos. Una malla ofrece varias ventajas sobre otras topologías de red. En primer lugar, el uso de los enlaces dedicados garantiza que cada conexión solo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos. En segundo lugar, una topología en malla es robusta. Si un enlace falla, no inhabilita todo el sistema.

Otra ventaja es la privacidad o la seguridad. Cuando un mensaje viaja a través de una línea dedicada solamente lo ve el receptor adecuado. Finalmente, los enlaces punto a punto hacen que se puedan identificar y aislar los fallos mas fácilmente. Esta facilidad permite que el gestor de red pueda descubrir la localización precisa del fallo y ayudar a buscar solución.

Las principales desventajas de la malla se relacionan con la cantidad de cable y el número de puertos de entrada/salida necesarios. En primer lugar, la instalación y reconfiguración de la red es difícil, debido a que cada dispositivo debe estar conectado a cualquier otro. En segundo lugar la masa de los cables puede ser mayor que el espacio disponible para acomodarla (en paredes, techos o suelos). Y finalmente, el hardware necesario para conectar cada enlace (puertos de E/S y cables) puede ser muy costoso. Por estas razones, las topologías, en malla se suelen instalar habitualmente en entornos reducidos.

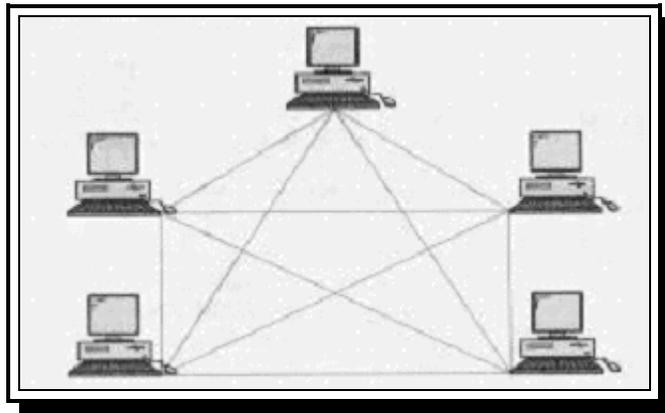


Figura 3.3 Malla

3.2.2 Estrella. En la topología estrella cada dispositivo cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central, habitualmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí. A diferencia de la topología en malla, la topología en estrella no permite el tráfico directo entre de dispositivos. El concentrador actúa como un intercambiador: si un dispositivo quisiera enviar datos a otro, envía los datos al controlador, que los retransmite al dispositivo final.

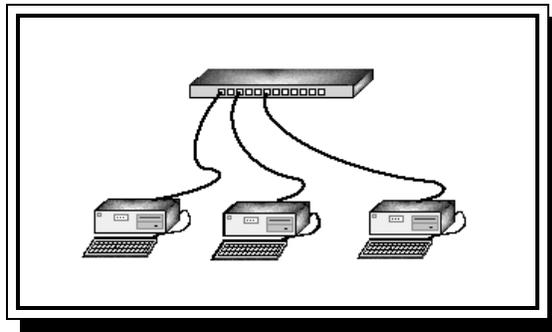


Figura 3.4 Topología en estrella

3.2.3 Árbol. La topología en árbol es una variante de la estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red; sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central.

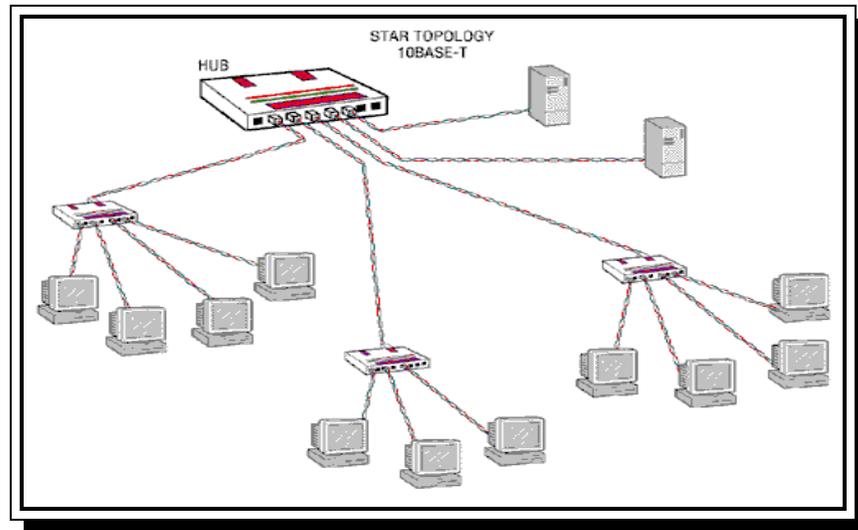


Figura 3.5 Topología en árbol

El concentrador central del árbol es un concentrador activo. Un concentrador activo contiene un repetidor, es decir, un dispositivo hardware que regenera los patrones de bits recibidos antes de retransmitirlos.

Los concentradores secundarios pueden ser activos o pasivos. Un concentrador pasivo proporciona solamente una conexión física entre los dispositivos conectados.

Las ventajas y desventajas de la topología en árbol son generalmente las mismas que las de una estrella. Sin embargo, la inclusión de concentradores secundarios tiene dos ventajas más. Primero permiten que se conecten más dispositivos a un único concentrador central y puede, por tanto, incrementar la distancia que puede viajar la señal entre dos dispositivos. Segundo, permite a la red aislar y priorizar las comunicaciones de distintas computadoras.

La tecnología de la TV por cable es un buen ejemplo de la topología en árbol, ya que el cable principal, que sale de las instalaciones centrales, se divide en grandes ramas y cada rama se divide en otras más pequeñas hasta que se llega a los consumidores finales. Los concentradores se usan cada vez que se divide el cable.

3.2.4 Bus. Las topologías anteriores describen configuraciones punto a punto. Sin embargo una topología en bus es multipunto. Un cable largo actúa como una red troncal que conectan todos los dispositivos de la red.

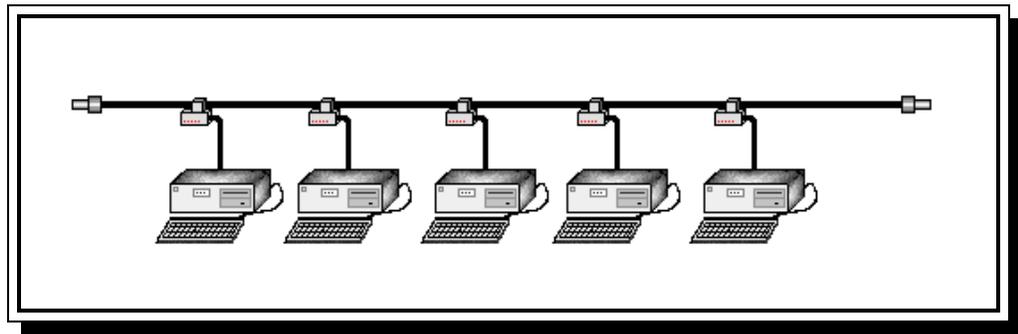


Figura 3.6 Topología bus

Los nodos se conectan al bus mediante cables de conexión (latiguillos) y sondas. Cuando las señales viajan a través de la red troncal, parte de su energía se transforma en calor por lo que la señal se debilita a medida que viaja por el cable. Por esta razón, hay un límite en el número de conexiones que un bus puede soportar y en la distancia entre estas conexiones. Entre las ventajas de la topología se incluye la sencillez de la instalación. El cable troncal puede tenderse por el camino más eficiente y, después, los nodos se pueden conectar al mismo mediante líneas de conexión de longitud variable. De esta forma se puede conseguir que un bus use menos cable que las otras topologías.

Entre sus desventajas se incluye lo dificultoso de su reconfiguración y del aislamiento de los fallos. Habitualmente los buses se diseñan para obtener una eficiencia óptima cuando se instalan. Por tanto, pueden ser difíciles añadir nuevos dispositivos. Como se dijo anteriormente, la reflexión de la señal en los conectores puede causar degradación de su calidad. Esta degradación puede ser controlada limitando el número y el espacio de los dispositivos conectados a una determinada longitud de cable. Añadir nuevos dispositivos puede obligar a modificar o reemplazar el cable troncal. Además, un fallo o rotura en el cable del bus interrumpe todas las transmisiones, incluso entre dispositivos que están en la parte de red que no falla. Esto se debe a que el área dañada refleja las señales hacia la dirección del origen, creando ruido en ambas direcciones.

3.2.5 Anillo. En una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino.

Cada dispositivo del anillo incorpora un repetidor. Cuando un dispositivo recibe una señal para otro dispositivo, su repetidor regenera los bits y los retransmite al anillo.

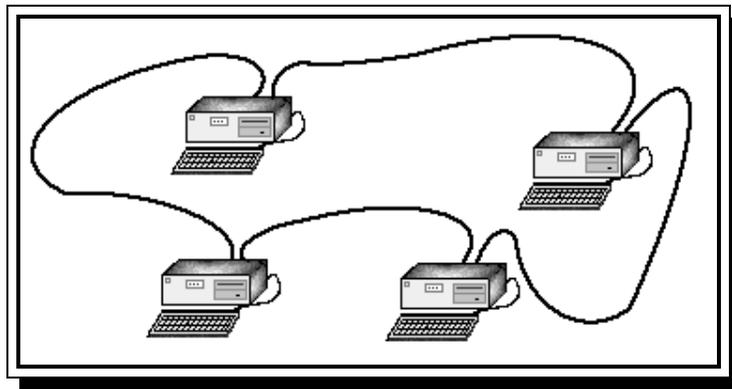


Figura 3.7 Topología en anillo

Un anillo es relativamente fácil de instalar y reconfigurar. Cada dispositivo está enlazado solamente a sus vecinos inmediatos (físicos o lógicos). Para añadir o quitar dispositivos, solamente hay que mover dos conexiones. Las únicas restricciones están relacionadas con aspectos del medio físico y el tráfico (máxima longitud del anillo y número de dispositivos).

Además, los fallos se pueden aislar de forma sencilla. Generalmente, en un anillo hay una señal en circulación continuamente. Si un dispositivo no recibe una señal en un periodo de tiempo especificado, puede emitir una alarma. La alarma alerta al operador de la red de la existencia del problema y de su localización.

Sin embargo, el tráfico unidireccional puede ser una desventaja. En anillos sencillos, una rotura del anillo puede inhabilitar toda la red. Esta debilidad se puede resolver usando un anillo dual o un conmutador capaz de puntear la rotura.

3.2.6 Topologías híbridas. A menudo, una red combina varias topologías mediante subredes enlazadas entre sí para formar una topología mayor. Por ejemplo, un departamento de una empresa puede decidir usar una topología de bus mientras otro puede tener un anillo. Ambas pueden ser conectadas entre sí a través de un controlador central mediante una topología en estrella.

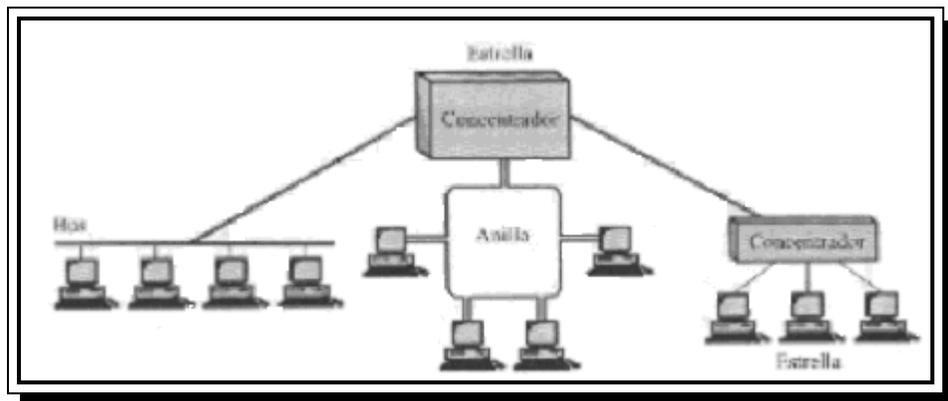


Figura 3.8 Topología híbrida

3.3 MODOS DE TRANSMISIÓN

El término modo de transmisión se usa para definir la dirección del flujo de las señales entre dos dispositivos entrelazados. Hay tres tipos de modos de transmisión: Simplex, semidúplex y full-dúplex.

3.3.1 Simplex. En el modo Simplex, la comunicación es unidireccional, como una calle en sentido único. Solamente una de las dos estaciones de enlace puede transmitir, la otra solo puede recibir. Los teclados y los monitores tradicionales son ejemplos de dispositivos simplex. El teclado solamente puede introducir datos; el monitor solo puede aceptar datos de salida.

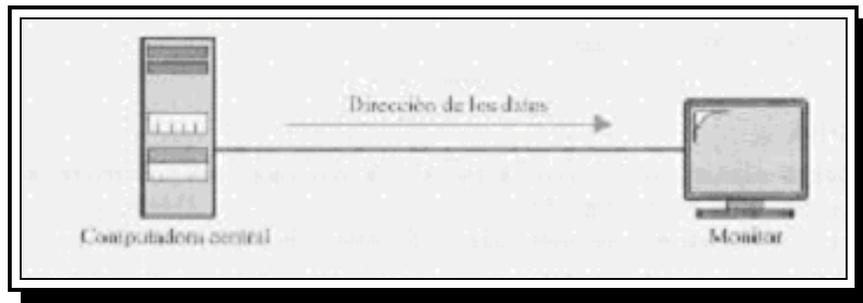


Figura 3.9 Símplex

3.3.2 Semidúplex. En el modo semidúplex, cada estación puede tanto enviar como recibir, pero no al mismo tiempo. Cuando un dispositivo está enviando, el otro solo puede recibir, y viceversa.

En la transmisión semidúplex, la capacidad total del canal es usada por aquel de los dos dispositivos que está transmitiendo. Los walkie-talkies son ejemplos de sistemas semidúplex.

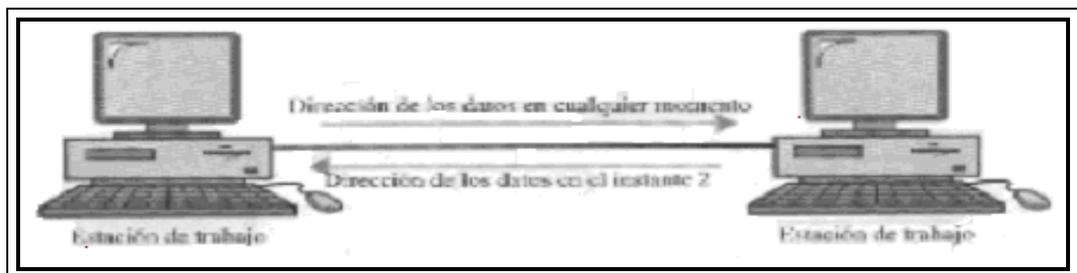


Figura 3.10 Semidúplex

3.3.3 Full-dúplex. En el modo full-dúplex, ambas estaciones pueden enviar y recibir simultáneamente. Las señales que van en cualquier dirección deben compartir la capacidad del enlace. Esta compartición puede ocurrir de dos formas: o bien el enlace debe contener caminos de transmisión físicamente separados, uno para enviar y otro para recibir, o es necesario dividir la capacidad del canal entre las señales que viajan en direcciones opuestas.

Un ejemplo habitual de la comunicación full-dúplex es la red telefónica. Cuando dos personas están hablando por teléfono, ambas pueden hablar y recibir al mismo tiempo.

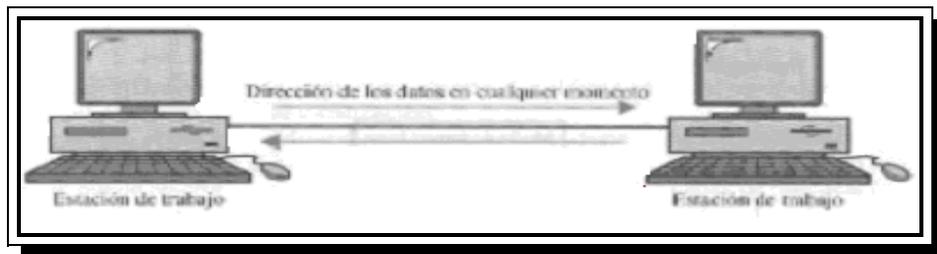


Figura 3.11 Full-Dúplex

3.4 Clases De Redes. Cuando se habla de redes, se suele hablar de tres clases principales: redes de área local, redes de área metropolitana y redes de área amplia.

3.4.1 Red de área local (LAN). Una red de área local (LAN, Local Area Network) suele ser una red de propiedad privada que conecta enlaces de una misma oficina, edificio o campus. Dependiendo de las necesidades de la organización donde se instale y del tipo de tecnología utilizada, una LAN puede ser tan sencilla como dos PC y una impresora situadas en la oficina de la casa de alguien o se puede extender por toda una empresa en incluir voz, sonido y periféricos de video. En la actualidad el tamaño de las LAN está limitado a unos pocos kilómetros. Las LAN están diseñadas para permitir compartir recursos entre computadoras personales o estaciones de trabajo. Los recursos a compartir pueden incluir hardware (por ejemplo una impresora), software (por ejemplo, un programa de aplicación) o datos. Un ejemplo frecuentemente de LAN, que se encuentran en muchos entornos de negocios, enlaza un grupo de trabajo de computadoras relacionadas con una cierta tarea, como por ejemplo estaciones de trabajo de ingeniería o PC de contabilidad.

Una de las computadoras puede tener un disco de gran capacidad y convertirse en servidora de otros clientes. El software se puede almacenar en este servidor central para que sea usado por todo el grupo según las necesidades de cada miembro. En este caso, el tamaño de la LAN puede estar determinado por restricciones en el número de licencias, por el número de usuarios por copia de software o por restricciones en el número de usuarios con licencia para acceder al sistema operativo. Además del tamaño las LAN se distinguen de otro tipo de redes por su medio de transmisión y su topología. En general, una LAN determinada usará un único medio de transmisión. Las topologías más frecuentes de las LAN son el bus, el anillo y la estrella.

Tradicionalmente, las LAN tienen tasas de datos en un rango de entre 4 y 16 Mbps. Sin embargo, actualmente las velocidades se han incrementado y pueden alcanzar los 100Mbps e incluso velocidades de Gb.

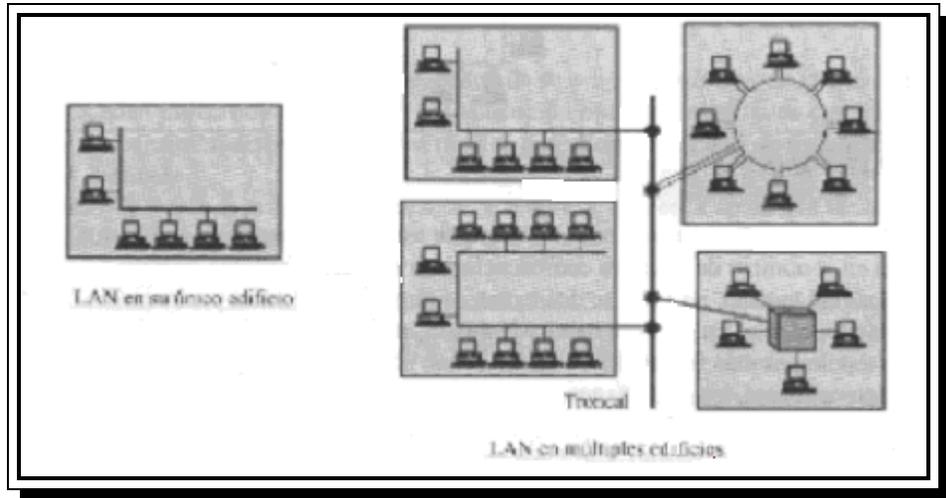


Figura 3.12 LAN

3.4.2 Redes de área metropolitana (MAN). La red de área metropolitana (MAN, Metropolitan Area Network) ha sido diseñada para que se pueda extender a lo largo de una ciudad entera. Puede ser una red única, como una red de televisión por cable, o puede ser una forma de conectar un cierto número de LAN en una red mayor, de forma que los recursos puedan ser compartidos de LAN a LAN y de dispositivo a dispositivo. Por ejemplo, una empresa puede usar una MAN para conectar las LAN de todas sus oficinas dispersas por la ciudad. Una MAN puede ser propiedad totalmente por una empresa privada, que será su operadora, o puede ser un servicio proporcionado por una empresa de servicio público, como una empresa de telefonía

local. Muchas compañías telefónicas tienen un servicio muy popular de MAN denominada Servicio de Conmutación de Datos (SMDS).

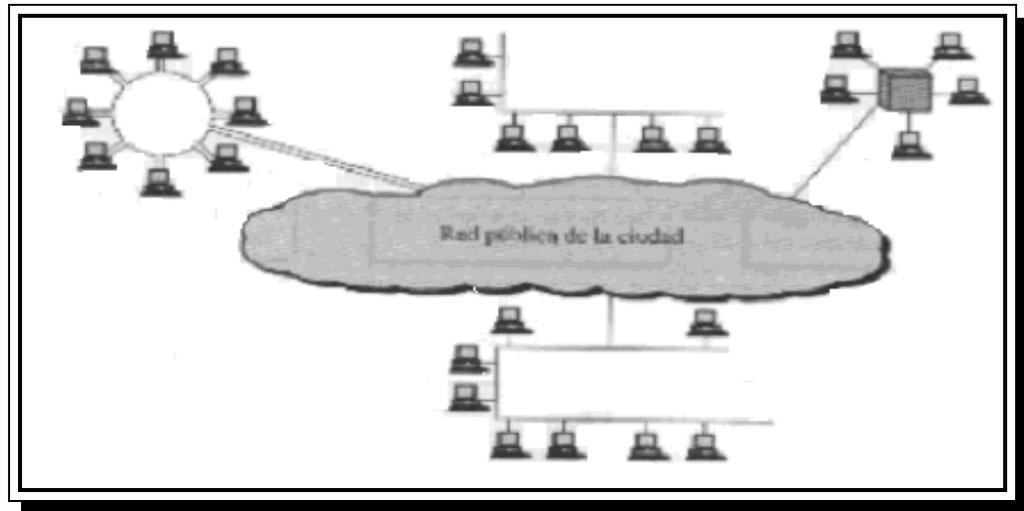


Figura 3.13 MAN

3.4.3 Red de área amplia (WAN). Una red de arrea amplia (WAN, Metropolitan Area Network) proporciona un medio de transmisión a larga distancia de datos, voz imágenes e información de video sobre grandes áreas geográficas que pueden extenderse a un país, un continente o incluso en el mundo entero. En contraste con las LAN (que dependen de su propio hardware para transmisión), las WAN pueden utilizar dispositivos de comunicación públicos, alquilados o privados, habitualmente en combinaciones, y además pueden extenderse a lo largo de un numero de kilómetros ilimitado. Una WAN que es una propiedad de una única empresa, que es la única que la usa, se denomina habitualmente red de empresa.

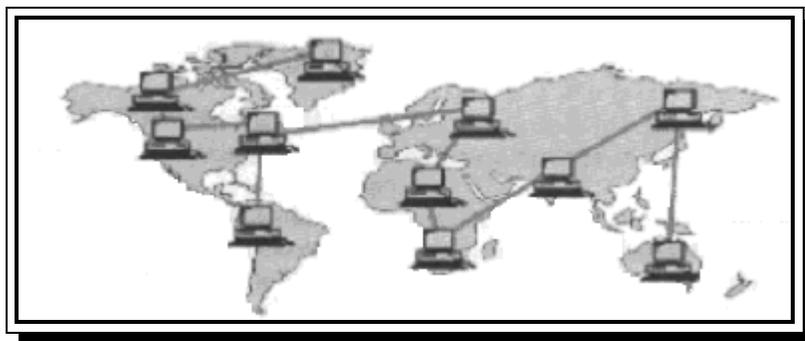


Figura 3.14 WAN

3.5 EL MODELO OSI

El modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) es una arquitectura por niveles para el diseño de sistemas de red que permite la comunicación entre todos los tipos de computadoras. Está compuesto por siete niveles separados, pero relacionados entre sí.

3.5.1 Niveles del modelo OSI.

3.5.1.1 Nivel físico. El nivel físico coordina las funciones necesarias para transmitir el flujo de datos a través de un medio físico. Trata con las especificaciones eléctricas y mecánicas de la interfaz y del medio de transmisión. También define los procedimientos y las funciones que los dispositivos físicos y las interfaces tienen que llevar a cabo para que sea posible la transmisión.

El nivel físico se relaciona con lo siguiente:

- ✓ **Características físicas de las interfaces y el medio.** El nivel físico define las características de la interfaz entre los dispositivos y el medio de transmisión. También define el tipo de medio de transmisión.
- ✓ **Representación de los bits.** Los datos del nivel físico están compuestos por un flujo de bits sin ninguna interpretación. Para que puedan ser transmitidos, es necesario codificarlos en señales eléctricas u ópticas. El nivel físico define el tipo de codificación.
- ✓ **Tasa de datos.** El nivel físico también define la tasa de transmisión: el número de bits enviados cada segundo. En otras palabras, el nivel físico define la duración de un bit.
- ✓ **Sincronización de los bits.** El emisor y el receptor deben estar sincronizados a nivel de bit. En otras palabras los relojes del emisor y el receptor deben estar sincronizados.
- ✓ **Configuración de la línea.** El nivel físico está relacionado con la conexión de dispositivos al medio, es decir, si la configuración es punto a punto o multipunto.
- ✓ **Topología física.** La topología física define cómo están conectados los dispositivos para formar una red.
- ✓ **Modo de transmisión.** El nivel físico también define la dirección de la transmisión entre dos dispositivos.

3.5.1.2 Nivel de enlace de datos. El nivel de enlace de datos transforma el nivel físico, un simple medio de transmisión, en un enlace fiable y es responsable de la entrega nodo a nodo. Hace que el nivel físico aparezca ante el nivel superior (nivel de red) como un medio libre de errores. Entre las responsabilidades específicas del nivel de enlace de datos se incluyen las siguientes.

- ✓ **Tramado.** El nivel de enlace de datos divide el flujo de bits recibidos del nivel de red en unidades de datos manejables denominados tramas.
- ✓ **Direccionamiento físico.** Si es necesario distribuir las tramas por distintos sistemas de la red, el nivel de enlace de datos añade una cabecera a la trama para definir la dirección física del emisor (dirección fuente) y/o receptor (dirección destino) de la trama. Si hay que enviar la trama a un sistema fuera de la red del emisor, la dirección del receptor es la dirección del dispositivo que conecta su red a la siguiente.
- ✓ **Control de flujo.** Si la velocidad a la que el receptor recibe los datos es menor que la velocidad de transmisión del emisor, el nivel de enlace de datos impone un mecanismo de control de flujo para prevenir el desbordamiento del receptor.
- ✓ **Control de errores.** El nivel de enlace de datos añade fiabilidad al nivel físico al incluir mecanismos para detectar y retransmitir las tramas defectuosas o perdidas. También usa un mecanismo para prevenir la duplicación de tramas defectuosas o perdidas. También usa un mecanismo para prevenir la duplicación de tramas. El control de errores se consigue normalmente a través de una cola que se añade al final de la trama.

- ✓ **Control de acceso.** Cuando se conectan dos o más dispositivos a un mismo enlace, los protocolos de nivel de enlace deben determinar en todo momento qué dispositivo tiene el control del enlace.

3.5.1.3 Nivel de red. El nivel de red es responsable de la entrega de un paquete desde el origen al destino y, posiblemente, a través de múltiples redes (enlaces). Mientras que el nivel de enlace de datos supervisa la entrega del paquete entre dos sistemas de la misma red, el nivel de red se asegura que cada paquete vaya del origen al destino, sean estos cuales sean.

Las responsabilidades específicas del nivel de red son:

- ✓ **Direccionamiento lógico.** El direccionamiento físico proporcionado por el nivel de enlace de datos gestiona los problemas de direcciones locales. Si un paquete cruza la frontera de la red, es necesario tener otro tipo de direcciones para distinguir los sistemas origen de los del destino. El nivel de red añade una cabecera al paquete que viene del nivel superior que, entre otras cosas incluye direcciones lógicas del emisor y el receptor.
- ✓ **Encaminamiento.** Cuando un conjunto de redes o enlaces independientes se conectan juntas para crear una red de redes, los dispositivos de conexión (encaminadores o pasarelas) encaminan los paquetes hasta su destino final. Una de las funciones del nivel de red es proporcionar estos mecanismos.

3.5.1.4 Nivel de transporte. El nivel de transporte es responsable de la entrega origen a destino (extremo a extremo) de todo el mensaje. Mientras que el nivel de red supervisa la entrega extremo a extremo de paquetes individuales, no reconoce ninguna relación entre estos paquetes. Trata a cada uno independientemente, como si cada pieza perteneciera a un mensaje separado, tanto como si lo es como si no. Por otro lado, el nivel de transporte asegura que todo el mensaje llega intacto y en orden, supervisando tanto el control de errores como el control de flujo a nivel origen a destino. Algunas de las responsabilidades específicas del nivel de transporte son las siguientes:

- ✓ **Direccionamiento en punto de servicio.** Las computadoras suelen ejecutar a menudo varios programas al mismo tiempo. Por esta razón la entrega desde el origen al destino significa la entrega no sólo de una computadora a otra, sino también desde un proceso específico (programa en ejecución) en una computadora a un proceso específico (programa en ejecución) en el otro.
- ✓ **Segmentación y reensamblaje.** Un mensaje se divide en segmentos transmisibles, cada uno de los cuales contiene un cierto número de secuencias. Estos números permiten al nivel de transporte reensamblar el mensaje correctamente a su llegada al destino e identificar y reemplazar paquetes que se han perdido en la transmisión.

- ✓ **Control de conexión.** El nivel de transporte puede estar orientado a conexión o no. Un nivel de transporte no orientado a conexión trata cada segmento como un paquete independiente y lo pasa al nivel de transporte de la maquina destino. Un nivel de transporte orientado a conexión establece una conexión con el nivel de transporte del destino antes de enviar ningún paquete. La conexión se corta después que se han transferido todos los paquetes de datos.
- ✓ **Control de flujo.** El control de flujo de este nivel se lleva a cabo de extremo a extremo y no sólo en un único enlace.
- ✓ **Control de errores.** El control de errores en este nivel se lleva a cabo de extremo a extremo y no solo en un único enlace. El nivel del transporte del emisor asegura que todo el mensaje llega al nivel de transporte del receptor sin errores. Habitualmente los errores se corrigen mediante retransmisiones.

3.5.1.5 Nivel de sesión. Los servicios provistos en los tres primeros niveles no son suficientes para algunos procesos. El nivel de sesión es el controlador de diálogo de la red. Establece, mantiene y sincroniza la interacción entre sistemas de comunicación. Algunas de sus responsabilidades son:

- ✓ **Control de diálogo.** El nivel de sesión permite que dos sistemas establezcan un dialogo. Permite que la comunicación entre dos procesos tenga lugar en el modo semidùplex o full-dùplex.
- ✓ **Sincronizaron.** El nivel de sesión permite que un proceso pueda añadir puntos de prueba en un flujo de datos.

3.5.1.6 Nivel de presentación. El nivel de presentación está relacionado con la sintaxis y la semántica de la información intercambiada entre dos sistemas. Las responsabilidades específicas del nivel de presentación incluyen:

- ✓ **Traducción.** Los procesos (programas en ejecución) en los sistemas intercambian habitualmente información en forma de tiras de caracteres, números, etc. Es necesario convertir la información a flujos de bits antes de transmitirla. Debido a que cada computadora utiliza un sistema de codificación distinto, el nivel de presentación es responsable de la interoperabilidad entre los distintos métodos de codificación. El nivel de presentación en el emisor cambia la información del formato dependiente del emisor a un formato común. El nivel de presentación en la maquina receptora cambia el formato comunes el formato especifico del receptor.
- ✓ **Cifrado.** Para transportar información sensible, un sistema debe ser capaz de asegurar la privacidad. El cifrado implica que el emisor transforma la información original a otro formato y envía el mensaje resultante por la red. El descifrado ejecuta el proceso inverso del proceso original para convertir el mensaje a su formato original.
- ✓ **Compresión.** La compresión de datos reduce el número de bits a transmitir. La compresión de datos es particularmente importante en la transmisión de datos multimedia tales como texto, audio y video.

3.5.1.7 Nivel de aplicación. El nivel de aplicación permite al usuario, tanto humano como software, acceder a la red. Proporciona las interfaces de usuario y soporte para servicios como el correo electrónico, el acceso y la transferencia de archivos, la gestión de datos compartidos y otros tipos de servicio para información distribuida. Algunos de los servicios provistos por el nivel de aplicación incluyen:

- ✓ **Terminal virtual de red.** Un terminal virtual de red es una versión de un terminal físico y permite al usuario acceder a una maquina remota. Para hacerlo, la aplicación crea una emulación software de un terminal en la maquina remota. La computadora del usuario habla al terminal software, que a su vez, habla al host y viceversa. La maquina remota cree que se está comunicando con uno de sus propios terminales y permite el acceso.
- ✓ **Transferencia, acceso y gestión de archivos (FTAM).** Esta aplicación permite al usuario acceder a archivos en una computadora remota (para cambiar datos o leer los datos), recuperar archivos de una computadora remota y gestionar o controlar los archivos de dicha computadora.
- ✓ **Servicios de correo.** Esta aplicación proporciona las bases para el envío y almacenamiento del correo electrónico.
- ✓ **Servicios de directorios.** Esta aplicación proporciona acceso a bases de datos distribuidas que contienen información global sobre distintos objetos de servicio.

4. REDES DE AREA LOCAL (LAN)

Una red de área local (LAN) es un sistema de transmisión de datos que permite que cierto número de dispositivos independientes se comuniquen entre sí dentro de un área geográfica limitada.

4.1 PROYECTO 802

En 1985, la Computer Society del IEEE comenzó el proyecto 802, para definir estándares que permitieran la intercomunicación entre equipos de distintos fabricantes y se ha dividido en las siguientes normas:

IEEE 802.1	Niveles de aplicación, transporte y red
IEEE 802.2	Subnivel LLC (control de enlaces lógicos) del nivel de enlace
IEEE 802.3, 802.4, 802.5	Subnivel MAC (Control de Acceso al Medio) del nivel de enlace y nivel físico implementado en la tarjeta de red.

Tabla 4.1 Normas del proyecto 802

El proyecto 802 no busca reemplazar ninguna parte del modelo OSI. En lugar de eso es una forma de especificar funciones del nivel físico, el nivel de enlace de datos y en menor extensión, el nivel de red para permitir la interconectividad de los principales protocolos LAN.

Modelo OSI	Modelo IEEE
NIVEL DE ENLACE	SUBNIVEL LLC
	SUBNIVEL MAC
NIVEL FÍSICO	NIVEL FÍSICO

Tabla 4.2 Comparación entre Modelo OSI y el Modelo IEEE

4.1.1 IEEE 802.1. El IEEE 802.1 es la parte del proyecto 802 dedicada a los aspectos de comunicación entre redes LAN y MAN. Aunque todavía no está completo, intenta resolver las incompatibilidades entre arquitecturas de redes sin que sea necesario hacer modificaciones en las direcciones no existentes, los medios de acceso y los mecanismos de recuperación de errores, entre otras.

4.1.2 LLC. En general, el modelo del Proyecto 802 del IEEE toma la estructura de una trama HDLC y la divide en dos funciones. Un conjunto contiene las porciones de usuario final de la trama: las direcciones lógicas, la información de control y los datos. Estas funciones son gestionadas por el control de enlace lógico (LLC) del IEEE 802.2. Se considera que el LLC es la capa superior del nivel de enlace de datos del IEEE 802 y es común a todos los protocolos LAN.

4.1.3 MAC. El segundo conjunto de funciones, el subnivel de control de acceso del medio (MAC), resuelve la contención en el acceso al medio compartido. Contiene especificaciones de sincronización, indicadores, flujo y control de error necesarias para llevar la información de un lugar a otro, así como las direcciones físicas de la siguiente estación que debe recibir y enrutar un paquete. Los protocolos MAC son específicos de las LAN que los usa.

4.1.4 Unidad de datos del protocolo (PDU). La unidad de datos del nivel LLC se denomina unidad de datos del protocolo (PDU). La PDU contiene cuatro campos que

resultan familiares de HDLC: un punto de acceso al servicio de destino (DSAP), un punto de acceso a servicio en el origen (SSAP), un campo de control y un campo de información.

4.1.4.1 DSAP y SSAP. DSAP y SSAP son direcciones que usa el LLC para identificar las pilas de protocolos en las máquinas receptoras y emisoras que están usando y generando los datos respectivamente. El primer bit del DSAP indica si la trama está destinada a un individuo o a un grupo. El primer bit del SSAP indica si la comunicación es una PDU de orden o de respuesta.

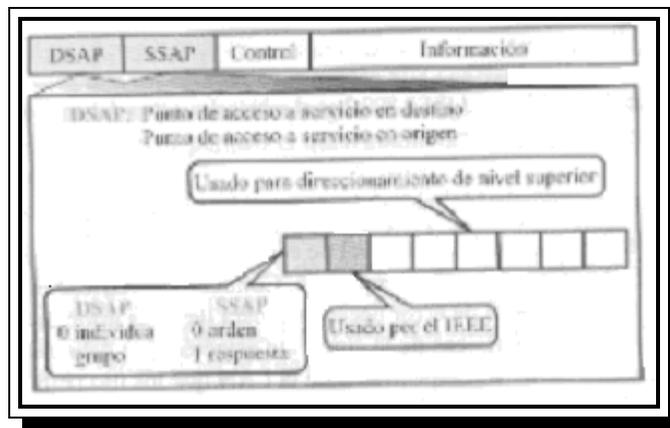


Figura 4.1 Formato PDU

4.1.4.2 Control. El campo de control de la PDU es idéntico al campo de control de HDLC. Al igual que en HDLC, las tramas PDU pueden ser tramas I, tramas S o tramas U y pueden transportar todos los códigos e información que transportan las tramas correspondientes de HDLC. La PDU no tiene campos indicadores, ni CRC ni dirección de estación. Estos campos se añaden en el subnivel bajo (el nivel MAC).

4.2 ETHERNET

El IEEE 802.3 proporciona una LAN estándar desarrollada originalmente por Xerox y ampliada posteriormente en un esfuerzo conjunto entre Digital Equipment Corporation, Intel Corporation y Xerox. El resultado se denominó Ethernet.

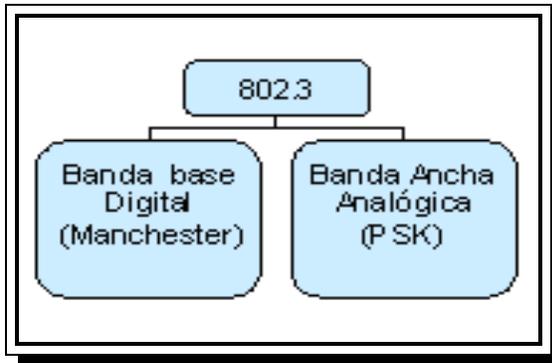


Figura 4.2 IEEE 802.3

El IEEE 802.3 define dos categorías: banda base y banda ancha, como se muestra en la figura 4.2. La palabra base especifica una señal digital (en este caso, codificación Manchester). La palabra ancha especifica una señal analógica (en este caso, codificación PSK). El IEEE divide la categoría de la banda base en cinco estándares distintos: **10Base5**, **10Base2**, **1Base-T**, **1Base5** y **100base-T**. El primero (10, 1 o 100) indica la tasa de datos en Mbps. El último número o letra (5, 2, 1 o T) indica la máxima longitud de cable o el tipo de cable. El IEEE define únicamente una especificación para la categoría de banda ancha: **10Broad36**. De nuevo, el primer número (10) indica la tasa de datos. El último número define la máxima longitud del cable. Sin embargo, la máxima longitud del cable puede cambiar usando dispositivos de red tales como puentes o repetidores.

4.2.1 Método de acceso: CSMA/CD. Siempre que múltiples usuarios tiene acceso incontrolado a una única línea, existe el peligro de que las señales se solapen y se destruyan entre sí. Estos solapamientos, que convierten las señales en ruido inútil, se denominan colisiones. A medida que se incrementa el tráfico en un enlace con múltiples accesos, se incrementan las colisiones. Por tanto, una LAN necesita un mecanismo para coordinar el tráfico, minimizar el número de colisiones que se producen y maximizar el número de tramas que se entregan con éxito. El mecanismo de acceso al medio usado en una Ethernet se denomina portadora sensible a acceso múltiple con detección de colisiones (CSMA/CD, Carrier Sense Multiple Access with Collision Detection) (estandarizado en el IEEE 802.3).

En CSMA/C, la estación que quiere transmitir escucha primero para estar seguro de que el enlace esta libre, a continuación transmite sus datos y después vuelva a escuchar. Durante la transmisión de datos, la estación comprueba si en la línea se producen los voltajes extremadamente altos que indican una colisión. Si se detecta una colisión, la estación deja de transmitir y espera una cantidad de tiempo predefinido para que la línea quede libre, enviando los datos de nuevo después de ello.

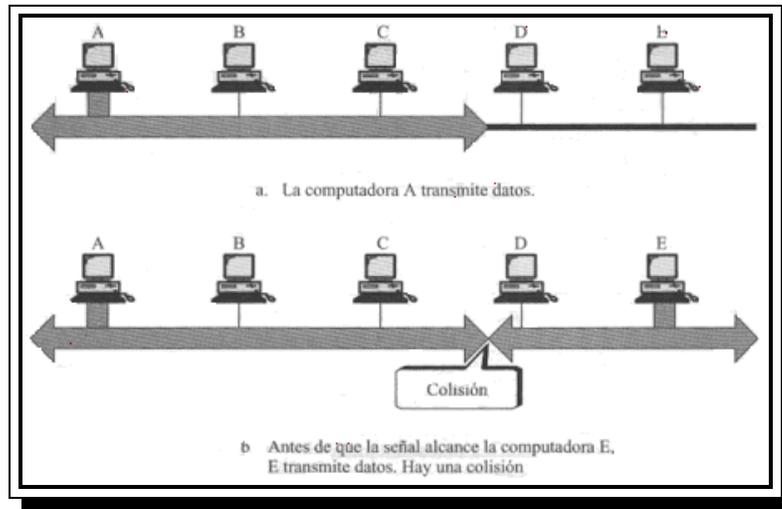


Figura 4.3 Colisión en CSMA/CD

4.2.2 Direccionamiento. Cada estación en red Ethernet (como una PC, estación de trabajo o impresora) tiene su propia tarjeta de interfaz de red (NIC, Network Interface Card). La NIC está situada habitualmente dentro de la estación y proporciona a dicha estación una dirección física de 6 bytes. El número de la NIC es único.

4.2.3 Formato de trama. El IEEE 802.3 especifica un tipo de trama que contiene siete campos: preámbulo, SFD, DA, SA, longitud/tipo de la PDU, trama 802.2 y el CRC. Ethernet no proporciona ningún mecanismo para reconocer las tramas recibidas, razón por la cual se le conoce como un medio no fiable.

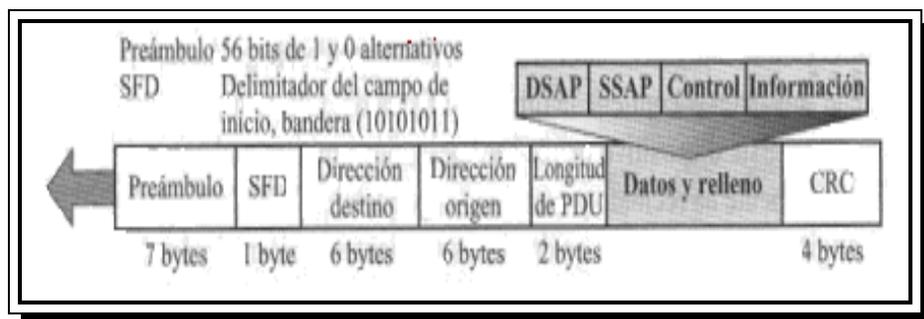


Figura 4.4 Trama MAC 802.3

- ✓ **Preámbulo.** El primer campo de la trama 802.3, el preámbulo contiene siete bytes de ceros y unos alternos que alertan al sistema receptor de la llegada de una trama y le permiten sincronizar su temporizador de entrada. El patrón 1010101 proporciona únicamente una alerta y un pulso de temporización; se confunde demasiado fácilmente para servir como un aviso útil de la llegada de flujo de datos.
- ✓ **Delimitador de comienzo de trama (SFD).** El segundo campo de la trama del 802.3 (un byte: 10101011) indica el comienzo de la trama. El SFD le dice el receptor que todo lo que reciba a continuación son datos, empezando por las direcciones.
- ✓ **Dirección de destino (DA).** El campo de dirección de destino incluye 6 bytes y contiene la dirección física del siguiente destino del paquete. Una dirección física del sistema es un patrón de bits codificado en su tarjeta de interfaz de red (NIC). Si el paquete debe atravesar de una LAN a otra para alcanzar su destino, el campo DA contiene la dirección física del encaminador que conecta la LAN actual con la siguiente. Cuando el paquete alcanza la red destino, el campo DA contiene la dirección física del dispositivo destino.
- ✓ **Dirección fuente (SA).** El campo de dirección fuente también tiene seis bytes y contiene la dirección física del último dispositivo en reenviar el paquete. Este dispositivo puede ser la estación emisora o el encaminador que mas recientemente ha recibido y reenviado el paquete.

- ✓ **Longitud/tipo de PDU.** Los dos bytes siguientes indican el número de bytes en el PDU entrante. Si la longitud del PDU es fija, este campo se puede usar para indicar el tipo o como base para otros protocolos.
- ✓ **Trama 802.2 (PDU).** Este campo de la trama 802.3 contiene toda la trama 802.2 como una unidad modular removible. La PDU puede ser de cualquier longitud entre 46 y 1500 bytes, dependiendo del tipo de trama y de la longitud del campo de información. La PDU es generada por el subnivel superior (LLC) y después añadida a la trama 802.3.
- ✓ **CRC.** El último campo de la trama 802.3 contiene la información de detección de error, en este caso un CRC-32.

4.2.4 Implementación. Todas las LAN Ethernet se configuran como buses lógicos, aunque se pueden implementar físicamente con topologías de bus o de estrella. Cada trama se transmite a cada estación del enlace, pero es leída únicamente por la estación a la cual va destinada.

4.2.4.1 10BASE-T: Ethernet de par trenzado. Es el estándar más popular, consta de una LAN con topología en estrella que usa cables de par trenzado sin blindaje (UTP) en lugar de cable coaxial. Proporciona una velocidad de datos de 10Mbps y tiene una longitud máxima (desde el concentrador a la estación) de 100 metros. En lugar de usar transceptores iguales, la Ethernet 10Base-T sitúa todas sus operaciones de red en un concentrador inteligente que tiene un puerto para cada estación. Las estaciones están conectadas al concentrador por conectores RJ-45 de cuatro pares. El concentrador

retransmite todas las tramas recibidas a las estaciones que tiene conectadas. La lógica en la NIC asegura que solamente la estación que va a abrir y leer una determinada trama es aquella a la cual va dirigida.

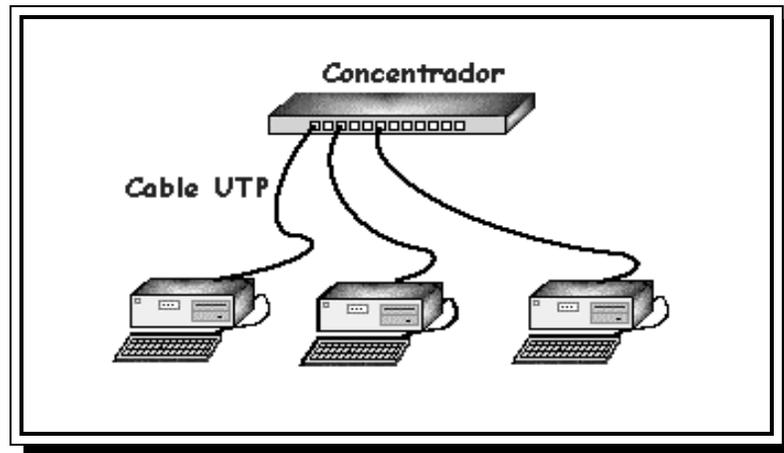


Figura 4.5 Conexión 10BASE-T

El peso y la flexibilidad del cable y la conveniencia de la clavija RJ-45 hacen que la 10Base-T sea la LAN del estándar 802.3 más fácil de instalar y mantener. Cuando sea necesario reemplazar una estación, basta con enchufar la nueva.

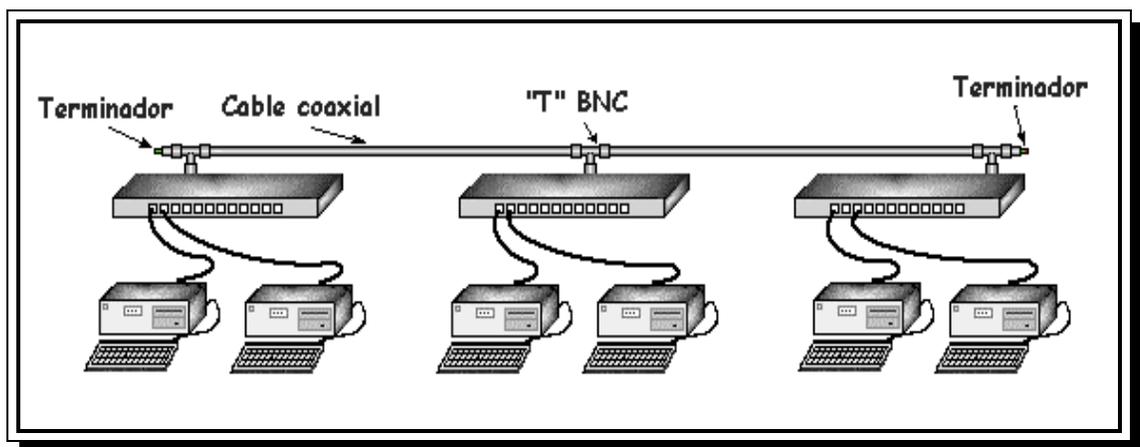


Figura 4.6 Topología 10BASE-T

4.3 OTRAS REDES ETHERNET

Durante la última década ha habido una gran revolución en las redes Ethernet. Se han diseñado varios esquemas nuevos para tratar de mejorar las prestaciones y la velocidad de las LAN Ethernet, tales como: Ethernet conmutada, Fast Ethernet y Gigabit Ethernet.

4.3.1 Ethernet conmutada. La Ethernet conmutada es un intento de mejorar las prestaciones de la Ethernet 10Base-T. La Ethernet 10Base-T es una red de medio compartido, lo que significa que todo el medio está involucrado en cada transmisión. Esto es así porque la topología, aunque físicamente es una estrella, se comporta como un bus lógico. Cuando una estación envía una trama al concentrador, la trama es retransmitida por todos los puertos (interfaces) y será recibida por todas las estaciones. En esta situación, solamente una estación puede enviar una trama en un instante dado. Si dos estaciones tratan de enviar tramas simultáneamente hay una colisión.

Sin embargo, si se reemplaza el concentrador por un conmutador, un dispositivo que puede reconocer la dirección de destino y puede encaminar la trama al puerto al que esta conectada dicha estación, el resto del medio no se ve involucrado en el proceso de transmisión. Esto significa que el conmutador puede recibir otra trama de otra estación al mismo tiempo y puede encaminar esa trama a su destino final. Teóricamente de esta forma no hay colisiones.

Usando un conmutador en lugar de un concentrador, se puede incrementar teóricamente la capacidad de una red con n dispositivos hasta N por 10 Mbps, debido a que 10Base-T usa dos pares de UTP para comunicación dúplex.

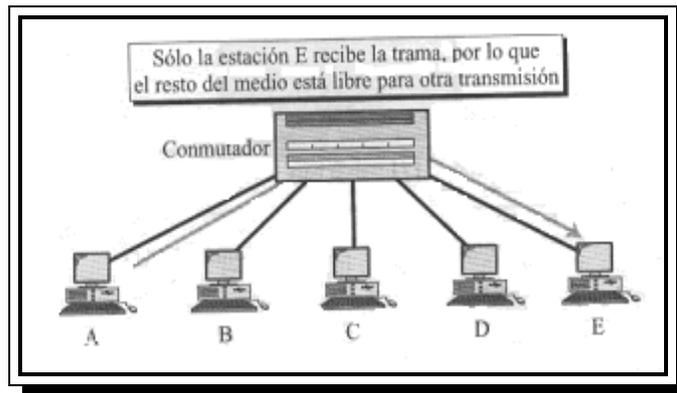


Figura 4.7 Una Ethernet que usa un conmutador

4.3.2 Fast Ethernet. A medida que las aplicaciones nuevas, como el diseño asistido por computadora (CAD), procesamiento de imagen y la utilización de audio y video en tiempo real, van siendo implementadas en las LAN, hay necesidad de tener LAN con una velocidad de datos mayor que 10 Mbps. La Fast Ethernet opera a 100Mbps. Afortunadamente, debido a la forma en que se diseñó Ethernet, es fácil incrementar la velocidad si decrece el dominio de la colisión (la máxima distancia que viajan los datos entre dos estaciones). El dominio de colisión de Ethernet está limitado a 2500 metros. Esta limitación es necesaria para permitir una tasa de datos de 10 Mbps usando en el método de acceso CSMA/CD.

Para que CSMA/CD funcione, una estación debería ser capaz de notar la colisión antes de que toda la trama se haya situado en el medio. Si se ha enviado toda la trama y no

se ha detectado la colisión, la estación asume que todo está bien, destruye la copia de la trama y envía la siguiente.

El tamaño mínimo de una trama Ethernet es 72 bytes o 576 bits. Enviar 576 bits a una velocidad de 10 Mbps consume 57.6 microsegundos. Antes de que se haya enviado el último bit, el primer bit debe haber alcanzado el fin del extremo del dominio y, si hay una colisión, debe ser notada por el emisor. Esto implica que durante el tiempo que tarda el emisor en transmitir 576 bits dicha colisión debe ser detectada. En otras palabras, la colisión debe ser detectada durante los 57.6 microsegundos. Este tiempo es suficiente para permitir que una señal haga un viaje de ida y vuelta de 5000 metros a la velocidad de propagación en un medio típico de transmisión como un cable de par trenzado.

Para incrementar el tamaño de los datos sin cambiar el tamaño mínimo de la trama, es necesario disminuir el tiempo de ida y vuelta. Con una velocidad de 100Mbps, el tiempo de ida y vuelta se reduce a 5.76 microsegundos. Esto significa que el dominio de colisión se debe reducir 10 veces, de 2500 metros a 250 metros. Esta disminución no es un problema debido a que las LAN conectan actualmente computadoras de sobremesa que no están separadas más allá de 50 o 100 metros del concentrador central. Esto significa que el dominio de colisión está entre 100 y 200 metros.

La Fast Ethernet es una versión de Ethernet con una tasa de datos de 100 Mbps. No hay ningún cambio en el formato de trama. No hay ningún cambio en el método de acceso. Los únicos dos cambios en el nivel MAC son las tasas de datos y el nivel de

colisión. La tasa de datos se incrementa en un factor de 10; el dominio de colisión se disminuye en un factor de 10.

En el nivel físico, la especificación desarrollada para la Fast Ethernet es una tecnología similar a la 10Base-T; sin embargo, para satisfacer al nivel físico de los distintos recursos disponibles, el IEEE ha diseñado dos categorías de Fast Ethernet: 100Base-X y 100Base-T4. La primera usa dos cables entre la estación y el concentrador; el segundo usa 4. La 100Base-X se divide a su vez en dos tipos: 100Base-TX y 100base-FX.

4.3.2.1 100Base-TX. El diseño de 100Base-TX usa dos cables de par trenzado sin blindaje (UTP) de categoría 5 o dos cables de par trenzado blindado (STP) para conectar una estación con el concentrador. Un par se usa para llevar las tramas desde la estación al concentrador y el otro para transportar las tramas desde el concentrador hasta la estación.

4.3.3 Gigabit Ethernet. La migración de 10 Mbps animó al comité del IEEE 802.3 a diseñar la Ethernet Gigabit, que tiene una tasa de datos de 1000Mbps o 1 Gbps. La estrategia es la misma; el nivel MAC y los métodos de acceso siguen siendo los mismos, pero se reduce el dominio de la colisión. Sin embargo, el medio físico (el medio de transmisión y el sistema de codificación) cambia. La Ethernet Gigabit se diseñó principalmente para uso con fibra óptica, aunque el protocolo no elimina el uso

de cables de par trenzado. La Ethernet Gigabit sirve habitualmente como troncal para conectar redes Fast Ethernet.

Se han diseñado cuatro implementaciones para la Ethernet Gigabit: 1.000Base-LX, 1.000Base-SX, 1.000base-CX y 1.00Base-T la codificación es 8B/10B, lo que significa que los grupos de 8 bits binarios.

Características	1.000Base-SX	1.000Base-LX	1.000Base-CX	1.000Base-T
Medio	Fibra óptica (multimodo)	Fibra óptica (multi o monomodo)	STP	UTP
Señal	Láser de onda corta	Láser de onda larga	Eléctrica	Eléctrica
Distancia máxima	550 m	550 m (multimodo) 5.000 m (monomodo)	25 m	25 m

Tabla 4.3 Comparación entre las implementaciones de Ethernet Gigabit

4.4 INTRANET

Una Intranet es una red o un conjunto de redes informáticas interconectadas pertenecientes a una misma institución. Como en todas las redes informáticas, el propósito fundamental de la Intranet es compartir información y recursos entre los distintos usuarios de la misma. Lo que distingue a una Intranet de otros tipos de redes es el protocolo usado para la comunicación entre los ordenadores, que es el TCP/IP, el mismo que se utiliza en Internet. Con lo cual una Intranet puede ser considerada como una Internet a pequeña escala. La ventaja de esto reside en que podremos utilizar el mismo software de comunicación disponible para Internet dentro de nuestra Intranet, con multitud de programas de libre distribución.

4.4.1 Compartición de recursos en la Intranet. El servicio Cliente para redes Microsoft, el protocolo TCP/IP y el servicio Compartir impresoras y archivos para redes Microsoft permiten montar una red par a par con equipos en los que se encuentre instalado Windows 95. Cada ordenador de la red puede actuar tanto como cliente como servidor. Actuando como servidor puede compartir carpetas (incluyendo unidades de disco completas) e impresoras. Como cliente podrá acceder a las carpetas (y a los archivos que contienen) y utilizar impresoras conectadas a otros ordenadores, si dichos recursos se encuentran compartidos en esos equipos. Mediante este sistema no es posible compartir otros recursos de la red tales como tarjetas de sonido, módems, escáneres, etc., para lo que se debe utilizar en cualquier caso software adicional.

4.5 MEDIOS DE TRANSMISION

El cable utilizado para formar una red se denomina . Los tres factores que se deben tener en cuenta a la hora de elegir un cable para una red son:

- ✓ Velocidad de transmisión.
- ✓ Distancia máxima entre los ordenadores que se van a conectar.
- ✓ Nivel de ruido e interferencias habituales en la zona que se va a instalar la red.

La elección de los cables es fundamental en la construcción de la red, pues determinan el límite de velocidad de ésta. Cada tipo de cable tiene sus ventajas e inconvenientes,

no existe un tipo ideal. Las principales diferencias entre los distintos tipos de cables radican en la anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la amortiguación de la señal y la distancia recorrida. Los medios de transmisión se pueden dividir en dos grandes categorías: guiados y no guiados.

4.5.1 Medios guiados. Los medios guiados son aquellos que proporcionan un conductor de un dispositivo al otro e incluyen cables de pares trenzados, cables coaxiales y cables de fibra óptica.

4.5.1.1 Cable coaxial .



Figura 4.8 Cable coaxial

Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas, y las interferencias externas, por lo que ha de estar apantallado para

reducirlas. Es utilizado generalmente para señales de televisión y para transmisiones de datos a alta velocidad a distancias de varios km.

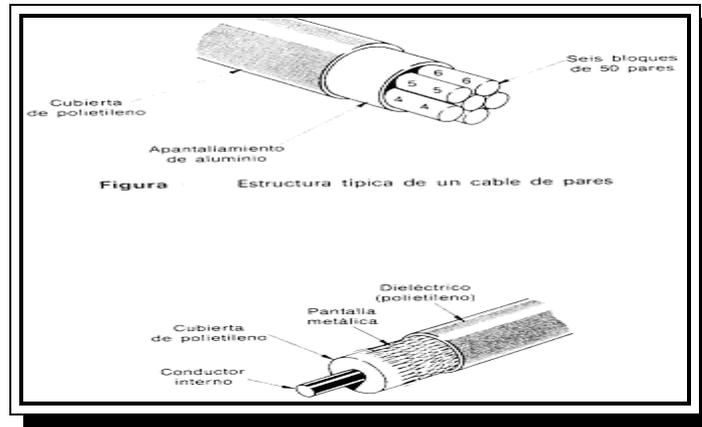


Figura 4.9 Composición del cable coaxial

Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive. Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos. La velocidad de transmisión suele ser alta, de hasta 100 Mbits/seg.; pero hay que tener en cuenta que a mayor velocidad de transmisión, menor distancia podemos cubrir, ya que el periodo de la señal es menor, y por tanto se atenúa antes.

La nomenclatura de los cables Ethernet tiene 3 partes:

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

CABLE	CARACTERÍSTICAS
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 Mb/seg.

Tabla 4.4 Características de la nomenclatura de los cables Ethernet

4.5.1.1.1 Tipos de cable coaxial

4.5.1.1.1.1 Thick (grueso). Este cable se conoce normalmente como "cable amarillo", fue el cable coaxial utilizado en la mayoría de las redes. Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Este cable es empleado en las redes de área local conformando con la norma 10Base2.

4.5.1.1.1.2 Thick (fino). Este cable se empezó a utilizar para reducir el coste de cableado de la redes. Su limitación está en la distancia máxima que puede alcanzar un tramo de red sin regeneración de la señal. Sin embargo el cable es mucho más barato y fino que el thick y, por lo tanto, solventa algunas de las desventajas del cable grueso. Este cable es empleado en las redes de área local conformando con la norma 10Base5.

4.5.1.2 Par trenzado. Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado, ya que está habilitado para comunicación de datos permitiendo frecuencias más altas transmisión. Con anterioridad, en Europa, los sistemas de telefonía empleaban cables de pares no trenzados.

El cable de par trenzado se trata de dos hilos de cobre aislados y trenzados entre sí, y en la mayoría de los casos cubiertos por una malla protectora. Los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor (dos pares paralelos constituyen una antena simple, en tanto que un par trenzado no). Normalmente una serie de pares se agrupan en una única funda de color codificado para reducir el número de cables físicos que se introducen en un conducto. El número de pares por cable son 4, 25, 50, 100, 200 y 300. Cuando el número de pares es superior a 4 se habla de cables multipar. Cada par de cable forma un camino eléctrico completo para transmisión de señales. La corriente que fluye a través de los hilos en cada par es igual, pero fluye en sentidos opuestos. Estas corrientes producen campos electromagnéticos que podrían transmitir ruido eléctrico a hilos cercanos. Sin embargo, los campos alrededor de los dos hilos tienen polaridades opuestas. Al trenzar los hilos, los campos se cancelan uno con el otro, lo cual minimiza el ruido eléctrico, o interferencia, generado por cada par de cables.

Se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer. Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando. Está dividido en categorías por el EIA/TIA:

- ✓ **Categoría 1:** Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbits/seg.
- ✓ **Categoría 2:** Cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbits/seg.
- ✓ **Categoría 3:** Velocidad de transmisión de 10 Mbits/seg. Con este tipo de cables se implementa las redes Ethernet 10-Base-T.
- ✓ **Categoría 4:** La velocidad de transmisión llega a 16 bits/seg.
- ✓ **Categoría 5:** Puede transmitir datos hasta 100 Mbits/seg.

El par trenzado tiene una longitud máxima limitada y, a pesar de los aspectos negativos, es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico y esto permite utilizarlo sin necesidad de obra. La mayoría de las mangueras de cable de par trenzado contiene más de un par de hilos por lo que es posible encontrar mangueras ya instaladas con algún par de hilos sin utilizarse. Además resulta fácil de combinar con otros tipos de cables para la extensión de redes.

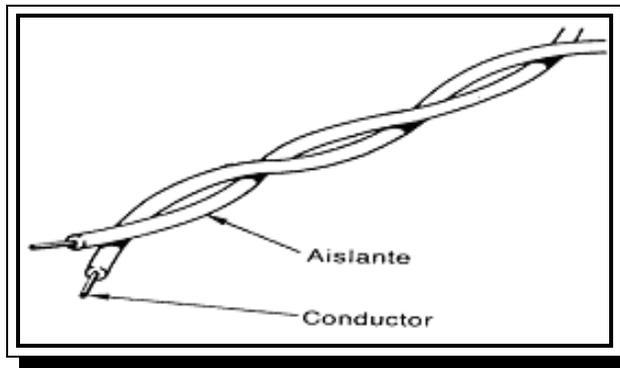


Figura 4.10 Cable de par trenzado

4.5.1.2.1 Tipos de cable de par trenzado.

4.5.1.2.1.1 Cable no blindado (UTP). Es el cable de par trenzado normal y se le referencia por sus siglas en inglés UTP (Unshield Twisted Pair; Par Trenzado no Blindado). Por él se pueden efectuar transmisiones digitales (datos) o analógicas (voz). Consiste en un mazo de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la diafonía. Un cable de pares trenzados puede tener pocos o muchos pares; en aplicaciones de datos lo normal es que tengan 4 pares. Las mayores ventajas de este tipo de cable son su bajo costo y su facilidad de manejo. Sus mayores desventajas son su mayor tasa de error respecto a otros tipos de cable, así como sus limitaciones para trabajar a distancias elevadas sin regeneración y la alta sensibilidad que presenta ante interferencias electromagnéticas. Para las distintas tecnologías de red local, el cable de pares de cobre no blindado se ha convertido en el sistema de cableado más ampliamente utilizado.

El estándar EIA-568 en el adendum TSB-36 diferencia tres categorías distintas para este tipo de cables.

- ✓ Categoría 3: Admiten frecuencias de hasta 16 Mhz
- ✓ Categoría 4: Admiten frecuencias de hasta 20 Mhz
- ✓ Categoría 5: Admiten frecuencias de hasta 100 Mhz

El cable UTP categoría 5 posee 4 pares bien trenzados entre sí:

- | | | |
|-----------------------------------|-------|------------------|
| ✓ Par 1: Blanco/Azul * Azul | ----- | Contactos: 5 * 4 |
| ✓ Par 2: Blanco/Naranja * Naranja | ----- | Contactos: 3 * 6 |
| ✓ Par 3: Blanco/Verde * Verde | ----- | Contactos: 1 * 2 |
| ✓ Par 4: Blanco/Marrón * Marrón | ----- | Contactos: 7 * 8 |

Las características generales del cable no blindado son:

- ✓ **Tamaño:** El menor diámetro de los cables de par trenzado no blindado permite aprovechar más eficientemente las canalizaciones y los armarios de distribución. El diámetro típico de estos cables es de 0'52 m
- ✓ **Peso:** El poco peso de este tipo de cable con respecto a los otros tipos de cable facilita el tendido.
- ✓ **Flexibilidad:** La facilidad para curvar y doblar este tipo de cables permite un tendido más rápido así como el conexionado de las rosetas y las regletas.
- ✓ **Instalación:** Debido a la amplia difusión de este tipo de cables, existen una gran variedad de suministradores, instaladores y herramientas que abaratan la instalación y puesta en marcha.

✓ **Integración:** Los servicios soportados por este tipo de cable incluyen: Red de Área Local ISO 8802.3 (Ethernet) y ISO 8802.5 (Token Ring), Telefonía analógica, Telefonía digital, Terminales síncronos, Terminales asíncronos, Líneas de control y alarmas

4.5.1.2.1.2 Cable blindado (STP). Cada par se cubre con una malla metálica, de la misma forma que los cables coaxiales, y el conjunto de pares se recubre con una lámina blindada. Se referencia frecuentemente con sus siglas en inglés STP (Shield Twisted Pair, Par Trenzado blindado). También conocido como par trenzado con pantalla (ScTP, sus siglas en inglés) o par trenzado con pantalla de hoja metálica, FTP. El empleo de una malla blindada reduce la tasa de error, para proteger a los conductores del ruido eléctrico pero incrementa el coste al requerirse un proceso de fabricación más costoso.

Cada uno de los pares es trenzado uniformemente durante su creación. Esto elimina la mayoría de las interferencias entre cables y además protege al conjunto de los cables de interferencias exteriores. Se realiza un blindaje global de todos los pares mediante una lámina externa blindada. Esta técnica permite tener características similares al cable blindado con unos costes por metro ligeramente inferior.

4.5.1.3 Fibra óptica.

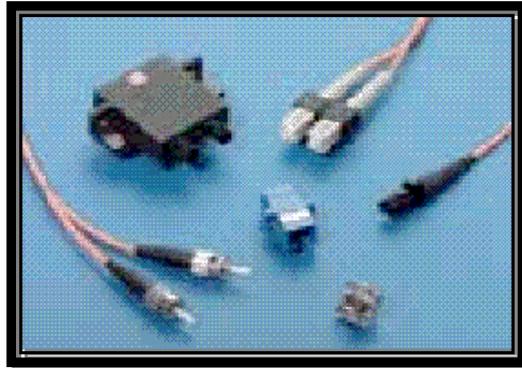


Figura 4.11 Fibra óptica

Las fibras ópticas son filamentos de vidrio de alta pureza extremadamente compactos. Fabricadas a alta temperatura con base en silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones.

Este cable está constituido por uno o más hilos de fibra de vidrio, cada fibra de vidrio consta de:

- ✓ Un núcleo central de fibra con un alto índice de refracción.
- ✓ Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- ✓ Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.

Las fibras ópticas no conducen señales eléctricas por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión. Tienen la capacidad de tolerar altas diferencias de potencial sin ningún circuito adicional de protección y no hay problemas debido a los cortos circuitos. Tienen un gran ancho de banda, que puede ser utilizado para incrementar la capacidad de transmisión con el fin de reducir el costo por canal; De esta forma es considerable el ahorro en volumen en relación con los cables de cobre.

Con un cable de seis fibras se puede transportar la señal de más de cinco mil canales o líneas principales, mientras que se requiere de 10,000 pares de cable de cobre convencional para brindar servicio a ese mismo número de usuarios, con la desventaja que este último medio ocupa un gran espacio en los ductos y requiere de grandes volúmenes de material, lo que también eleva los costos.

Comparado con el sistema convencional de cables de cobre donde la atenuación de sus señales, (decremento o reducción de la onda o frecuencia) es de tal magnitud que requieren de repetidores cada dos kilómetros para regenerar la transmisión; en el sistema de fibra óptica se pueden instalar tramos de hasta 70 Km. Sin que halla necesidad de recurrir a repetidores lo que también hace más económico y de fácil mantenimiento este material.

La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta, y es convertida en señal eléctrica en el extremo receptor.

Las características generales de la fibra óptica son:

- ✓ Ancho de banda. La fibra óptica proporciona un ancho de banda significativamente mayor que los cables de pares (blindado/no blindado) y el coaxial. Aunque en la actualidad se están utilizando velocidades de 1,7 Gbps en las redes públicas, la utilización de frecuencias más altas (luz visible) permitirá alcanzar los 39 Gbps. El ancho de banda de la fibra óptica permite transmitir datos, voz, vídeo, etc.
- ✓ Distancia. La baja atenuación de la señal óptica permite realizar tendidos de fibra óptica sin necesidad de repetidores.
- ✓ Integridad de datos. En condiciones normales, una transmisión de datos por fibra óptica tiene una frecuencia de errores o BER (Bit Error Rate) menor de 10^{-11} . Esta característica permite que los protocolos de comunicaciones de alto nivel, no necesiten implantar procedimientos de corrección de errores por lo que se acelera la velocidad de transferencia.
- ✓ Duración. La fibra óptica es resistente a la corrosión y a las altas temperaturas. Gracias a la protección de la envoltura es capaz de soportar esfuerzos elevados de tensión en la instalación.

- ✓ Seguridad. Debido a que la fibra óptica no produce radiación electromagnética, es resistente a las acciones intrusivas de escucha. Para acceder a la señal que circula en la fibra es necesario partirla, con lo cual no hay transmisión durante este proceso, y puede por tanto detectarse.
- ✓ No presenta difusión natural (se trata de un soporte unidireccional).
- ✓ Los quipos terminales son demasiado costosos.

La fibra también es inmune a los efectos electromagnéticos externos, por lo que se puede utilizar en ambientes industriales sin necesidad de protección especial. Uno de los parámetros más característicos de las fibras es su relación entre los índices de refracción del núcleo y de la cubierta que depende también del radio del núcleo y que se denomina frecuencia fundamental o normalizada; también se conoce como apertura numérica y es adimensional.

4.5.1.3.1 Tipos de fibra óptica.

4.5.1.3.1.1 Fibras multimodo de índice escalonado. Las fibras multimodo de índice escalonado están fabricadas a base de vidrio, con una atenuación de 30 dB/Km., o plástico, con una atenuación de 100 dB/Km. Tienen una banda de paso que llega hasta los 40 Mhz por kilómetro. En estas fibras, el núcleo está constituido por un material uniforme cuyo índice de refracción es claramente superior al de la cubierta que lo rodea. El paso desde el núcleo hasta la cubierta conlleva por tanto una variación brutal del índice, de ahí su nombre de índice escalonado.

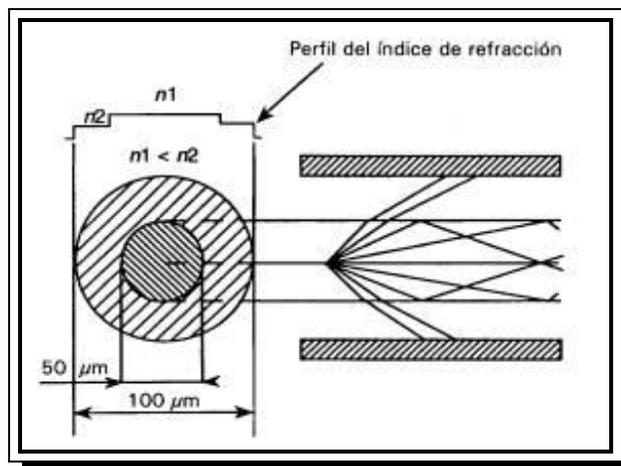


Figura 4.12 Estructura de una Fibra Multimodo de Índice Escalonado

4.5.1.3.1.2 Fibras multimodo de índice de gradiente gradual. Las fibras multimodo de índice de gradiente gradual tienen una banda de paso que llega hasta los 500MHz por kilómetro. Su principio se basa en que el índice de refracción en el interior del núcleo no es único y decrece cuando se desplaza del núcleo hacia la cubierta. Los rayos luminosos se encuentran enfocados hacia el eje de la fibra, como se puede ver

en el dibujo. Estas fibras permiten reducir la dispersión entre los diferentes modos de propagación a través del núcleo de la fibra.

La fibra multimodo de índice de gradiente gradual de tamaño 62,5/125 μm (diámetro del núcleo/diámetro de la cubierta) está normalizado, pero se pueden encontrar otros tipos de fibras:

- ✓ Multimodo de índice escalonado 100/140 μm .
- ✓ Multimodo de índice de gradiente gradual 50/125 μm
- ✓ Multimodo de índice de gradiente gradual 85/125 μm .

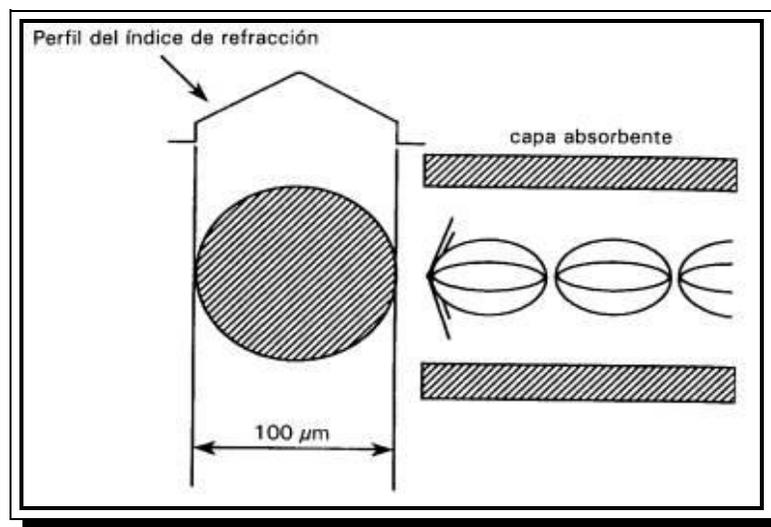


Figura 4.13 Estructura de una Fibra Multimodo de Índice de Gradiente Gradual

4.5.1.3.1.3 Fibras monomodo. Potencialmente, este último tipo de fibra ofrece la mayor capacidad de transporte de información. Tiene una banda de paso del orden de los 100 GHz/Km. Los mayores flujos se consiguen con esta fibra, pero también es la más compleja de implantar. El dibujo muestra que sólo pueden ser transmitidos los rayos que tienen una trayectoria que sigue el eje de la fibra, por lo que se ha ganado el

nombre de "monomodo" (modo de propagación, o camino del haz luminoso, único). Son fibras que tienen el diámetro del núcleo en el mismo orden de magnitud que la longitud de onda de las señales ópticas que transmiten, es decir, de unos 5 a 8 μm . Si el núcleo está constituido de un material cuyo índice de refracción es muy diferente al de la cubierta, entonces se habla de fibras monomodo de índice escalonado. Los elevados flujos que se pueden alcanzar constituyen la principal ventaja de las fibras monomodo, ya que sus pequeñas dimensiones implican un manejo delicado y entrañan dificultades de conexión que aún se dominan mal.

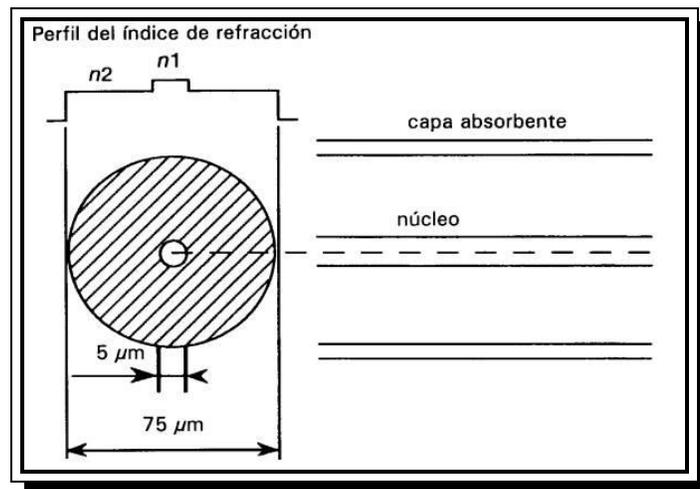


Figura 4.14 Estructura de Fibra Monomodo

4.5.1.3.2 Elementos básicos de un sistema de fibra óptica. Hay tres elementos primarios en un sistema de fibra óptica para comunicaciones:

- a. **El transmisor.** Es decir, la unidad que debe generar los rayos de luz, que puede ser conectada y desconectada muy rápidamente y/o modulada por algún tipo de señales que representen información. Se encarga de transformar las ondas

electromagnéticas en energía óptica o en luminosa, por ello se le considera el componente activo de este proceso.

- b. **La fibra óptica.** El cual debe tener una cubierta y un "encapsulamiento", así como una pureza que le hagan fuerte y transparente a las frecuencias de luz que se van a utilizar. Debe poder ser empalmada y reparada cuando sea necesario y tener capacidad para llevar los rayos de luz a una distancia razonable antes de que una estación repetidora tenga que reamplificar la luz para hacer posible que ésta atraviese la distancia casi total en la cual debe viajar. En algunos casos hay que usar muchas estaciones repetidoras.
- c. **Receptor.** Se encarga de reconvertir esos rayos de luz en voltajes y corrientes analógicas o digitales de forma que la estación del usuario pueda separar y utilizar las señales de información que se habían transmitido.

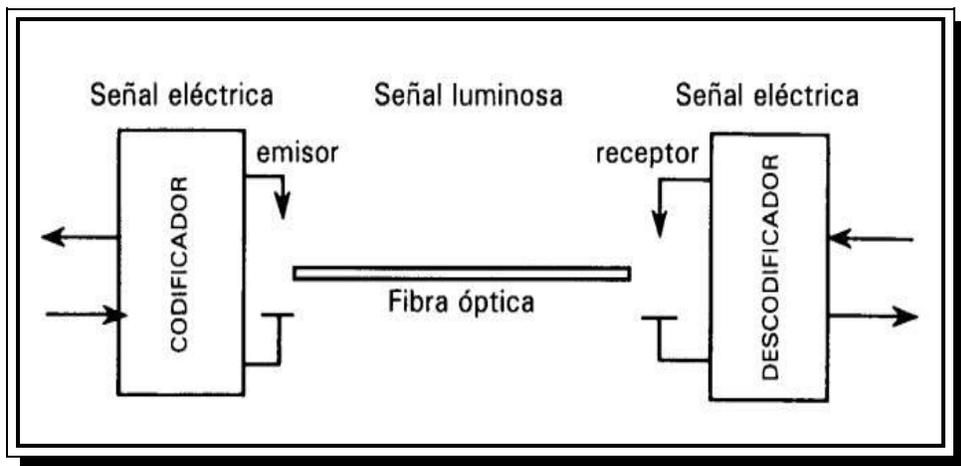


Figura 4.15 Elementos básicos de un sistema de fibra óptica

4.5.1.3.3 Sistemas de conexión. La información digital es modulada por un emisor de luz que puede ser:

- ✓ Un diodo electroluminiscente LED, que no incluye cavidad láser.
- ✓ Un diodo láser.
- ✓ Un láser modulado.

El fenómeno de dispersión es menos acentuado si se utiliza un láser, por tanto, éste permite obtener una potencia óptica superior a la de los LED, pero con un costo mayor. Además, la vida útil de un láser es inferior a la de un diodo LED. Sin embargo, su utilización es necesaria en el caso de la fibra monomodo. Se distinguen dos tipos de receptores:

- ✓ Los diodos PIN (Positive Intrinsic Negative).
- ✓ Los diodos de avalancha.

Son los componentes extremos (emisores y receptores) los que limitan la velocidad que se puede alcanzar con las fibras. Las conexiones permanentes son realizadas uniendo los extremos finales (por soldadura), las provisionales se realizan por medio de conectores o bornes que permiten múltiples conexiones y desconexiones.

4.5.1.4 Aplicaciones. Los cables de fibra óptica tienen muchas aplicaciones en el campo de las comunicaciones de datos:

- ✓ Conexiones locales entre ordenadores y periféricos o equipos de control y medición.
- ✓ Interconexión de ordenadores y terminales mediante enlaces dedicados de fibra óptica.
- ✓ Enlaces de fibra óptica de larga distancia y gran capacidad.

4.5.1.5 Comparación entre los diferentes medios de transmisión. En el siguiente cuadro se presenta una comparativa de los distintos tipos de cables descritos.

	Par Trenzado	Par Trenzado Blindado	Coaxial	Fibra Óptica
Tecnología ampliamente probada	Si	Si	Si	Si
Ancho de banda	Medio	Medio	Alto	Muy Alto
Hasta 1 Mhz	Si	Si	Si	Si
Hasta 10 Mhz	Si	Si	Si	Si
Hasta 20 Mhz	Si	Si	Si	Si
Hasta 100 Mhz	Si (*)	Si	Si	Si
27 Canales video	No	No	Si	Si
Canal Full Duplex	Si	Si	Si	Si
Distancias medias	100 m	100 m	500 (Ethernet)	2 km.(Multi.) 100km(Mono.)
Inmunidad Electromagnética	Limitada	Media	Media	Alta
Seguridad	Baja	Baja	Media	Alta
Coste	Bajo	Medio	Medio	Alto

Tabla 4.5 Comparación entre los diferentes medios de transmisión

4.5.1.6 Rendimiento de cables según su ancho de banda.

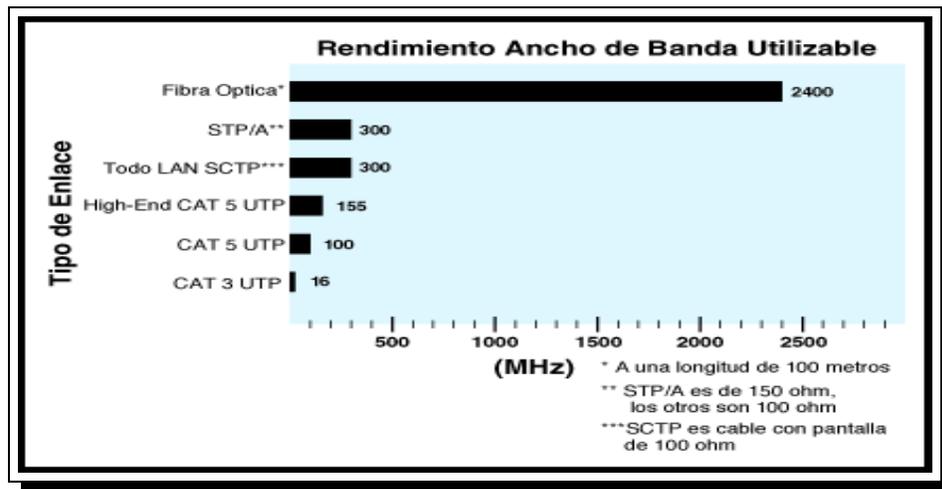


Figura 4.16 Rendimiento de cables según ancho de banda

4.5.2 Medios de transmisión no guiados.

4.5.2.1 Comunicaciones vía satélite. Los satélites artificiales han revolucionado las comunicaciones desde los últimos 20 años. Actualmente son muchos los satélites de comunicaciones que están alrededor de la tierra dando servicio a numerosas empresas, gobiernos, entidades. Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (canal de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (canal de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión. De esta manera se impide que los canales de subida y de bajada se interfieran, ya que trabajan en bandas de frecuencia diferentes.

La capacidad que posee un satélite de recibir y retransmitir se debe a un dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de los Ghz. La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria, que se encuentra a 36000 Km. sobre el ecuador. Esto permite que el satélite gire alrededor de la tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la tierra.

Existe un retardo de unos 0.5 segundos en las comunicaciones debido a la distancia que han de recorrer las señales. Los cambios en los retrasos de propagación provocados por el movimiento en órbita de un satélite geoestacionario necesitan transmisiones frecuentes de tramas de sincronización.

Los satélites tienen una vida media de siete a 10 años, pero pueden sufrir fallos que provocan su salida de servicio. Es, por tanto, necesario disponer de un medio alternativo de servicio en caso de cualquier eventualidad.

Las estaciones terrenas suelen estar lejos de los usuarios y a menudo se necesitan caros enlaces de alta velocidad. Las estaciones situadas en la banda de bajas frecuencias (la banda C) están dotadas de grandes antenas (de unos 30 metros de diámetro) y son extremadamente sensibles a las interferencias. Por este motivo suelen

estar situadas lejos de áreas habitadas. Las estaciones que trabajan en la banda Ku disponen de una antena menor y son menos sensibles a las interferencias. Utilizar un enlace de microondas de alta capacidad sólo ayudaría a complicar los problemas de ruido que presente el enlace con el satélite.

Las comunicaciones con el satélite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estación. Es necesario utilizar técnicas de encriptación para garantizar la privacidad de los datos.

Los satélites geoestacionarios pasan por periodos en los que no pueden funcionar. En el caso de un eclipse de Sol en el que la tierra se sitúa entre el Sol y el satélite, se corta el suministro de energía a las células solares que alimentan el satélite, lo que provoca el paso del suministro de energía a las baterías de emergencia, operación que a menudo se traduce en una reducción de las prestaciones o en una pérdida de servicio.

En el caso de tránsitos solares, el satélite pasa directamente entre el Sol y la Tierra provocando un aumento del ruido térmico en la estación terrena, y una pérdida probable de la señal enviada por el satélite.

Los satélites geoestacionarios no son totalmente estacionarios con respecto a la órbita de la tierra. Las desviaciones de la órbita ecuatorial hacen que el satélite describa una figura parecida a un ocho, de dimensiones proporcionales a la inclinación de la órbita con respecto al ecuador. Estas variaciones en la órbita son corregidas desde una estación de control.

Actualmente hay un problema de ocupación de la órbita geostacionaria. Cuando un satélite deja de ser operativo, debe irse a otra órbita, para dejar un puesto libre. La separación angular entre satélites debe ser de 2 grados (anteriormente era de 4). Esta medida implicó la necesidad de mejorar la capacidad de resolución de las estaciones terrenas para evitar detectar las señales de satélites próximos en la misma banda en forma de ruido.

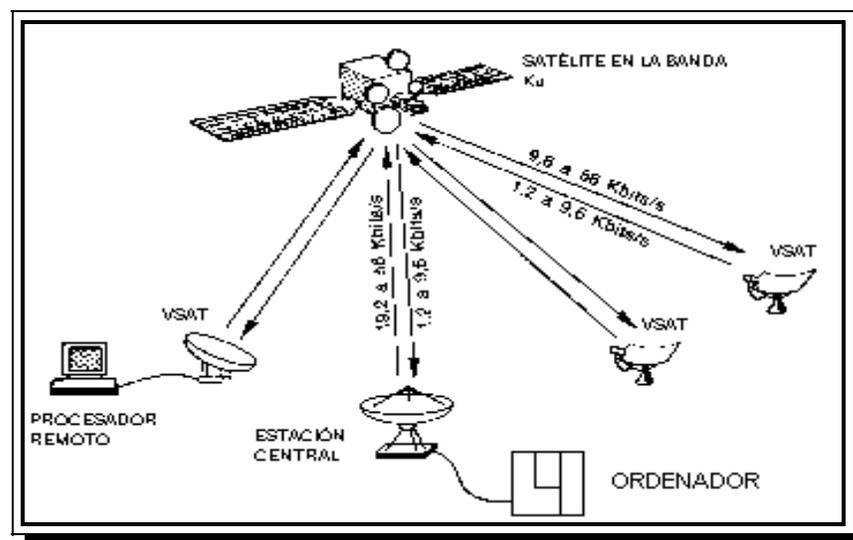


Figura 4.17 Red de datos AT&T con satélite y ordenador central

4.5.2.2 Microondas. Los enlaces de microondas se utilizan mucho como enlaces allí donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda de SHF, de modo que es necesario disponer de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores.

Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2,4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionar hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo.

Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11} dependiendo de la relación señal/ruido en los receptores. Pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores. Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las súper altas frecuencias, SHF, utilizándose para las redes inalámbricas la banda de los 18-19 Ghz. Estas redes tienen una propagación muy localizada y un ancho de banda que permite alcanzar los 15 Mbps.

La red Rialta de Motorola es una red de este tipo, la cual va a 10 Mbps y tiene un área de cobertura de 500 metros.



Figura 4.18 Antena de Microondas

4.5.2.3 Luz infrarroja. Permite la transmisión de información a velocidades muy altas: 10 Mbits/seg. Consiste en la emisión/recepción de un haz de luz; debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

Los infrarrojos son ondas electromagnéticas que se propagan en línea recta, siendo susceptibles de ser interrumpidas por cuerpos opacos. Su uso no precisa licencias administrativas y no se ve afectado por interferencias radioeléctricas externas, pudiendo alcanzar distancias de hasta 200 metros entre cada emisor y receptor. Infra LAN es una red basada en infrarrojos compatible con las redes Token Ring a 4Mbps, pudiendo utilizarse independientemente o combinada con una red de área local convencional.



Figura 4.19 Luz infrarroja

5. EQUIPOS DE RED

Dos o más dispositivos interconectados con el objetivo de compartir datos o recursos pueden formar una red. Una LAN puede necesitar cubrir más distancia de la que el medio de transmisión admite. O el número de estaciones puede ser demasiado grande para que la entrega de las tramas o la gestión de red se hagan de forma eficiente. Los dispositivos de red pueden ser activos o pasivos.

5.1 EQUIPOS ACTIVOS

5.1.1 Tarjeta de red o adaptador.

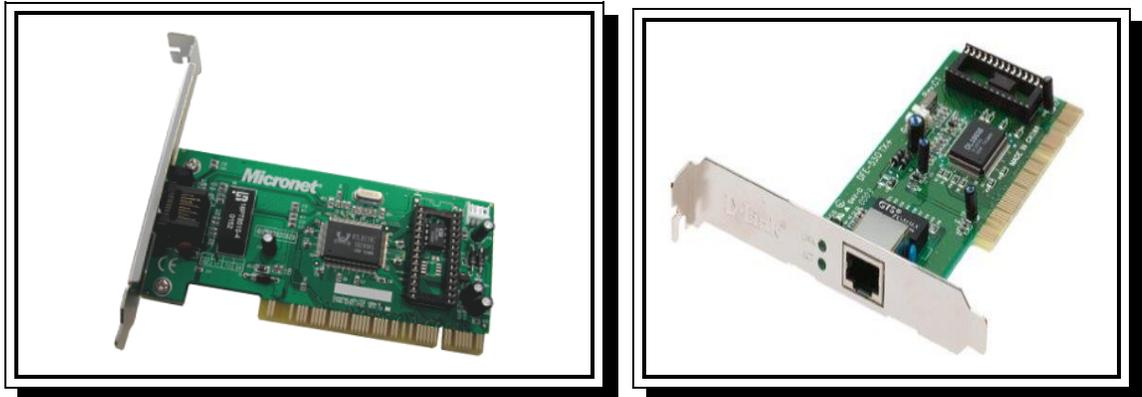


Figura 5.1 Tarjetas de red

Un adaptador o tarjeta de red es el elemento fundamental en la composición de la parte física de una red de área local. Cada adaptador de red es una interface hardware entre la plataforma o sistema informático y el medio de transmisión físico por el que se transporta la información de un lugar a otro.

El adaptador puede venir incorporado o no con la plataforma hardware del sistema. En gran parte de los ordenadores personales hay que añadir una tarjeta separada, independiente del sistema, para realizar la función de adaptador de red. Esta tarjeta se inserta en el bus de comunicaciones del ordenador personal convenientemente configurada. En otros sistemas, el hardware propio del equipo ya incorpora el adaptador de red. Una tarjeta de red es un dispositivo electrónico que consta de las siguientes partes:

- ✓ Interface de conexión al bus del ordenador.
- ✓ Interface de conexión al medio de transmisión.

- ✓ Componentes electrónicos internos, propios de la tarjeta.
- ✓ Elementos de configuración de la tarjeta: puentes, conmutadores, etc.

La conexión de la tarjeta de red al hardware del sistema sobre el que se soporta el host de comunicaciones se realiza a través del interface de conexión. Cada ordenador transfiere internamente la información entre los distintos componentes (CPU, memoria, periféricos) en paralelo a través del bus interno. Los distintos componentes, especialmente los periféricos y las tarjetas, se unen a este bus a través de una serie de conectores, llamados slots de conexión, que siguen unas especificaciones concretas.

Por tanto, un slot es el conector físico en donde se pincha la tarjeta. Es imprescindible que la especificación del slot de conexión coincida con la especificación del interface de la tarjeta. La velocidad de transmisión del slot, es decir, del bus de interno del ordenador, y el número de bits que es capaz de transmitir en paralelo, serán los primeros factores que influirán decisivamente en el rendimiento de la tarjeta en su conexión con el procesador central.

La tecnología más consolidada para PC compatibles es ISA, aunque debido a su bajo rendimiento ha sido sustituida por la tecnología PCI, que está implantada en la mayor parte de las plataformas modernas. Las tarjetas ISA son apropiadas si las necesidades de transmisión no son muy elevadas, por ejemplo, para ordenadores que se conecten a través de una Ethernet a 10 Mbps sin demasiadas exigencias de flujo de información. En el caso de que sean necesarias velocidades de transmisión más altas, es recomendable la tecnología PCI. El resto de las tecnologías no están extendidas.

La salida hacia el cable de red requiere un interface de conectores especiales para red, como por ejemplo: BNC, RJ-45, RJ-58, etc., dependiendo de la tecnología de la red y del cable que se deba utilizar. Normalmente, la tarjeta de red debe procesar la información que le llega procedente del bus del ordenador para producir una señalización adecuada al medio de transmisión, por ejemplo, una modulación, un empaquetamiento de datos, un análisis de errores, etc.

La tarjeta de red debe ponerse de acuerdo con el sistema operativo del host y su hardware, en el modo en el que se producirá la comunicación entre ordenador y tarjeta. Esta configuración se rige por una serie de parámetros que deben ser determinados en la tarjeta en función del hardware y software del sistema, de modo que no colisionen con los parámetros de otros periféricos o tarjetas. Los principales son:

- ✓ **IRQ, interrupción.** Es el número de una línea de interrupción con el que se avisan sistema y tarjeta de que se producirá un evento de comunicación entre ellos. Por ejemplo, cuando la tarjeta recibe una trama de datos, ésta es procesada y analizada por la tarjeta, activando su línea IRQ, que le identifica unívocamente, para avisar al procesador central que tiene datos preparados para el sistema. Valores típicos para el IRQ son 3, 5, 7, 9 y 11.
- ✓ **Dirección de E/S.** Es una dirección de memoria en la que escriben y leen el procesador central del sistema y la tarjeta, de modo que les sirve de bloque de memoria para el intercambio mutuo de datos. Tamaños tópicos de este bloque de memoria (o buffer) son 16 y 32 kb. Este sistema de intercambio de datos entre el

host y la tarjeta es bastante rápido, por lo que es muy utilizado en la actualidad, pero necesita procesadores más eficientes. La dirección de E/S se suele expresar en hexadecimal, por ejemplo, DC000H.

- ✓ **DMA, acceso directo a memoria.** Cuando un periférico o tarjeta necesita transmitir datos a la memoria central, un controlador hardware apropiado llamado controlador DMA pone de acuerdo a la memoria y a la tarjeta sobre los parámetros en que se producirá el envío de datos, sin necesidad de que intervenga la CPU en el proceso de transferencia. Cuando un adaptador de red transmite datos al sistema por esta técnica (DMA), debe definir qué canal de DMA va a utilizar, y que no vaya a ser utilizado por otra tarjeta. Este sistema de transferencia se utiliza poco en las tarjetas modernas.
- ✓ **Dirección de puerto de E/S.** El puerto de Entrada/Salida es un conjunto de bytes de memoria en los que procesador central y periféricos intercambian datos de Entrada/Salida y del estado en el que se efectúan las operaciones. Tipo de transceptor. Algunas tarjetas de red incorporan varias salidas con diversos conectores, de modo que se puede escoger entre ellos en función de las necesidades. Algunas de estas salidas necesitan transceptor externo y hay que indicárselo a la tarjeta cuando se configura.

Tradicionalmente, estos parámetros se configuraban en la tarjeta a través de puentes (jumpers) y conmutadores (switches). Actualmente está muy extendido el modo de configuración por software, que no requiere la manipulación interna de hardware: los parámetros son guardados por el programa configurado que se suministra con la tarjeta

en una memoria no volátil que reside en la propia tarjeta. Algunas tarjetas de red incorporan un zócalo para inserción de un chip que contiene una memoria ROM (de sólo lectura) con un programa de petición del sistema operativo del host a través de la red. De este modo, el host puede cargar su sistema operativo remotamente.

En la última generación de tarjetas, la configuración se realiza de manera automática: elección del tipo de conector, parámetros de comunicación con el sistema, etc., aunque requiere hardware especializado en el host. Esta tecnología de autoconfiguración de llama Plug & Play (enchufar y funcionar).

No todos los adaptadores de red sirven para todas las redes. Existen tarjetas apropiadas para cada tecnología de red: Ethernet, Token Ring, FDDI, etc. Además, algunas tarjetas que sirven para el mismo tipo de red tienen parámetros de acuerdo con ciertas especificaciones. Por ejemplo, una tarjeta Ethernet puede estar configurada para transmitir a 10 Mbps o a 100 Mbps, dependiendo del tipo de red Ethernet a la que se vaya a conectar. También se puede elegir el tipo de conexión: 10Base2, 10Base5, 10 BaseT, 100 BaseT, etc. Algunos adaptadores de red no se conectan directamente al bus de comunicaciones interno del ordenador, sino que lo hacen a través de otros puertos de comunicación serie o paralelo. Requieren controladores especiales para su correcto funcionamiento y su rendimiento no es tan alto como en las tarjetas conectadas al bus.

5.1.2 Hub o concentrador.

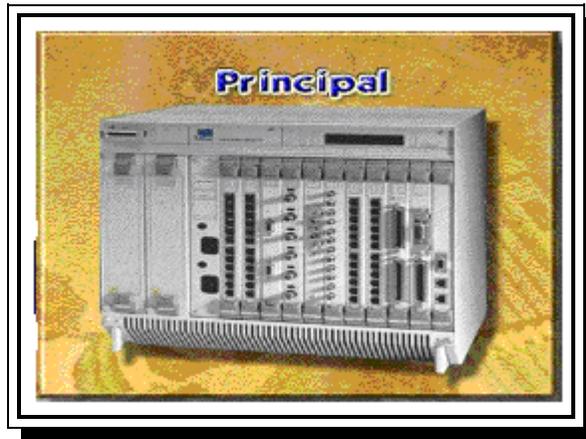


Figura 5.2 Hub físico

Los hub son dispositivos que interconectan host dentro de una red. Es el dispositivo de interconexión más simple que existe. Sus principales características son:

- ✓ Se trata de un armario de conexiones donde se centralizan todas las conexiones de una red, es decir un dispositivo con muchos puertos de entrada y salida.
- ✓ No tiene ninguna función aparte de centralizar conexiones.
- ✓ Se suelen utilizar para implementar topologías en estrella física, pero funcionando como un anillo o como un bus lógico.

Pueden conectarse varios concentradores entre si para que se puedan conectar más ordenadores a la red. En la figura 5.3 aparecen conectados dos conectores de cuatro puertos. Ahí, ambos conectores usan cable UTP (10BASE-T) y clavijas RJ-45 para la conexión. Se utiliza un puerto en cada concentrador para conectarse con el otro concentrador. El cable empleado para conectar los concentradores es un cable de par

trenzado “cruzado” que es el mismo que podríamos utilizar para conectar solo 2 ordenadores entre si y poder ahorrarnos el hub.

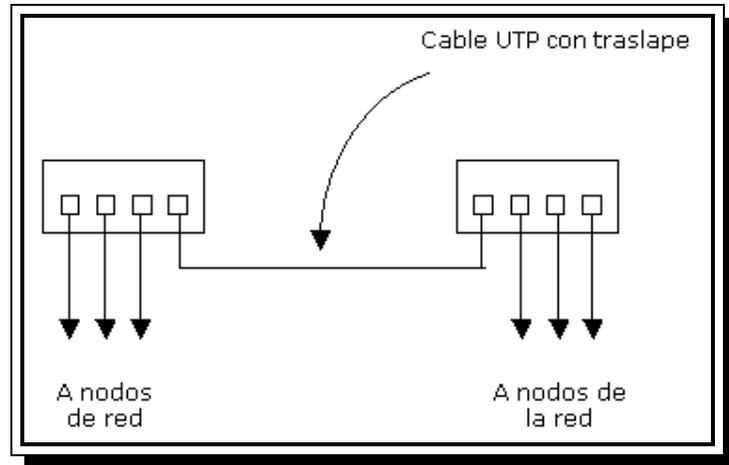


Figura 5.3 Conexiones entre hubs

Muchos Concentradores tienen un conector BNC en la parte trasera, además de los conectores normales RJ-45. El conector BNC permite que se enlacen Concentradores por medio de un cable coaxial Thin Ethernet. Al disponer del conector BNC, no se tiene que desperdiciar un puerto RJ-45 en cada concentrador, si queremos unirlos. Además en este puerto pueden conectarse más ordenadores de la red cuya tarjeta de red tenga salida BNC.

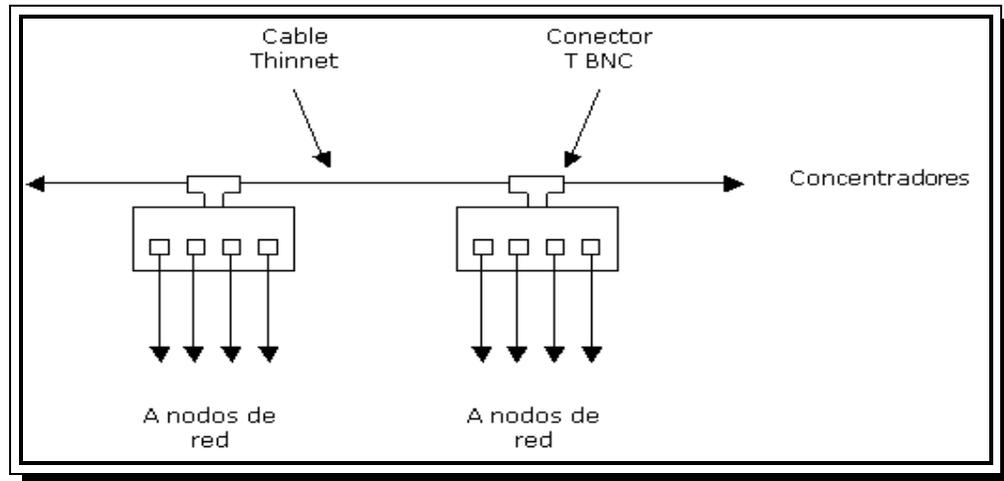


Figura 5.4 Conexiones entre hubs con conector BNC

5.1.2.1 Clases de hubs.

5.1.2.1.1 Hubs activos: Permiten conectar nodos a distancias de hasta 609 metros, suelen tener entre 8 y 12 puertos y realizan funciones de amplificación y repetición de la señal. Los más complejos además realizan estadísticas.



Figura 5.5 Hub activo

5.1.2.1.2 Hubs pasivos: son simples armarios de conexiones. Permiten conectar nodos a distancias de hasta 30 metros. Generalmente suelen tener entre 8 y 12

puertos. Los hubs son un punto central de conexión para los ordenadores de la red cuando están dispuestos de acuerdo a una topología de estrella. Suelen tener bocas RJ-45 para par trenzado y algún conector BNC para cable coaxial.

5.1.2.2 Funcionamiento. Un HUB tal como dice su nombre es un concentrador. Simplemente une conexiones y no altera las tramas que le llegan. Para entender como funciona veamos paso a paso lo que sucede (aproximadamente) cuando llega una trama.

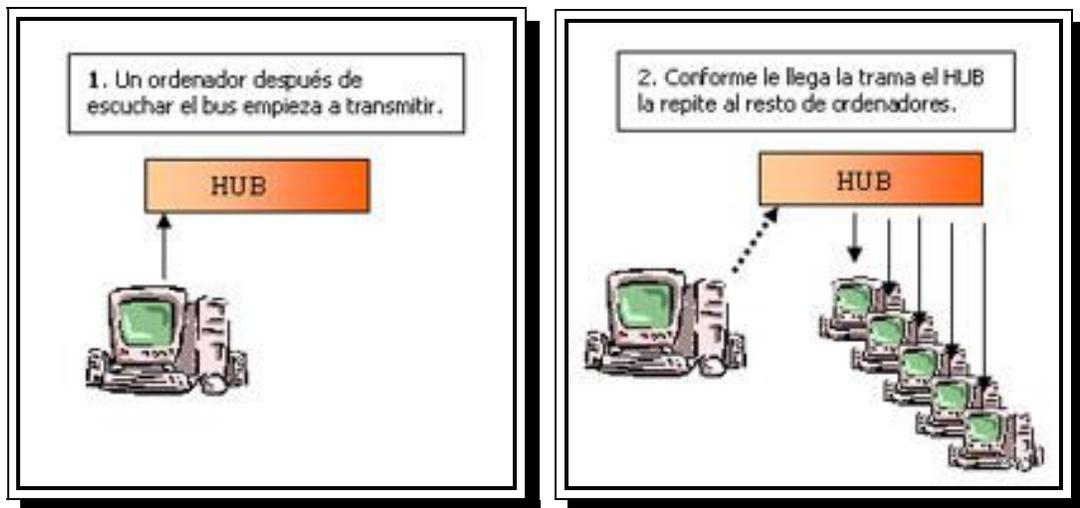


Figura 5.6 Funcionamiento del hub

Visto lo anterior podemos sacar las siguientes conclusiones:

- El hub envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el hub envía la información a todos los ordenadores que están conectados a él.

- b. Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea que otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

- c. Un hub funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el hub no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 Mb le transmitiera a otro de 10 Mb algo se perdería el mensaje.

5.1.3 Switch.



Figura 5.7 Switch

Un switch es un dispositivo diseñado para resolver problemas de rendimiento en la red, debidos a anchos de banda pequeños y embotellamientos. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC. Por ejemplo cuando montamos una red local de 10Mbits/s con un hub, ese ancho de banda se comparte entre todas las estaciones. Si todas las estaciones utilizan la red al mismo tiempo se

producirán colisiones y el rendimiento de la red disminuirá. Con el switch esos 10Mbps/s no se comparten sino que se conmutan, podríamos decir que cada estación tendrían siempre disponibles los 10Mbps/s. Un switch es como un hub pero con inteligencia, sabe a quien debe enviar los paquetes y evita que se produzcan colisiones en la red.



Figura 5.8 Switch de 24 puertos

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.



Figura 5.9 Switch comercial

5.1.3.1 Funcionamiento. Normalmente un switch no tiene ningún tipo de gestión, es decir, no se puede acceder a él. Sólo algunos switch tienen algún tipo de gestión pero suele ser algo muy simple. Veamos cómo funciona un switch.

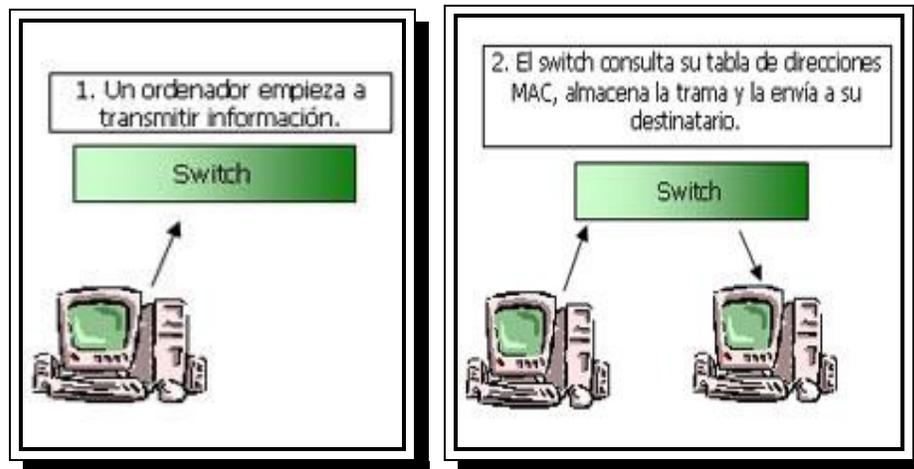


Figura 5.10 Funcionamiento del switch

- El switch conoce los ordenadores que tiene conectados a cada uno de sus puertos. Cuando en la especificación de un switch se lee algo como "8k MAC address table" se refiere a la memoria que el switch destina a almacenar las direcciones. Un switch cuando se enchufa no conoce las direcciones de los ordenadores de sus puertos, las aprende a medida que circula información a través de él. Cuando un switch no conoce la dirección MAC de destino envía la trama por todos sus puertos, al igual que un hub. Cuando hay más de un ordenador conectado a un puerto de un switch este aprende sus direcciones MAC y cuando se envían información entre ellos no la propaga al resto de la red, a esto se llama filtrado.

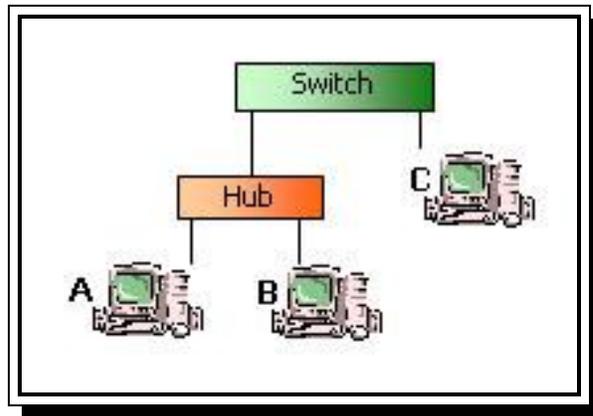


Figura 5.11 Filtrado

El tráfico entre A y B no llega a C, esto es el filtrado. Las colisiones que se producen entre A y B tampoco afectan a C. A cada parte de una red separada por un switch se le llama segmento.

- El switch almacena la trama antes de reenviarla. A este método se llama store & forward, es decir almacenar y enviar. Hay otros métodos como por ejemplo Cut-through que consiste en recibir los 6 primeros bytes de una trama que contienen la dirección MAC y a partir de aquí ya empezar a enviar al destinatario. Cut-through no permite descartar paquetes defectuosos. Un switch de tipo store & forward controla el CRC de las tramas para comprobar que no tengan error, en caso de ser una trama defectuosa la descarta y ahorra tráfico innecesario. El store & forward también permite adaptar velocidades de distintos dispositivos de una forma más cómoda, ya que la memoria interna del switch sirve de buffer. Obviamente si se envía mucha información de un dispositivo rápido a otro lento otra capa superior se encargará de reducir la velocidad. Otro de los métodos es el Fragment-fre que consiste en recibir los primeros 64 bytes de una trama porque es en estos donde se

producen la mayoría de colisiones y errores. Así pues cuando vemos que un switch tiene 512KB de RAM es para realizar el store & forward. Esta RAM suele estar compartida entre todos los puertos, aunque hay modelos que dedican un trozo a cada puerto.

- Un switch moderno también suele tener lo que se llama Auto-Negotiation, es decir, negocia con los dispositivos que se conectan a él la velocidad de funcionamiento, 10 Mb ó 100, así como si se funcionara en modo full-dùplex o half-dùplex.
- Velocidad de proceso: todo lo anterior requiere que el switch tenga un procesador que, debe ser lo más rápido posible. También hay un parámetro conocido como back-plane o plano trasero que define el ancho de banda máximo que soporta un switch. El back plane dependerá del procesador, del número de tramas que sea capaz de procesar. Por ejemplo 100megabits x 2 (cada puerto puede enviar 100 Mb y enviar 100 más en modo full-dùplex) x 8 puertos = 1,6 Gb. Así pues, un switch de 8 puertos debe tener un back-plane de 1,6 Gb para trabajar bien. Lo que sucede es que para disminuir costos esto se reduce ya que es muy improbable que se produzca la situación de tener los 8 puertos enviando a tope. Pero la probabilidad a veces no es cierta.
- Si un nodo puede tener varias rutas alternativas para llegar a otro, un switch tiene problemas para aprender su dirección ya que aparecerá en dos de sus entradas. A esto se le llama loop. El protocolo de Spanning Tree Protocol IEEE 802.1d se

encarga de solucionar este problema, aunque los “switch” domésticos no suelen tenerlo.

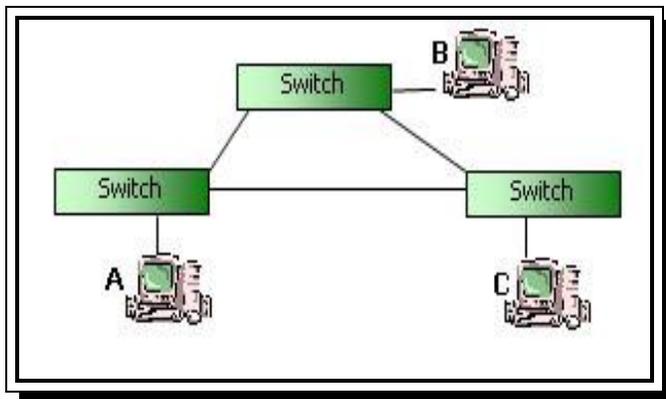


Figura 5.12 Conexiones entre switch

5.1.4 Puentes o bridges. Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN. Los puertos revisan la dirección asociada con cada paquete de información. Luego, si la dirección es la correspondiente al otro segmento de red, el puente pasara el paquete al segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del segmento de red actual, no pasara el paquete al otro lado. Considere el caso de dos redes separadas, una que opera en Thin Ethernet y la otra basada en un esquema de cableado propio con adaptadores de red propios. La función del puente es transmitir la información enviada por un nodo de una red al destino pretendido en otra red.

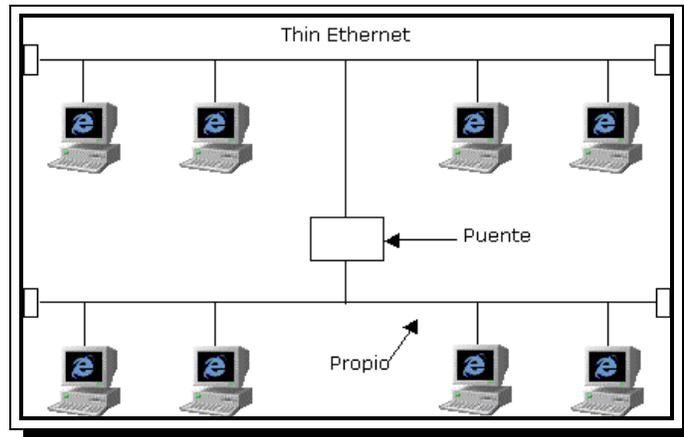


Figura 5.13 conexión de dos LANs por medio de un puente

Los puentes también suelen emplearse para reducir la cantidad de tráfico de red de un segmento de red. Mediante la división de un solo segmento de red en dos segmentos y conectándolos por medio de un puente, se reduce el tráfico general en la red. Para ayudar a ilustrar este concepto utilizaremos la siguiente figura donde antes de incorporar un puente a la red, todo el tráfico de la red está en un segmento. AB representa la información enviada del nodo A al B, BC la del nodo B al C y CD la del nodo C al D. Mediante la incorporación de un puente y la división del segmento del cable de red en dos segmentos, solo dos actividades suceden en cada segmento en vez de tres. El puente mantendrá aislada la actividad de la red en cada segmento, a menos que el nodo de un segmento envíe información al nodo de otro segmento (en cuyo caso el puente pasaría la información).

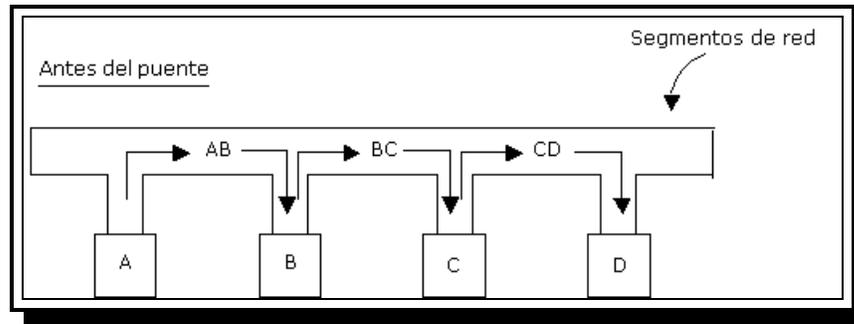


Figura 5.14 Segmentos de red antes del puente

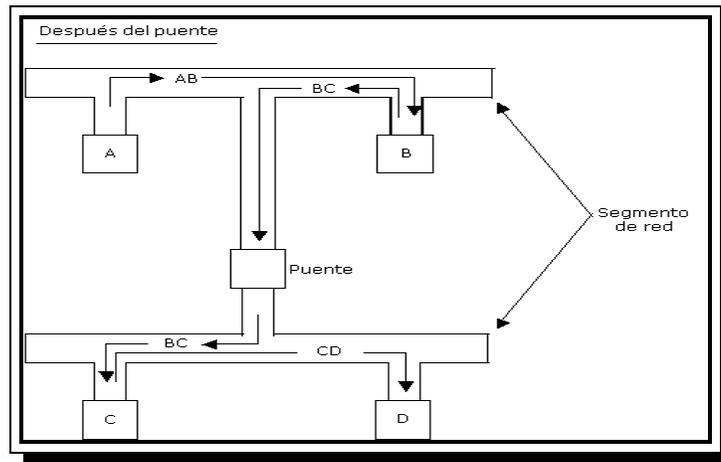


Figura 5.15 Segmentos de red después del puente

Un puente también sirve para conectar dos segmentos de red Thin Ethernet por medio de comunicaciones inalámbricas, en la figura esta conectado un puente a cada segmento de red. El puente incluye un transmisor y un receptor para enviar la información adecuada entre segmentos.

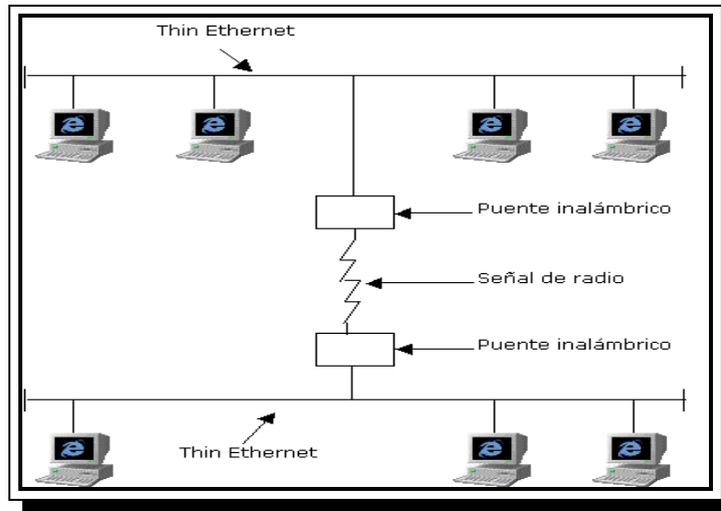


Figura 5.16 Puentes para redes inalámbricas

Los puentes vienen en todas formas y tamaños. En muchos casos, un puente es un dispositivo similar a una computadora con conectores a los que se conectan redes separadas. En otros casos, un puente es, de hecho, una computadora con un adaptador para cada red que va a conectarse. Un software especial permite el paso de la información adecuadamente a través de los adaptadores de la red de un segmento de red al segmento de red de destino.

5.1.5 Ruteador o Router.



Figura 5.17 Router

Los ruteadores son similares a los puentes, solo que operan a un nivel diferente. Los ruteadores requieren por lo general que cada red tenga el mismo protocolo. Con un protocolo común, el ruteador permite ejecutar funciones mas avanzadas de las podría permitir un puente, como conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token ring. Los ruteadores también suelen ser lo suficientemente inteligentes para determinar la ruta mas eficiente para el envío de datos, en caso de haber mas de una ruta.

El encaminador interconecta redes de área local operando en el nivel 3 de OSI como muestra la figura 5.18, por tanto, su funcionalidad está fuertemente condicionada por el protocolo de red. Esto hace que su rendimiento sea menor, ya que emplea tiempo de proceso en analizar los paquetes del nivel de red que le llegan, sin embargo, permiten una organización muy flexible de la interconexión de las redes.

Hay dos tipos fundamentales de encaminadores, según que la red a la que deben servir esté orientada a la conexión o no. Además, hay que tener en cuenta el protocolo de red que debe encaminar. Un router que encamine TCP/IP no sirve para encaminar ningún otro protocolo. Los encaminadores comerciales suelen tener capacidad para encaminar los protocolos más utilizados, todos ellos en el nivel 3: IP, IPX, AppleTalk, DECnet, XNS, etc.

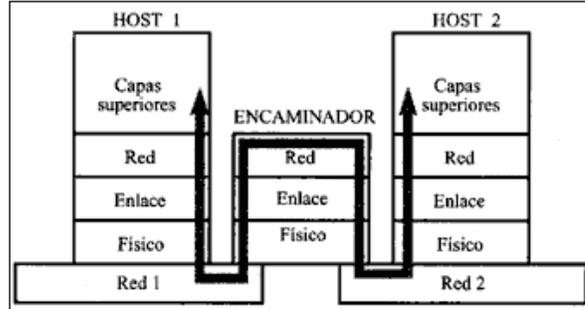


Figura 5.18 Router en el modelo OSI

Las características fundamentales de los encaminadores se pueden resumir del modo que sigue:

- ✓ Interpretan las direcciones lógicas de la capa 3, en lugar de las direcciones MAC o capa de enlace, como hacen los puentes o los conmutadores.
- ✓ Son capaces de cambiar el formato de la trama, ya que operan en un nivel superior a la que operan los switch.

Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que el switch al reenviar los paquetes. Permitiendo también unir redes que funcionan con protocolos diferentes. El ruteador realiza dos funciones básicas:

- ✓ Es responsable de crear y mantener tablas de ruteo para cada capa del protocolo de red, estas tablas son creadas de forma estática o bien dinámica. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado en el contenido de la especificación del protocolo en la tabla de ruteo.

- ✓ La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retardo y condiciones de tráfico. La desventaja es que el proceso adicional de procesamiento de las cabeceras de los paquetes en el ruteador puede incrementar el tiempo de espera o reducir el rendimiento del ruteador cuando se compara con una simple arquitectura de switch.

El ruteador se debe usar cuando se necesita:

- ✓ Segmentar la red dentro de dominios individuales de broadcast.
- ✓ Suministrar un envío inteligente de paquetes.
- ✓ Soportar rutas redundantes en la red.
- ✓ Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambientes LAN y WAN.
- ✓ Redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- ✓ Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

Entonces, ¿cual es la selección más óptima para el diseño de la red?

- ✓ Si se requiere soporte para rutas redundantes, envío inteligente de paquetes o acceder la WAN, se debe seleccionar un ruteador.

- ✓ Si solo se quiere incrementar el ancho de banda para descongestionar el tráfico, un switch probablemente será la mejor selección.
- ✓ No se debe olvidar que el switch es de propósito general y tiene un bajo costo por puerto en comparación con el ruteador.

5.1.6 Gateways o pasarelas. Se trata de ordenadores que trabajan a nivel de aplicación del modelo OSI de la ISO. Es el más potente de todos los dispositivos de interconexión de Intranets. Permite interconectar Intranets de diferentes arquitecturas; es decir, de diferentes topologías y protocolos; no sólo realiza funciones de encaminamiento como los routers, sino que también realiza conversiones de protocolos, modificando el empaquetamiento de la información para adaptarla a cada Intranet. Un gateway hace todo lo que hace un ruteador, pero a diferencia de este, la compuerta puede hacer cambios de protocolos, por lo que es ideal para conectar dos redes totalmente distintas.

5.1.7 DTU. (DTU, Data Terminal Unit), es un equipo que provee el puerto de conexión al equipo del cliente. Es el equipo utilizado en la gran mayoría los circuitos cuando se requiere de servicio digital de hasta 128 Kbps. La DTU posee dos puertos de salida, es un equipo administrable y configurable por software y trabaja con interfaces V.35 y RS-232. Además disponemos de DTU para velocidades hasta 1 Mbps. Las características del DTU son:

- ✓ Caso plástico moldeado
- ✓ Cable de conexión en espiral, retractil
- ✓ Mensaje en pantalla hasta 16 caracteres en 2 líneas
- ✓ Mensaje de información del status del DTU
- ✓ Indicaciones audio y visuales de la lectura o de la transferencia de datos
- ✓ Teclado de membrana con 21 teclas, codificado con colores de función
- ✓ Tres modos de funcionamiento: Verificación, lectura, y programación
- ✓ Hasta 64 lecturas

5.1.8 Grupos de trabajo. En la figura se ve un típico ambiente de grupos de trabajo en una red interna. Tiene dos concentradores y puede crecer hasta 20, con 200 usuarios.

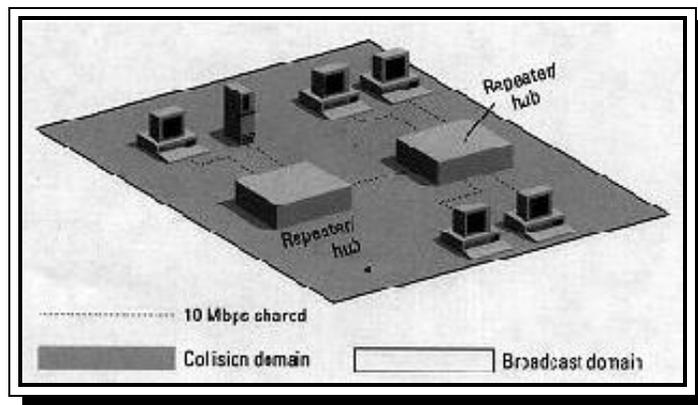


Figura 5.19 Grupos de trabajo

Aquí el administrador quiere maximizar el ancho de banda de los servicios y dividir los PCs en pequeños dominios de colisiones que compartan 10 Mbps y sólo un número limitado de usuarios importantes requerirán 10 Mbps dedicados para sus aplicaciones.

5.1.8.1 Opción #1: Solución con ruteador

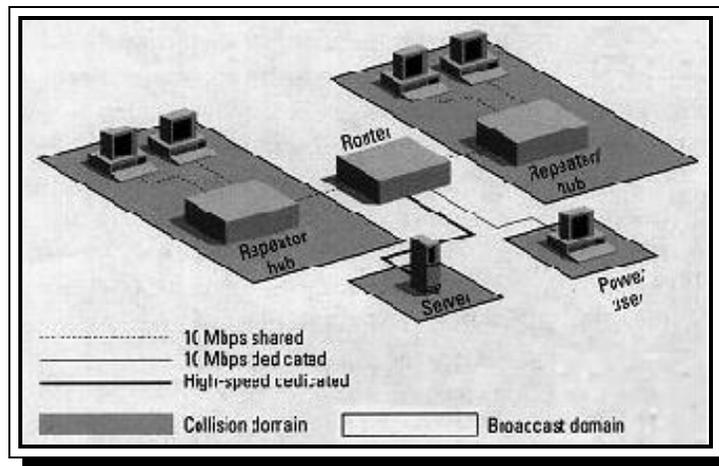


Figura 5.20 Solución con ruteador

El ruteador es configurado con una interface dedicada de alta velocidad al servidor y un número grande de interfaces Ethernet, las cuales son asignadas a cada uno de los concentradores y usuarios importantes. Y para instalarlo, el administrador de red divide los dominios grandes de broadcast en dominios pequeños.

La selección de ruteador no se ha basado en lo económico o en tecnología. Desde una perspectiva de costo, el ruteador tiene un alto costo por puerto y un gasto a largo plazo en su manejo, mayor que el del switch. Desde una perspectiva tecnológica el ruteador proporciona pocos paquetes de salida. Probablemente también los niveles de tráfico de broadcast no justifiquen la complejidad adicional de separarlos.

5.1.8.2 Opción #2: Solución con switch.

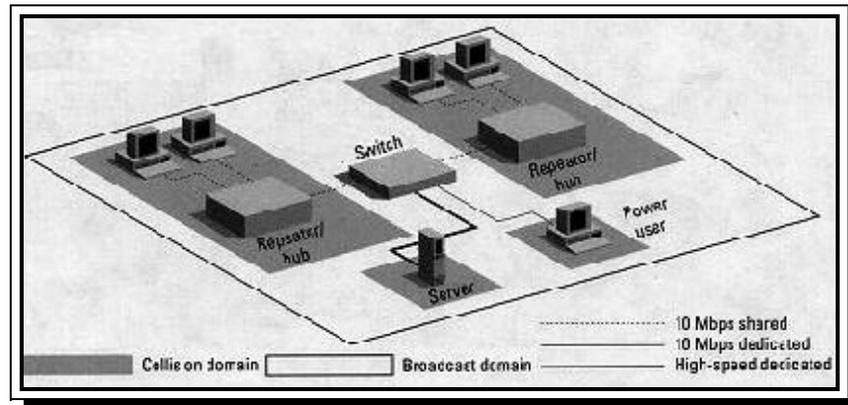


Figura 5.21 Solución con switch

La figura muestra el mismo grupo de trabajo, pero con un switch. En este ambiente el dominio de broadcast se divide en 4 dominios de colisiones, donde los usuarios atados a dichos dominios comparten 10 Mbps. Los accesos dedicados a servidores y usuarios poderosos, eliminan la competencia por acceder al medio y el servidor local tiene un interface de alta velocidad para eliminar posibles cuellos de botella. Además de garantizar que los paquetes no se perderán por la limitación del buffer, cuando el tráfico de varios puertos sea enviado a un solo destino. Si se tiene un dispositivo backbone colapsado en la central de datos de alta velocidad, se puede poner un segundo módulo al switch e ir migrando suavemente.

Si únicamente se quiere dar ancho de banda a los grupos de trabajo, el switch es la mejor solución, pues sus ventajas son mayores a las del ruteador para este tipo de aplicaciones dado que:

El switch ofrece mayor velocidad, al enviar su salida a todos los puertos a la vez. El rendimiento de su salida puede ser crítico, cuando el cliente y el servidor don puestos en segmentos diferentes, pues la información debe pasar por diversos dispositivos de la red interna. El switch da mayor rendimiento por puerto en términos de coste que un ruteador. El coste es un factor importante, pues limita la compra de dispositivos y el poder dividir en segmentos de red.

5.2 EQUIPOS PASIVOS

5.2.1 Armarios y gabinetes.



Figura 5.22 Armario

Los armarios y gabinetes se usan para un montaje profesional del cableado estructurado, o bien para pequeños concentradores, dependiendo su tamaño; su objetivo es evitar tener todos los cables sueltos y sin orden, además son ideales para esos lugares donde son necesarias frecuentes tareas de mantenimiento del cableado.

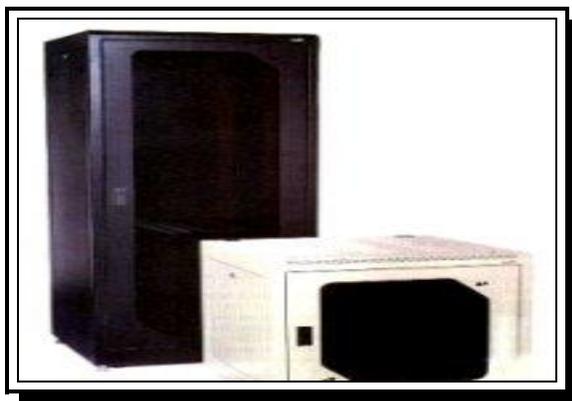


Figura 5.23 Armario y gabinete

5.2.2 Racks

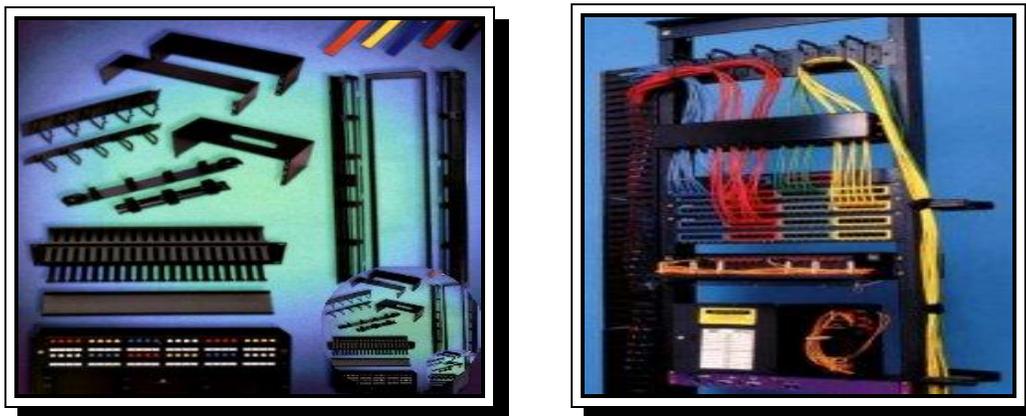


Figura 5.24 Racks

El Rack es un tipo de armario, ideal para mantener las funciones electrónicas y el cableado en formato; permite aislar los hubs, switches, routers o telefonía del polvo y otros elementos.

5.2.3 Patch-panel

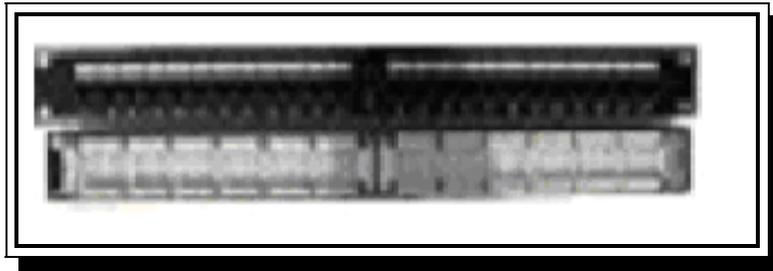


Figura 5.25 Patch-panel

Son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos. Un Patch-Panel posee una determinada cantidad de puertos (RJ-45 End-Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas.

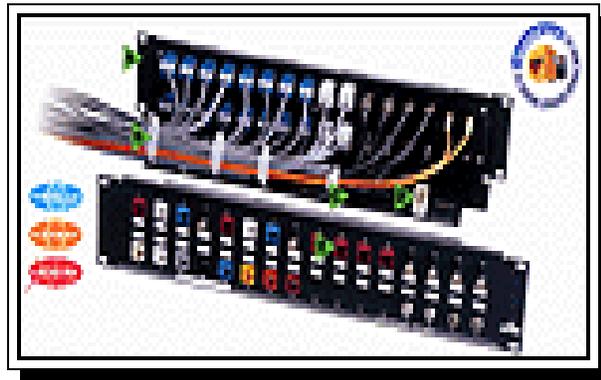


Figura 5.26 Patch-panel con cableado

En estos conectores es donde se ponchan las cerdas de los cables provenientes de los cajetines u otros Patch-panel. La idea del Patch-Panel además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan equipos en una red, de una mejor manera. Para ponchar las cerdas de un cable Twisted Pair en el Patch-Panel se usa una ponchadora al igual que en los cajetines.

5.2.4 Bandejas.

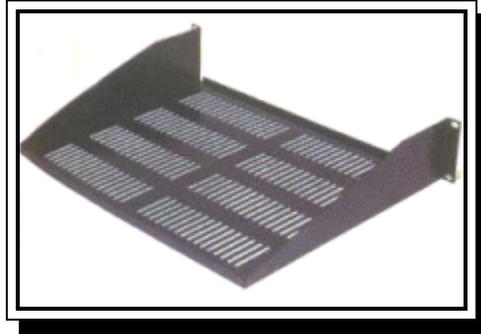


Figura 5.27 Bandejas

Las bandejas son útiles para colocar elementos de ancho no estándar, o para soporte de los equipos activos de red en los armarios o gabinetes; tales como hubs, switch etc.

5.2.5 Organizador de cables

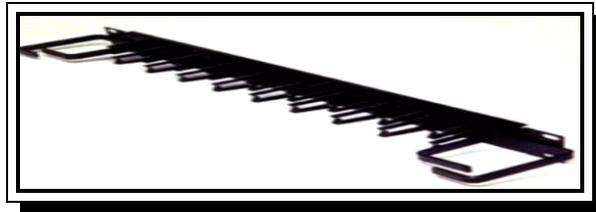


Figura 5.28 Organizador de cables

5.2.6 Patch-cords

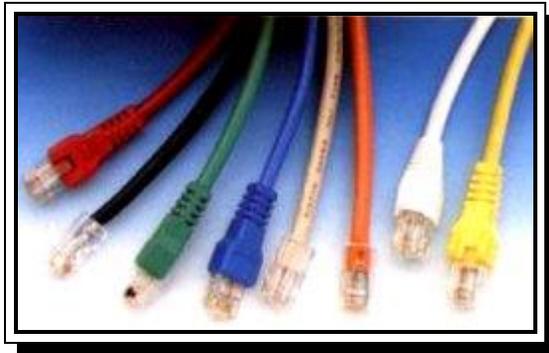


Figura 5.29 Patch-cord

Los patch-cord son cables de varias medidas de largo, para conectar entre los concentradores y los patch-panels, y los puntos de red y los PCs

5.2.7 Patch-cord para fibra óptica.



Figura 5.30 Patch-cord para fibra óptica

5.2.8 Canaletas.

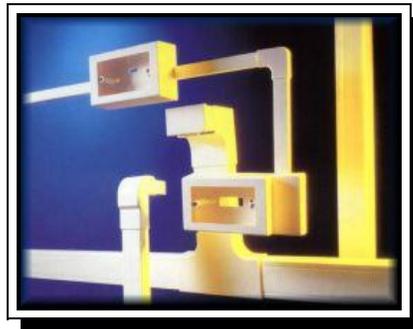


Figura 5.31 Canaletas

Las canaletas son útiles en las situaciones, donde no se tiene tubería disponible para pasar los cables de la red, y se debe hacer de modo superficial. Se podría dividir en dos tipos dependiendo del uso que se le dé:

- ✓ Las de distribución. Recorren las distintas zonas del edificio y por ellas van los cables de todas los puntos de red.
- ✓ Las finales. Llevan tan solo los cables de cada una de las rosetas

6. CABLEADO ESTRUCTURADO



Figura 6.1 Cableado estructurado

6.1 EVOLUCIÓN DE LOS SISTEMAS DE CABLEADO

A principios de la década de los 80, cuando las computadoras se comenzaron a enlazar a fin de intercambiar información, se usaron muchos modelos de cableado diferentes. Algunas compañías construyeron sus sistemas basados en cable coaxial. Otras pensaron que el bicoaxial u otros tipos trabajarían mejor. Con esos cables tenían que seguirse ciertos parámetros a fin de hacer funcionar el sistema. Se tenían que usar cierto tipo de conectores, se tuvieron que establecer longitudes máximas de tendido, y fueron necesarias topologías particulares.

A través de la definición de cada aspecto de sus sistemas, los fabricantes "encerraban" a los consumidores dentro de sistemas que eran propiedad privada de cada quien. El sistema de un fabricante no trabajaba con el de otro, ni utilizaba cualquier otro tipo de cable. Si un consumidor decidía cambiar sistemas, no solo necesitaba comprar nueva electrónica y programación, sino que también necesitaba cambiar el cableado. Localizar fallas en los sistemas privados era muy difícil y tardado, comparado con los actuales sistemas de cableado estructurado. Un problema en cualquier estación de trabajo podía traer la caída del sistema completo, sin dejar indicio al administrador de la red, de donde pudo haber ocurrido el problema. Eventualmente se encontraba la causa del problema, tal como una conexión rota. Una vez terminadas las reparaciones, se levantaba el sistema de nuevo en línea. El proceso podía durar horas o días, dejando a los usuarios paralizados. Con tales sistemas, los traslados, adiciones, o cambios eran también difíciles. Cada vez que se agregaba una nueva máquina, se tenía que instalar cable nuevo e insertarlo en el anillo, o anexarlo a la línea. Aún más, pudiera tenerse que dar de baja el sistema completo para agregar un nuevo usuario.

Estos factores contribuyeron a aumentar la frustración entre los administradores de redes, quienes constantemente buscaban formas más fáciles de mantener sus redes, reducir los tiempos fuera de servicio, y bajar costos. De hecho, los estudios han mostrado que hasta un 70% de las caídas de red en un sistema privado no estructurado, es atribuible al cableado. Como parte de su acuerdo operativo para 1984, AT&T ya no se hizo responsable del cableado al interior de las instalaciones del cliente y desde entonces, el proveedor del servicio mantiene el sistema solo hasta el punto de

acometida. Más allá de este punto, el mantenimiento y actualización del sistema telefónico, fue responsabilidad del cliente.

Como resultado, los administradores de redes tenían (y muchos) problemas, 2 sistemas de cableado distintos que demandan total y particular atención. El deseo de un sistema que pudiera usarse para cualquier aplicación, sin los consecuentes problemas y dolores de cabeza de los sistemas anteriores, creció exponencialmente hasta la llegada del cableado estructurado.

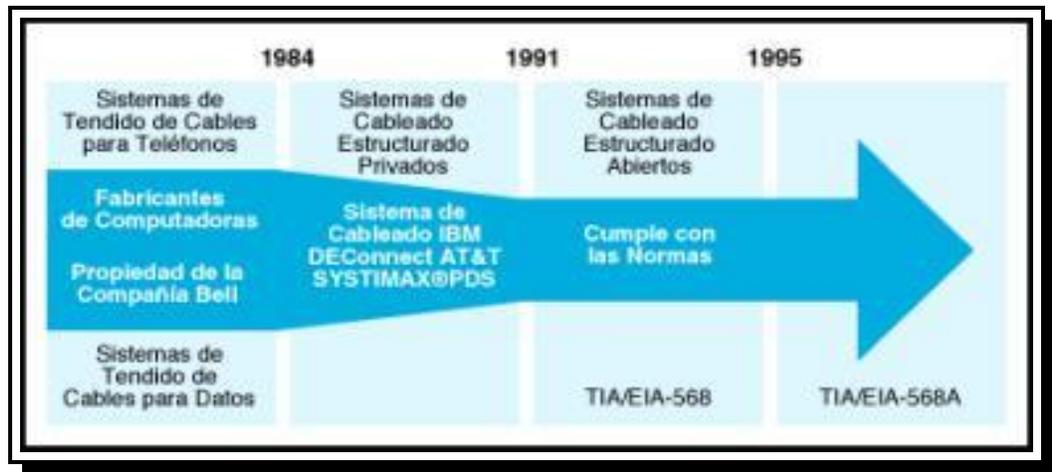


Figura 6.2 Esquema de la evolución en los sistemas de cableado

En síntesis los sistemas de cableado de lugares utilizados para servicios de telecomunicaciones, han experimentado una constante evolución con el correr de los años. Los sistemas de cableado para teléfonos fueron en una oportunidad especificados e instalados por las compañías de teléfonos, mientras que el cableado para datos estaba determinado por los proveedores del equipo de computación. Después de la división de la compañía AT&T en los Estados Unidos, se hicieron intentos para simplificar el cableado, mediante la introducción de un enfoque más

universal. A pesar de que estos sistemas ayudaron a definir las pautas relacionadas con el cableado, no fue sino hasta la publicación de la norma sobre tendido de cables en edificios ANSI/EIA/TIA-568 en 1991, que estuvieron disponibles las especificaciones completas para guiar en la selección e instalación de los sistemas de cableado.

6.2 CONSIDERACIONES

El cableado que "cumple con las normas" está previsto para acomodar una amplia variedad de aplicaciones de sistemas (por ejemplo, voz, fax, módem, mainframe y LAN), utilizando un esquema de cableado universal. A pesar de que este enfoque ha simplificado los métodos de cableado y de la selección de los componentes, quedan todavía varios puntos claves que hay que tener en cuenta:

- ✓ Requerimientos de funcionamiento y de ancho de banda
- ✓ Aplicaciones en redes apoyadas
- ✓ Costo durante la vida útil
- ✓ Características del producto
- ✓ Apoyo técnico y servicio

Estos puntos son importantes porque contemplan varios aspectos relacionados con la especificación, compra, y mantenimiento de un sistema de cableado. Estas preguntas sirven como base a la hora de instalar un sistema de cableado:

- ✓ ¿Cuánto tiempo va a permanecer el sistema en uso?

- ✓ ¿Qué demandas de funcionamiento y de aplicación se le impondrán al sistema?
- ✓ ¿Existen requerimientos físicos especiales en el edificio que deberán ser considerados?
- ✓ ¿Qué tipo de apoyo es necesario para el producto y el diseño?

A pesar de que las normas han avanzado lo suficiente para poner un poco de orden a los sistemas de cableado, estas consideraciones adicionales lo llevan un paso más allá para arribar a la selección de un sistema que es flexible, confiable, manejable y a prueba del futuro.

6.3 DEFINICIÓN

El cableado estructurado es un sistema de cableado diseñado en una jerarquía lógica que adapta todo el cableado existente, y el futuro, en un único sistema. Un sistema de cableado estructurado exige una topología en estrella, que permite una administración sencilla y una capacidad de crecimiento flexible.

También podría decirse que es la organización de cables dentro de un edificio que recoge las necesidades de comunicación (teléfonos, ordenadores, fax, módems, etc.) actuales y futuras de las empresas. Este tipo de instalaciones hay que tenerlas en cuenta del mismo modo que se hace con la electricidad, agua, gas, etc.

A la hora de realizar el cableado de un edificio hay que tener en cuenta que la tecnología varía a tal velocidad que las nuevas tendencias pueden hacer quedar

obsoleta cualquier solución adoptada que no prevea una gran capacidad de adaptabilidad.

Por este motivo aparece el concepto de “cableado estructurado”. Su intención es:

- ✓ Capacidad de crecimiento a bajo costo.
- ✓ Base para soportar todas las tecnologías de niveles superiores sin necesidad de diferentes tipos de cableado
- ✓ Realizar una instalación compatible con las tecnologías actuales y las que estén por llegar.
- ✓ Tener la suficiente flexibilidad para realizar los movimientos internos de personas y máquinas dentro de la instalación.
- ✓ Estar diseñado e instalado de tal manera que permita una fácil supervisión, mantenimiento y administración. Es fácilmente gestionable y muy fiable

6.4 CARACTERÍSTICAS

Entre las características generales de un sistema de cableado estructurado destacan las siguientes:

- ✓ La configuración de nuevos puestos se realiza hacia el exterior desde un nodo central, sin necesidad de variar el resto de los puestos. Sólo se configuran las conexiones del enlace particular.
- ✓ La localización y corrección de averías se simplifica ya que los problemas se pueden detectar a nivel centralizado.

- ✓ Mediante una topología física en estrella se hace posible configurar distintas topologías lógicas tanto en bus como en anillo, simplemente reconfigurando centralizadamente las conexiones.

6.5 SUBSISTEMAS DE CABLEADO ESTRUCTURADO

Un sistema de cableado estructurado se puede dividir en cuatro subsistemas básicos:

- ✓ Subsistema de Administración.
- ✓ Subsistema de Distribución de Campus.
- ✓ Subsistema horizontal.
- ✓ Subsistema vertical.

Cada subsistema tiene una variedad de cables y productos diseñados para proporcionar una solución adecuada a cada caso. Los distintos elementos que lo componen son los siguientes:

- ✓ Repartidor de Campus (CD; Campus Distributor).
- ✓ Cable de distribución (Backbone) de Campus.
- ✓ Repartidor Principal o del Edificio (BD; Building Distributor)
- ✓ Cable de distribución (Backbone) de Edificio.
- ✓ Subrepartidor de Planta (FD; Floor Distributor).
- ✓ Cable Horizontal.
- ✓ Punto de Transición opcional (TP; Transition Point).
- ✓ Toma ofimática (TO).
- ✓ Punto de acceso o conexión.

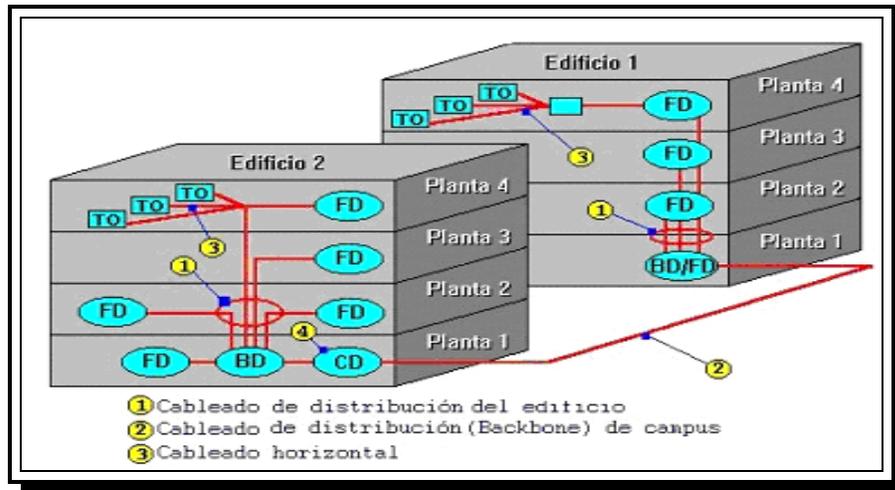


Figura 6.3 Distribución de los subsistemas de cableado estructurado

6.5.1 Subsistema de administración. Los elementos incluidos en este sistema son entre otros:

- ✓ Armarios repartidores.
- ✓ Equipos de comunicaciones.
- ✓ Sistemas de Alimentación Ininterrumpida (SAI).
- ✓ Cuadros de alimentación.
- ✓ Tomas de tierra.

6.5.1.1 Armarios repartidores. Los armarios repartidores de planta (FD) deberán situarse, siempre que haya espacio disponible, lo más cerca posible de la(s) vertical(es). En la instalación de los repartidores de edificio (BD) y de campus (CD) debe considerarse también su proximidad a los cables exteriores. En el caso de instalarse equipos de comunicaciones será necesario instalar una acometida eléctrica y la ventilación adecuada. Los repartidores de planta deberán estar distribuidos de

manera que se minimicen las distancias que los separan de las rosetas, a la vez que se reduzca el número de ellos necesarios.

Los módulos de regletas deberán permitir especialmente:

- ✓ La interconexión fácil mediante cables conectores (patch cords) y cables puente o de interconexión entre distintas regletas que componen el sistema de cableado estructurado.
- ✓ La integridad del apantallamiento en la conexión de los cables caso de utilizarse sistemas apantallados.
- ✓ La prueba y monitorización del sistema de cableado.

Los módulos de regletas se deben unir en el momento del montaje a un portaetiquetas que permita la identificación de los puntos de acceso, de los cables y de los equipos. Los repartidores conectados juntos forman una estructura jerárquica tal como se muestra en la siguiente figura:

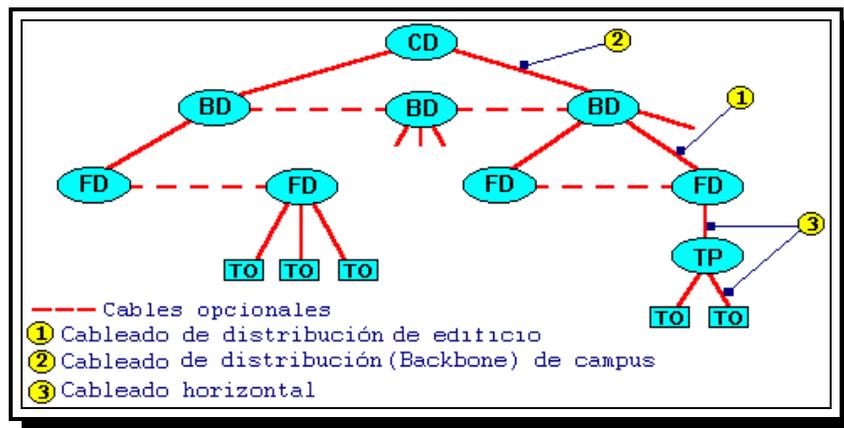


Figura 6.4 Estructura jerárquica de los repartidores

Esta forma jerárquica proporciona al sistema de cableado de un alto grado de flexibilidad necesario para acomodar una variedad de aplicaciones, configurando las diferentes topologías por la interconexión de los cables puentes y los equipos terminales. El repartidor de campus se conecta a los repartidores de edificio asociados a través del cable de distribución o backbone del campus. El repartidor de edificio se conecta a sus subrepartidores vía el cable de distribución del edificio.

6.5.2 Subsistema Horizontal. Se extiende desde el subrepartidor de planta (FD) hasta el punto de acceso o conexión pasando por la toma ofimática. Está compuesto por:

- ✓ El cable propiamente dicho
- ✓ La roseta de conexión del área de trabajo
- ✓ El mecanismo de conexión en el patch-panel
- ✓ Los latiguillos en el armario de comunicaciones.
- ✓ Las canaletas.

6.5.2.1 Cableado horizontal. Se conoce con el nombre de cableado horizontal a los cables usados para unir cada área de trabajo con el patch-panel. Todo el cableado horizontal deberá ir canalizado por conducciones adecuadas. En la mayoría de los casos, se eligen para esta función las canaletas.

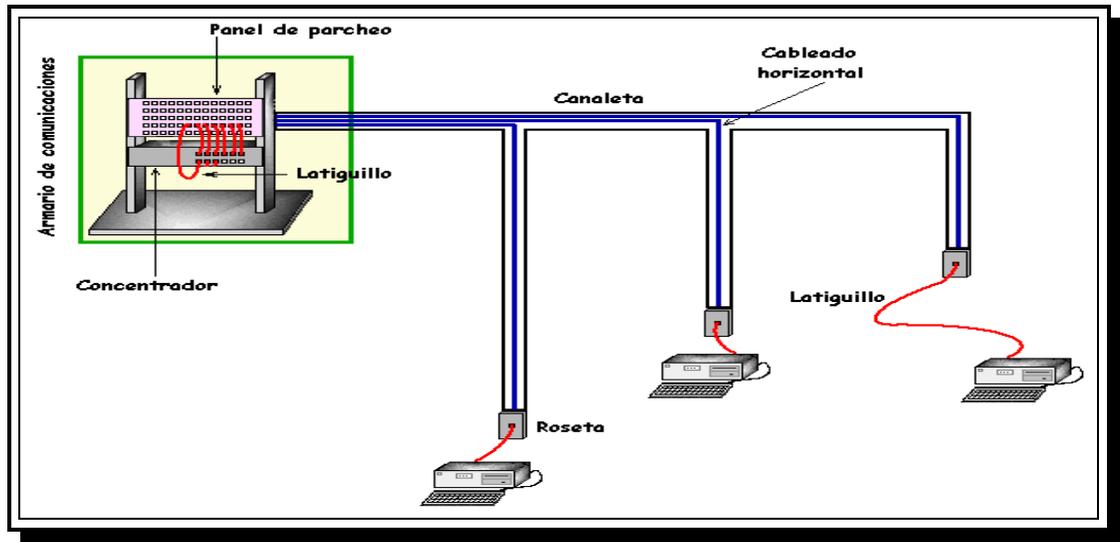


Figura 6.5 Cableado horizontal

Las canaletas van desde el patch-panel hasta los puntos de red de cada uno de los puestos de la red. La topología usada es en estrella teniendo en cuenta que cada mecanismo de conexión en el punto de red está conectado a su propio mecanismo de conexión en el patch-panel del armario de comunicaciones. Cada cable horizontal no podrá superar los 90 metros con independencia del tipo de cable. Además los cables para el parcheo en el armario de comunicaciones no podrán tener más de 6 metros y no podrá superar los 3 metros el cable de conexión del puesto de trabajo a la roseta. La suma de los cables puente, cordones de adaptación y cables de equipos no deben sumar más de 10 metros; estos cables pueden tener diferentes características de atenuación que el cable horizontal, pero la suma total de la atenuación de estos cables ha de ser el equivalente a estos 10 metros.

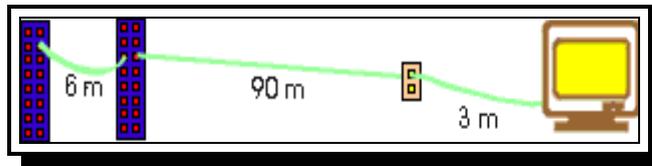


Figura 6.6 Distancias permitidas entre los diferentes puntos de conexión

El cableado horizontal típicamente, contiene más cable que el cableado del backbone y es menos accesible que el cableado del backbone. Los cables se colocarán horizontalmente en la conducción empleada y se fijarán en capas mediante abrazaderas colocadas a intervalos de 4 metros.

6.5.2.2 Área de trabajo. Se define como la zona donde están los distintos puestos de trabajo de la red. En cada uno de ellos habrá un toma de red que permita conectar el dispositivo o dispositivos que se quieran integrar en la red.

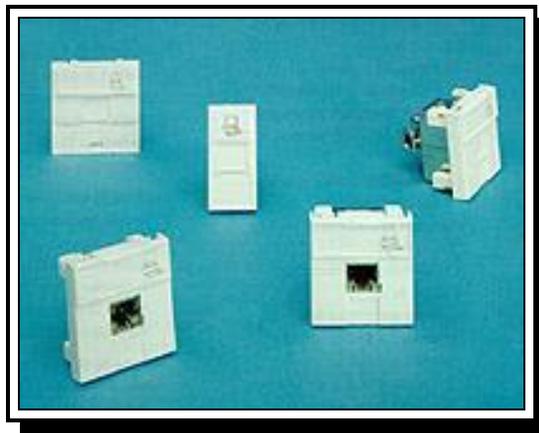


Figura 6.7 Tomas de red

El área de trabajo comprende todo lo que se conecta a partir de las tomas de conexión de red hasta los propios dispositivos a conectar (ordenadores e impresoras fundamentalmente). Están también incluidos cualquier filtro, adaptador, etc., que se necesite. Éstos irán siempre conectados en el exterior del toma. Si el cable se utiliza

para compartir voz, datos u otros servicios, cada uno de ellos deberá tener un conector diferente en el propio toma de conexión. Al cable que va desde el toma hasta el dispositivo a conectar se le llama latiguillo o patch-cord y no puede superar los 3 metros de longitud.

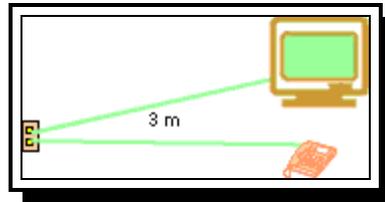


Figura 6.8 Distancia requerida desde el toma hasta el PC

6.5.3 Subsistema vertical. El cableado vertical (o de "backbone") 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 colindantes. En el cableado vertical es usual utilizar fibra óptica o cable UTP, aunque en algunos casos se puede usar cable coaxial. 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.

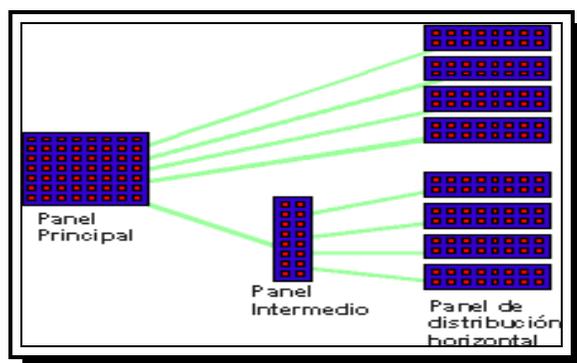


Figura 6.9 Mecanismos de conexión entre los paneles principales e intermedios

En el cableado vertical están incluidos:

- ✓ Los cables del "backbone".
- ✓ Los mecanismos en los paneles principales e intermedios
- ✓ Los patch-cord usados para el parcheo
- ✓ Los mecanismos que terminan el cableado vertical en los armarios de distribución horizontal.

6.6 EJEMPLO DE UN CABLEADO ESTRUCTURADO TÍPICO

- ✓ Ensamblajes para Conexiones Provisionales de Cables.
- ✓ Salidas de información.
- ✓ Cable Horizontal.
- ✓ Productos para Interconexión.
- ✓ Cable Principal

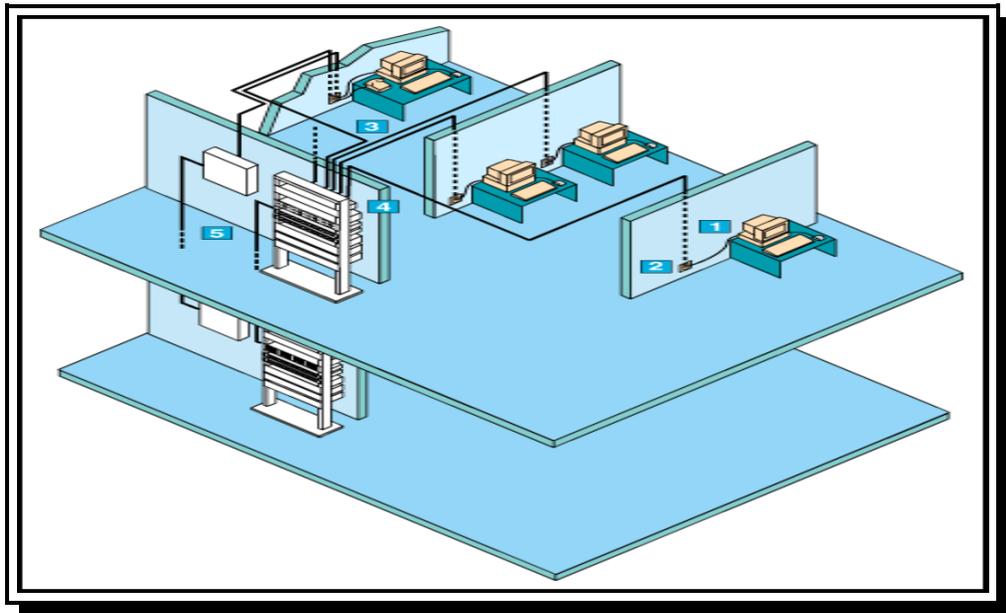


Figura 6.10 Cableado estructurado típico

7. PROTOCOLO TCP/IP

Un protocolo de comunicaciones define las normas que posibilitan establecer una comunicación entre varios equipos o dispositivos, ya que estos equipos pueden ser diferentes entre sí.

Un protocolo define:

- ✓ Como las computadoras se identificarán unas a otras sobre una red.
- ✓ La forma que los datos deben tomar para ser transmitidos.
- ✓ Como la información debiera ser procesada una vez que llega a su destino.

Existen dos tipos de protocolos: protocolos de bajo nivel y protocolos de red. Los protocolos de bajo nivel controlan la forma en que las señales se transmiten por el cable o medio físico. Los protocolos de red organizan la información (controles y datos) para su transmisión por el medio físico a través de los protocolos de bajo nivel.

7.1 DEFINICIÓN DE PROTOCOLO TCP/IP

El Protocolo de control de transmisión/protocolo entre redes (TCP/IP) es un conjunto de protocolos que definen cómo se intercambian todas las transmisiones a través de Internet. Su denominación proviene de sus dos protocolos más populares TCP/IP, y se está utilizando desde hace muchos años, demostrando su efectividad a gran escala.

7.1.1 TCP/IP e Internet. TCP/IP y el concepto de interconexión de redes se han desarrollado juntos, cada uno dando forma al crecimiento del otro. Es necesario comprender cómo se relaciona TCP/IP con la entidad física de cualquier internet a la que sirve. Internet bajo TCP/IP opera como una única red que conecta muchas computadoras de cualquier tamaño y forma. Internamente, una internet (o, más específicamente, Internet) es una interconexión de redes físicas independientes (como LAN) conectadas juntas por dispositivos de interconexión de redes.

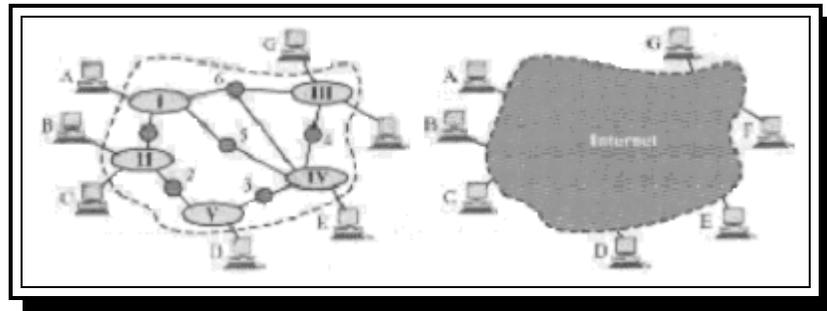


Figura 7.1 Una internet de acuerdo a TCP/IP

7.1.2 TCP/IP y OSI. El Protocolo de control de transmisión (TCP) fue desarrollado antes que el modelo OSI. Por tanto, los niveles del protocolo TCP/IP no coinciden exactamente con los del modelo OSI. El protocolo TCP/IP consta de cinco niveles: físico, de enlace de datos, de red, de transporte y de aplicación. El nivel de aplicación en TCP/IP se puede considerar cómo una combinación de los niveles de sesión, de presentación y de aplicación del modelo OSI. En el nivel de transporte, TCP/IP define dos protocolos: TCP y el Protocolo de data grammas de usuario (UDP). En el nivel de red, el principal protocolo definido por TCP/IP es el Protocolo entre redes (IP), aunque hay algunos otros protocolos que soportan la transferencia de datos en este nivel.

En los niveles físicos y de enlace de datos, TCP/IP no define ningún protocolo específico. Una red en TCP/IP puede ser una red de área local (LAN), una red de área metropolitana (MAN) o una red de área amplia (WAN).

7.1.3 Encapsulado. La Figura 7.2 muestra el encapsulado de las unidades de datos en niveles diferentes del conjunto de protocolos TCP/IP. La unidad de datos creada en el nivel de aplicación se denomina mensaje. TCP o UDP crea una unidad de datos denominada segmento o datagrama de usuario. El nivel IP a su vez crea una unidad de datos denominada datagrama. La transferencia de datagramas a través de Internet es responsabilidad del protocolo TCP/IP. Sin embargo, para ser capaz de transferirlo físicamente de una red a otra, el datagrama debe encapsularse en una trama en el nivel de enlace de datos de la red subyacente y finalmente ser transmitido por el medio de transmisión.

7.2 NIVEL DE RED

En el nivel de red (o, más precisamente, nivel de redes interconectadas), TCP/IP ofrece el protocolo entre redes (IP). IP, a su vez, contiene cuatro protocolos: ARP, RARP, ICMP e IGMP.

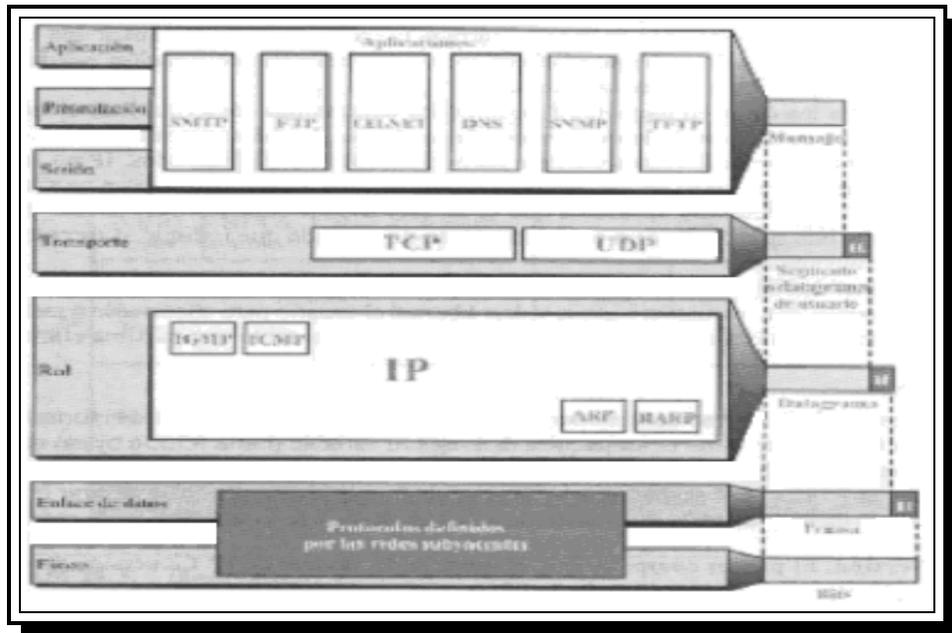


Figura 7.2 TCP/IP y el modelo OSI

7.2.1 Protocolo IP. IP es el mecanismo de transmisión utilizado por los protocolos TCP/IP, Es un protocolo basado en datagramas sin conexión y no fiable, ofrece un servicio de mejor entrega posible. Por mejor entrega posible lo que se quiere indicar es que IP no ofrece comprobaciones ni seguimientos. IP asume que los niveles subyacentes no son fiables e intenta que la transmisión llegue a su destino lo mejor que puede, pero sin ofrecer garantías. Las transmisiones a través de redes físicas pueden ser destruidas debido a varias razones. El ruido puede causar errores en los bits durante la transmisión por el medio; un encaminador congestionado puede descartar un datagrama si es incapaz de retransmitirlo antes de que se supere un límite de tiempo; el encaminamiento puede hacer que los datagramas entren en un bucle y sean destruidos al final, y los enlaces desactivados pueden hacer que no haya camino para alcanzar al destino.

Si la fiabilidad es importante, IP debe ser utilizado con un protocolo fiable como TCP. IP transporta los datos en paquetes denominados datagramas, cada uno de los cuales es transportado de forma independiente. Los datagramas pueden viajar a través de encaminadores diferentes y llegar fuera de secuencia o duplicados. IP no se encarga de realizar un seguimiento de los encaminadores ni ofrece facilidades para reordenar los datagramas una vez recibidos. Debido a que es un servicio sin conexión, IP no crea circuitos virtuales para la entrega. No hay un establecimiento de llamada que indique al receptor la llegada de una transmisión.

La funcionalidad limitada de IP no debería ser considerada como una debilidad, sin embargo. IP ofrece funciones de transmisión básicas y deja libertad al usuario para añadir sólo aquellas facilidades necesarias para una aplicación concreta, permitiendo por tanto una máxima eficiencia.

7.2.1.1 Datagramas. Los paquetes en el nivel IP se denominan datagramas. La Figura 7.3 muestra el formato de un datagrama IP. Un datagrama es un paquete de longitud variable (hasta 65.536 bytes) que consta de dos partes: una cabecera y datos. La cabecera puede incluir de 20 a 60 bytes y contiene información esencial para el encaminamiento y la entrega. Es habitual en TCP/IP mostrar la cabecera en secciones de cuatro bytes.

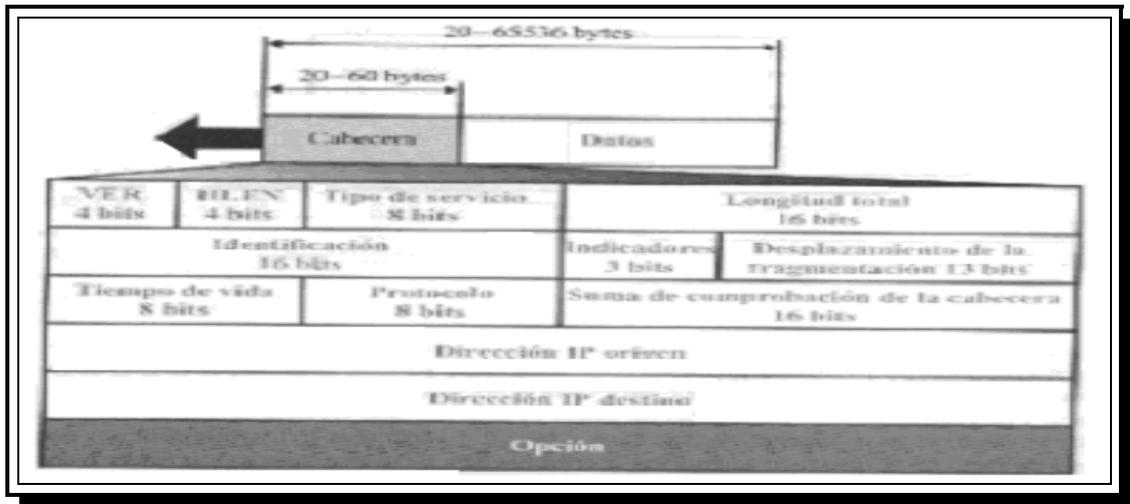


Figura 7.3 Datagrama IP

7.3 DIRECCIONAMIENTO

Además de la dirección física (contenida en la interfaz de red) que identifica el dispositivo individual, Internet requiere una convención en el direccionamiento: una dirección que identifique la conexión de una estación a la red. Cada dirección Internet costa de cuatro bytes (32 bits), que definen tres campos: la clase, el identificador de la red y el identificador de la estación. Estas partes son de longitud variable dependiendo de las clases de direcciones.

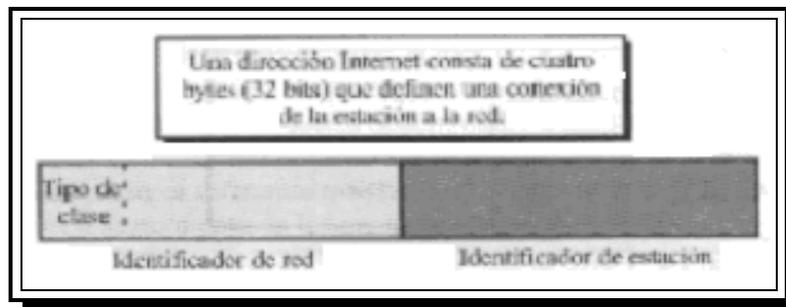


Figura 7.4 Dirección Internet

7.3.1 Clases de redes. Actualmente hay cinco patrones diferentes en uso, cada uno de los cuales define una clase de dirección. Estas clases están diseñadas para cubrir las necesidades de tipos diferentes de organizaciones. Por ejemplo, una dirección de clase A son las que tienen la numeración más baja. Sólo utilizan un byte para identificar la clase y la red, y deja tres bytes disponibles para números de estaciones. Esta división significa que las redes de clase A pueden tener más estaciones que las redes de clase B y C, que ofrecen campos de dos y de tres bits, respectivamente, para los identificadores de las estaciones. Actualmente las clases A y B están llenas. Sólo hay direcciones disponibles en la clase C.

La clase D se reserva para direcciones de multienvío. El multienvío permite que copias de un datagrama puedan enviarse a un grupo de estaciones en lugar de a una estación individual. Es similar a la difusión, pero la difusión requiere que el paquete llegue a todos los destinos posibles. El multienvío permite la transmisión a un subconjunto seleccionado. Las direcciones de clase E se han reservado para uso futuro. La Figura 7.5 muestra la estructura de cada una de las clases de direcciones IP.

	0	1	2	3	4	8	16	24	31	
Clase A	0	red				host				
Clase B	1	0	red				host			
Clase C	1	1	0	red				host		
Clase D	1	1	1	0	grupo de multicast (multidifusión)					
Clase E	1	1	1	1	(direcciones reservadas: no se pueden utilizar)					

Figura 7.5 Clases de direcciones IP

7.3.2 Nodos con más de una dirección. Como ya se ha indicado, una dirección Internet define la conexión del nodo a su red. Por tanto, cualquier dispositivo conectado a más de una red (por ejemplo, un encaminador) debe tener más de una dirección Internet. En realidad, un dispositivo tiene una dirección diferente para cada red a la que se encuentra conectado.

7.3.2.1 Ejemplo de interconexión entre tres redes. A continuación veremos un ejemplo de interconexión de 3 redes. Cada host (ordenador) tiene una dirección física que viene determinada por su adaptador de red.

Estas direcciones se corresponden con la capa de acceso al medio y se utilizan para comunicar dos ordenadores que pertenecen a la misma red. Para identificar globalmente un ordenador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP sabremos si pertenece a nuestra propia red o a una distinta (todas las direcciones IP de la misma red comienzan con los mismos números).

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
		A3-BB-05-17-29-D0	10.10.0.1
B	00-E0-4C-33-79-AF	10.10.0.7	
R2	B2-42-52-12-37-BE	10.10.0.2	Red 3
		00-E0-89-AB-12-92	
C	A3-BB-08-10-DA-DB	200.3.107.73	Red 3
D	B2-AB-31-07-12-93	200.3.107.200	

Tabla 7.1 Tabla de direccionamiento

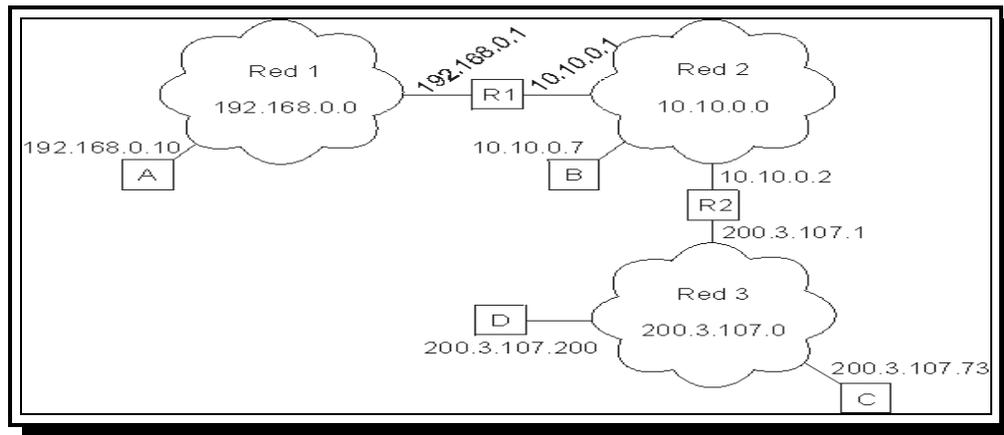


Figura 7.6 Ejemplo de interconexión de redes

7.4 SUBREDES

Una dirección IP tiene 32 bits. Una porción de la red indica la dirección de la red (identificador de red) y la otra porción indica la estación (o encaminador) en la red (identificador de estación). Esto significa que exista una jerarquía en el direccionamiento IP. Para alcanzar una estación en Internet, se debe primero alcanzar la red que utiliza la primera porción de la dirección. A continuación se debe alcanzar la estación utilizando la segunda porción de la dirección (identificador de estación). En otras palabras, las direcciones IP de las clases A, B y C están diseñadas con dos niveles de jerarquía.

Sin embargo, en muchos casos, estos dos niveles de jerarquía no son suficientes. Por ejemplo, considere una organización con una dirección de clase B. La organización tiene un direccionamiento jerárquico con dos niveles, pero no puede tener más de una dirección física, como se ve en la figura 7.7. Con este esquema, la organización se encuentra limitada a dos niveles de jerarquía. Las estaciones no pueden organizarse

en grupos, y todas ellas se encuentran situadas al mismo nivel. La organización tiene una red con muchas estaciones.

Una solución en este problema son las subredes, una división de una red en pequeñas redes denominadas: subredes. Por ejemplo, la figura 7.8 muestra la red de la figura 7.7 dividida en tres subredes.

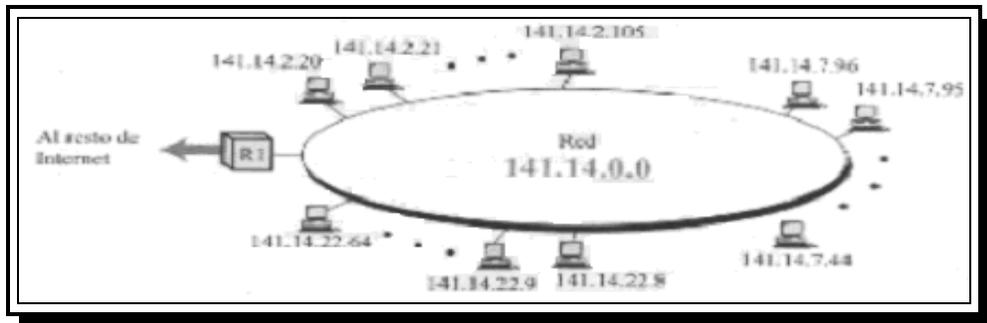


Figura 7.7 Una red con dos niveles de jerarquía sin subredes

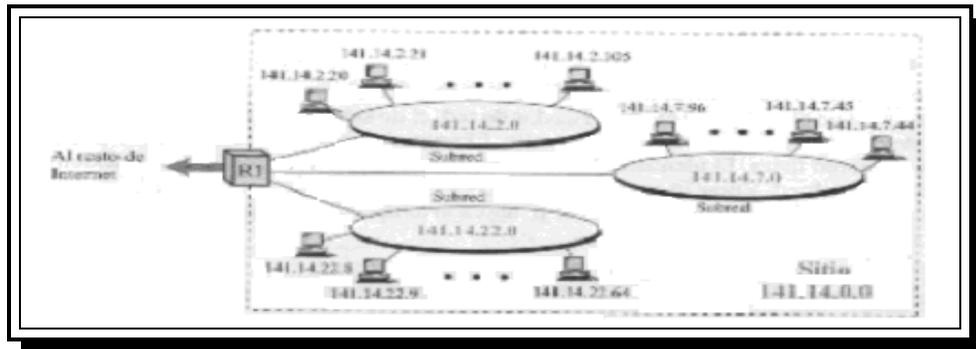


Figura 7.8 Una red con tres niveles de jerarquía (subredes)

7.4.1 Tres niveles de jerarquía. Añadir subredes crea un nivel intermedio de jerarquía en el sistema de direccionamiento IP. Ahora se tienen tres niveles: el identificador de red, el de subred y el de estación. El identificador de red es el primer nivel; define el

sitio. El segundo nivel es el identificador de subred; define la subred física. El identificador de estación es el tercer nivel; define la conexión de la estación a la subred.

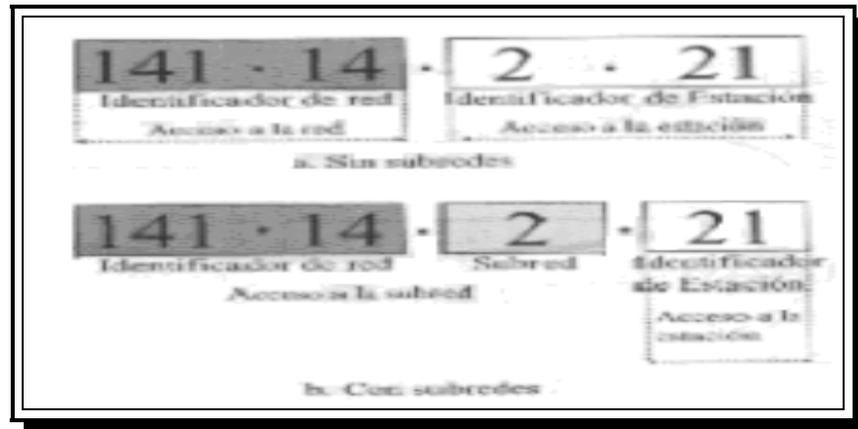


Figura 7.9 Dirección de una red con y sin subredes

El encaminamiento de un datagrama IP ahora involucra tres etapas: entrega al sitio, entrega a la subred y entrega a la estación.

7.4.2 Enmascaramiento. El enmascaramiento es el proceso que extrae la dirección de la red física de una dirección IP. El enmascaramiento puede realizarse con o sin subredes. Si no se tienen subredes, el enmascaramiento extrae la dirección de red a partir de una dirección IP. Si se tienen subredes, el enmascaramiento extrae la dirección de la subred a partir de la dirección IP. Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Tabla 7.2 Máscara de subred

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

148.120.33.110 10010100.01111000.00100001.01101110 (dirección de una máquina)

255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)

148.120.0.0 10010100.01111000.00000000.00000000 (dirección de su subred)

<-----RED-----> <-----HOST----->

Al hacer el producto binario de las dos primeras direcciones obtenemos la tercera. Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la

misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

148.120.33.89 10010100.01111000.00100001.01011001 (dirección de una máquina)

255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)

148.120.0.0 10010100.01111000.00000000.00000000 (dirección de su subred)

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

148.115.89.3 10010100.01110011.01011001.00000011 (dirección de una máquina)

255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)

148.115.0.0 10010100.01110011.00000000.00000000 (dirección de su subred)

7.4.3 Direcciones IP especiales y reservadas. No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
Red	todos 0	Red indicada	192.168.1.0
todos 1		Difusión a mi red	255.255.255.255
Red	todos 1	Difusión a la red indicada	192.168.1.255

127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1
-----	--------------------------------	---------------------------	-----------

Tabla 7.3 Direcciones IP reservadas

Difusión o broadcasting es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Tabla 7.4 Rango de direcciones IP reservadas

Por ejemplo, si estamos construyendo una red privada con un número de ordenadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer ordenador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas, tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros ordenadores podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en un ordenador de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

7.5 OTROS PROTOCOLOS EN EL NIVEL DE RED

TCP/IP dispone de otros protocolos en el nivel de red: ARP, RARP, ICMP y IGMP.

7.5.1 Protocolo de resolución de direcciones (ARP). El protocolo de resolución de direcciones (ARP, Address Resolution Protocol) asocia una dirección IP con una dirección física. En una red física típica, como una LAN, cada dispositivo conectado a un enlace se encuentra identificado mediante una dirección física normalmente impresa en la tarjeta de interfaz de red (NIC). Las direcciones físicas tienen jurisdicción local y pueden cambiarse fácilmente. Por ejemplo, si la NIC de una máquina falla, cambia la dirección física. La dirección IP, por su parte, tiene jurisdicción universal y no puede cambiar. ARP se utiliza para encontrar la dirección física del nodo a partir de su dirección Internet.

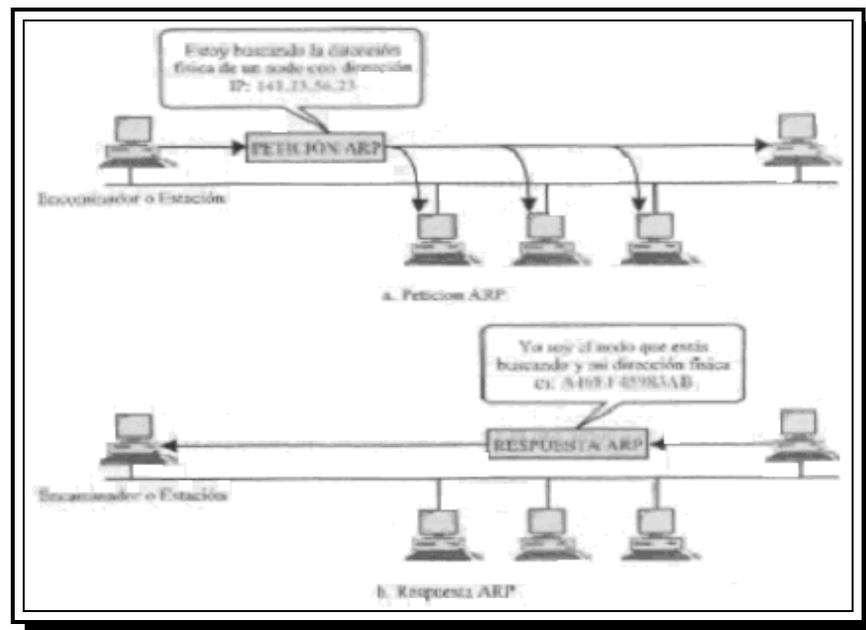


Fig. 7.10. A.R.P.

7.5.2 Protocolo de resolución inversa de direcciones (RARP). El protocolo de resolución inversa de direcciones (RARP, Reverse Address Resolution protocol) permite a una estación descubrir su dirección internet cuando sólo conoce su dirección física. RARP funciona de manera similar a ARP. La estación que desea recuperar su dirección interna difunde un paquete de petición RARP que contiene su dirección física a todas las estaciones de su red física. Un servidor en la red reconoce el paquete RARP y devuelve la dirección internet de la estación.

7.5.3 Protocolo de mensajes de control de internet (ICMP). El Protocolo de mensajes de control de internet (ICMP, Internet Control Message protocol) es un mecanismo utilizado por las estaciones y los encaminadores para enviar notificaciones sobre datagramas con problemas de vuelta al emisor. IP es esencialmente un protocolo sin conexión no fiable. ICMP, sin embargo, permite a IP informar al emisor si un datagrama no se ha entregado. Un datagrama viaja de encaminador a encaminador hasta que alcanza uno que puede entregarlo a su destino final. Si el encaminador es incapaz de encaminar o entregar el datagrama debido a condiciones inusuales (enlaces desactivados o dispositivos apagados) o debido a la congestión de la red, ICMP permite informar al emisor original. ICMP utiliza un esquema de prueba/respuesta de eco para probar si un destino es alcanzable y está respondiendo. También maneja los mensajes de error y de control, pero su única función es informar de problemas, no corregirlos. La responsabilidad de la corrección cae en el emisor.

7.5.4 Protocolo de mensajes de grupos de Internet (IGMP). El protocolo IP puede estar involucrado en dos tipos de comunicación: unidestino y multienvío. La comunicación unidestino se realiza entre un emisor y un receptor. Es una comunicación uno a uno. Sin embargo, en algunas ocasiones se necesita enviar el mismo mensaje a un gran número de receptores de forma simultánea. Este tipo de comunicación se denomina multienvío, que es una comunicación uno a muchos. El multienvío tiene muchas aplicaciones. El direccionamiento IP soporta el multienvío. Todas las direcciones IP de 32 bits que comienzan con 1110 (clase D) son direcciones de multienvío. Con 28 bits restantes para la dirección del grupo, se encuentran más de 250 millones de direcciones disponibles. Algunas de estas direcciones se encuentran permanentemente asignadas.

7.6 NIVEL DE TRANSPORTE

El nivel de transporte está representado en TCP/IP por dos protocolos: TCP y UDP. De estos, UDP es el más simple; ofrece una funcionalidad de transporte que no asegura secuencia, cuando la fiabilidad y la seguridad son menos importantes que el tamaño y la velocidad. La mayoría de las aplicaciones, sin embargo, requieren una entrega extremo a extremo fiable y hacen uso de TCP. El protocolo IP entrega un datagrama desde una estación origen a una estación destino, mediante un protocolo estación a estación. Los sistemas operativos actuales, sin embargo, soportan entornos multiusuario y de multiproceso. Se denomina proceso a un programa en ejecución. Una estación que recibe un datagrama puede estar ejecutando varios procesos con-

currentes, y cualquiera de ellos puede ser el posible destinatario de la transmisión. De hecho, aunque hemos estado hablando de estaciones que envían mensajes a otras estaciones de la red, es realmente un proceso origen el que envía un mensaje a un proceso destino.

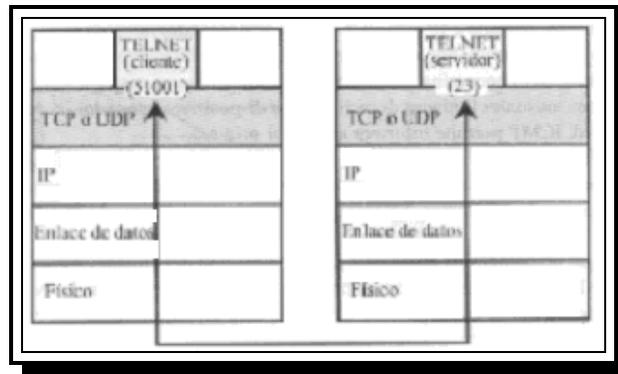


Figura 7.11 Direcciones de puertos

Los protocolos de transporte del conjunto de protocolos TCP/IP definen un conjunto de conexiones conceptuales para los procesos individuales denominados puertos del protocolo o sencillamente puertos. Un puerto es un punto de destino (normalmente un buffer) que almacena datos para ser utilizados por un proceso particular. La interfaz entre los procesos y sus puertos correspondientes es ofrecida por el sistema operativo de la estación. El protocolo IP es un protocolo estación a estación, lo que significa que puede entregar un paquete de un dispositivo físico a otro. Los protocolos de nivel de transporte de TCP/IP son protocolos puerto a puerto, que trabajan encima de los protocolos IP para entregar el paquete desde un puerto origen a los servicios IP en el comienzo de la transmisión y desde los servicios IP al puerto de destino en el final.

Cada puerto se define como una dirección, que es un entero positivo, que se transporta en la cabecera del paquete del nivel de transporte. Un datagrama IP utiliza la dirección Internet de 32 bits de la estación. Una trama en el nivel de transporte utiliza la dirección del puerto del proceso de 16 bits, suficiente para permitir hasta 65.536 (de 0 a 65.535) puertos.

7.6.1 Protocolo de datagramas de usuario (UDP). El protocolo de datagramas de usuario (UDP) es el más simple de los dos protocolos de transporte TCP/IP estándar. Es un protocolo de nivel de transporte extremo a extremo que añade sólo direcciones de puertos, control de errores mediante sumas de comprobación y la información de longitud de los datos del nivel superior. El paquete producido por el protocolo UDP se denomina datagrama de usuario (véase la Figura 24.15). A continuación se realiza una breve descripción de sus campos.

- ✓ **Dirección del puerto origen.** Es la dirección del programa de aplicación que ha creado el mensaje.
- ✓ **Dirección del puerto destino.** Es la dirección del programa de aplicación que recibirá el mensaje.
- ✓ **Longitud total.** Este campo define la longitud total del datagrama de usuario en bytes.
- ✓ **Suma de comprobación.** Esta suma de comprobación es un campo de 16 bits utilizado para la detección de errores.

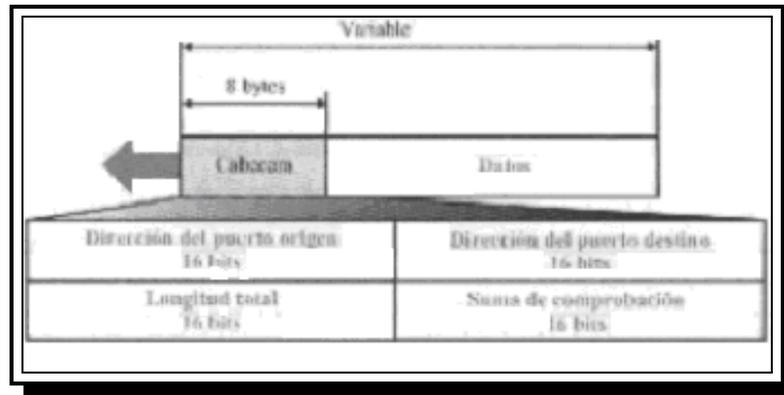


Figura 7.12 Formato de un datagrama UDP

UDP proporciona sólo las funciones básicas necesarias para la entrega extremo a extremo de una transmisión. No ofrece funciones de secuenciamiento ni de reordenación y no puede especificar el paquete dañado cuando se informa de un error (por lo que debe usarse con ICMP). UDP puede descubrir que ha ocurrido un error; ICMP puede, a continuación, informar al emisor de que un datagrama de usuario se ha dañado o se ha descartado. Tampoco tiene, sin embargo, la capacidad para especificar qué paquete se ha perdido. UDP contiene solo una suma de comprobación; no contiene un identificador o número de secuencia para un segmento de datos concreto.

7.6.2 Protocolo de control de transmisión (TCP). El Protocolo de control de transmisión (TCP) proporciona servicios completos de transporte a las aplicaciones. TCP es un protocolo de transporte puerto a puerto que ofrece un flujo fiable. El término y/K/o, en este contexto, significa orientado a conexión: se debe establecer una conexión entre ambos extremos de la transmisión antes de poder transmitir datos. Al crear esta conexión, TCP genera un circuito virtual entre el emisor y el receptor que se encuentra activo durante la duración de la transmisión. (Las conexiones durante la

duración de un intercambio entero son diferentes y son manejadas por funciones de sesión en las aplicaciones individuales.) TCP comienza cada transmisión informando al receptor de que hay datagramas en camino (el establecimiento de la conexión) y finaliza cada transmisión con una terminación de conexión. De esta forma, el receptor conoce la transmisión entera en lugar de un único paquete.

IP y UDP tratan los datagramas que pertenecen a una única transmisión como unidades independientes, no relacionadas entre sí. La llegada de cada datagrama al destino es, por tanto, un evento distinto e inesperado por el receptor. TCP, por otro lado, como un servicio orientado a conexión, es responsable de la entrega fiable del flujo entero de bits contenido en el mensaje inicialmente generado por la aplicación emisora. La fiabilidad se asegura mediante la detección de errores y la retransmisión de las tramas con errores; todos los segmentos deben ser recibidos y confirmados antes de que la transmisión se considere completa y se descarte el circuito virtual.

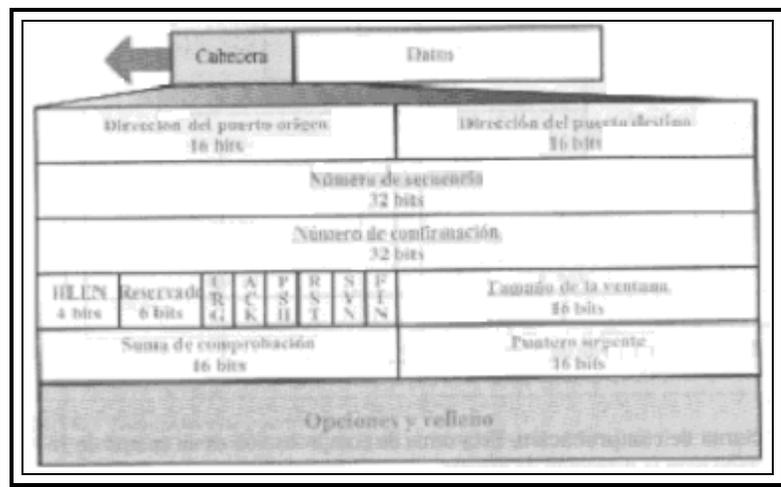


Figura 7.13 Formato del segmento TCP

En el extremo emisor de cada transmisión, TCP divide las transmisiones largas en unidades de datos más pequeñas y empaqueta cada una de ellas en una trama denominada segmento. Cada segmento incluye un número de secuencia para la posterior reordenación de los segmentos en el receptor, junto con un número identificador de confirmación y un campo que indica el tamaño de la ventana deslizante utilizada en las confirmaciones. Los segmentos se transportan por la red dentro de datagramas IP. En el extremo receptor, TCP captura cada datagrama y reordena la transmisión de acuerdo a los números de secuencia.

7.6.2.1 El segmento de TCP. El ámbito de los servicios ofrecidos por TCP requiere que la cabecera del segmento sea amplia (véase la Figura 24.16). Una comparación del formato del segmento de TCP con el formato de un datagrama de usuario UDP muestra las diferencias entre los dos protocolos. TCP ofrece un rango comprensible de funciones de fiabilidad pero sacrifica la velocidad (deben establecerse conexiones, hay que esperar confirmaciones, etc.). Debido a que UDP utiliza un tamaño de trama más pequeño, éste es mucho más rápido que TCP, pero es menos fiable. A continuación se realiza una breve descripción de los campos del segmento.

- ✓ **Dirección del puerto origen.** Esta dirección define el programa de aplicación de la computadora origen.
- ✓ **Dirección del puerto destino.** Este campo define el programa de aplicación de la computadora destino.

- ✓ **Número de secuencia.** Un flujo de datos del programa de aplicación se puede dividir en dos o más segmentos TCP. El campo con el número de secuencia muestra la posición de los datos en el flujo de datos original.
- ✓ **Número de confirmación.** El número de confirmación de 32 bits se utiliza para confirmar la recepción de datos desde el otro dispositivo que participa en la comunicación. Este número es válido sólo si el bit ACK del campo de control (explicado más adelante) está activo. En este caso, define el número de secuencia del byte que se espera a continuación.
- ✓ **Longitud de la cabecera (LC).** Este campo de cuatro bits indica el número de palabras de 32 bits (cuatro bytes) de la cabecera TCP. Los cuatro bits pueden definir hasta 15. Este valor se multiplica por 4 para obtener el número total de bytes de la cabecera. Por tanto, el tamaño de la cabecera puede ser de hasta una máximo de 60 bytes (4 x 15). Puesto que el tamaño mínimo de la cabecera es de 20 bytes, se dispone de 40 bytes disponibles para la sección de opciones.
- ✓ **Reservado.** Este campo de seis bits se reserva para uso futuro.
- ✓ **Control.** Cada bit del campo de control de seis bits funciona de forma individual e independiente. Un bit puede definir el uso de un segmento o servir como una comprobación de la validez de otros campos. El bit urgente, cuando se activa, valida el campo de puntero urgente. Este bit y el puntero indican que los datos del segmento son urgentes. El bit ACK, cuando se activa, valida el campo con el número de confirmación. Ambos se utilizan juntos y tienen funciones diferentes, dependiendo del tipo de segmento. El bit PSH se utiliza para informar al emisor de que se necesita un mayor ancho de banda. Si es posible, los datos deben colocarse

en caminos con mayores anchos de banda. El bit RST se utiliza para reiniciar la conexión cuando hay confusión en los números de secuencia. El bit SYN se utiliza para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con el bit ACK activo) y la recepción de confirmación (con el bit ACK activo). El bit FIN se utiliza en la terminación de la conexión en tres tipos de segmentos: petición de terminación, confirmación de terminación (con el bit ACK activo) y confirmación de la confirmación de terminación (con el bit ACK activo).

- ✓ **Tamaño de la ventana.** Este campo de 16 bits define el tamaño de la ventana deslizante.
- ✓ **Suma de comprobación.** Este campo de 16 bits se utiliza para la detección de errores.
- ✓ **Puntero urgente.** Este es el último campo requerido en la cabecera. Su valor es válido sólo si el bit URG del campo de control se encuentra activado. En este caso, el emisor está informando al receptor de que hay datos urgentes en la porción de datos del segmento. Este puntero define el final de los datos urgentes y el comienzo de los datos normales.
- ✓ **Opciones y relleno.** El resto de la cabecera TCP define los campos opcionales. Se utilizan para enviar información adicional al receptor o para alineamiento.

8 PROCESO DE TRABAJO

El proceso de trabajo a seguir para realizar el cableado y conexión de la red local de la Universidad pasará por los siguientes puntos:

- ✓ Diseño y planificación de la red
- ✓ Implementación
- ✓ Montaje de la red
- ✓ Configuración
- ✓ Mantenimiento del cableado

8.1 DISEÑO Y PLANIFICACIÓN DE LA RED

Para el diseño de ésta red se siguieron los siguientes pasos:

- a. Segmentar la universidad: por bloques y pisos, Ej. bloque 1 piso2
- b. Hacer el levantamiento de la red actual
- c. Crear modelo de red de área local para cada dependencia: se diseña cada red (segmento), ignorando por ahora las interconexiones de redes.
- d. Interconectar las redes que operan en la CUC: después que cada segmento se haya diseñado y aprobado.

8.1.1 Segmentar la Universidad. Para que éste diseño sea óptimo y más fácil de manejar, inicialmente segmentaremos la Universidad por bloques y pisos, donde a cada división se le asignará un nombre de acuerdo a la dependencia que allí se encuentre:

Bloque1 Piso1 → Oficinas de Admisiones y Registros y Contabilidad

Bloque1 Piso2 → Departamentos Administrativos y Facultad de Ingenierías

Bloque1 Piso3 → Área de Laboratorios y Sala de Profesores Tiempo Completo

Bloque1 Piso4 → Bienestar Universitario

Bloque2 Piso1 → Procesos Técnicos y Salas de Audiovisuales

Bloque2 Piso3 → Sala de UPS

Bloque2 Piso4 → Facultad de Administración de Empresas

Bloque3 Piso1 → Laboratorios de Ingeniería y Cafetería

Bloque3 Piso2 → Facultad de Derecho

Bloque3 Piso3 → Facultad de Contaduría y Psicología

Bloque32 años Piso2 → Facultad de Arquitectura

Bloque5 Piso2 → Dirección de Análisis y Dirección de Tecnología de Telecomunicaciones

8.1.2 Levantamiento de la red actual. El levantamiento de la red consiste en analizar la situación del cableado en cada dependencia y conocer exactamente las conexiones de cada uno de los hubs y la red o redes que son manejadas por cada equipo, además el levantamiento de la red permite saber exactamente las deficiencias presentes en la red, y los equipos que son aprovechables para el nuevo diseño. La red actual cuenta con el medio de transmisión cable UTP ct5, y en muchas ocasiones el cableado dispuesto, no cumple con ningún estándar.

Como se muestra en la figura 8.1, la Universidad tiene 2 redes separadas, como son la red de Admisiones y Contabilidad, cada una de estas redes funciona de forma independiente, con su respectivo servidor, impidiendo así la comunicación lógica entre todas las dependencias que conforman la Universidad. Por otro parte la Universidad también cuenta con la red de Internet, que se recibe con par de cobre, y luego se distribuye a todas las salas que lo requieren, pero en general se observó que la mayoría de los PCs requieren éste servicio de red.

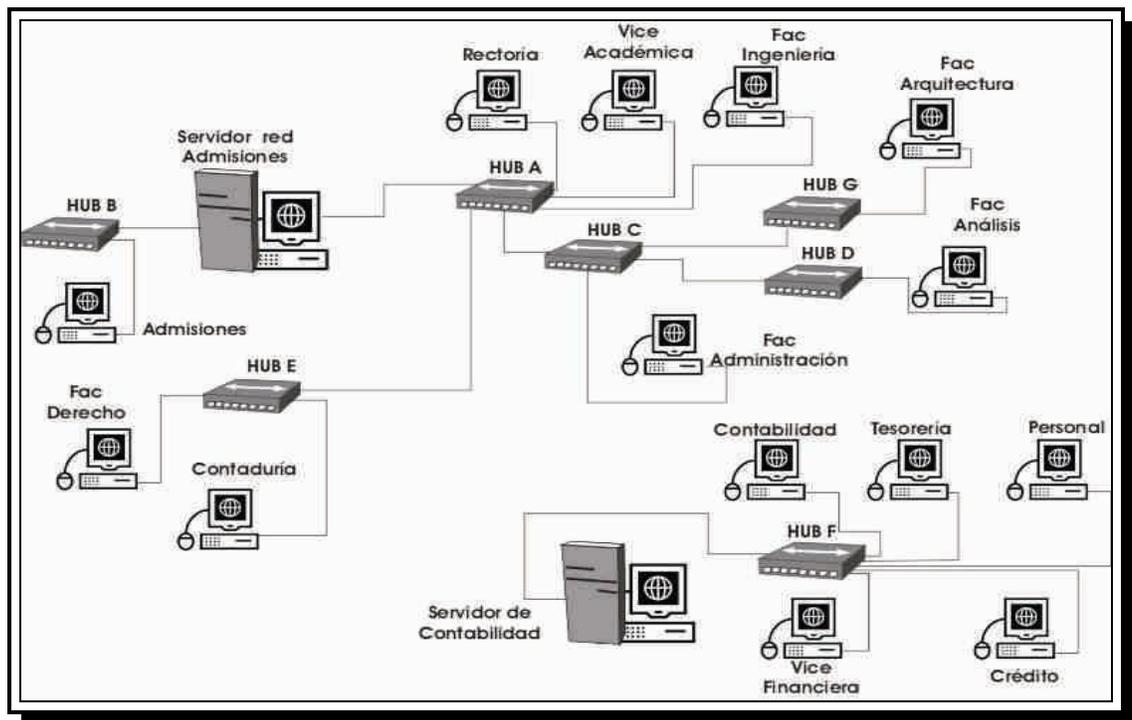


Figura 8.1 Estructura lógica de las actuales redes CUC

Este proceso de levantamiento de la red se realizó acudiendo directamente a cada dependencia, para revisar el cableado, y además encuestando al personal adscrito en

cada oficina, para conocer en que estaba fallando la red actual y que servicios de red se requerían.

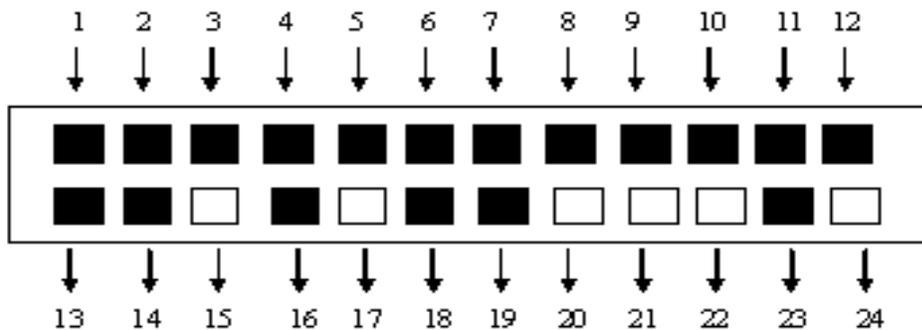
8.1.2.1 Bloque1 Piso1. En el bloque 1, piso 1 están las oficinas de admisiones donde se encuentran dos hubs (A y B) y el servidor que maneja dicha red; los datos tomados fueron los siguientes:

- ✓ No hay racks para los hubs.
- ✓ No hay patch-panels y no hay organizador de cables
- ✓ La red en general es muy lenta
- ✓ El software actual que maneja le red es obsoleto
- ✓ El cableado está degradado y no cumple con estándares
- ✓ Se requiere los servicios de la red de Internet

Descripción específica de los hubs:

Hub A

Red: Admisiones y Registros



■ → TIENEN CONECTORES

16: ESTA CONECTADO AL SERVIDOR

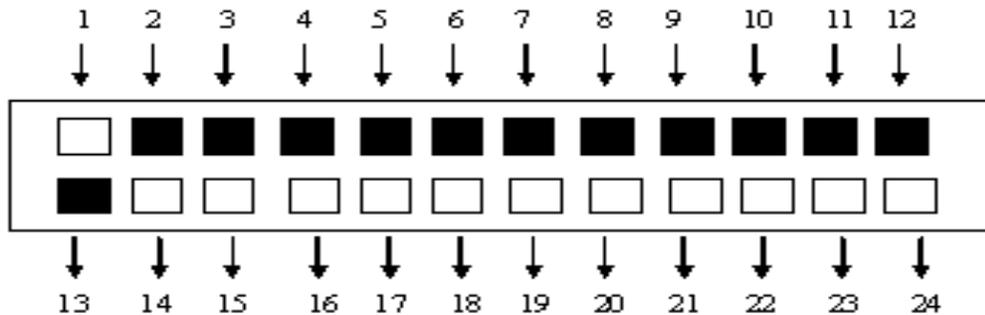


□ → NO ESTA CONECTADO

TERMINAL	DEPENDENCIA	EQUIPO	ESTÁNDAR
1	Ingeniería	Ing.02	No cumple
2	Ingeniería	Ing.01	No cumple
4	Ingeniería	No hay	No cumple
5	Ingeniería	No hay	No cumple
6	Rectoría	No hay	No cumple
7	Ingeniería	No hay	No cumple
8	Ingeniería	No hay	No cumple
11	Rectoría Ejecutiva	01	No cumple
12	Rectoría Ejecutiva	02	No cumple
18	Derecho	Hub E	No cumple
19	Vic. Académica	01	No cumple

Hub B

Red: Admisiones y Registros



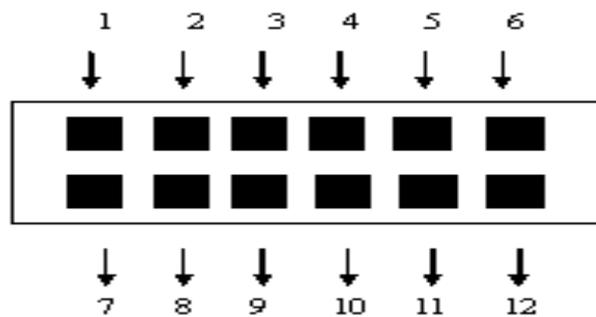
TERMINAL	DEPENDENCIA	EQUIPO	ESTÁNDAR
2	Admisiones	1	No cumple
3	Admisiones	2	T568A
4	Admisiones	3	T568A
5	Admisiones	4	T568A
6	Admisiones	5	T568A
7	Admisiones	6	No cumple
8	Admisiones	7	No cumple
9	Admisiones	8	T568A
10	Admisiones	9	T568A
11	Admisiones	10	T568A

12	Admisiones	11	T568A
13	Admisiones	12	No cumple

También se ubica la dependencia de contabilidad donde se encuentra el hub F con su respectivo servidor, allí se notó que la red es muy lenta y además se necesita la red de Admisiones e Internet.

Hub F

Red: Contabilidad



■ → 10: conectado al servidor

DEPENDENCIA	EQUIPOS	TERMINAL	ESTÁNDAR
Contabilidad	01	6	T568A
	02	4	No cumple
	03	1	T568A
Tesorería	01	11	T568
	02	12	T568
	03	5	T568
Personal	01	8	T568
Vic. Financiera	01	7	T568
Crédito	01	2	T568

8.1.2.2 Bloque1 Piso2. En esta división se encuentra la Facultad de Ingenierías, donde se recibe la red de admisiones, que llega a los equipos de la oficina del decano y a las secretarias que están en la recepción, pero las demás oficinas también requieren los servicios de red

8.1.2.3 Bloque2 Piso4. En esta división se encuentra la Facultad de Administración de Empresas, donde se tomaron los siguientes datos:

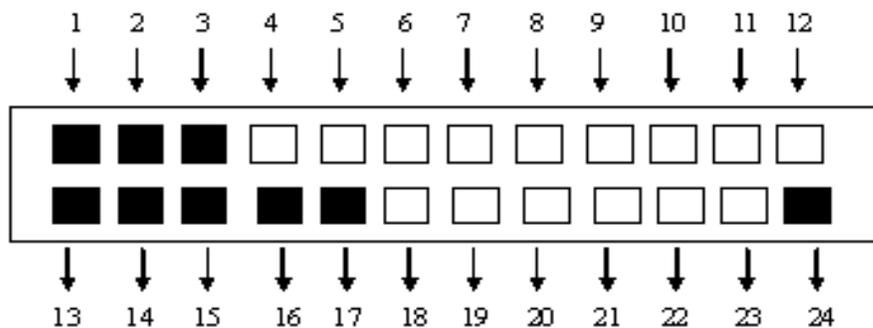
- ✓ Se necesita un equipo en la recepción de dicha facultad, y dos equipos en la sala de profesores.
- ✓ En la oficina de decanatura, que se encuentra en esta división se necesitan 2 equipos y se requiere el servicio de Internet.
- ✓ En la secretaría; la red de admisiones presenta muchos problemas, y el equipo actual es obsoleto.

8.1.2.4 Bloque3 Piso2. En esta división se encuentra la Facultad de Derecho, aquí está ubicado el hub D que recibe la red de admisiones. El hub de esta dependencia no tiene patch-panel y en general la red es lenta, y el cableado no cumple estándares.

Características específicas del hub:

Hub E

Red: Admisiones y Registros



TERMINAL	DEPENDENCIA	EQUIPO	STANDAR
1	Admisiones (Hub A)		No cumple
2	Derecho	Der.02	No cumple
3	Derecho	No hay equipo	No cumple
13	Contaduría	Cont.01	No cumple
14	Contaduría	Cont.05	T568A
15	Contaduría	Cont.02	No cumple
16	Contaduría	Cont.03	No cumple
17	Contaduría	Cont.04	T568A
24	Derecho	Der.01	No cumple

8.1.2.5 Bloque3 Piso3. Aquí encontramos la Facultad de Contaduría, donde se observó lo siguiente:

- ✓ Se necesita la red de Internet.
- ✓ La red de admisiones, presenta deficiencias.

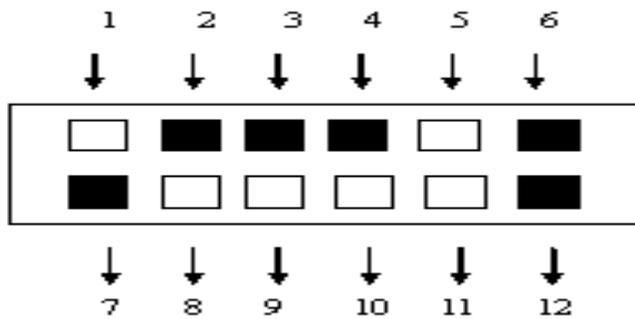
8.1.2.6 Bloque5 Piso2. En el bloque 5, piso 2 se encuentra la oficina de Dirección de Análisis, donde se tomaron las siguientes observaciones:

- ✓ La oficina cuenta con el servicio de la red de admisiones.
- ✓ Se necesita un equipo para la sala de admisiones y dos equipos para la sala de profesores.

Características específicas del hub

Hub D

Red: Admisiones y registros



TERMINAL	DEPENDENCIA	EQUIPO	ESTÁNDAR
2	Análisis Sala Prof.	No hay	No cumple
3	Análisis Sala Prof.	No hay	No cumple
4	Análisis Sala Prof.	No hay	No cumple
7	Análisis	Ana.01	No cumple
12	Arquitectura (Hub C)		No cumple

También se encuentra la oficina de Dirección de Tecnología de Telecomunicaciones, donde se tomaron los siguientes datos:

- ✓ Se necesita la red de Admisiones,
- ✓ Se requiere un equipo, para reemplazar el actual.

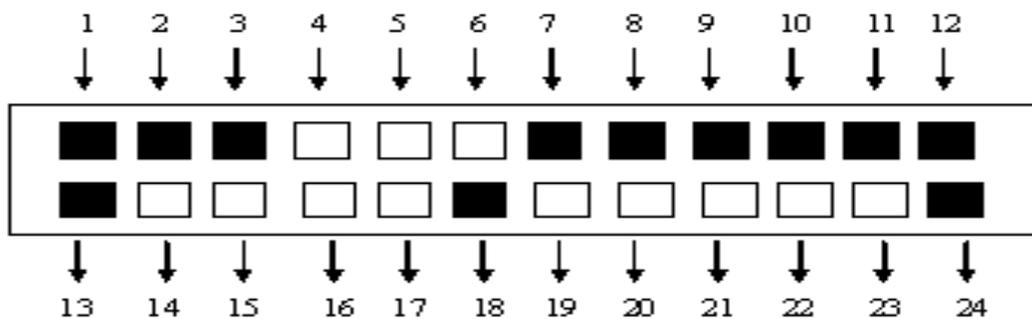
8.1.2.7 Bloque 32 años, Piso 2. En este bloque, está ubicada la facultad de Arquitectura, donde se tomaron los siguientes datos:

- ✓ En la oficina del Decano y la oficina Fundadores no hay servicio de red y se necesita.

Características específicas del hub

Hub C

Red: Admisiones y Registros



TERMINAL	DEPENDENCIA	EQUIPO	ESTÁNDAR
1	Arquitectura	Hub C	T568A
7	Administración	Adm.01	T568A
8	Administración	No hay	No cumple
9	Administración	No hay	No cumple
11	Administración	Adm.02	No cumple
12	Administración	No hay	No cumple
18	Análisis (Hub D)	Hub D	No cumple
24	Admisiones (Hub A)		No cumple

8.1.3 Modelo de red de área local para cada dependencia. Una vez se ha segmentado la universidad y hecho el pertinente levantamiento de la red, se procede a elaborar un modelo de red para cada división ignorando por ahora las interconexiones de redes.

En el diseño para cada dependencia se utilizan switches, porque como se sabe, el switch es un dispositivo diseñado para resolver problemas de rendimiento en la red, debidos a anchos de banda pequeños y embotellamientos, también implica un cambio en el cableado horizontal por cable UTP cat 5e, asegurando que cumpla con los debidos estándares de certificación.

El mecanismo de conexión se muestra en la figura 8.2. Donde 1 es le switch designado previamente, A es el patch-cord que se encarga de conectar un puerto del switch con B

que es el patch-panel, de B sale un cable 2, que es conducido dentro de las canaletas hasta C, que es un toma de red, de donde se conecta otro patch-cord D que finalmente se conecta al punto 3 que es el PC; y así se realiza con cada computador, creando una configuración de línea punto a punto.

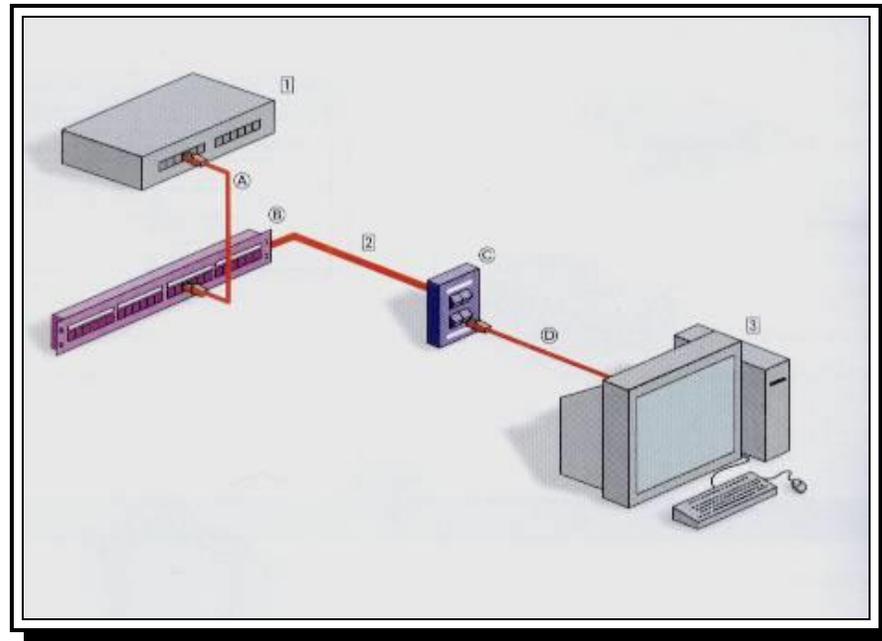


Figura 8.2 Mecanismo de conexión

Cada switch será ubicado en un gabinete con su respectivo rack, un patch-panel y un organizador de cables, para mejor entendimiento, mantenimiento y protección de la red. En todos los centros de cableado se tendrá especial cuidado en la señalización de cada uno de los latiguillos que se conecten a los switch, es decir, se especificará exactamente a qué puerto del patch-panel se conecta un punto de red en específico y con que otro elemento activo se conectará para fines de distribución.

Se revisará cada equipo con el fin de verificar si se encuentra instalada y configurada la tarjeta de red y si esta contiene Fast Ethernet, además a cada PC, se le debe configurar una identificación única y su respectiva dirección IP, para que así no presente, problemas en la configuración general al momento de interconectar las LANs.

Cada switch tiene un nombre de identificación, y se ha especificado según la segmentación descrita. La ubicación de estos en cada bloque y piso se muestra en cada uno de los planos adjuntos, donde además se indican los equipos a los cuales se distribuye la red.

Bloque1 Piso1 → Switch A (Sw A), de 24 puertos, para Admisiones y Registros

→ Switch B (Sw B), de 24 puertos, para el Dpto de Contabilidad

Bloque1 Piso2 → Switch C (Sw C), de 24 puertos, para las Oficinas Administrativas

→ Switch D (Sw D), de 24 puertos, para la Facultad de Ingenierías

Bloque1 Piso3 → Switch E (Sw E), de 24 puertos

Bloque1 Piso4 → Switch F (Sw F), de 24 puertos

Bloque2 Piso1 → Switch G (Sw G), de 24 puertos

Bloque2 Piso3 → No se ubicará switch, pues la red se tomará del switch H

Bloque2 Piso4 → Switch H (Sw H), de 24 puertos

Bloque3 Piso1 → No se ubicará switch, pues la red se tomará del switch I

Bloque3 Piso2 → Switch I (Sw I), de 24 puertos

Bloque3 Piso3 → No se ubicará switch, pues la red se tomará del switch I

Bloque32 años Piso2 → Switch J (Sw J), de 12 puertos

Bloque5 Piso2 → Switch K (Sw K), de 24 puertos

La figura 8.3 muestra como se deben realizar las conexiones entre los switch, para que se interconecten entre sí, por medio del cableado vertical o backbone, partiendo de un switch maestro que se especifica al momento de integrar las LANs

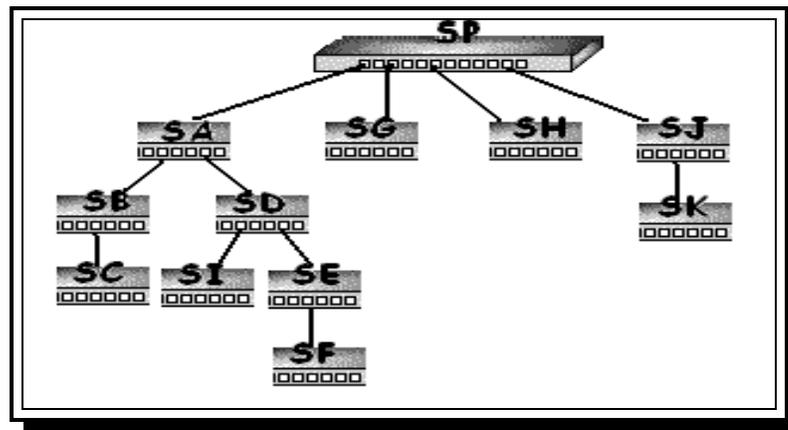


Figura 8.3 Interconexión entre switches

8.1.4 Interconectar las redes que operan en la CUC. Una vez se diseñan los modelos de red para cada dependencia y se interconectan entre sí mediante el cable de backbone, se procede a crear una estructura física y lógica, que permita integrar las

redes que operan en la Universidad, para que así puedan ser transmitidas y se cumpla los objetivos propuestos.

8.1.4.1 Descripción del diseño: El objetivo de éste diseño es crear un sistema de cableado estructurado, que permita interconectar tres redes independientes en una sola LAN, con todos los soportes de seguridad pertinentes. La figura 8.4 muestra el diseño general de esta red y como puede notarse el proceso es el siguiente:

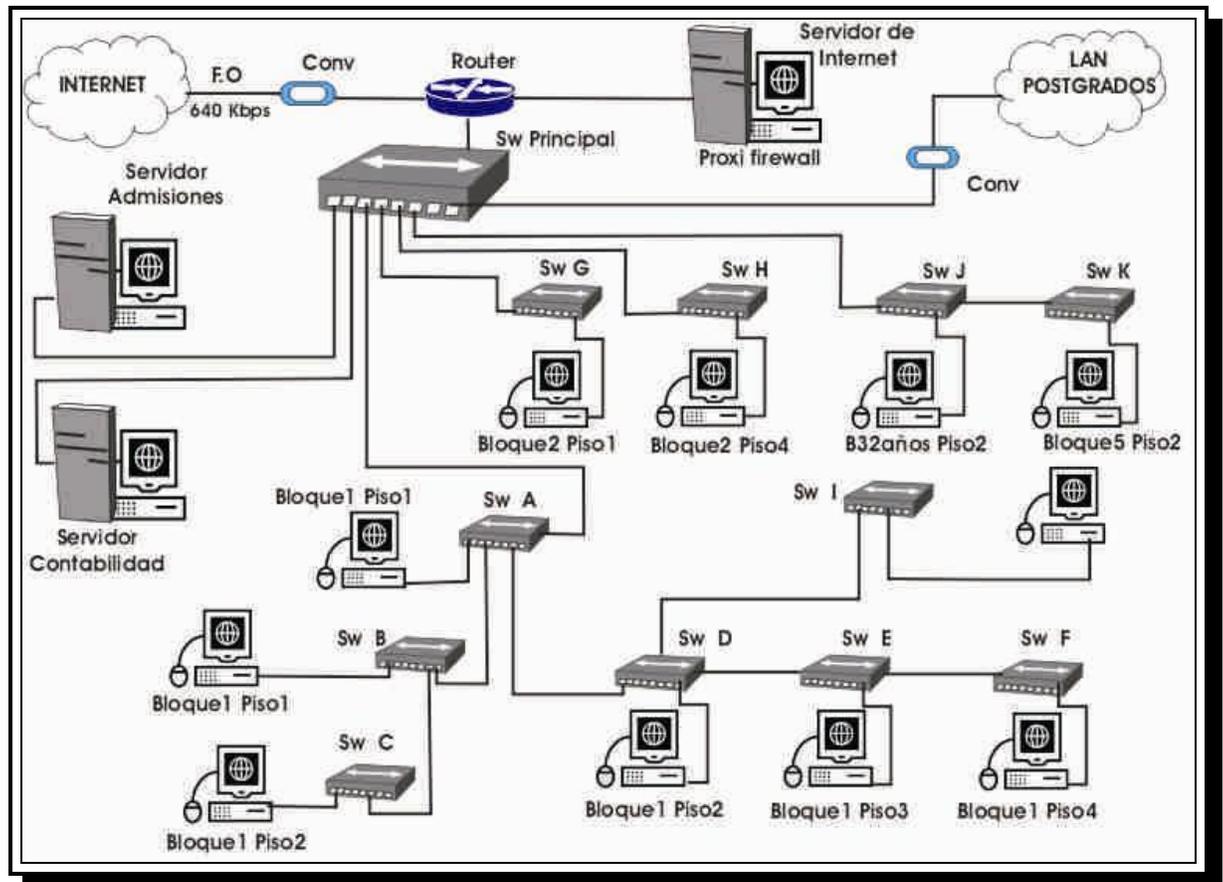


Figura. 8.4. Estructura lógica de la LAN CUC

La Internet es recibida por medio de fibra óptica a 640 Kbps, esta fibra óptica se debe conectar a un convertidor, que transforma las señales de luz en impulsos eléctricos; el

convertidor tiene una entrada para la fibra óptica y una salida para un conector RJ45 hembra, es por esta salida que se conecta la línea de Internet a un router, este router va a permitir que con una sola cuenta de acceso a Internet, puedan conectarse todos los puestos de la LAN a "la red de redes". Para los ordenadores locales será totalmente transparente la conexión con Internet, ya que en el momento que necesiten cualquier servicio de ésta, será el router el encargado de interconectar nuestra LAN con el resto del mundo, este router es quien se encarga de enrutar la Internet hasta un PC, que será el servidor de Internet, puesto que es allí donde se configuran los servicios de la red de Internet; este servidor de Internet cuenta además con un servidor Proxy Firewall que son instalados en la misma computadora. Los servidores Proxy son computadoras que aceleran su navegación almacenando copias locales de los sitios Web que se visitan frecuentemente. Esto significa que después que se accede a un sitio por primera vez, no tendrá que esperar otra vez que la página se cargue. En lugar de esto, los sitios Web que ya se han visitado se cargan rápidamente desde el Proxy local. El servidor Proxy también actualiza las páginas cada vez que se vuelve a visitar un sitio, asegurando que se verá la última versión.

En tanto que el Firewall es un sistema de defensa basado en el hecho de que todo el tráfico de entrada o salida a la red debe pasar obligatoriamente por un sistema de seguridad capaz de autorizar, denegar, y tomar nota de aquello que ocurre en la red. Comúnmente los Firewall apagan el ruteo de paquetes en el host, previniendo el acceso a través de la capa de direcciones IP. Esto quiere decir que ataques basados en direcciones IP no pueden penetrar esta red de área local.

Del router se hace una conexión con un switch maestro, a este switch, se le conectan los servidores de la redes de Admisiones y Contabilidad, es este switch principal, el que va a permitir que cada computador, tenga una conexión con todo el servicio de la red a través de los diferentes switches esclavos que son dispuestos en cada dependencia. El switch maestro es un dispositivo administrable, el cual actúa como un conmutador que utiliza las direcciones de destino del nivel de red para encontrar el enlace de salida por el cual debería comunicarse un paquete de información. Este switch, puede programarse para así habilitar o deshabilitar el acceso de un determinado host, a un servicio de red en específico; lo que quiere decir que si algún computador necesita las redes de Admisiones y Contabilidad, como es el caso, se debe programar el switch, para que habilite este servicio; pero en las salas de Internet para estudiantes y otras oficinas, donde no es conveniente que los alumnos ingresen a las otras redes, se bloqueará las vías de acceso a éstas.

8.1.4.2 Ventajas del diseño:

- ✓ Se crea una conexión unificada, donde todos los computadores están unidos físicamente, mas no lógicamente, así que en el momento de realizar algún tipo cambio en su conexión lógica, solo se necesita reconfigurar el switch principal. Además se pueden soportar futuras aplicaciones, pues es un sistema de cableado estructurado.
- ✓ Se pueden configurar diversas VLAN's, así por ejemplo, en la sala de profesores, se puede crear una conexión virtual, entre ésta área y la red de admisiones, para que

los docentes, puedan ingresar las notas de los estudiantes, desde su respectivo computador, claro que este sería un acceso tan solo para compartir archivos, sin que ellos puedan ingresar a la base de datos del sistema.

8.1.4.3 Recomendaciones:

Para que el funcionamiento de esta LAN, sea óptimo se anexan las siguientes recomendaciones:

- ✓ Se deben cambiar algunos PC's que se encuentran obsoletos, o en su defecto actualización de los presentes.
- ✓ El software de la red de Admisiones se debe cambiar por uno más robusto, para que soporte mejor la cantidad de información que se presenta en esa dependencia.
- ✓ Se debe adquirir un sistema llamado RAS, este es un software que permite crear una cuenta de acceso externa para todo el personal que labora y estudia en la CUC, con el fin de que cada estudiante o docente pueda ingresar desde cualquier computador a la red interna de la Universidad, con sus respectivas limitaciones de acceso, para preservar siempre la seguridad de la red; de esta manera los alumnos, por ejemplo pueden retirar sus notas y su respectivo recibo de consignación que le corresponda sin tener que dirigirse a las instalaciones de la Universidad. Este servicio se adquiere con los operadores locales, tales como EDT o METROTEL.
- ✓ La red podría llevarse hasta la sede de postgrados por medio de WLAN, es decir LANs inalámbricas, así se evita la instalación de cableado, pero para ello se debe realizar un estudio un poco más detallado, ya que las instalaciones de WLAN, requieren someter a los equipos actuales a algunos cambios.

- ✓ Para los servicios de Firewall es preferible instalarlo en otro computador, que actúe como servidor Firewall, ya que no es muy recomendable tener al mismo equipo realizando tareas tan complicadas, o bien disponer de un equipo lo suficientemente eficiente, para ello.

8.1.4.4 Especificaciones generales de diseño.

8.1.4.4.1 Cuarto de Telecomunicaciones: El área donde funcionará el cuarto de telecomunicaciones es la ubicada en la sala de UPS que está ubicada en el bloque2 piso3, debido a que se considera que ese sitio es estratégico en cuanto a la seguridad que brinda a los equipos de comunicación de la red; además, en esa dependencia labora personal capacitado para solventar algún tipo de problema que pueda presentarse con éstos.

8.1.4.4.2 Topología de la red. Se consideró conveniente adoptar como topología de red la tipo estrella extendida o árbol, debido a las numerosas ventajas que esta puede proporcionar al diseño, siendo la principal de ellas el permitir centralizar la administración de la red de modo que si se requiere desconectar un terminal de la misma no es necesario suspender el funcionamiento de la red. Además, en este tipo de topologías la tasa de transferencia de datos es muy alta y el fallo en una de las estaciones de la red no afecta o perjudica al resto de las estaciones que la conforman.

8.1.4.4.3 Protocolo de bajo nivel. El estándar que se utilizará en el diseño de la red será Fast Ethernet según la norma IEEE 802.3. Esta tecnología presenta como

ventajas principales el bajo costo de su implementación y la capacidad de proteger las estaciones conectadas a la red del riesgo que implica la posibilidad de que un usuario desconecte intencionalmente o no, una estación o cable. Adicionalmente este estándar define el uso del cable UTP categoría 5e, el cual permite velocidades de hasta 200 Mbps, lo cual se adapta a los requerimientos de velocidad de la red; por otro lado el método de acceso al medio que especifica la norma es el CSMA/CD (acceso múltiple por detección de portadora con detección de colisiones). Este método consiste en comprobar si la línea esta libre antes de comenzar la transmisión, verificando si se ha producido una colisión durante la transmisión, de haberse producido una colisión se detiene la transmisión y se vuelve a transmitir el bloque de datos después de un tiempo de espera aleatorio.

8.1.4.4.4 Sistemas Operativos. El Sistema operativo de red que se utilizará para los servidores es Windows NT. Para el caso de los servidores de red se utilizará el Windows NT Server, ya que soporta el protocolo TCP/IP (el cuál se requiere para poder establecer conexiones a Internet) y proporciona una interfaz amigable al Administrador de la red. Para las estaciones de trabajos se empleará el sistema operativo Windows 98, debido a que, además de presentar una interfaz de fácil manejo a los usuarios, proporciona a éstos el soporte para ejecutar el conjunto de aplicaciones que cumplen con los requerimientos de información y trabajos que se manejan en las dependencias adscritas a las áreas de estudio.

Por otra parte, es importante destacar que el sistema operativo Windows NT puede manejar un máximo de 250 estaciones, lo cual no genera inconvenientes dado que el número de estaciones a conectar en la red es considerablemente inferior a esa cantidad. De acuerdo a lo especificado anteriormente, se puede apreciar que Windows NT posee las características apropiadas para cumplir con los requerimientos de la red propuesta.

8.1.4.4.5 Protocolos de comunicación. El protocolo de comunicación a utilizar en la red para permitir la conexión a Internet, la conexión de múltiples redes y además el manejo de los errores en la transmisión de los datos, es el TCP/IP, ya que administra el enrutamiento y el envío de datos, y controla la transmisión por medio del uso de señales de estado predeterminados. Dicho protocolo es comúnmente utilizado por todos los computadores conectados a Internet, de manera que éstos puedan comunicarse entre sí.

Aunque también se utilizará el protocolo NetBEUI como soporte pues es una buena elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el enrutamiento de mensajes hacia otras redes. En realidad bastaría también sólo TCP/IP para todas las exigencias, pero es mejor tener siempre también el NetBEUI que es un protocolo fácil de manejar y no entorpece el sistema.

8.1.4.4.6 Elección de los elementos pasivos.

- a. **Cable.** El cable elegido para el proyecto es cable UTP multifilar categoría 5e, que es el cable que se va a introducir en las canaletas, y para los patch-cord se usará, también el cable UTP cat5e, pero más flexible, pues los hilos flexibles soportan mejor el movimiento que los rígidos.

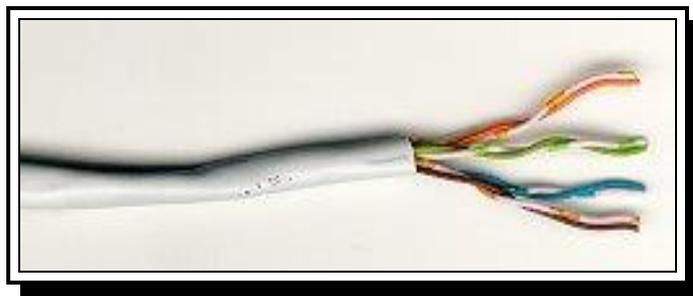


Figura 8.5. Cable UTP cat5e.

El estándar utilizado para todas las conexiones de cableado es el T568A, con el fin de estandarizar el cableado.

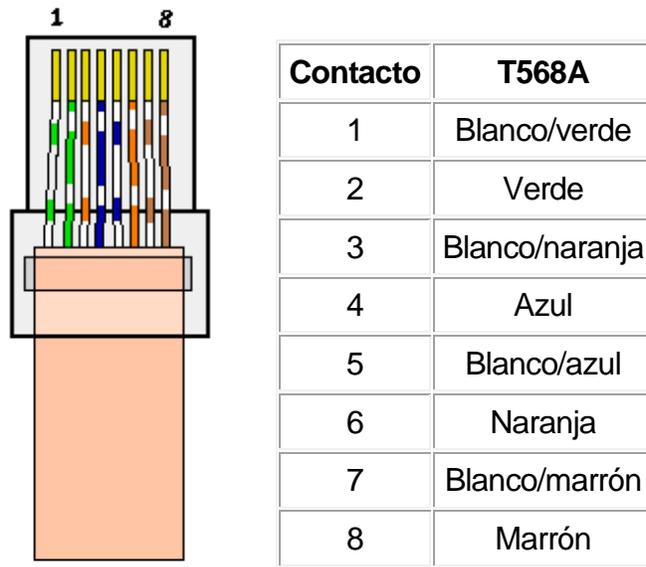


Figura 8.6. Estándar T568A

b. **Sistema de cableado.** El sistema de cableado estructurado en este proyecto presenta muchas ventajas, puesto que la configuración de nuevos puestos se realiza hacia el exterior desde un nodo central, sin necesidad de variar el resto de los puestos, pues sólo se configuran las conexiones del enlace particular. La localización y corrección de daños se simplifica ya que los problemas se pueden detectar a nivel centralizado. Tanto el cableado vertical, que es el va dentro de las canaletas, como el cableado vertical que hace las conexiones entre edificios y de un switch a otro, es el cable UTP cat5e, o bien podría instalarse el UTP cat6, para el cableado vertical.

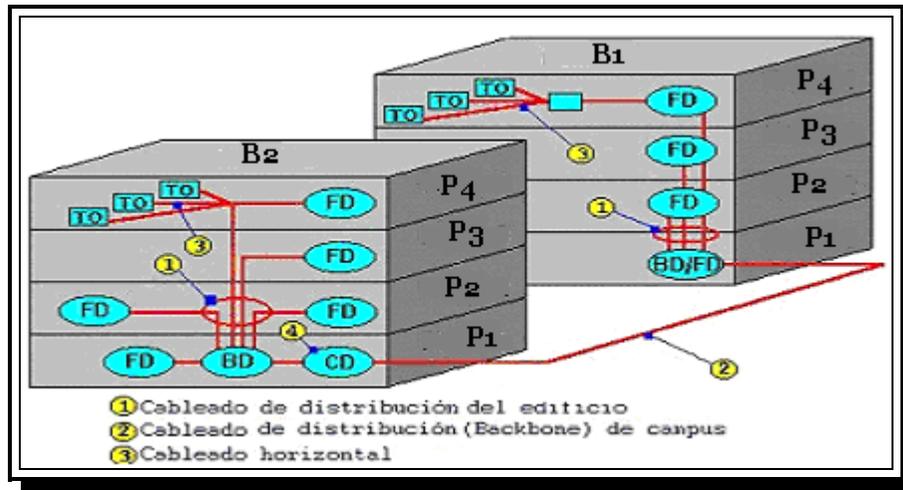


Figura 8.7. Sistema de cableado

- c. **Tomas de red.** En el mercado existen varios tipos de tomas de red con sus respectivos conectores. En este diseño los tomas de red deben cumplir con la reglamentación y la mejor forma de hacerlo es comprobar que sea de categoría 5e.
- d. **Patch-panel.** En la mayoría de los casos se usarán patch-panel de 24 puertos, y es uno por cada switch.



Figura 8.8. Patch-panel de 24 puertos

Para el conexionado del patch-panel se usarán patch-plug, estos son conectores, que conectan el patch-panel, con los puntos de red.



Figura 8.9. Patch-plug

e. **Conectores.** Los conectores usados son los RJ45 macho y se usarán para la construcción de los patch-cords de conexión externa de todos los dispositivos. Es importante saber que en el mercado existen conectores de varias calidades y que en muchos casos, un mal contacto producido por un mal conector, nos puede bajar el rendimiento de una LAN. Para el presente proyecto se ha elegido un conector de categoría 5e y de la calidad suficiente para que permita contactos seguros.

REFERENCIA		DESCRIPCIÓN
NMP-8215	5-05047393	CONECTOR RJ 45 / 8 PINES 50 MICRONES



Figura 8.10. Conectores RJ45

f. **Canaletas.** Las canaletas a usar son de dos cavidades con un tabique central para poder separar en dos grupos los cables que vallan por su interior.

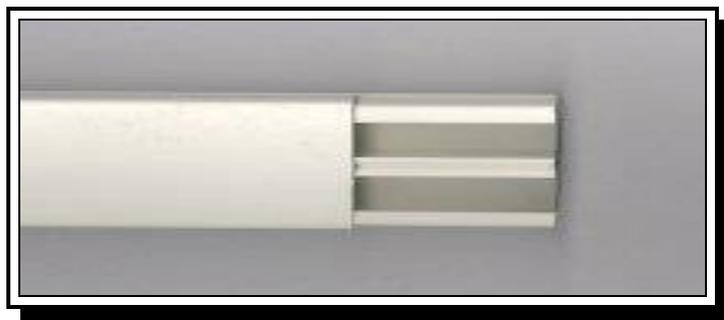


Figura 8.11. Canaleta de dos cavidades

8.1.4.4.7 Elección de los elementos activos

a. **La tarjeta de red.** Es el dispositivo que nos permite conectar la estación (ordenador u otro equipo de red) con el medio físico de transmisión (cable). Deben estar diseñadas para el mismo protocolo de bajo nivel Fast Ethernet y de la misma velocidad de transmisión del resto de los dispositivos de la red. Para este proyecto se requiere una tarjeta PCI de 10/100 Mb/s con conector RJ45.

b. **Router.**



Figura 8.12. Router

El router a utilizar es un equipo con 4 puertos, 10/100 BASE TX y 2 puertos análogos.

c. **Switch maestro.** El switch maestro, es un switch administrable, inteligente y programable, de 16 puertos 10/100 BASE TX, y con opciones para las configuraciones de VLANs.

Este equipo es el switch principal, de donde se empezará a extender toda la red.

SWITCHES INTELIGENTES

Todos los equipos de la familia de los Switch Inteligentes permiten:

- Administración por consola y/o remotamente
- Manejo de SNMP
- Configuración de VLAN
- Nivel 3
- Aplicaciones Gigabit Ethernet
- Puertos 10/100/1000 Base Tx
- Puertos 100/1000 Base Fx
- Montaje en Rack



REFERENCIA	DESCRIPCIÓN
WGSW-2400	Switch Apilable (Stackable) hasta 154 puertos. Unidad base de 24 puertos 10/100 Base Tx, con 3 slots en la parte posterior para futuras expansiones* de puertos 100/1000 Base Fx, 5/0/1000 Base Tx, 255 VLAN's.
WGSW-2400	Módulo de stack de 4Gbps por puerto. Switch de 24 puertos 10/100 Base Tx, con 3 slots en la parte posterior para futuras expansiones* de puertos Gigabit en fibra óptica y/o 10/100/1000 Base Tx. Procesos Switching de 6.4 Gbps.
WGSW-1600	Switch de 16 puertos 10/100 Base Tx, con 3 slots en la parte posterior para futuras expansiones* de puertos Gigabit en fibra óptica y/o puertos 100/1000 Base Tx. Módulo 24 puertos 10/100 Base Tx. 255 VLAN's. Procesos Switching de 9.6 Gbps.
WGSW-2400	Switch de 24 puertos 10/100 Base Tx, con 3 slots en la parte posterior* para 1 puerto 100 Base Tx. Procesos Switching de 4.8 Gbps.
WGSW-2600	Switch de 26 puertos 10/100/1000 Base Tx y 24 puertos 10/100 Base Tx.

Figura 8.13. Switch maestro

d. **Switches esclavos.** Los switches esclavos, son switches en su mayoría de 24 puertos que se ubicarán en cada una de las dependencias y serán sometidos a la programación del switch principal.

SWITCHES ESCLAVOS

Todos los equipos de la familia de los Switch Esclavos permiten:

- Monitoreo por consola
- Configuración de VLAN
- Puertos 10/100 Base Tx
- Puertos 100 Base Fx
- Puerto Up-Link para conectarlos en Cascada
- Montaje en Rack



REFERENCIA	DESCRIPCIÓN
FNSW-1000S	Switch de 16 puertos 10/100 Base Tx, con 1 slot en la parte posterior para 1 puerto 100 Base Fx, 4 puertos por medio VLAN y Protocolo Switching de 4.2 Gbps
FNSW-2400S	Switch de 24 puertos 10/100 Base Tx, con 1 slot en la parte posterior para 1 puerto 100 Base Fx, 4 puertos por medio VLAN y Protocolo Switching de 4.2 Gbps
FNSW-001ST	Módulo de 1 puerto 100 Base Fx, con cable ST para Switch FNSW-1000S y FNSW-2400S
FNSW-001SC	Módulo de 1 puerto 100 Base Fx, con cable SC para Switch FNSW-1000S y FNSW-2400S
FNSW-500	Switch de 8 puertos 10/100 Base Tx
FNSW-0000F	Switch de 6 puertos 100 Base Fx, con cable ST y 2 puertos 100 Base Tx
FNSW-0000E	Switch de 8 puertos 100 Base Fx, con cable ST

Figura 8.14. Switches esclavos

e. **Elección del recorrido.** El recorrido, parte de la sala de UPS, donde se ubica el switch principal, de allí se reparte a cada una de las dependencias por medio del cable de backbone. En todo caso los cables irán dentro de las canaletas y se tendrán en cuenta las siguientes reglas:

- Deben de estar al menos a 30 cm de distancia de las luces fluorescentes.
- La distancia entre los cables de la red y los de la corriente eléctrica debe de ser superior a 30 cm. Si tienen que cruzarse, deberán de hacerlo en ángulo recto para evitar el acoplamiento
- Se intentará buscar recorridos comunes para compartir la canaleta.
- También hay que cuidar el aspecto estético. Se intentará pasar las canaletas por sitios lo menos visibles posible.

- No deberán de estar en lugares ni demasiado accesibles por cuestiones de seguridad, ni en lugares de difícil acceso para facilitar el montaje y el mantenimiento.
- El trazado de las canaletas debe respetar las condiciones requeridas por el cableado a instalar, curvatura de los cables, paso por zonas no permitidas, distancias a conducciones eléctricas, etc.

8.2 IMPLEMENTACIÓN

Como este diseño no podrá ser instalado, en toda la Universidad debido a factores ajenos a nuestra voluntad, se implementará una muestra en el Laboratorio de Automatismo que se encuentra en el bloque1, piso3; donde se representará de forma simplificada, como funciona y se administra una red. Este diseño cuenta con un montaje de cableado estructurado, capaz de soportar la interconexión entre los diferentes computadores que se encuentran dispuestos en esta sala. La distribución de los computadores y al ubicación de los equipos activos y pasivos se muestran en el plano.

8.3 MONTAJE DE LA RED

El montaje de la red es descrito para cada LAN

8.3.1 Colocación de canaletas. Una vez decidido el recorrido por el que van a transcurrir las canaletas, se procede a su colocación. El proceso a seguir será:

- ✓ Medir la distancia que se quiere cubrir.
- ✓ Cortar las canaletas a la medida apropiada con la segueta. En el caso de tener que realizar algún ángulo de 90°, cortaremos los extremos de las canaletas a unir en inglete con lo que se conseguirá un ajuste perfecto. La canaleta siempre se corta con la tapa puesta, con esto nos evitaremos tener que realizar dos cortes por separado, uno para el cuerpo de la conducción y otro para la tapa.
- ✓ Sobre la canaleta prefijada, realizar los taladros necesarios para garantizar su perfecta sujeción a la pared. El número de taladros dependerá de la longitud del tramo a fijar pero podría servir de referencia realizar un taladro cada metro o metro y medio
- ✓ Introducir los tacos en cada uno de los taladros realizados
- ✓ Atornillar los tornillos en cada uno de los tacos colocados con lo que dejaremos perfectamente sujeta la canaleta a la pared.

8.3.2 Fijación de los puntos de red y el patch-panel. Tanto los puntos de red como el patch-panel deben de ser fijados a la pared con sus respectivos tornillos. En este se fijan los cajas que los contiene y más adelante se realizarán las conexiones pertinentes.

El proceso a seguir es:

- ✓ Presentar la caja del elemento a fijar en la pared. Se tendrá en cuenta que la canaleta llegue justo hasta el borde de la caja para conseguir que no se vean ninguno de los cables que lleva en su interior.
- ✓ Realizar los taladros necesarios.

- ✓ Atornillar las cajas a la pared.

8.3.3 Cableado. Llegó el momento de introducir los cables en las canaletas. Habrá que llevar un cable desde cada una de los puntos de red hasta el patch-panel. Las normas a tener en cuenta a la hora de trabajar con los cables son:

- ✓ No se deberá someter a los cables a tracciones fuertes. Nunca superiores a 10 kg
- ✓ Nunca debe doblarse un cable en un ángulo menor de 90°.
- ✓ En los lugares donde el número de cables sea elevado, se pueden usar presillas para garantizar su inmovilidad pero sin presionar demasiado.
- ✓ No se debe trenzar el cable.

El proceso a seguir es:

- ✓ Medir la distancia de cada uno de los tramos del cable a introducir en las canaletas.
Es conveniente prever que hay que dejar un trozo de cable en cada uno de los extremos para permitir el trabajo de conexionado.
- ✓ Cortar los cables a las medidas adecuadas.
- ✓ Comenzar a introducir cables en la canaleta por el extremo del punto de red.
- ✓ Conforme que el cable está siendo introducido en la canaleta, es conveniente ir poniendo la tapa a la canaleta para conseguir que no se salga con los movimientos y tracciones lógicas del proceso de trabajo
- ✓ Cuando se esté trabajando en los tramos de distribución, o sea, en los lugares donde son varios los cables que hay que embutir, es conveniente introducirlos todos a la vez para no tener que abrir varias veces las tapas de las canaletas.

8.3.4 Conexión de los puntos de red. El mecanismo usado en los puntos de red es el mismo que se usará en el patch-panel y esta compuesto por un conector RJ-45 hembra en su parte frontal con nueve conexiones para otros tantos hilos en su parte trasera. De los nueve, ocho son hilos para datos de información y el noveno se usa para conexión de tierra. El proceso a seguir en la conexión del cable al mecanismo del conector es el que sigue:

- a. Pelar el cable aproximadamente 3 cm. Este proceso se realizará con la parte destinada a tal efecto de la ponchadora.
- b. Abrir las trampillas con las que se cubren los contactos del mecanismo.

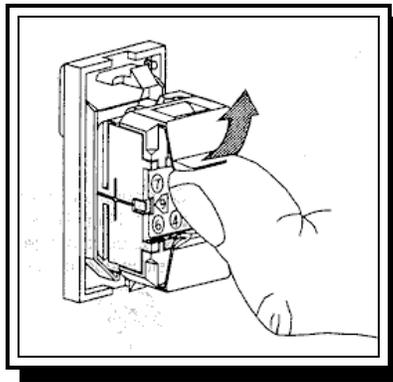


Figura 8.15. Mecanismo de Conexión

- c. Comprobar la posición en la que conectaremos cada hilo del cable. El código de colores de cableado está regulado por la norma T568A.
- d. Destrenzar los pares individuales del cable, y hacer la conexión de los distintos hilos a su respectivo contacto que se hará de uno en uno. Para ello, se toma uno de los hilos y se coloca en su contacto correspondiente y luego se le hace presión con una ponchadora de impacto.

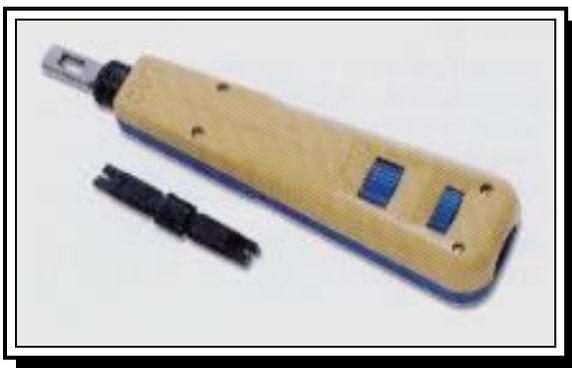


Figura 8.16. Ponchadora de impacto.

- e. Es conveniente recordar que el hilo no hay que pelarlo ya que las propias cuchillas del contacto lo harán.
- f. Una vez conectados todos los hilos, proceder a cerrar la roseta sobre la caja de superficie.

8.3.5 Desconexión. Si en algún momento se necesitara desconectar algún hilo, el proceso sería el siguiente:

- a. Abrir la trampilla que cubre los contactos.
- b. Desanclar el hilo de la pestaña de retención
- c. Tirar del hilo verticalmente hacia fuera del contacto. Con esto se liberará de las cuchillas que lo sujetan.

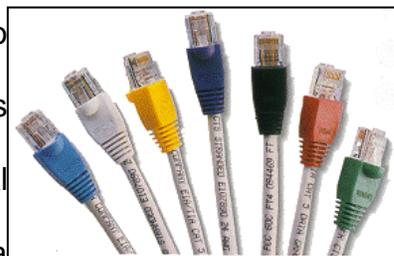
8.3.6 Conexión del patch-panel. Para el conexión de cada patch-panel se debe ubicar cada hilo en cada contacto del patch-plug, según la norma T568A, y luego ubicarla en la parte posterior de este. El proceso es similar al usado para los puntos de red, aunque en esta ocasión no se necesita la ponchadora.



Figura 8.17. Conexión del Patch-Panel

8.3.7 Construcción de los patch-cord. El proceso de construcción del patch-cord es como sigue:

- a. Se corta un trozo de cable de la medida necesaria para cubrir cómodamente la distancia entre el patch-panel y el switch o en su caso entre el punto de red y el PC. La práctica nos aconseja que el corte sea totalmente perpendicular al cable, ya que de esta manera se garantiza que la longitud de los hilos es siempre la misma.



- b. Introducir en el cable la bota de plástico del conector que va a cumplir funciones de sujeción y a su vez de protección.
- c. Se pelan ambos extremos. Se cortará aproximadamente 1 cm del aislante de la cubierta.
- d. Se separan los hilos y se colocan en el orden determinado por la norma T568A.

- e. Se introducen los hilos en el conector RJ-45 macho hasta el final de éste respetando el orden de los colores del cable
- f. Introducir el conector en la ponchadora y presionar hasta escuchar el click que nos indica que el conector está seguro.
- g. Cubrir el conector con la capucha de plástico que ayudará a hacer más solidario el cable al conector.

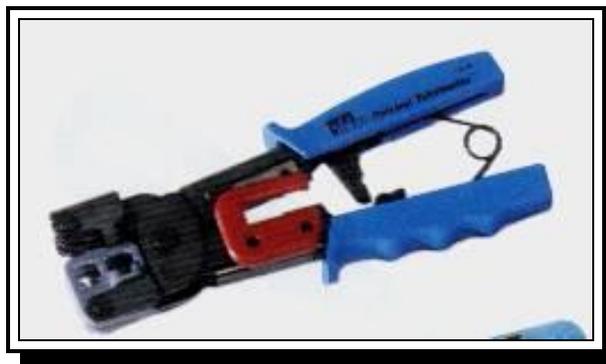


Figura 8.18. Ponchadora

8.3.8 Cable cruzado (Crossover). Si en cualquier momento se necesita conectar un dispositivo de red (PC, router, etc.) directamente a otro sin pasar por un concentrador, se debe usar un cable cruzado donde el par de transmisión de un extremo se comunique con el par de recepción del otro. La conexión sería como sigue:

Cable cruzado	
Extremo 1	Extremo 2
Pin 1	Pin 3
Pin 2	Pin 6
Pin 3	Pin 1
Pin 6	Pin 2

Tabla 8.1. Crossover

8.3.9 Verificación del cableado. Es importante comprobar que está bien todo el trabajo realizado hasta el momento antes de proceder a la conexión de los dispositivos que componen la red local. Para verificar el cableado de la red, se utiliza un comprobador de cables que va a dar información sobre el estado de los mismos. Indicará tanto cortes como cruces de una forma bastante intuitiva para el cable UTP.



Figura 8.19. Comprobador de cables

Está compuesto por dos partes que se conectan a ambos extremos del cable a comprobar. Una de ellas es la unidad principal donde están todos los indicadores y mandos de funcionamiento y la otra es el terminador.

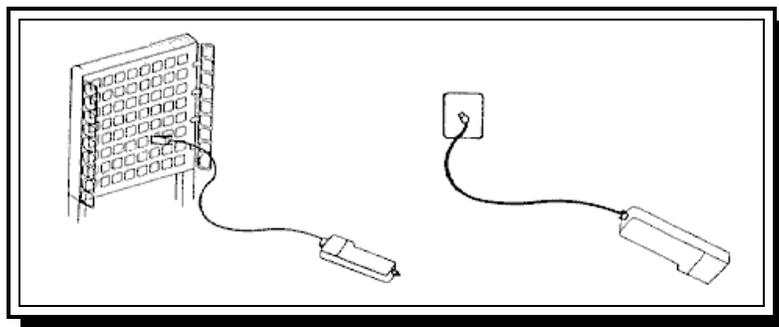


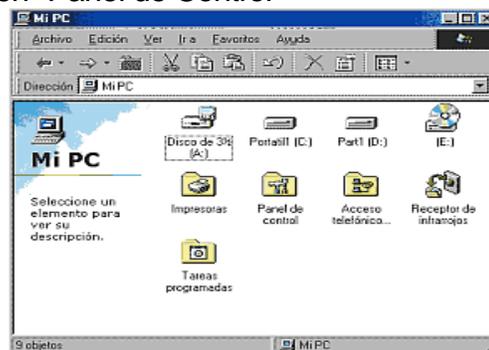
Figura 8.20. Figura Verificación del cableado

8.3.10 Conexión del switch. Antes de proceder a la conexión del switch, debe estar ubicado en su respectivo gabinete, con su patch-panel y el organizador de cables. Las conexiones a realizar en cada switch consisten en unir mediante patch-cord cada uno de los conectores usados en el patch-panel con uno de los puertos del mismo del mismo.

8.4 CONFIGURACIÓN

Una vez instalada la tarjeta de red y el software de red, se debe instalar y configurar los protocolos de red, necesarios para que los equipos puedan comunicarse entre si, el procedimiento es el siguiente:

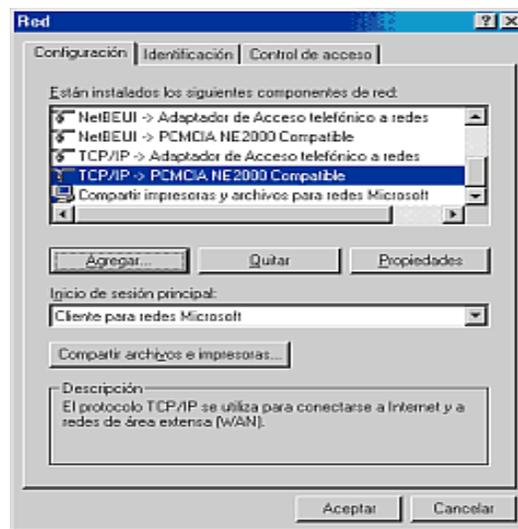
a. Desde "Mi PC", se pulsa en "Panel de Control"



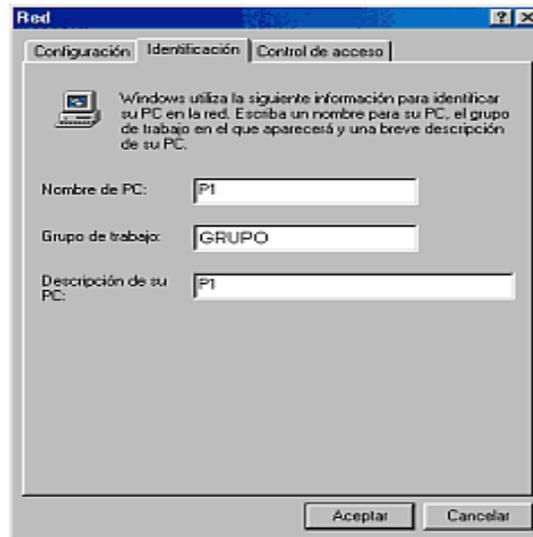
b. Se pulsa en el icono de "Red"



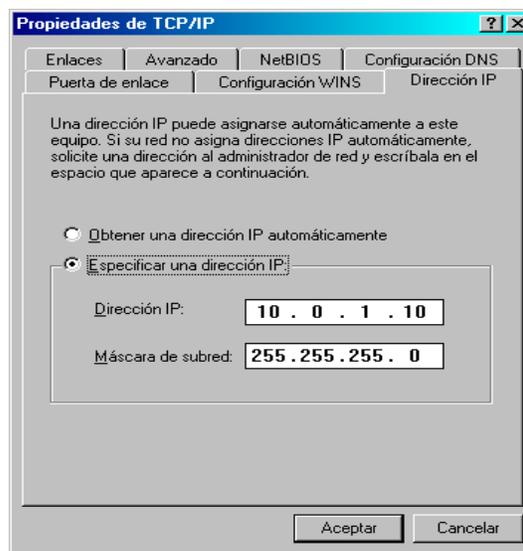
c. Pulsando en el botón "Agregar" se debe ir añadiendo los protocolos "TCP/IP" y "NetBEUI"; el servicio "Compartir impresoras y archivos para redes Microsoft", y el "Cliente para redes Microsoft". Todos estos protocolos y servicios sirven para que los puestos se comuniquen entre sí, y con la excepción del TCP/IP, no es necesario configurarlos. Es posible que más adelante alguna aplicación o juego en red necesite usar otro protocolo. En ese caso deberíamos volver a este menú e instalarlos.



d. Ahora se tiene que asignar un nombre a cada equipo



- e. Luego en configuración/TCP/IP se hace pulsa en especificar una dirección IP e ingrese una dirección IP y una submáscara. Se deben emplear series secuenciales así como 10.0.0.2, 10.0.0.3 y así sucesivamente. Cada computadora obtiene una submáscara 255.255.255.0. Cada dirección IP en su red local debe ser única, y sólo puede variar el número en el final del grupo, en otras palabras, no cambia la porción 10.0.0 de la dirección.



En el momento de hacer las configuraciones en cada equipo, se debe tratar de forma independiente las redes de Admisiones y Contabilidad, es decir que en el formato designado a la identificación de red en la dirección IP, debe ser independiente para cada una de estas redes, así teniendo cada red su respectivo identificación se facilita la programación del switch, y por ende el bloqueo de las vías de acceso, a equipos que no las requieran y el router se encarga de los accesos a Internet.

8.5 MANTENIMIENTO DEL CABLEADO DE UNA RED INFORMÁTICA

Si una vez terminado el montaje de la red se ha hecho respetando las normas establecidas, el mantenimiento de un sistema de cableado es prácticamente nulo en condiciones normales. Es importante que el administrador de la red esté pendiente de las obras o reformas que se realicen en le edificio y que puedan afectar al correcto funcionamiento de la instalación. Habrá que tener especial cuidado con:

- ✓ Los albañiles y pintores pueden desmontar o cortar los cables cuando les estorban pensando que después se pueden empalmar.
- ✓ Los electricistas usan las canaletas de cables de datos para meter cables eléctricos o tiran canaletas paralelas a poca distancia.
- ✓ Se comparte las tomas de corriente de los elementos activos o de los puestos de trabajo con estufas, acondicionadores de aire, ventiladores o maquinas con motores eléctricos.

- ✓ Se instalan equipos eléctricos que producen interferencias cerca de los cables de la red.
- ✓ Se mueven canalizaciones de forma que los nuevos trazados no respetan los requerimientos
- ✓ Se intercambian los cables de conexión de teléfono y puesto de trabajo.

9. GLOSARIO

ACCESO LOCAL: Uso de un terminal conectado directamente de una computadora.

ACCESO MÚLTIPLE (MA): Método de acceso a una línea en el que cada estación puede acceder a ella libremente.

ALGORITMO DE ENCAMINAMIENTO: Algoritmo utilizado por un encaminador, para determinar el camino óptimo para un paquete.

ANCHO DE BANDA: Diferencia entre las frecuencias más alta y más baja de una señal compuesta. También mide la capacidad de transmisión de información de una línea o una red.

BANDA ANCHA: Se refiere a una tecnología en la que la señal comparte el ancho de banda de un medio.

BANDA BASE: Se refiere a una tecnología en la que la señal se transmite directamente a través de un canal sin modular una portadora.

BIT: Dígito binario; unidad más pequeña de información.

BLOQUEO: Un evento que ocurre cuando una red de conmutación está trabajando a su completa capacidad y no puede aceptar más entradas.

BYTE: Grupo de ocho bits.

CABECERA: Información de control que se añade al comienzo de unos datos.

CAMINO: Canal a través del cual se transmiten las señales.

CIRCUITO VIRTUAL (VC): Circuito lógico entre la computadora emisora y la receptora. La conexión se establece una vez que las dos computadoras lo acuerdan. Después de la conexión, todos los paquetes siguen la misma ruta y llegan en secuencia.

CLIENTE: Programa que inicia la comunicación con otro programa denominado servidor.

COLISIÓN: Evento que ocurre cuando dos transmisores emiten al mismo tiempo a través de un canal diseñado para una única transmisión a la vez; los datos serán destruidos.

CONGESTIÓN: Red con excesivo tráfico que provoca la degradación general del servicio.

DATAGRAMA: En conmutación de paquetes una unidad de datos independiente.

DIODO DE EMISIÓN DE LUZ (LED): Emisor de luz para fibra óptica; normalmente limitada a distancias cortas.

DISTORSIÓN: Cualquier cambio en una señal como consecuencia del ruido, atenuación u otras influencias.

EMISOR: Sistema que origina un mensaje.

ENCAPSULADO: Técnica en la que la unidad de datos de un protocolo se sitúa dentro de la porción del campo de datos de la unidad de datos de otro protocolo.

ENMASCARAMIENTO: Proceso que extrae la dirección de la red física a partir de una dirección IP.

ESTABLECIMIENTO DE CONEXIÓN: Etapa preliminar necesaria para una conexión lógica antes de transferir datos.

EQUIPOS ACTIVOS: Se conoce como equipo activo aquel que tiene algún tipo de circuitería electrónica y por lo tanto tienen alimentación eléctrica.

INTERCONEXIÓN DE REDES: Conexión de varias redes, utilizando dispositivos de interconexión como encaminadores o pasarelas.

INTERFAZ: Límite entre dos equipos. También se refiere a las características mecánicas, eléctricas y funcionales de la conexión.

MENSAJE: Datos enviados desde un origen a un destino.

MÓDEM: Dispositivo para modular o remodular. Convierte una señal digital en una señal analógica y viceversa.

MULTIENVÍO: Método de transmisión que permite que varias copias de un mismo paquete sean enviadas a un grupo seleccionado de receptores.

NODO: Un dispositivo de comunicación direccionable.

PÁGINA WEB: Unidad de hipertexto o hipermedia disponible en la Web.

PAQUETE: Sinónimo de unidad de datos; utilizado mayormente en el nivel de red.

SEGMENTACIÓN: División de un mensaje en varios paquetes; normalmente realizado en el nivel de transporte.

SEGURIDAD: Protección de una red de accesos no autorizados, virus y catástrofes.

SERVICIO ORIENTADO A CONEXIÓN: Servicio de transferencia de datos que involucra el establecimiento y terminación de una conexión.

SERVICIO SIN CONEXIÓN: Servicio para transferir datos sin establecimiento ni terminación de la conexión.

SERVIDOR: Programa que ofrece servicios a otros programas denominados clientes.

TABLA DE ENCAMINAMIENTO: Tabla que contiene la información que necesita un router para encaminar los paquetes. La información puede incluir la dirección de red, el costo, etc.

TEMPORIZACIÓN: Factor de un protocolo que se refiere al instante en que los datos se deben enviar y la velocidad de la transmisión.

TERMINADOR: Dispositivo electrónico que evita las reflexiones de las señales al final del cable.

VELOCIDAD DE PROPAGACIÓN: Tasa a la que viaja una señal o un bit; medida por espacio/segundos.

VIDEOCONFERENCIA: Servicio que permite a un grupo de usuarios intercambiar información a través de una red.

VLAN: (Virtual Local Area Networks; Redes virtuales de área local) forman grupos lógicos para definir los dominios de broadcast. Aunque físicamente estén conectadas las máquinas al mismo equipo, lógicamente pertenecerán a una VLAN distinta dependiendo de sus aplicaciones con lo que se logra un esquema más enfocado a necesidades independientes.

10. CONCLUSIÓN

La evolución de las redes de computadoras, ha incrementado la eficiencia de las transmisiones de datos hasta el punto que ninguna entidad debe mantenerse ajena a este servicio, pues las redes representan en gran parte el desarrollo, eficiencia y modernización de cualquier entidad tendiente a evolucionar.

Existen diversos métodos para interconectar redes de computadoras, pues son muchos los equipos, medios de transmisión, configuraciones y protocolos de red de los que se disponen; es por ello que no se puede generalizar, sobre que equipo se debe utilizar, o bien que medio de transmisión es el correcto; puesto que cada red tiene sus propias exigencias, en lo que a ancho de banda y eficiencia se refiere; y es gracias a esta variedad de recursos, que se puede escoger cuales son los elementos y protocolos que se ajustan a nuestras necesidades particulares de conexión, es por ello que a la hora de realizar un diseño, se tiene que conocer inicialmente los servicios que debe prestar la red en estudio y en base a esto analizar la diversidad de recursos con que se cuenta y la forma más práctica de adaptarlas a un caso en particular.

Diseñar una LAN, incluye una gran responsabilidad y un estudio detallado de lo que se requiere, por parte de quien realiza esta tarea, con el fin lograr un mayor rendimiento en los medios de transmisión y en los equipos a utilizar para la optimización de los procesos; la idea básica tiende a crear una autopista de información, con un soporte lo suficientemente robusto, como para tolerar todo el tráfico de información y la gran

transferencia de datos que se presenten; asimismo contar con la ventaja de poder crear diversas conexiones lógicas entre los equipos, pues aunque estos estarán conectados físicamente, no quiere decir que tengan que comunicarse, porque las interacciones entre PC's realmente se establece mediante conexiones lógicas.

En el estudio de éste proyecto fueron muchos los aspectos que se tuvieron que considerar, y para nosotros fue muy satisfactorio, el poder brindar a la Corporación Universitaria de la Costa la oportunidad de contar con una LAN, lo suficientemente eficiente y práctica, como para mejorar los problemas presentes en el manejo de sus oficinas, ya que este diseño reduce el tiempo de trabajo del personal que labora en las dependencias administrativas y por ende aumenta la eficiencia y productividad general de la Universidad.

BIBLIOGRAFÍA

EVANS, Tim. Redes De Área Local. Ed. Prentice-Hall. México, 1997

CURRID, C. Cerril. Redes de Computación.. Ed. Macrobit. México, 1996

GREER, Tyson. Redes de Cómputo. Ed. Mc Graw Hill. Madrid,1998

TERD, Sydney. TCP/IP Arquitectura, Protocolos, Implementación y Seguridad. Ed. Mc Graw Hill. Madrid, 2000

TANEMBAUN, Andrés. Redes De Computadores. Ed. Prentice Hall. México, 2000

FOROUZAN, Behrouz A. Transmisión De Datos y Redes De comunicaciones. Ed. Mc Graw Hill. Madrid, 2001