

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA DE TELEMÁTICA

IMPLEMENTACIÓN DE UNA RED LAN Y TARJETAS DE ADQUISICIÓN

DE DATOS COMPARTIDOS CON CONEXIÓN A INTERNET EN EL

LABORATORIO DE INSTRUMENTACIÓN VIRTUAL

POR

CBOS. AGUAS NIETO LUIS

**Proyecto de grado presentado como requisito parcial para la obtención
del título de:**

TECNÓLOGO EN TELEMÁTICA

2005

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. CBOS: AGUAS NIETO LUIS, como requerimiento parcial para la obtención del título de TECNÓLOGO EN TELEMÁTICA.

Sr. Ing. Pablo Pilatásig
DIRECTOR DEL PROYECTO

DEDICATORIA

Los elevados principios de solidaridad, amistad, respeto y consideración se encuentran fortalecidos hoy; que se a cumplido una más de mis aspiraciones y esperanzas por el éxito alcanzado, quiero dedicar este trabajo a mis queridos padres, hermanos y a mi esposa leal y valerosa compañera de mi vida.

LUIS

AGRADECIMIENTO

Mi agradecimiento al Instituto Tecnológico Superior Aeronáutico, a sus Autoridades y Maestros, ya que me abrieron las puertas a una educación formal, para alcanzar un espíritu de superación.

Mi inmensa gratitud al Ing. Pablo Pilatásig, por su ayuda y colaboración para finalizar este presente proyecto como a todas las personas que confiaron y pusieron sus esperanzas en mi persona, apoyándome para no desmayar jamás.

Y por su puesto a Dios por haberme permitido culminar esta etapa de mi vida con eficacia y éxito

LUIS

ÍNDICE DE CONTENIDO

Portada	I
Certificación	II
Dedicatoria	III
Agradecimiento	IV
Índice de Contenidos	V
Índice de figuras	IX
Índice de tablas	XI
Introducción	1
Definición del Problema	2
Objetivos	2
Justificación	3
Alcance	3
CAPITULO I : MARCO TEÓRICO	
1. Redes de Datos	4
1.1 Introducción	4
1.2 Características de la red	5
1.3 Tipos	5
1.3.1 Redes LAN	6
1.3.2 Redes MAN	9
1.3.3 Redes WAN	13
1.2 Arquitectura de la Red LAN	16
1.2.1 Redes Ethernet	16

1.2.2 Presentaciones Ethernet	17
1.2.3 Redes Token Ring	30
1.3 Cables	36
1.3.1 Par Trenzado	37
1.3.2 Cable Coaxial	42
1.3.3 Conectores	44
1.3.4 Ponchada de Cables	45
1.4 Dispositivos	47
1.4.1 Hub	47.
1.4.2 Swicht	47
1.4..3 Repetidores	49
1.4.4 Bridge o Puente	50
1.4..5 Router o Enrutador	51
1.4.6 Pasarela o Gateways	52
1.5 Estándares y protocolos	54
1.5.1 Como trabajan los protocolos	63
1.5.2 Funciones del protocolo	65
1.5.3 Tipos de protocolos	68
1.5.4 Protocolo Data Socket de la National Instruments	75

1.6 Dirección IP	80
1.6.1 Creación de dirección propia	81
1.6.2 Grupo de direcciones	81
1.6.3 Mascara de red	83

CAPITULO 2: IMPLEMENTACION DE LA RED LAN

2.1 Implementación de la red	84
2.1.1 Estudio del lugar	84
2.1.2 Características del lugar	85
2.1.2.2 Conexión del Swicht	85
2.1.2.3 Conexión de las computadoras	86
2.2 Construcción del cableado	86
2.3 Instalación de las tarjetas	88
2.4 Implementación de controladores de la tarjeta de red	90
2.4.1 Configuración de la red	90

CAPITULO 3: ANÁLISIS ECONÓMICO

3.1 Costos de accesorios empleados	93
------------------------------------	----

CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones	94
4.2 Recomendaciones	95
GUIAS DEL USUARIO	96
ANEXOS	
GLOSARIO	
BIOGRAFIA	

ÍNDICE DE FIGURAS

Fig 1.1	Red de Datos	5
Fig 1.2	Redes LAN	7
Fig 1.3	Redes MAN	10
Fig 1.4	Redes WAN	14
Fig 1.5	Vista previa una red Ethernet	17
Fig 1.6	Presentación de una Ethernet	18
Fig 1.7	Conector BNC	21
Fig 1.8	Conector T	22
Fig 1.9	Combinando Thicknet y Thinnet	26
Fig 1.10	Red Token Ring.	31
Fig 1.11	Red Arc Net en topología estrella	36
Fig 1.12	Conector	38
Fig 1.13	Cable UTP	39
Fig 1.14	Cable Coaxial	43
Fig 1.15	Cable fino	44
Fig 1.16	Cable grueso	44
Fig 1.17	Conectores RJ 45	45
Fig 1.18	Ponchada de cables	46
Fig 1.19	HUB	47
Fig 1.20	SWICHT	49
Fig 1.21	Repetidores	50

Fig 1.22	Puente	51
Fig 1.23	Enrutador	52
Fig 1.24	Conexión de un Bridge	53
Fig 1.25	Conexiones entre Routers y Bridge	53
Fig 1.26	Conexiones entre Bridge y Routers	54
Fig 1.27	Panel frontal	79
Fig 1.28	Icono y conector	79
Fig 2.1	Análisis de red	85
Fig 2.2	Conexión de computadoras	86
Fig 2.3	Cable pasado por la canaleta	86
Fig 2.4	Ubicación del switch en el laboratorio	87
Fig 2.5	Conexión de los cables al Swicht	88
Fig 2.6	Implementación de las tarjetas	88
Fig 2.7	Llanura para la tarjeta Ethernet	89
Fig 2.8	Cajetines	89
Fig 2.9	Configuración de red	90
Fig 2.10	Configuración de conexión de la red	91
Fig 2.11	Configuración de direcciones IP y máscaras	91

ÍNDICE DE TABLAS

Tabla 1.1	Características de longitudes posibles y ancho de banda	41
Tabla 1.2	Nivel de Atenuación permitido según la velocidad	42
Tabla 1.3	Código de colores para ponchar	46
Tabla 1.4	Mascaras de red	83
Tabla 3.1	Costo total del proyecto	93

INTRODUCCIÓN

El Instituto Tecnológico Superior Aeronáutico, prepara tecnólogos capaces de afrontar las principales tecnologías del futuro. Una de las principales ramas es la Carrera de Telemática , la misma que se encarga de preparar a los alumnos en cuanto a todos los sistemas de comunicación e informática , por lo que se considera necesario la implementación de una Red LAN con Tarjetas de Adquisición de Datos en el Laboratorio de Instrumentación Virtual ya que de esta manera se realiza un aporte a la labor educativa del instituto dentro del Área de Telemática , por lo cual es conveniente mejorar las condiciones bajo las cuales los educandos adquieren los conocimientos necesarios referente a dicho proyecto.

Definición del problema

En la actualidad el Instituto Tecnológico Superior Aeronáutico cuenta con un laboratorio de Instrumentación Virtual, cuyo funcionamiento no está al cien por ciento ya que para ello requiere de equipos (PCs.) conectadas en una red por lo que he considerado necesario la implementación de una red LAN y tarjetas de adquisición de datos compartidos con conexión a Internet en dicho laboratorio.

Objetivos

OBJETIVO GENERAL.

- Implantar una red LAN y tarjeta de adquisición de datos compartidos con conexión a Internet en el laboratorio de instrumentación virtual.

OBJETIVOS ESPECÍFICOS

- Estudiar la implementación de una red LAN en el laboratorio de instrumentación virtual.
- Conectar las PCs a la red
- Realizar pruebas de operación de la red instalada

Justificación

Los grandes avances tecnológicos han dependido en gran parte del desarrollo de las comunicaciones, por lo cual el Instituto Tecnológico Superior Aeronáutico no puede quedar al margen de los mismos.

Es por ello, que se desea implementar una red LAN y tarjetas de adquisición de datos compartidos en el Laboratorio de Instrumentación Virtual con la finalidad de que la adquisición realizada a National Instruments por parte del Instituto no se vea rezagada en sus aplicaciones, por no contar con los equipos necesarios para que los estudiantes puedan realizar sus prácticas utilizando tanto el software como el hardware con el que cuenta este laboratorio.

Además, dentro de los proyectos a futuro es convertirlo en un laboratorio remoto accesible al personal docente y estudiantes a través del Internet, por lo que esta red también se conectará al servicio de Internet con el que cuenta el Instituto Tecnológico Superior Aeronáutico.

Alcance

Al finalizar este proyecto se logrará mejorar los servicios que ofrece hasta el momento al personal docente y estudiantes del Instituto Tecnológico Superior Aeronáutico el Laboratorio de Instrumentación Virtual, ya que permitirá a través de la red realizar prácticas y proyectos ilimitados utilizando LABVIEW y el hardware deseado.

CAPÍTULO I

Red de Datos

1.1 Introducción.-

Los Servicios de Redes de Datos consisten en una amplia gama de soluciones que ayudan a las empresas a proporcionar acceso a los usuarios a la información vital de la empresa y a las aplicaciones que necesitan para realizar su trabajo de un modo más eficaz, así como ampliar su alcance en el mercado de un modo seguro y eficaz. Estos servicios facilitan la conexión con empleados locales o con aquellos que se encuentran en otros lugares, así como con clientes y socios comerciales, al mismo tiempo que disminuyen sus inversiones en personal y sistemas de red.

Con los Servicios de Redes de Datos las empresas no necesitan crear y proporcionar un soporte para un funcionamiento continuo de las redes, con lo cual pueden dedicarse por completo a su empresa. Este servicio de gestión de redes proporciona servicios esenciales de conectividad TCP/IP, SNA y multiprotocolo; gestión de redes, cambios, y características de seguridad que facilitan el enlace con empleados locales o que se encuentran en otros lugares, así como con clientes y socios comerciales. Los Servicios IBM de Redes de Datos proporcionan ayuda para el diseño, la instalación e incluso la configuración de redes en ubicaciones geográficamente distantes.

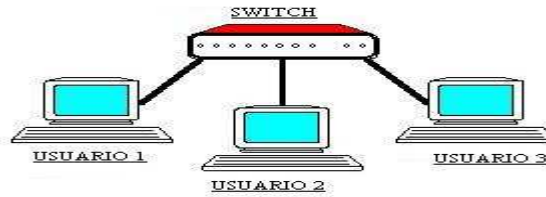


Fig. 1.1 Red de Datos

1.2 Características de la Red:

- Acceso a aplicaciones de redes privadas para empleados que se encuentran fuera de la oficina o aquellos trabajadores que viajan con frecuencia.
- Alcance global con soporte local y un solo punto de contacto.
- Más de 1.100 puntos de representación en 52 países.
- Acceso a otras redes de todo el mundo.
- Diseño de redes para obtener soluciones rentables y proteger las inversiones en tecnología

Ventajas

- Integración de varios puntos en un mismo enlace
- Posibilidad de Crecimiento hacia otros puntos para integración en la misma red

1.3 Tipos de Red:

- ❖ Lan
- ❖ Wan
- ❖ Man

1.3.1 Redes LAN

El termino LAN (Local Área Network) alude a una red a veces llamada subred instalada en una misma sala, oficina o edificio. Los nodos o punto finales de una LAN se conectan a una topología de la red compartida utilizando un protocolo determinando. Con la autorización adecuada, se puede acceder a los dispositivos de la LAN, esto es estaciones de trabajo, impresora , etc., desde cualquier otro dispositivo de la misma. Las aplicaciones software desarrolladas para la LAN (mensajerilla electrónica, procesamiento de texto, hojas electrónicas, etc.) también permiten ser compartidas por lo usuarios.

Características de una LAN

Tienen un diámetro pequeño, de unos cuantos kilómetros como máximo. Un edificio, un campuz universitario, etc.

Normalmente usan la tecnología de broadcast: un solo cable con todas las máquinas conectadas.

El tamaño es restringido, así el tiempo de transmisión del peor caso es conocido.

Velocidades típicas son de 10 a 100 Mbps

Su velocidad de transmisión es de unos megabits/seg en función de su velocidad se divide en:

- **LAN** cuando en su velocidad es de 1 y 20 Mbit/seg.
- **HSLN** (High Speed Local Networks) redes de alta velocidad, con una velocidad del orden de 100 Mbit/seg.
- Su tasa de errores es pequeña.
- Suele tratarse de redes privadas.

- Las dos arquitecturas LAN más utilizadas son:
 - Ethernet.
 - Token Ring.

Usos de una red local

Lo primero que se puede preguntar un usuario cuando se plantea la posibilidad de instalación o utilización de una red local, es saber cómo va a mejorar su trabajo en el ordenador al utilizar dicho entorno. La respuesta va a ser diferente según el tipo de trabajo que desempeñe. Así una red local proporciona la facilidad de compartir recursos entre sus usuarios. Esto es:

- Compartir ficheros.
- Compartir impresoras.
- Se puede utilizar aplicaciones específicas de la red.
- Prestaciones cliente/servidor
- Acceso a sistemas de comunicación global.

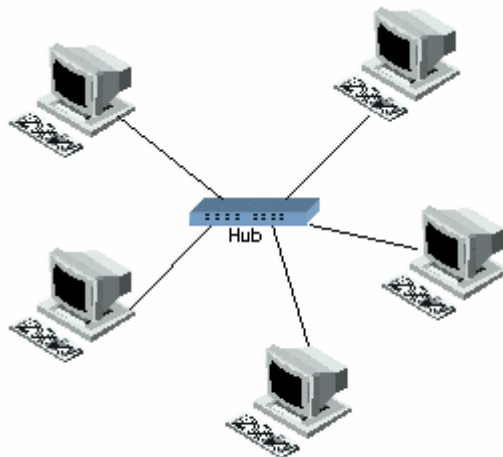


Fig. 1.2 Redes LAN

Aplicaciones.

Existen un gran número de aplicaciones que aprovechan las redes locales para que el trabajo sea más provechoso. El tipo de aplicaciones más importantes son los programas de correo electrónico. Un programa de correo electrónico permite el intercambio de mensaje entre los usuarios. Los mensajes pueden consistir en texto, sonido, imágenes, etc. y llevar asociados cualquier tipo de ficheros binarios. En cierto modo el correo electrónico llega a sustituir ciertas reuniones y además permite el análisis más detallado del material que el resto de usuario nos remita.

Aplicaciones Cliente/Servidor.

Es muy importante en las redes locales para las aplicaciones que manejan grandes volúmenes de información, los programas que dividen su trabajo en dos partes, una parte cliente que se lo realiza en el ordenador del usuario y la otra parte en el servidor que se realiza en un servidor con dos fines:

- Aliviar la carga de trabajo del ordenador cliente.
- Reducir el tráfico de la red.

Ventajas y Desventajas de una LAN

Ventajas

- Se puede compartir periféricos que se encuentren conectados a cada una de las computadoras, impresoras, grabadoras, etc.
- Se puede compartir información que se encuentre en cada una de las computadoras. (se puede compartir todo o parte, según se determine en cada computadora)

- Ya no se requerirá a los disquetes para pasar archivos de una red a otra
- Usar la conexión de Internet en cada una de las máquinas (para esto se necesita un programa proxy o ADSL, con el router puede conectar sin problemas)
- Se puede utilizar un disco duro para guardar archivos y copias de seguridad de las otras máquinas.
- Se puede jugar en red

Desventajas

- No pueden cubrir distancias muy grandes

1.3.2 Redes MAN

Metropolitan Área Network. Este término describe a una red que provee una conectividad digital de un área regional a una metropolitana. La MAN realiza el enlace entre las LANs Y WANs.

Una red de área metropolitana (MAN) es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

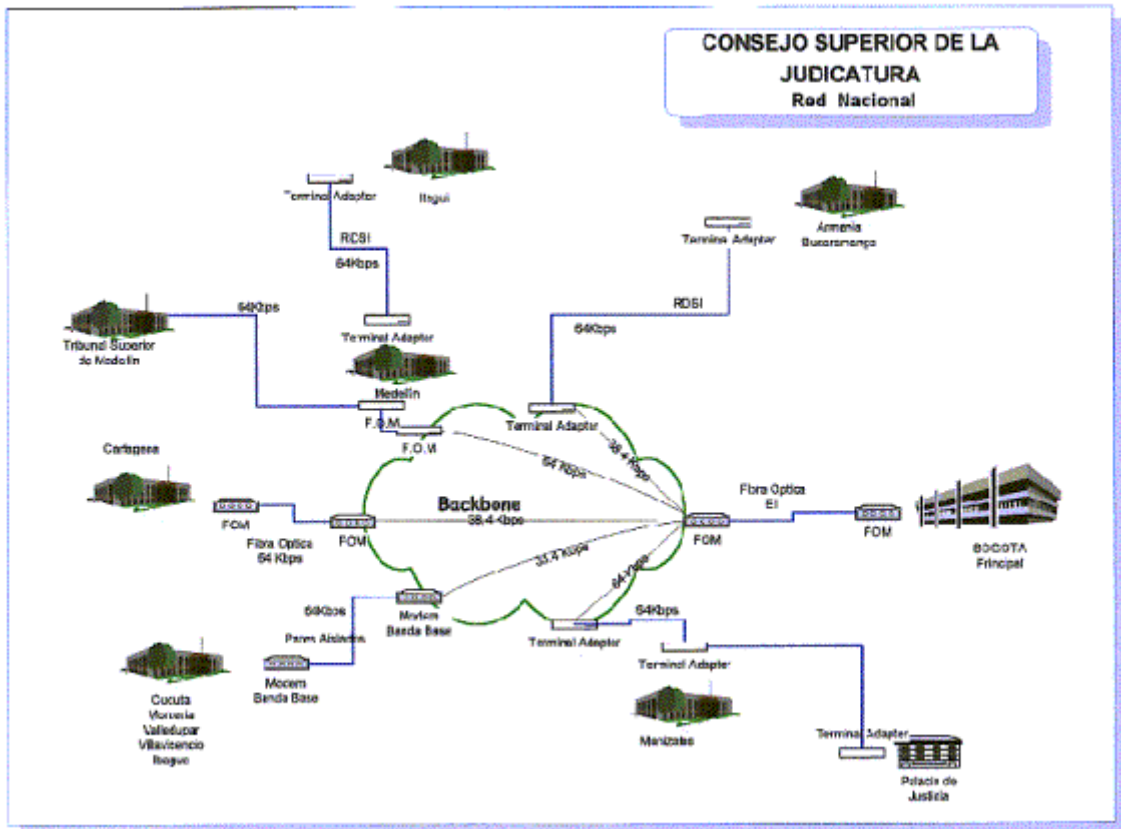


Fig. 1.3 Redes MAN

Características de una Red MAN

Ancho de banda

El elevado ancho de banda requerido por grandes ordenadores y aplicaciones compartidas en red es la principal razón para usar redes de área metropolitana en lugar de redes de área local.

Nodos de red

Las redes de área metropolitana permiten superar los 500 nodos de acceso a la red, por lo que se hace muy eficaz para entornos públicos y privados con un gran número de puestos de trabajo.

Extensión de red

Las redes de área metropolitana permiten alcanzar un diámetro entorno a los 50 kms, dependiendo el alcance entre nodos de red del tipo de cable utilizado, así como de la tecnología empleada. Este diámetro se considera suficiente para abarcar un área metropolitana.

Distancia entre nodos

Las redes de área metropolitana permiten distancias entre nodos de acceso de varios kilómetros, dependiendo del tipo de cable. Estas distancias se consideran suficientes para conectar diferentes edificios en un área metropolitana o campuz privado.

Tráfico en tiempo real

Las redes de área metropolitana garantizan unos tiempos de acceso a la red mínimos, lo cual permite la inclusión de servicios síncronos necesarios para aplicaciones en tiempo real, donde es importante que ciertos mensajes atraviesen la red sin retraso incluso cuando la carga de red es elevada.

Integración voz/datos/vídeo

Adicionalmente a los tiempos mínimos de acceso, los servicios síncronos requieren una reserva de ancho de banda; tal es el caso del tráfico de voz y vídeo. Por este motivo las redes de área metropolitana son redes óptimas para entornos de tráfico multimedia, si bien no todas las redes metropolitanas soportan tráficos isócronos (transmisión de información a intervalos constantes).

Alta fiabilidad

Fiabilidad referida a la tasa de error de la red mientras se encuentra en operación. Se entiende por tasa de error el número de bits erróneos que se transmiten por la red. En general la tasa de error para fibra óptica es menor que la del cable de cobre a igualdad de longitud. La tasa de error no detectada por los mecanismos de detección de errores es del orden de 10⁻²⁰. Esta característica permite a la redes de área metropolitana trabajar en entornos donde los errores pueden resultar desastrosos como es el caso del control de tráfico aéreo.

Alta seguridad

La fibra óptica ofrece un medio seguro porque no es posible leer o cambiar la señal óptica sin interrumpir físicamente el enlace. La rotura de un cable y la inserción de mecanismos ajenos a la red implican una caída del enlace de forma temporal.

Inmunidad al ruido

En lugares críticos donde la red sufre interferencias electromagnéticas considerables la fibra óptica ofrece un medio de comunicación libre de ruidos.

Ventajas y Desventajas de la Red MAN

Ventajas

Una vez comprada, los gastos de explotación de una red privada de área metropolitana, así como el costo de una LAN, es inferior que el de una WAN, debido a la técnica soportada y la independencia con respecto al tráfico demandado.

- Una MAN privada es más segura que una WAN.
- Una MAN es más adecuada para la transmisión de tráfico que no requiere asignación de ancho de banda fijo.
- Una MAN ofrece un ancho de banda superior que redes WAN tales como X.25 o Red Digital de Servicios Integrados de Banda Estrecha (RDSI-BE).

Desventajas

- Limitaciones legales y políticas podrían desestimar al comprador la instalación de una red privada de área metropolitana. En esta situación, se podría usar una red pública de área metropolitana.
- La red de área metropolitana no puede cubrir grandes áreas superiores a los 50 Km. de diámetro.
- La tecnología más extendida para la interconexión de redes privadas de múltiples edificios es FDDI (Fiber Distributed Data Interface; Interfase de Datos Distribuidos por Fibra). FDDI es una tecnología para RAL que es extensible a redes metropolitanas gracias a las características de la fibra óptica que ofrece el ancho de banda y las distancias necesarias en este entorno.

1.3.3 Redes WAN

Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas máquinas se llaman Hosts. Los hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un host a otro. La separación entre los aspectos exclusivamente de comunicación de la red (la

subred) y los aspectos de aplicación (hosts), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos o canales) mueven los bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. Como término genérico para las computadoras de conmutación, les llamaremos enrutadores.

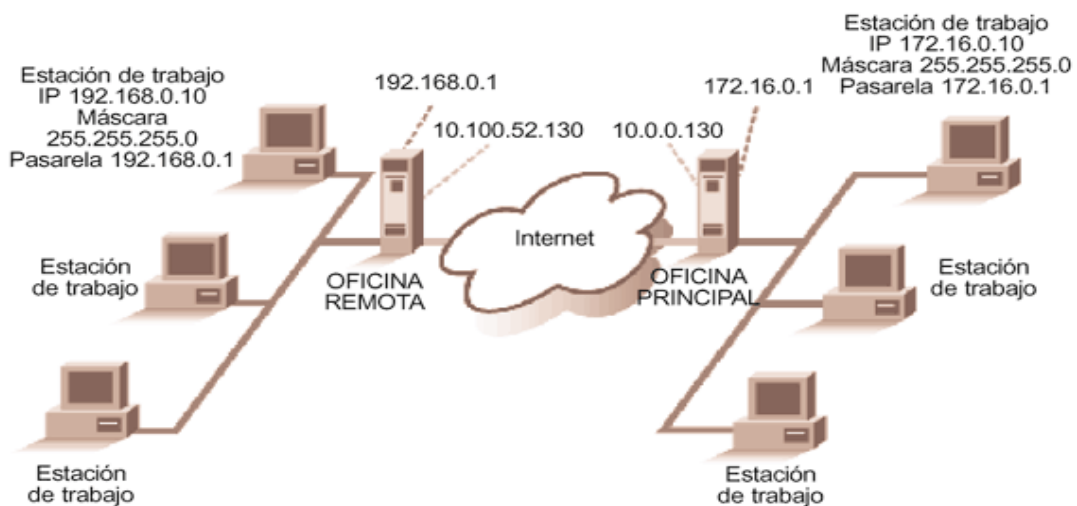


Fig. 1.4 Redes WAN

Características de una Red WAN

Los canales suelen proporcionarlos las compañías telefónicas (como la propia Compañía Telefónica Española), con un determinado coste mensual si las líneas son alquiladas, y un costes proporcional a la utilización si son líneas normales conmutadas.

Los enlaces son relativamente lentos (de 1200 Kbit / s a 1.55Mbit / s).

Las conexiones de los ETD con los ECD son generalmente más lentas (150 bit / s a 19.2 Kbit / s).

Las líneas son de mejor calidad que los canales en las WAN.

Debido a las diferencias entre las redes de área local y las redes de cobertura amplia, sus topologías pueden tomar formas muy diferentes.

La estructura de las WAN tiende a ser más irregular, debido a la necesidad de conectar múltiples terminales, computadores y centros de conmutación. Como los canales están alquilados mensualmente (a un precio considerable), las empresas y organizaciones que los utilizan tienden a mantenerlos lo más ocupados posible. Para ello, a menudo los canales "serpentean" por una determinada zona geográfica para conectarse a los ETD allí donde estén. Debido a eso la topología de las WAN suele ser más irregular.

Ventajas y Desventajas de la Red WAN

Ventajas

- Los ETD y los ECD están separados por distancias que varían desde algunos kilómetros hasta cientos de kilómetros.
- Las líneas son relativamente propensas a errores (si se utilizan circuitos telefónicos convencionales).
- Puede utilizarse un ECD para conmutar entre diferentes configuraciones, pero no tan frecuentemente como en las WAN.

Desventajas

- Pueden ser muy costosas

1.2 Arquitectura de la Red LAN

Introducción.

Las arquitecturas de la red combinada estándares, topologías y protocolos para reducir una red funcional son las que veremos a continuación.

1.2.1 Redes ETHERNET.

Son redes que siguen el estándar 802.3 del IEEE, utiliza el método CSMA/CD de acceso a la red a una velocidad de transferencia de 10Mbits/seg. Utiliza la topología lógica de bus, aunque con ciertos componentes puede utilizar la topología física de estrella.

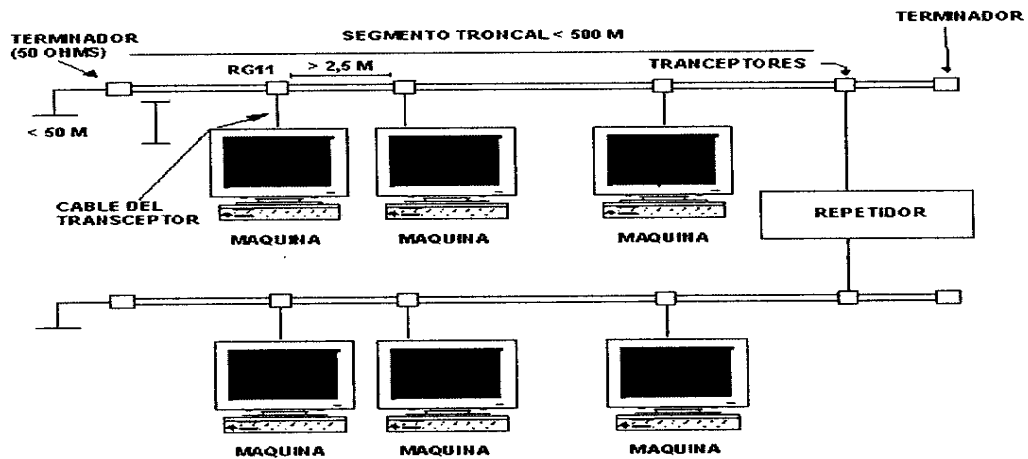


Fig 1.5 Vista previa una red Ethernet

1.2.2 Presentaciones Ethernet.

Ethernet es actualmente la arquitectura de red más popular. Esta arquitectura de banda base usa una topología de bus, usualmente transmite a 10 Mbps, y confía en CSMA/CD (método de acceso) para regular el tráfico en el segmento principal de cable.

El medio de Ethernet es pasivo, lo que permite apagar el ordenador y que no falle a menos que el medio no sea físicamente cortado o esté impropriamente terminado.

La siguiente lista es un resumen de las características de Ethernet:

- **Topología tradicional:** bus lineal
- **Otras topologías:** bus en estrella
- **Tipos de arquitectura:** banda base
- **Método de acceso:** CSMA/CD
- **Especificaciones:** IEEE 802.3
- **Velocidad de transferencia:** 10 Mbps ó 100 Mbps
- **Tipos de cable:** Thicknet, Thinnet, UTP

nivel de red (IP ó IPX) (2 bytes)

- **CRC**

Campo de chequeo de errores para determinar si la trama ha llegado sin ser corrompida. (2 bytes en 16 bits, 4 bytes en 32).

Preámbulo + Destino + Origen + Tipo + Dato + CRC

Las redes Ethernet incluyen una velocidad de cableado y de alternativas de topología.

Los estándares IEEE de 10 Mbps.

Existen 4 diferentes topologías Ethernet de 10 Mbps.

- 10BaseT
- 10Base2
- 10Base5
- 10BaseFL

10BaseT.

En 1990, el comité IEEE publicó la especificación 802.3 para usar Ethernet sobre cable de par trenzado. 10BaseT (10 Mbps, banda base, sobre cable de par trenzado) es una red Ethernet que típicamente utiliza cable UTP (par trenzado no blindado) para conectar ordenadores. Mientras que 10BaseT normalmente usa UTP, los STP (par trenzado blindado) también funcionarán sin cambiar ninguno de los parámetros 10BaseT.

La mayoría de las redes de este tipo están configuradas en un diseño de estrella pero internamente usan un sistema de señalización de bus como las otras configuraciones Ethernet. Típicamente el hub de una red 10BaseT sirve como un repetidor multipuerta y a menudo está localizado en un cuarto de cableado en el edificio.

Cada ordenador está situado en el punto final del cable conectado al hub. Cada ordenador tiene 2 pares trenzados, un par es usado para transmitir y el otro para recibir datos.

La longitud máxima de un segmento 10BaseT es de 100 metros (328 pies) hasta el hub. Los repetidores pueden extender esta longitud de cable. La longitud mínima de cable entre ordenadores es de 2,5 metros (8 pies). Una red 10BaseT puede servir a 1024 ordenadores.

Es fácil hacer movimientos y cambios moviendo un cable en un patch panel. Otros dispositivos en la red no se verán afectados por un cambio en el patch panel, no como una red Ethernet tradicional de bus.

Los patch panel debería ser comprobado para ratios más altos que 10Mbps. Los últimos hubs pueden proporcionar conexiones para segmentos de cable thin y thick Ethernet.

Esta implementación es fácil también convertir cable thick Ethernet a cable de 10BaseT enganchando un mini transceptor (transceiver) a la puerta AUI de cualquier tarjeta de red.

Sumario

- **cable:** Categoría 3, 4 ó 5 UTP.
- **conectores:** RJ-45 al final de los cables.
- **Transceptores:** Cada ordenador necesita uno, algunas tarjetas lo llevan incorporado.
- **Distancia desde el transceptor al hub:** 100 metros máximo.
- **Backbone para los hubs:** Coaxial o fibra óptica para juntar una gran LAN.

- **Ordenadores totales**

por Lan sin componentes

1024 por la especificación .

de conectividad:

10base2.

Esta topología es llamada 10Base2 por la especificación IEEE 802.3 porque transmite a 10 Mbps en banda base y puede llevar una señal aproximadamente 2 veces 100 metros (la distancia actual es 185 metros).

Este tipo de red usa cable coaxial delgado (thin) o thinnet, que tiene una longitud máxima de segmento de 185 metros. Hay también una longitud mínima de cable de 0,5 metros (20 pulgadas). Hay un máximo de 30 ordenadores por segmento de 185 metros.

Los componentes del cableado thinnet son:

- Conectores de barril BNC
- Conectores T BNC
- Terminadores BNC

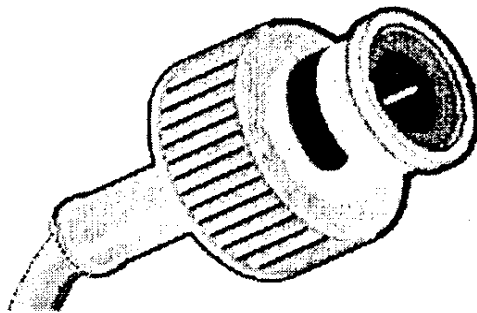


Fig 1.7 Conector BNC

Las redes thinnet generalmente usan una topología de bus local. Los estándares de IEEE para thinnet no permiten un cable transceptor (transceiver) desde un conector T hasta el ordenador. En lugar de eso, se conecta una T directamente a la tarjeta de red.

Se puede usar un conector de barril para unir segmentos de cable thinnet, para extender la longitud total. Es decir si se necesita una longitud de 30 metros, pero tiene un tramo de 25 y otro de 5 m, puede usar un conector de barril para unirlos. Sin embargo, el uso de barriletes debería estar reducido al mínimo porque cada conexión en el cable reduce la calidad de la señal. Una red thinnet es una forma económica de soportar un pequeño departamento o grupo de trabajo. El cable usado para éste tipo de red es:

- Relativamente barato.
- Fácil de instalar.
- Fácil de configurar.

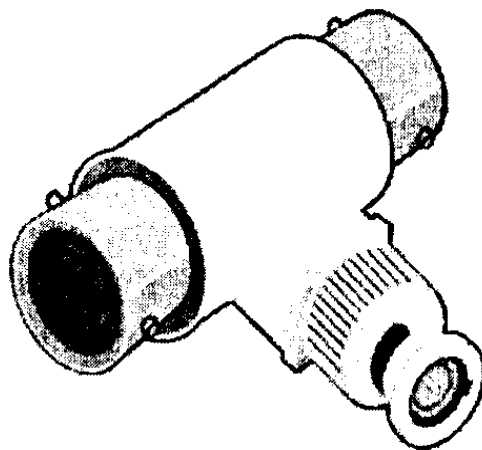


Fig 1.8 Conector T

Una simple red thinnet puede soportar un máximo de 30 nodos (ordenadores y repetidores) IEEE 802.3

La regla 5-4-3

Una red thinnet puede combinar hasta 5 segmentos de cable conectados por 4 repetidores, pero sólo 3 segmentos pueden tener conectadas estaciones. Así que, dos segmentos están sin explotar y son a menudo referidos como enlaces ínter repetidores. Esto se conoce como la regla 5-4-3.

De cada puerta del repetidor puede salir otro cable con 30 PCs. Los segmentos intermedios sirven para incrementar la longitud total de la red.

Debido a que los límites normalmente de Ethernet puede ser demasiado pequeños para un gran negocio, los repetidores se pueden usar para juntar segmentos Ethernet y extender la red a un total de 925 metros.

Sumario 10Base2

- **Latitud máxima de segmento:** 185 m. (607 pies)
- **Conexión de la tarjeta de red:** Conector T BNC
- **Segmentos y Repetidores:** 5 segmentos/4 repetidores
- **Ordenadores por segmento:** 30 ordenadores por segmento
- **Segmentos con ordenadores:** 3 de los 5 segmentos
- **Longitud máxima de la red:** 925 m. (3035 pies)
- **Máximo n° de PCs por red sin Componentes de conectividad:** 1025 por la especificación

10Base5.

La especificación IEEE para esta topología es de 10 Mbps, banda base y segmentos de 500m. (5 de 100 m). También es llamada estándar Ethernet. Esta topología hace uso del cable coaxial thick o Thicknet. Thicknet usa generalmente una topología de bus y puede soportar 100 nodos (estaciones, repetidores, etc.) por segmento Backbone, o segmento troncal (Trunk) es el cable principal desde el que los cables Transceptores (transceivers) están conectados a las estaciones y repetidores. Un segmento Thicknet puede ser de 500m. De largo para una longitud total de red de 2500 m, (8200 pies). Las distancias y tolerancias para el Thicknet son más grandes que las de thinnet.

Los componentes de cableado Thicknet son:

- Transceptores (transceiver) (Transmit and Receive) proporciona comunicación entre el ordenador y el cable principal de LAN y están localizados en los conectores vampiro enganchados al cable.
- Cables Transceiver. El drop cable conecta al transceiver a la tarjeta de red.
- Conector DIX o AUI. Es el conector del cable transceiver.
- N-series conectores, incluyendo N-series conectores tipo barril y N-series terminadores.

Los componentes Thicknet trabajan de la misma forma que lo hacen los thinnet.

La regla 5-4-3 en Thicknet.

Una red Thicknet puede tener un máximo de 5 segmentos Backbone conectados usando repetidores (basado en la especificación IEEE 802.3) de los cuales 3 pueden acomodar ordenadores. La longitud de los cables transceiver no se usa para medir la distancia soportada en el cable; solo se usa la longitud de inicio a fin de cable en sí mismo.

Entre conexiones, el segmento mínimo de cable Thicknet es de 2.5m. (8 pies). Esta medida excluye el cable transceiver. Thicknet fue diseñado para soportar un Backbone para un gran departamento o un edificio entero.

Sumario 10Base5

Máxima longitud de segmento: 500 metros.

- **Transceiver:** conectados al segmentos(en la derivación)
- **Máxima distancia del ordenador Al transceiver:** 50 metros (164 pies)
- **Mínima distancia entre transceiver:** 2,5 metros (8 pies)
- **Segmento trunk y repetidores:** 5 segmentos y 4 repetidores
- **Segmentos que pueden tener ordenadores:** 3 de los 5
- **Longitud máxima total de los segmentos unidos:** 2500 metros (8200 pies)
- **Máximo numero de ordenadores por segmento:** 100 por especificación

Combinando Thicknet y Thinnet.

Es común en las grandes redes combinar Ethernet thci y thin. Thicknet es bueno para Backbones con thinnet como segmentos en ramas. ¿Qué es lo hace que el cable Thicknet sea el cable principal cuando las distancias largas? Se puede recordar que

Thicknet tiene un gran núcleo de cobre y puede, por lo tanto, transportar a más distancia que thinnet.

El transceiver se engancha al cable thicknet y el conector AUI del cable del transceiver se pincha en el repetidor. Los segmentos ramificados de thinnet se conectan a los ordenadores de la red.

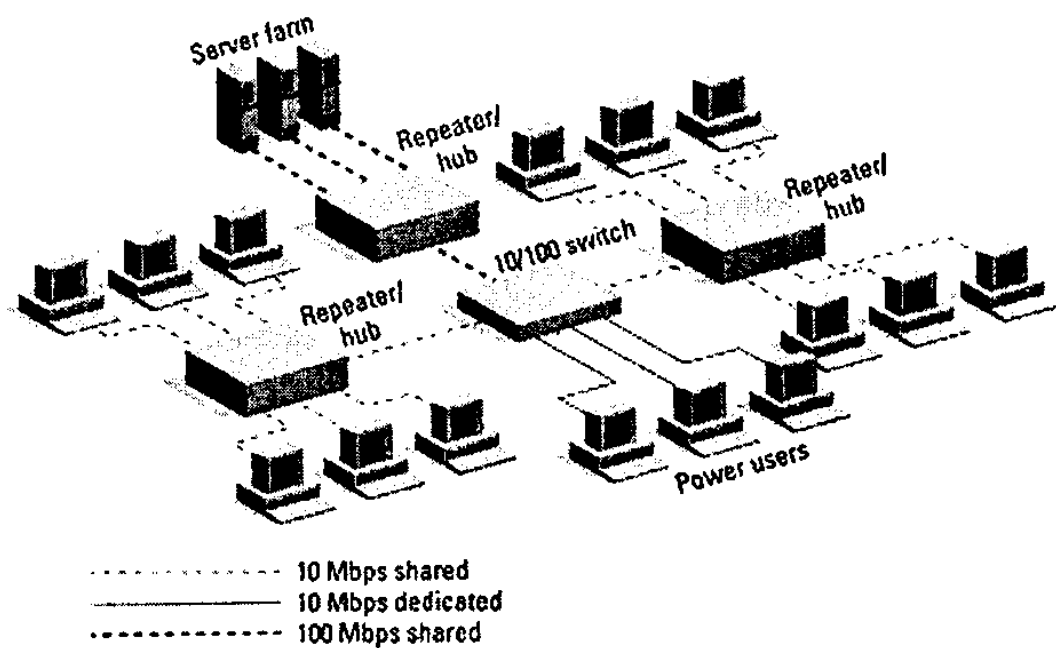


Fig. 1.9 Combinando Thicknet y Thinnet.

10BaseFL.

El comité IEEE publicó una especificación para usar Ethernet sobre cable de fibra óptica. 10BaseFL (10 Mbps, banda base, sobre cable de fibra óptica) es una red Ethernet que usa cable de fibra óptica para conectar ordenadores y repetidores.

La razón primaria para usar 10BaseFL es para que haya un cable largo entre los repetidores, como entre edificios. La máxima distancia para un segmento 10BaseFL es de 2000 metros.

El estándar de 100 Mbps IEEE.

Los nuevos estándares Ethernet están empujando los límites tradicionales más allá del original de 10 Mbps. Estas nuevas capacidades están siendo desarrolladas para manejar aplicaciones de alto ancho de banda como

- CAD (diseño ayudado por ordenador)
- CAM (fabricación asistida por ordenador)
- Video
- Almacenamiento de imágenes y documentos.

Dos estándares Ethernet emergentes que pueden cumplir con el incremento de mandado, son:

- 100BaseVG-AnyLAN Ethernet (de HP)
- 100BaseXEthernet (Fast Ethernet)

Ambos, Fast Ethernet y 100BaseVG-AnyLAN, son como de 5 a 10 veces más rápidos que el estándar Ethernet. Son compatibles con el cableado existente 10BaseT. Este es el método que permitirá actualizaciones Plug and Play desde las instalaciones existentes 10BaseT.

100VGAnyLAN

100VG (Voice Grade-Calidad de Voz) AnyLAN es una tecnología de networking emergente que combina elementos de Ethernet y Token Ring.

Originalmente desarrollado por el comité IEEE 208.12. la especificación 208.12 es un estándar para transmitir tramas Ethernet 802.3 y paquetes Token Ring 802.5

A esta tecnología se la conoce con los siguientes nombres, todos referidos al mismo tipo de red:

- 100VG-AnyLAN
- 100BaseVG
- VG
- AnyLAN

Especificaciones.

Algunas especificaciones actuales son:

- Un ratio de datos mínimo de 100 Mbps
- Capacidad de soportar una topología de estrella en cascada sobre Categoría 3, 4 y 5 de cable de par trenzado y fibra óptica.
- El método de acceso de prioridad en demanda, que permite dos niveles de prioridad (alto y bajo).
- Capacidad de soportar una opción para filtrar individualmente tramas direccionadas al hub para aumentar la privacidad.
- Soporte para tramas Ethernet y paquetes Token Ring.

Topología.

Una red 100VG-AnyLAN está constituida con una topología de estrella con todos los ordenadores conectados a un hub. La red se puede expandir añadiendo hubs hijos al central. Los hubs hijos actúan como ordenadores, para sus hubs padres. Los hubs padres controlan la transmisión de los ordenadores conectados a sus hijos.

- TX Tipo de cable -Cable de par trenzado usando
2 pares de calidad datos
- FX Tipo de cable -Enlace de fibra óptica con dos
Filamentos

Consideraciones de funcionamiento.

Ethernet puede usar varios protocolos de comunicación incluyendo TCP/IP, que trabaja bien en el entorno Unix. Esto hace favorita en las comunidades científicas y académicas.

Segmentación.

Se segmenta cuando hay muchos ordenadores. El funcionamiento de Ethernet puede ser mejorado dividiendo un segmento de estados en dos menos poblados y juntándolos con un bridge o un router. Esto reduce el tráfico en cada segmento, debido a que hay menos ordenadores intentando transmitir en el segmento, mejora el tiempo de acceso.

División de segmentos es una buena táctica si un gran número de nuevos usuarios se están conectando a la red o se incorporan nuevas aplicaciones de alto ancho de banda, como bases de datos o programas de video.

1.2.3 Redes Token Ring.

Fue desarrollada por IBM y adoptada por IEEE como estándar IEEE 802.5 en 1986. Hay placas compatibles de General Instruments, Proteon, 3Com y UngermannBass. Por definición un *token – ring * consiste en un conjunto de estaciones conectadas en cascada formando un anillo (ring) en el que la información es transferida de una estación activa a la siguiente. Cada estación recibe y regenera los bits que recibe, de

forma tal que actúa como repetidor cuando está activa. Cuando la información vuelve a la estación, que originó la transmisión, el mensaje es retirado de circulación.

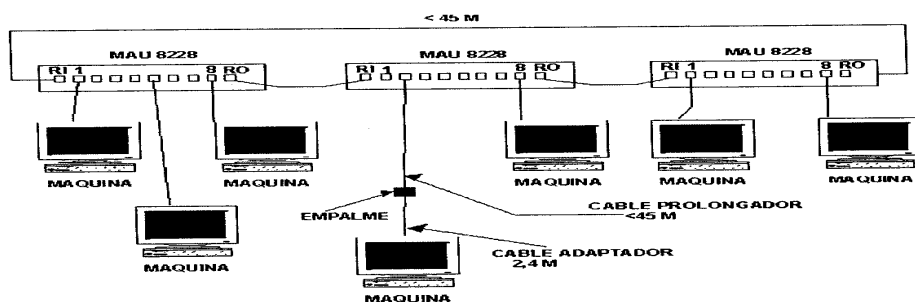


Fig 1.10 Red Token Ring.

La velocidad de transmisión original era de unos 4 Mbits/s, pero existen velocidades de 16 Mbits/s. La codificación es Manchester diferencial.

Cuando se desea armar una red Token Ring, lo intuitivo sería pensar un bus unido por sus extremos. Sin embargo, la topología que aparenta esta red es la de una estrella (se la suele describir como * star – wired ring *). Esto se debe a que el anillo está contenido en un dispositivo denominado 8228 Multistation Access Unit (MAU).

Las máquinas se conectan a las bocas 1 al 8 del 8228 mediante unos cables llamados adaptadores (pues el conector incluido en la placa es destino al del 8228) o par de lóbulo (lobe pair, el nombre surge de considerar a cada * punta * de la estrella como un lóbulo de ella). Si la red tiene más de 8 puestos, se forma un anillo de 8228 conectado con salida de uno (Ring Output, RO) con la entrada del siguiente (Ring Input, RI). Los 8228 poseen un relevador por cada boca; la estación que se conecta, debe activar el relé para insertarse en el anillo.

La LAN Ethernet se utiliza para transportar datos entre dispositivos de red, como por ejemplo, impresoras y servidores de archivos. Ethernet se conoce como una tecnología de medios compartidos, es decir, todos los dispositivos están conectados a los mismos medios de entrega. Medio de entrega es el método utilizado para transmitir y recibir

datos. Por ejemplo, una carta manuscritas puede enviar (transmitir) utilizando uno de varios medios de entrega, tales como el servicio de correo o un fax.

Hay dos formas de cablear el sistema: * small movable cabling system * y * large nonmovable cabling system*.

En el primer caso, se tiene los siguientes límites:

- Hasta 96 estaciones.
- Hasta 12 unidades 8228.
- Distancia máxima entre 8228 y una estación: 45.7 m (150 pies), a los que hay que sumarle 2.4 m (8 pies) del adaptador.
- Distancia máxima entre 8228 y una estación: 45.7 m (150 pies).
- No pasar el cable por exteriores ni por conductos de ventilación, no exponerlos a más de 75 grados Celsius, ni a interferencia eléctrica.
- En segundo caso, se puede conectar hasta 260 estaciones, pero se usa un montaje físico diferente.

La transmisión se efectúa mediante dos pares trenzados, pero hay de diversas clases, definidas por IBM con números de tipo. El tipo 1 posee 2 pares AWG 22 como blindaje. Se usan principalmente para conectar MAUs. El tipo 2 ofrece 2 pares AWG 22 blindados y 4 pares AWG 26 sin blindaje; los pares extras son para conectar el teléfono con el mismo cable. El tipo telefónico sin blindaje. Es una alternativa barata al tipo 1. La ventaja de usar cable tipo 3 es que en muchas empresas donde hay centrales telefónicas internas, quedan pares disponibles, por lo que no hay que hacer un nuevo tendido; la desventaja es que se limitan el alcance y la cantidad de dispositivos que se pueden soportar (72 en vez de 255). El tipo 6 consta de 2 pares de cables (no alambres) de AWG 26 sin blindaje; es flexible y se usan para los alargues entre el cable adaptador y el 8228. el cable 9 consta de dos pares de AWG 26 blindados. Tiene menor alcance

que el tipo 1 (aprox. 66%) pero es más barato. Todos los cables mencionados hasta acá soportan 16 Mbit/s excepto el 3 que llega sólo a 4 Mbit/s. Por último, el tipo 9 no es un cable sino una fibra óptica de 140micrones. Soportan hasta 250 Mbit/s.

Características.

- Las estaciones se conectan a la red a través del receptor.
- La red consiste en un conjunto de repetidores unidos mediante un enlace punto a punto.
- El repetidor es un dispositivo sencillo capaz de recibir datos por un enlace y transmitirlos bit a bit por el otro.
- Los enlaces son unidireccionales.

Su **control del método de acceso** es el Token Passing

Cuando una estación emite un paquete, éste se transmite bit a bit por el anillo y puede ser recibido por el resto de los receptores conectados, pasándose a la propia estación si a ella iba dirigido el paquete.

Para que el anillo sea eficaz se necesitan tres funciones:

- Inserción de datos: los datos son insertados a través del repetidor al anillo bit a bit, después de haber puesto la dirección destino. Los datos se agrupan en paquetes.
- Recepción de datos: si la dirección destino coincide con la estación a la cual sirve el repetidor, este copiará los datos a la unidad. Si no es así, transmiten los datos nuevamente a través del anillo.
- Eliminación de datos: trata de evitar que los paquetes circulen indefinidamente. Los paquetes pueden ser eliminados o bien por el repetidor unido a la estación destino o el repetidor unido a la estación origen.

Uno de los protocolos utilizado es el * **Token Passing** *. Por el anillo circula constantemente un **token** o **testigo**. Cuando una estación quiere transmitir captura el token, lo transforma en token ocupado y empieza a transmitir. En este caso la estación que emite es la encargada de eliminar los paquetes y de generar un nuevo token no ocupado. Tiene un mecanismo de prioridades.

ArcNet.

Fue desarrollada por Datapoint e introducida en 1977, su nombre es la abreviación de Attached Resource Computing Network. La no participación en el comité IEEE 802 dio lugar a que ninguna norma 802 la tenga en cuenta. Sin embargo, cuatro factores contribuyeron a hacerla tan popular que es un estándar de facto:

1. A partir de 1982, se comenzaron a vender los chips, por lo que aparecieron * segundas fuentes * de esta placa (Davong, Nestar, Standard Microsystems, Tiara y Waterloo entre otros).
2. El precio es bastante inferior a Ethernet y Token Ring.
3. Es muy confiable
4. En muchos lugares de EEUU había cableados con coaxial de 93 ohm en estrella provenientes de hosts con terminales IBM 3270. ArcNet permite que al reemplazar las terminales por computadoras el cableado se aproveche.

En su versión original, es una red con topología tipo estrella, con protocolo de pasaje * token *, trabaja en banda base y es capaz de transmitir a 2.5 Mbit/s. La placa ArcNet se conecta con el hub mediante un cable coaxial de 93 ohm RG62. hay dos tipos de hub: pasivos y activos.

Los pasivos consisten en una caja con 4 entradas vinculadas mediante resistores, de valor tal que si tres entradas cualesquiera están terminadas en su impedancia característica. Esta conexión permite adaptar impedancias y evitar reflexiones, pero a costa de una atenuación alta.

Justamente la atenuación limita la distancia máxima entre cada máquina y el hub a 30 m. Un hub activo aparte de los resistores de terminación, tiene amplificadores, por lo que se pueden conectar máquinas hasta 600 m del hub. Los hubs activos pueden ser internos (generalmente de 4 bocas) o externos (generalmente de 8).

Es posible conectar un hub a otro pero se deben respetar estas reglas:

- No se pueden conectar hubs pasivos entre sí.
- Cualquier entrada no usada en un hub pasivo debe llevar un terminador de 93 ohm.
- Ningún cable conectado a un hub pasivo puede tener más de 30 m.
- Un hub activo puede estar conectado a una máquina, a otro hub activo o un pasivo.
- Las bocas no usadas en un hub activo no necesitan un terminador. Pero es conveniente usarlo.
- Tanto los enlaces entre dos hubs activos como los efectuados entre hubs activos y máquinas pueden ser de hasta 600 m.
- Ninguna máquina puede estar a más de 6 m de otra
- No crear ningún lazo
- Para efectuar pruebas entre dos máquinas, no es necesario un hub, se las puede conectar directamente pues las placas posee terminadores internos
- En la actualidad se la puede considerar obsoleta

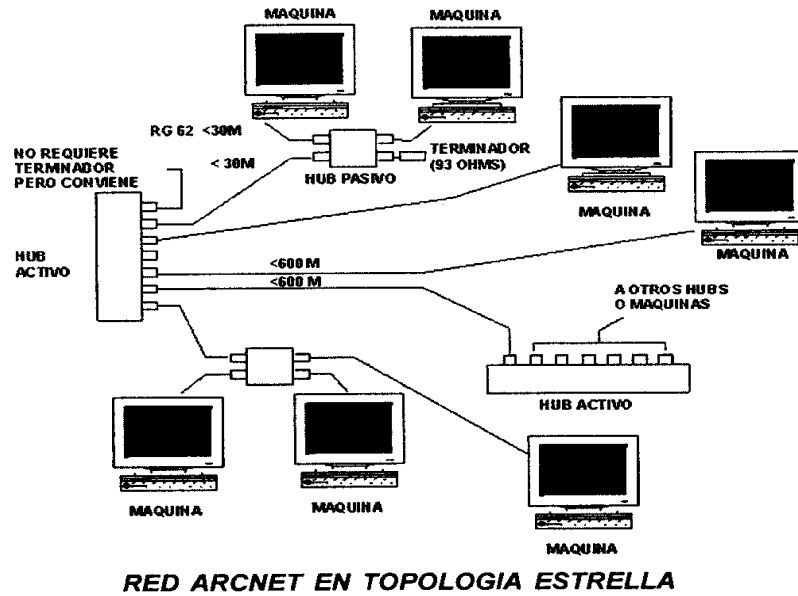


Fig. 1.11. Red Arc Net en topología estrella

Existen versiones de ArcNet para topología bus y para transmisión por par trenzado, pero no se popularizaron. También se desarrolló una versión denominada *plus* de mayor velocidad de transmisión pero hasta el momento su penetración en el mercado es casi nula.

1.3 Cables

En las redes se utilizan dos tipos de cables como son:

- Cable de par trenzado.
- Cable coaxial.

1.3.1 Cable de Par Trenzado.-

El cableado estructurado o par trenzado consiste básicamente en dos o más cables entrelazados entre sí, a manera de trenza, pudiendo ir más o menos protegido.

Constituye el modo más simple y económico de todos los medios de transmisión.

Sin embargo, presenta una serie de inconvenientes. En todo conductor, la resistencia eléctrica aumenta al disminuir la sección del conductor, por lo que hay que llegar a un compromiso entre volumen y peso, y la resistencia eléctrica del cable. Esta última está afectada directamente por la longitud máxima. Cuando se sobrepasan ciertas longitudes hay que recurrir al uso de repetidores para restablecer el nivel eléctrico de la señal.

Tanto la transmisión como la recepción utilizan un par de conductores que, si no están apantallados, son muy sensibles a interferencias y diafonías producidas por la inducción electromagnética de unos conductores en otros (motivo por el que en ocasiones percibimos conversaciones telefónicas ajenas a nuestro teléfono). Un cable apantallado es aquel que está protegido de las interferencias eléctricas externas, normalmente a través de un conductor eléctrico externo al cable, por ejemplo una malla.

Un modo de subsanar estas interferencias consiste en trenzar los pares de modo que las intensidades de transmisión y recepción anulen las perturbaciones electromagnéticas sobre otros conductores próximos.

Con este tipo de cable es posible alcanzar velocidades de transmisión comprendidas entre 2Mbps y 100 Mbps en el caso de las señales digitales. Es el cable más utilizado en telefonía y telex.

Existen varios tipos de cables:

1. Cables STP (Shielded Twisted Pair) de 2 pares trenzados, apantallado par a par y con pantalla global.

2. Cables FTP (Foiled Twisted Pair) de 2 pares trenzados, sin apantallado par a par pero con pantalla global.
3. Cables UTP (Unshielded) de 2 pares trenzados, sin apantallar.

De los mencionados los más importantes son:

Cable UTP.

Es un cable de pares trenzados y sin recubrimiento metálico externo, de modo que es sensible a las interferencias; sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las mismas líneas del cable. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz, disminuyendo sensiblemente, o incluso impidiendo, la capacidad de transmisión.

Es un cable barato, flexible y sencillo de instalar. La impedancia de un cable UTP es de 100 ohmios. En la figura 1.12 se puede observar los distintos pares de un cable UTP.

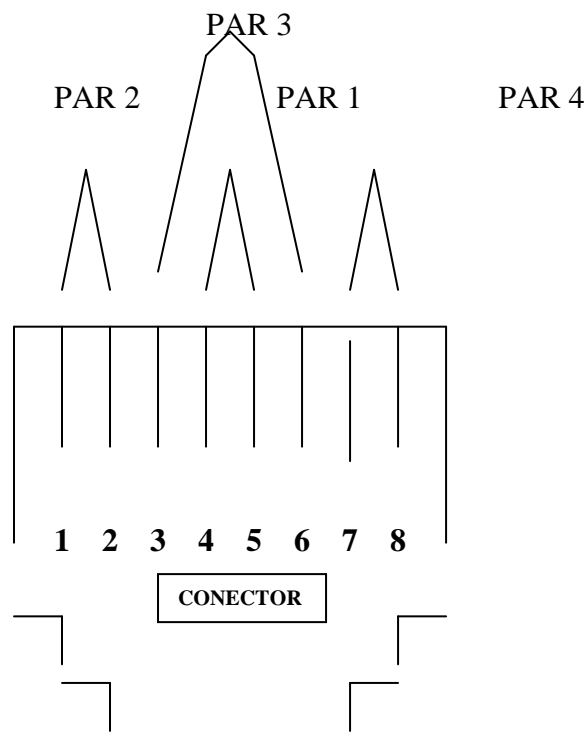


Fig 1.12 Conector

CABLE STP

Este cable es semejante al UTP pero se le añade un recubrimiento metálico para evitar las interferencias externas. Por tanto, es un cable más protegido, pero menos flexible que el primero. El sistema de trenzado es idéntico al del cable UTP.

La resistencia de un cable STP es de 150 ohmios, estos tipos de cables tienen aplicación en muchos campos. El cable de cuatro pares está siendo utilizado como la forma de cableado general en muchas empresas, como conductores para la transmisión telefónica de voz, transporte de datos, etc. RDSI utiliza también este medio de transmisión.

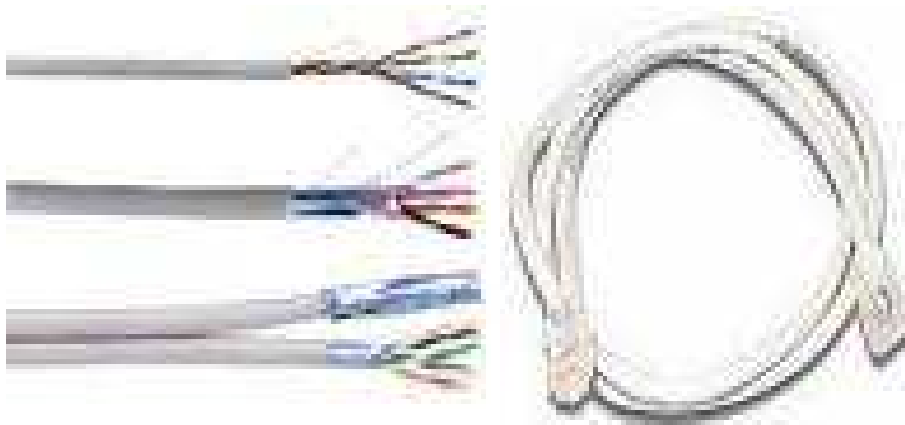


Fig 1.13 Cable UTP

Estructura de cables para un cable UTP en una red Ethernet o para una conexión RDSI, dependiendo de la elección de los pares.

Categorías y clases.

En los cables de pares hay que distinguir dos calificaciones:

- **Las categorías:** Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea, e impedancia.

Categoría 3: el cable UTP categoría 3 y las conexiones del Hardware han sido probados y certificados, para cumplir ciertas especificaciones a una velocidad máxima de 16 Mhz y una agradable velocidad de datos de 10Mbps.

Categoría 4: los productos categorías 4 han sido probados y certificados a una velocidad máxima de 20 Mhz y agradable velocidad de datos de 16 Mbps.

Categoría 5: los productos categoría 5 han sido probados y certificados a una velocidad máxima de 100 Mhz y pueden soportar una velocidad de transmisión de datos de 100 Mbps.

Las categorías 1 y 2: existen pero no son reconocidas en las 568A. Los productos de categoría 2 deben ser usados a una velocidad de transmisión menor a 4Mbps para dato y voz, mientras que la categoría 1 deberá ser usado por voz y velocidad muy pequeña para la transmisión como el RS232.

- **Las clases:** Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de esta características.

Tabla 1.1 Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados

CLASES	Clase A	Clase B	Clase C	Clase D
Ancho de banda	100khz	1 Mhz	20 Mhz	100 Mhz
En categoría 3	2 km	100 m	100 m	no existe
En categoría 4	3km	150 m	150 m	no existe
En categoría 5	3km	160 m	160 m	100 m

Dado que el UTP de categoría 5 es barato y fácil de instalar, se esta incrementando su utilización en las instalaciones de redes de área local con topología en estrella, mediante el uso de conmutadores y concentradores.

La aplicaciones típicas de la categoría 3 son transmisiones de datos hasta 10 Mbps (por ejemplo, la especificación 10BaseT); para la categoría 4, 16 Mbps, y para la categoría 5 (por ejemplo, la especificación 100baseT), 100 Mbps.

En concreto, este cable UTP de categoría 5 viene especificado por las características de la tabla 1.2 (especificaciones TSB - 36) referidas a un cable estándar de 100 metros de longitud.

Tabla 1.2 Nivel de atenuación permitido según la velocidad de transmisión para un cable UTP

Velocidad de transmisión	Nivel de atenuación
4 Mbps	13 dB
10 Mbps	20 dB
16 Mbps	25 dB
100 Mbps	67 dB

Es posible utilizar la lógica de las redes FDI (Fiber Distributed Data Interface) utilizando como soporte cable UTP de categoría 5 en la clase D, ya que la velocidad de transmisión es de 100 Mbps como el FDI. Por esta razón se le suele llamar TPDDI, Twisted Pair Distributed Data Interface.

1.3.2 Cable Coaxial

Esta formado por un hilo conductor de cobre rodeado de un material aislante, además está recubierto de una malla de cobre o aluminio que actúa como conductor y que sirve de protección. Tiene además una capa exterior aislante. Puede ser de **banda base** o de **banda ancha**.

Presenta propiedades mucho más favorables frente a interferencias y a la de longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales.



Fig 1.14 Cable Coaxial

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro.

Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utiliza dos tipos de cable coaxial: fino y grueso.

Cable coaxial delgado o fino

Conector BNC

Diámetro de solo 0.5 cm

El RG-58 es el usado en las redes Ethernet 10BASE2 del estándar 802.3

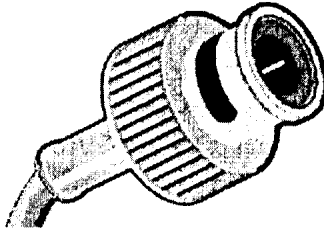


Fig 1.15 Cable fino

Cable coaxial grueso

Conector DIX

Diámetro de 1 cms

Es usado en las redes Ethernet 10BASE5 del estándar 802.3

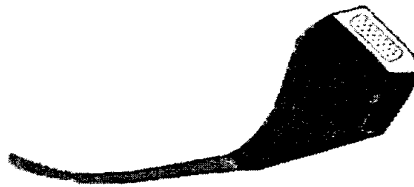


Fig 1.16 Cable grueso

El cable coaxial es capaz de llegar a anchos de banda comprendidos entre los 80 Mhz y los 40 Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de la señal analógica seriamos capaces de tener, como mínimo del orden de 10.000 circuitos de voz.

1.3.3 Conectores

Los conectores normalmente utilizados son:

Conector BNC.

Es el conector utilizado cuando se utiliza cable coaxial. Como ya hemos dicho, la malla de cable coaxial y el hilo central están separados, así que es muy importante que a la hora de grimpar este conector al cable dichos hilos se hallen separados.

Conector RJ-45.

Se utiliza con el cable UTP. Esta compuesto de 8 vías con 8 *muelas* que a la hora de grimpar el conector pinchará el cable y harán posible la transmisión de datos.

Por eso será muy importante que todas las muelas queden al ras del conector.

Conector RJ-49

Igual que el anterior, pero recubierto con una platina metálica para que haga contacto con la que recubre el cable STP.

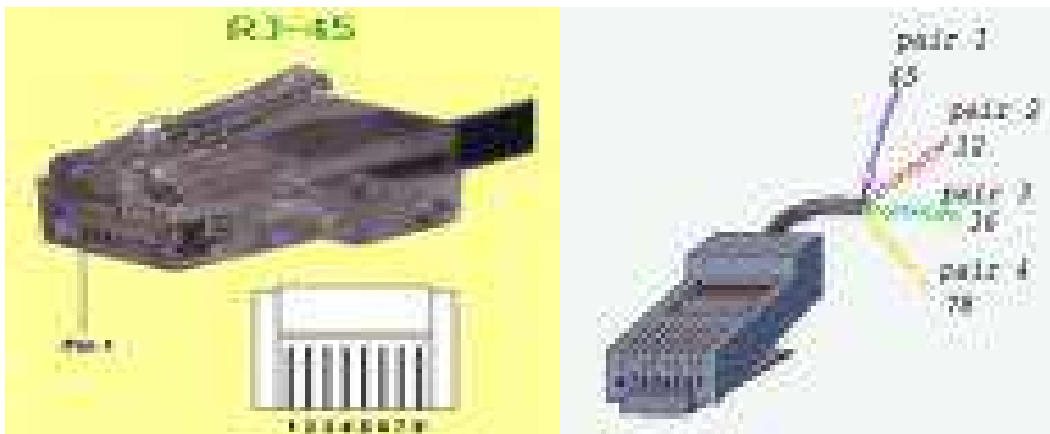
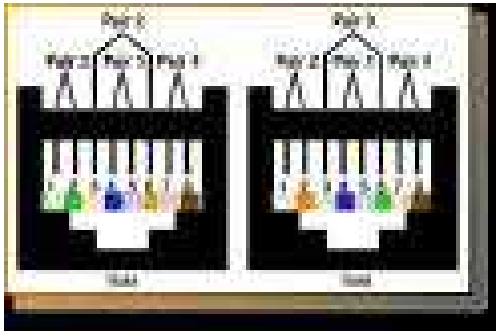


Fig. 1.17 Conectores RJ 45

1.3.4 Ponchada de Cables.

Cuando hablamos de *ponchado*, nos referimos a la relación de colores de los cuatro pares de hilos del cable UTP.



Par 1: T1,R1 = AZUL
 Par 2: T2,R2 = NARANJA
 Par 3: T3,R3 = VERDE
 Par 4: T4,R4 = CAFE

Fig. 1.18 Ponchada de cables

La tabla 1.3 de posición de los pares de hilos para el estándar EIA/TIA 568-A y la figura muestra las posiciones que puede tener un conector.

Tabla 1.3 Código de colores para ponchar

PIN	COLOR / HILO
PAR 3 1	VERDE
PAR 3 2	BLANCO/VERDE
PAR 2 3	BLANCO/NARANJA
PAR 1 4	BLANCO/AZUL
PAR 1 5	AZUL
PAR 2 6	NARANJA
PAR 4 7	CAFÉ
PAR 4 8	BLANCO/CAFÉ

1.4 Dispositivos

1.4.1 Hub.

Conecta físicamente varios ordenadores en red. Físicamente es como un bus con un determinado número de conexiones. Pueden conectarse en cascada. Actúan permitiendo el paso en todas las posibles direcciones



Fig 1.19 HUB

1.4.2 Swicht

Los switches son dispositivos de enlace de datos que, al igual que los puentes permiten que múltiples segmentos físicos de Lan se interconectan para formar una sola red de mayor tamaño.

De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto del swicht como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto del switch funciona como un puente individual y otorga el ancho de banda total del medio de cada host. Los swicht de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de capa dos de dirección MAC destino, los switches pueden realizar

transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación repetidora antes de que la totalidad del paquete ingrese al switch. Esto provoca el nivel de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionaría rápidamente con tráfico, colisiones y virtualmente no ofrecerían ningún ancho de banda. Al dividir redes de gran tamaño en unidades autónomas, los puentes y los switches ofrecen varias ventajas.

Un puente, o switch, reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que solo se envía un solo porcentaje de tráfico los puentes y los switch amplían la longitud efectiva en una LAN. Permitiendo la conexión de estaciones distantes que anteriormente no están permitidas.

Aunque los puentes y los switch comparten los atributos los más importantes todavía existen varias diferencias entre ellos los switch son significativamente más veloces porque realizan la conmutación por hardware mientras que los puentes los hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN de 100 Mbps se pueden conectar mediante un switch estos pueden soportar densidades de puerto más altas que los puentes algunos switch soportan la conmutación por el método cut-through que reduce la latencia y las demoras de la red. Mientras que los puentes soportan solo la conmutación de tráfico de guardar y enviar.

Por último los switch reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.



Fig 1.20 SWICHT

1.4.3 Repetidores.

Este dispositivo es el más rápido. Se usa para extender las longitudes físicas de las redes, pero no contiene inteligencia para funciones de enrutamiento. Un repetidor se utiliza cuando dos segmentos están acercando sus longitudes físicas máximas, las cuales son limitadas en cableado.

Los repetidores permiten interconectar redes iguales actuando únicamente como repetidor y amplificador.

Se utilizan principalmente para extender ,1a distancia máxima de las LAN y unir distintas Lan entre sí.

Sus características son:

- Elemento no inteligente, no analiza la información.
- Transmisión transparente
- No realiza filtrado de trama

- No aísla ningún segmento: si dos estaciones quieren transmitir a la vez sus paquetes colisionarán.

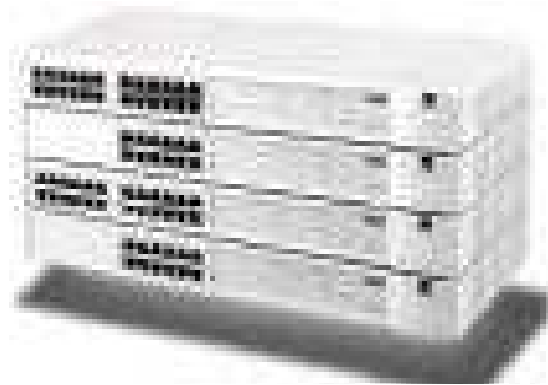


Fig 1.21 Repetidores

1.4.4 Bridge o Puente

Surge de la necesidad de conectar varias redes entre si. Realizan la conexión a **nivel de enlace**.

Enlaza Redes LAN con diferentes protocolos o topologías.

Utilizan direcciones físicas, por lo que filtran el tráfico de paquetes de información en función de una tabla de **direcciones físicas**, determinando por cual de sus puertos pasa, o si no pasa.

Tienen varias salidas o puertos, lo que permite enlazar distintas redes LAN entre si. Analizan cada bloque, buscando por la dirección física a la que va dirigido, hacia que puerto debe dejar pasar a ese bloque, pudiendo llegar a no dejar pasar una trama si no corresponde a ninguna de las direcciones que tiene asignadas en su tabla de direcciones.

De esta forma aumentan el rendimiento de cada una de las redes que el puente separa.

Solucionan los problemas de colisión.

Trabaja en las capas físicas y de enlace de datos del modelo de referencia OSI, no cuida que los protocolos de red estén en uso, sólo prueba la transferencia de paquetes entre las redes. Con el empleo de un puente la información se intercambia entre los nodos por medio de direcciones físicas. El puente normalmente se utiliza para dividir una gran red dentro de área pequeña, con lo que se reduce la carga de tráfico y se incrementa el rendimiento. Algunos modelos cuentan con 2 o más puertos LAN o una combinación de puerto de LAN y WAN.

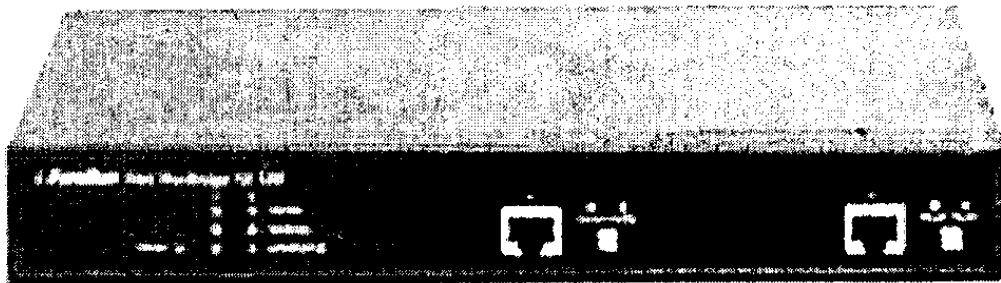


Fig 1.22 Puente

1.4.5 Router o Enrutador

Este dispositivo se emplea para traducir la información de una red a otra. La información se intercambia mediante direcciones lógicas. Funciona en la capa de red del modelo de referencia OSI; por lo que aunque un enrutador tiene acceso a la información física sólo se intercambia información lógica. Físicamente puede recibir dos o más puertos LAN, o una combinación de puertos LAN y WAN.

Realizan una función parecida a los puentes, pero decidiendo hacia donde direcciona cada paquete en función de las direcciones lógicas de red y de algunas variables de la

red, como puede ser la densidad de ocupación de los caminos posibles, buscando agilizar al máximo el tráfico.

Puede seleccionar rutas distintas para dos paquetes que vayan al mismo destino, buscando agilizar el tráfico en la red. Esta decisión la realizará según los protocolos de decisión que se utilizan.

Puede tener varias direcciones IP, una para cada una de las redes a las que esta conectado.



Fig 1.23 Enrutador

1.4.6 Pasarela o Gateways

Cuando se necesita comunicar redes de diferentes clases, como un red de computadoras mainframe de IBM a una red de PCs, nos encontramos que es necesario reempaquetar los datos completamente. No solo es necesario modificar las direcciones a las cuales se dirigen los paquetes, sino que puede ser necesario convertir los datos para que la red destino pueda utilizarlos.

Funcionamiento de los Bridge y Routers

Veamos como funcionan los bridge y los routers con un ejemplo:

Tenemos dos redes LAN independientes, pero conectadas entre sí. Según se conecten a través de un bridge o un router su funcionamiento se presentará de la siguiente forma.

Queremos enviar un paquete desde la computadora de dirección física A-1, de la LAN 1, a la computadora de dirección física B-2, de la LAN 2. En primera instancia, el paquete llegará a todas las computadoras de la LAN 1 y al bridge o router que esté conectado a esta LAN.

Si ambas LAN se conectan con un bridge, será a nivel de enlace donde se determinará si el paquete pasa o no a la otra LAN.

La trama que se prepara a nivel de enlace lleva las direcciones físicas de origen y de destino. Si en la tabla de direcciones del bridge se encuentra la dirección destino, el paquete pasará a la LAN 2. En esta LAN el paquete volverá a llegar a todas las computadoras, pero solo la computadora de dirección física destino, la B-2, recibirá el paquete.

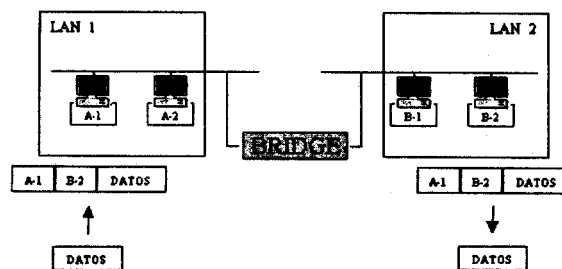


Fig 1.24 Conexión de un Bridge

Si ambas LAN se conectan por medio de un router, su funcionamiento es diferente.

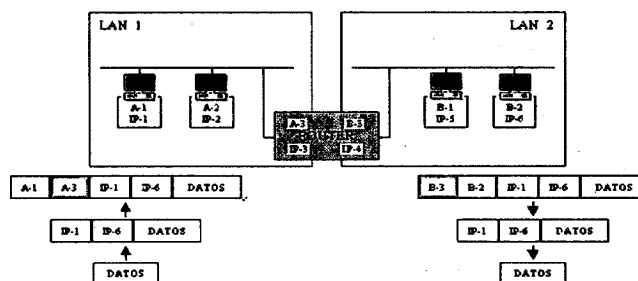


Fig 1.25 Conexiones entre Routers y Bridge

En la computadora origen se determina como dirección IP destino del paquete (nivel red) la correspondiente a la computadora B-2, pero la dirección física destino que se determina en la trama (nivel enlace) será la correspondiente al puerto de entrada del router, en este caso A-3. El paquete llegará a todas las computadoras de la LAN 1 y al router a ella conectada.

Cuando el paquete llega al router, la trama es cambiada y las direcciones origen (A-1) y destino (A-3) son sustituidas por las correspondientes al puerto del router (B-3) y a la computadora a la que corresponde la dirección IP que lleva el paquete como dirección IP destino (B-2). Con estas nuevas direcciones físicas origen y destino el paquete es introducido a la LAN 2, llegando a todas las computadoras que la integran, pero solo la computadora cuya dirección física coincide con la dirección destino lo recibe.

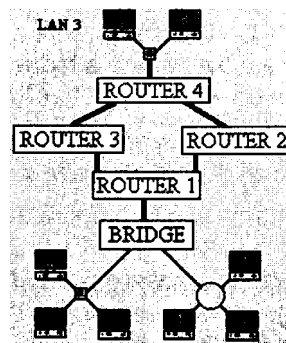


Fig. 1.26 Conexiones entre Bridge y Routers

1.5 Estándares y Protocolo

Para facilitar la fabricación de equipos y asegurar su interconexión, surgió la necesidad de definir normas que fueran reconocidas internacionalmente. Estos estándares fueron definidos por ciertas organizaciones internacionales entre las que cabe destacar:

- **ISO (International Standards Organization)** , Ha desarrollado un modelo 'de referencia para las redes de ordenadores conocido como OSI (Open Systeminterconnect). Su representante estaunidense es ANSÍ
- **CCITT (Consultive Committe on Internationat Telegraphy and Telephony)** Desarrolló el estándar X.25, X.400, X.500 y X.29, que han tenido su mayor impacto en las redes WAN.
- **IEEE (Institute of Electrical and Electronic Engineers).** Ha desarrollado él proyecto 802.

Definimos como **protocolo de comunicaciones** al conjunto de normas, convenciones y procedimientos que regulan la comunicación de datos y la compartición de procesos entre diferentes equipos, totalmente o en alguno de sus aspectos.

Estándares

El Modelo OSI

La organización ISO definió siete niveles funcionales, contemplando una parte de los elementos afectados al estudiar la comunicación entre computadoras.

Cada nivel se sustenta en el inferior a manera de pirámide. Los niveles son:

7. Nivel de APLICACIÓN
6. Nivel de PRESENTACIÓN
5. Nivel de SESIÓN
4. Nivel de TRANSPORTE
3. Nivel de RED
2. Nivel de ENLACE

1. Nivel FÍSICO

Nivel de Aplicación

Nivel 7, el nivel más alto del modelo OSI, es el nivel de Aplicación. (Donde se ejecuta la aplicación) Sirve como ventana para que los procesos de aplicación accedan a los servicios de red. Esta capa representa los servicios que directamente soportan las aplicaciones de usuario, como software para transferencia de ficheros, para acceso a bases de datos y para e-mail. Los niveles más bajos soportan esas tareas interpretadas en el nivel de aplicación. El nivel de Aplicación maneja los accesos generales a la red, control de flujo y recuperación de errores.

Nivel de Presentación

Nivel 6, el nivel de Presentación, determina el formato usado para intercambiar datos entre ordenadores de red. Puede ser llamado el nivel traductor (Conversación). En el ordenador que envía, este nivel traduce datos desde un formato enviado hacia abajo por el nivel de Aplicación dentro de un comúnmente reconocido, forma o intermediario. En el ordenador que recibe, este nivel traduce el formato intermediario en un formato útil para el nivel de Aplicación de ese ordenador. El nivel de Presentación es responsable de la conversión de protocolo, traducción de los datos, de encriptar los datos, cambiar o convertir el set de caracteres y expandir los comandos gráficos. El nivel de Presentación también maneja compresión de datos para reducir el número de bits que necesitan ser transmitidos. Una utilidad conocida como Redirector opera en éste nivel. El propósito del Redirector es redirigir las operaciones de input/output a recursos en un servidor.

Nivel de Sesión

Nivel 5, el nivel de Sesión, permite a dos aplicaciones en diferentes ordenadores establecer, usar, y finalizar una conexión llamada sesión. Este nivel desempeña reconocimiento de nombre y las funciones, como seguridad, necesarias para permitir a dos aplicaciones comunicarse a través de la red. El nivel de Sesión provee sincronización entre tareas de usuario situando checkpoints en la corriente de datos. De esta forma, si la red falla, sólo el dato después del último checkpoint tiene que ser retransmitido. Este nivel también implementa diálogo de control entre procesos de comunicación, regulando qué lado transmite, cuando y cuan largo, y así sucesivamente.

Nivel de Transporte

Nivel 4, el nivel de Transporte, proporciona un nivel de conexión adicional, inferior al del nivel de Sesión. El nivel de Transporte asegura que los paquetes son transmitidos libres de error, en secuencia y sin pérdidas o duplicaciones. Este nivel reempaqueta mensajes, dividiendo mensajes largos en varios paquetes y juntando pequeños paquetes juntos en otro paquete. Esto permite que los paquetes sean transmitidos eficientemente por la red. En el punto de recepción, el nivel de Transporte desempaqueta los mensajes, reensambla los mensajes originales y típicamente envía un reconocimiento de recepción.

El nivel de Transporte proporciona control de flujo, manejo de errores y está involucrado/envuelto en solventar los problemas concernientes a la transmisión y recepción de paquetes.

Nivel de Red

Nivel 3, el nivel de Red, es responsable de direccionar mensajes y traducir direcciones lógicas y nombres en direcciones físicas. Este nivel también determina la ruta desde el origen al ordenador destino. Determina que camino deberían tomar los datos basado en las condiciones de la red, prioridad del servicio y otros factores. También maneja

problemas de tráfico en la red, como packet switching, enrutamiento y control de congestión de datos.

Si la tarjeta de red en el router no puede transmitir un pedazo (un trozo) de datos tan largo como lo envía el ordenador, el nivel de Red en el router lo compensa rompiendo el dato en pequeñas unidades. En el ordenador destino, el nivel de Red reensambla los datos.

Nivel de Enlace

Nivel 2, el nivel de Enlace, envía tramas de datos desde el nivel de Red al nivel Físico (Comunicación entre dos máquinas). En el lado receptor, empaqueta los bits en crudo desde el nivel Físico en tramas de datos. Una trama de datos es una estructura organizada y lógica en la que los datos pueden ser situados. En una trama de datos simple, el ID del emisor representa la dirección del ordenador que está enviando la información; el ID del destinatario representa la dirección del ordenador al que se está enviando la información. La información de control es usada para el tipo de trama, enrutamiento e información de segmentación. Dato es la información en sí misma. El chequeo de redundancia cíclica CRC representa corrección de errores e información de verificación para asegurar que la trama de datos es recibida propiamente.

El nivel de Enlace es responsable de proporcionar transferencia libre de errores de las tramas desde un ordenador a otro a través del nivel Físico. Esto permite al nivel de Red asumir virtualmente transmisiones libres de errores sobre la conexión de red. Generalmente, cuando el nivel de Enlace envía una trama, espera un acuse de recibo desde el receptor. El nivel de Enlace del receptor detecta cualquier problema con la

trama que pueda haber ocurrido durante la transmisión. Las tramas que no obtuvieron acuse de recibo, o las que fueron dañadas durante la transmisión, son reenviadas.

Nivel físico

Nivel 1, el nivel más bajo del modelo OSI, es el nivel Físico. Este nivel transmite la corriente no estructurada de bits en crudo sobre un medio físico (como es el cable de red). El nivel Físico relaciona las interfaces eléctricas, ópticas, mecánicas y funcionales con el cable. El nivel Físico también transporta las señales que transmiten datos, generadas por todos los niveles más altos.

El nivel Físico es responsable de transmitir bits (ceros y unos) de un ordenador a otro. Los bits en si mismos no tienen un significado definido en éste nivel. Este nivel define 'en codificación' de datos (data encoding) y sincronización de bit, asegurando que cuando un host transmisor envía un bit 1, se recibe como un bit 1, no un bit 0. Este nivel también define cuan larga es la duración de un bit y cómo cada bit es trasladado en el impulso apropiado eléctrico u óptico para el cable de red.

Cualquier comunicación en red usa todos los niveles, aunque algunos puedan estar en blanco.

Ante la necesidad de definir ciertos estándares de LAN la IEEE inició un proyecto conocido como 802 (Feb. 1980) Estuvo en desarrollo más o menos a la vez que el estándar ISO y ambos compartieron información que resultó en dos modelos compatibles.

El proyecto 802 definió los estándares de red para los componentes físicos de una red, la tarjeta de red y el cable, que son tenidos en cuenta por el nivel Físico y el de Enlace del modelo OS1.

Esos estándares, llamados especificaciones 802, tienen varias áreas de responsabilidad incluyendo:

- Tarjetas de red
- Componentes de WAN
- Componentes usados para crear redes de par trenzado y coaxial.

Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transmiten datos por el medio físico. Esto incluye conexión, mantenimiento y desconexión de dispositivos de red.

Categorías IEEE 802

El estándar de red 802 define 12 categorías que pueden ser identificadas por su número 802 como sigue:

802.1 Internetworking

802.2 Lógico Link Control (LLC)

802.3 CSMA/CD (Ethernet) Múltiple acceso de Detección de Portadora con Detección de Colisión.

802.4 Token Bus LAN

802.5 Token Ring LAN

802.6 Metropolitan Área Network (MAN)

802.7 Broad band Technical Advisory Group.

802.8 Fiber-Optic Technical Advisory Group.

802.9 Redes con Voz y Datos integrados.

802.10 Seguridad de red.

802.11 Redes sin hilos

802.12 LAN con Acceso de Prioridad de Demanda, 100 Base VG-Any Lan.

Mejoras al Modelo OSI

Los dos niveles OSI más bajos, el nivel Físico y el de Enlace de Datos, definen cómo múltiples ordenadores pueden usar simultáneamente la red sin interferir unos con otros.

El proyecto IEEE 802 trabajó con las especificaciones en esos dos niveles para crear las que han definido los entornos de LAN dominantes.

El comité de los estándares 802 decidió que se necesitaba más detalle en el nivel de Enlace.

Dividieron este nivel en dos subniveles:

- **Subnivel superior: LLC (Logical Link Control)** Control de error y flujo, control de enlace lógico. Proporciona un servicio de enlace de datos a los niveles superiores de la pila de niveles OSI.
- **Subnivel inferior: MAC (Media Access Control)** Control de acceso al medio. Proporciona el acceso compartido al nivel físico de la red.

Subcapa de Control de Enlace Lógico (Logical Link Control LLC)

Esta capa maneja la comunicación de enlace de datos y define el uso de puntos de interface lógica, llamados SAPs (access points puntos de acceso). Otros ordenadores pueden referirse y usar SAPs para transferir información desde la subcapa LLC (Logical Link Control) a los niveles OSI superiores. Esos estándares están definidos por 802.2.

La subcapa MAC es la más baja de las dos, proporcionando acceso compartido para las tarjetas de red de los ordenadores al nivel Físico.

Subcapa de Control de Acceso al Medio (MAC-Media Access Control)

La capa MAC - Media Access Control comunica directamente con la tarjeta de red y es responsable de repartir datos libres de errores entre dos ordenadores en la red.

Las categorías 802.3,802.4,802.5 y 802.12 definen estándares para esta subcapa y el nivel 1 OSI, el nivel Físico.

Protocolo

Un protocolo es el conjunto de normas para comunicar dos o más entidades (objetos que se intercambian información). Son reglas y procedimientos para comunicarse. Por ejemplo, los diplomáticos de un país se adhieren al protocolo para que les guíe en la relación con los diplomáticos de otros países. El uso de las reglas de comunicación se aplica de la misma manera en el entorno de los ordenadores. Cuando varios ordenadores están en red, las reglas y procedimientos técnicos que gobiernan su comunicación e interacción se llaman protocolos.

Los elementos que definen un protocolo son:

- **Sintaxis:** formato, codificación y niveles de señal de datos.
- **Semántica:** información de control y gestión de errores.
- **Temporización:** coordinación entre la velocidad y orden secuencia) de las señales.

Pero, además de esto, hay 3 puntos a tener en cuenta cuando se piensa en protocolos en un entorno de red:

1. Hay varios protocolos. Mientras cada protocolo permite comunicaciones básicas, tienen propósitos diferentes y realizan tareas diferentes. Cada protocolo tiene sus propias ventajas y restricciones.
2. Algunos protocolos trabajan en varios niveles OSI. El nivel en el que trabaja un protocolo describe su función.

Por ejemplo, un cierto protocolo trabaja en el nivel Físico, significando que el protocolo en ese nivel asegura que el paquete de datos pasa a través de la tarjeta de red y sale al cable.

3. Varios protocolos pueden trabajar juntos en los que es conocido como un stack de protocolos, o suite.

Igual que la red incorpora funciones en cada nivel del modulo OSI, diferentes protocolos también trabajan juntos a diferentes niveles en un único stack de protocolos. Los niveles en el stack de protocolos o corresponden con los niveles del modelo OSI. Tomados juntos, los protocolos describen la totalidad de funciones y capacidades del stack.

1.5.1 Como Trabajan los Protocolos

La totalidad de la operación técnica de transmitir datos por la red tiene que ser rota en pasos discretos y sistemáticos. En cada paso, ciertas acciones tienen lugar porque no lo tienen en cualquier otro paso. Cada paso tiene sus propias reglas y procedimientos, o protocolo. Los pasos tienen que ser llevados a cabo en un orden consistente que es el mismo en cada ordenador de la red. En el ordenador emisor, esos pasos tienen que ser cumplidos desde arriba abajo. En la máquina receptora, los pasos se llevarán a cabo desde abajo a arriba.

El ordenador emisor

En el ordenador emisor, el protocolo:

- Rompe el dato en secciones más pequeñas, llamadas paquetes, que el protocolo pueda manejar.
- Añade información de direccionamiento a los paquetes para que el ordenador de destino en la red pueda saber que el dato le pertenece.

- Prepara el dato para la transmisión actual a través de la tarjeta de red y fuera, por el cable.

El ordenador receptor

En el ordenador receptor, un protocolo lleva a cabo la misma serie de pasos en orden inverso.

El ordenador receptor:

- Retira los datos del cable.
- Introduce los paquetes de datos en el ordenador a través de la tarjeta de red.
- Limpia los paquetes de datos, de toda la información de transmisión añadida por el ordenador emisor.
- Copia el dato desde los paquetes a un buffer para reensamblarlos.
- Pasa los datos reensamblados a la aplicación en una forma utilizable. Ambos, el emisor y el receptor necesitan realizar cada paso de la misma forma para que el dato parezca el mismo cuando se recibe que cuando se envió.

Por ejemplo, dos protocolos podrían romper el dato en paquetes y añadir información varia de secuencia, "Timing" y chequeo de error, pero cada uno lo podría hacer de diferente forma. Por lo tanto, un ordenador usando uno de esos protocolos no seria capaz de comunicarse con éxito con un ordenador utilizando el otro protocolo.

Características de un Protocolo

Las características más importantes de un protocolo son:

- 1.- Directo/indirecto:** los enlaces punto a punto son directos pero los enlaces entre dos entidades en diferentes redes son indirectos ya que intervienen elementos intermedios.

2.- Monolítico/estructurado:

monolítico es aquel en que el emisor tiene el control en una sola capa de todo el proceso de transferencia. En protocolos estructurados, hay varias capas que se coordinan y que dividen la tarea de comunicación.

3.- Simétrico/asimétrico: los simétricos son aquellos en que las dos entidades que se comunican son semejantes en cuanto a poder tanto emisores como consumidores de información. Un protocolo es asimétrico si una de las entidades tiene funciones diferentes de la otra (por ejemplo en clientes y servidores).

4.- Normalizado/no normalizado: los no normalizados son aquellos creados específicamente para un caso concreto y que no va a ser necesario conectarlos con agentes externos. En la actualidad, para poder intercomunicar muchas entidades es necesaria una normalización.

1.5.2 Funciones del Protocolo

1. Segmentación y ensamblado: generalmente es necesario dividir los bloques de datos en unidades pequeñas e iguales en tamaño, y este proceso se le llama segmentación. El bloque básico de segmento en una cierta capa de un protocolo se le llama PDU (Unidad de datos de protocolo). La necesidad de la utilización de bloque es por:

- La red sólo admite la transmisión de bloques de un cierto tamaño.
- El control de errores es más eficiente para bloques pequeños
- Para evitar monopolización de la red para una entidad, se emplean ataques pequeños y así una compartición de la red.
- Con bloques pequeños las necesidades de almacenamiento temporal son menores.

Hay ciertas desventajas en la utilización de segmentos:

- La información de control necesaria en cada bloque disminuye la eficiencia en la transmisión.
- Los receptores pueden necesitar interrupciones para recibir cada bloque, con lo que en bloques pequeños habrá más interrupciones.
- Cuantas más PDU, más tiempo de procesamiento.

2. Encapsulado: se trata del proceso de adherir información de control al segmento de datos. Esta información de control es el direccionamiento del emisor/ receptor, código de detección de errores y control de protocolo.

3. Control de conexión: hay bloques de datos sólo de control y otros de datos y control. Cuando se utilizan diagramas, todos los bloques incluyen control y datos ya que cada PDU se trata como independiente. En circuitos virtuales hay bloques de control que son los encargados de establecer la conexión del circuito virtual. Hay protocolos más sencillos y otros más complejos, por lo que los protocolos de los emisores y receptores deben de ser compatibles al menos. Además la fase de establecimiento de conexión (en circuitos virtuales) está la fase de transferencia y la de corte de conexión. Si se utilizan circuitos virtuales habrá que numerar los PDU y llevar un control en el emisor y en el receptor de los números.

Entrega ordenada: el envío de PDU puede acarrear el problema de que si hay varios caminos posibles, lleguen al receptor PDU desordenados o repetidos, por lo que el receptor debe de tener un mecanismo para reordenar los PDU. Hay sistemas que tienen un mecanismo de numeración con módulo algún número; esto hace que el módulo sean lo suficientemente alto como para que sea imposible que haya dos segmentos en la red al mismo tiempo y con el mismo número.

Control de flujo: hay controles de flujo de parada y espera o de ventana deslizante. El control de flujo es necesario en varios protocolos o capas, ya que el problema de saturación del receptor se puede producir en cualquier capa del protocolo.

Control de errores: generalmente se utiliza un temporizador para retransmitir una trama una vez que no se ha recibido confirmación después de expirar el tiempo del temporizador. Cada capa de protocolo debe tener su propio control de errores.

Direccionamiento: cada estación o dispositivo intermedio de almacenamiento debe tener una dirección única.

A su vez, en cada terminal o sistema final puede haber varios agentes o programas que utilizan la red, por lo que cada uno de ellos tiene asociado un puerto. Además de estas direcciones globales, cada estación o terminal de una subred debe tener una dirección de subred (generalmente en el nivel MAC).

Hay ocasiones en las que se usa un identificador de conexión; esto se hace así cuando dos estaciones establecen un circuito virtual y a esa conexión la numeran (con un identificador de conexión conocido por ambas). La utilización de este identificador simplifica los mecanismos de envío de datos ya que por ejemplo es más sencillo que el direccionamiento global. Algunas veces se hace necesario que un emisor emita hacia varias entidades a la vez y para eso se les asigna un direccionamiento similar a todas.

Multiplexación: es posible multiplexar las conexiones de una capa hacia otra, es decir que de una única conexión de una capa superior, se pueden establecer varias conexiones en una capa inferior (y al revés).

Servicios de transmisión: los servicios que puede prestar un protocolo son:

- Prioridad: hay mensajes (los de control) que deben tener prioridad respecto a otros.

Grado de servicio: hay datos que deben retardarse y otros acelerarse (vídeo).

- Seguridad.

1.5.3 Tipos de Protocolos

En una red, tienen que trabajar juntos varios protocolos para asegurar que el dato está:

- Preparado
- Transferido
- Recibido
- Manejado

El trabajo de los distintos protocolos debe estar coordinado para que no haya conflictos u operaciones incompletas. La respuesta a este esfuerzo de coordinación se llama "layering".

Protocolos de Red

Los protocolos de red proveen lo que es llamado servicios de enlace. Estos protocolos manejan direccionamiento e información de enrutamiento (routing), chequeo de errores y peticiones de retransmisión. Los protocolos de red también definen las reglas para la comunicación en un entorno particular de networking, como Ethernet o Token Ring.

Los más populares son:

- IP (Protocolo de Internet) El protocolo TCP/IP para enrutar paquetes.
- IPX (ínter network packet exchange) El protocolo de Netware para lanzamiento de paquetes y enrutamiento.
- NWLink-La implementación de Microsoft del protocolo IPX/SPX.
- Net BEUI - Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones Net BIOS y aplicaciones.
- DDP (datagram delivery protocol) Un protocolo Apple Talk de transporte de datos.

Protocolos Estándar

El modelo OSI se usa para definir qué protocolos deberían utilizarse en cada nivel. Los productos de diferentes fabricantes que suscriben este modelo pueden comunicarse con los otros.

Net BEUI no es rutable (nivel 3 y 4)

Net BIOS FUNCIONA EN NIVEL 5 (Sesión)

TCP/IP e IPX/SPX son rutables.

El ISO, el IEEE, ANSÍ y CCITT, ahora llamado ITU, han desarrollado protocolos que mapean alguno de los niveles del modelo OSI.

Los protocolos IEEE en el nivel Físico son:

- 802.3 (Ethernet)

Esto es, una red en bus lógico que puede transmitir datos a 10 Mbps. El dato es transmitido por el cable a todos los ordenadores.

Solo aquellos que reciben el dato acusan recibo de la transmisión. El protocolo CSMA/CD regula el tráfico de red permitiendo una transmisión cuando el cable está limpio y no hay otro ordenador transmitiendo.

- 802.4 (paso de testigo) Este es un diseño de bus que usa un esquema de paso de testigo. Cada ordenador recibe el dato pero sólo el único direccionado responde. Un testigo que viaja por el cable determina qué ordenador está capacitado para transmitir.

- 802.5 (Token Ring)

Es una red en anillo lógico que transmite a 4 Mbps o a 16 Mbps. A veces es difícil llamarlo anillo, parece como una estrella con cada ordenador ramificándose desde un hub. El anillo está dentro del hub. Un testigo viajando alrededor del anillo determina qué ordenador puede enviar datos.

Dentro del nivel de Enlace (Data Link), la IEEE tiene definidos protocolos para facilitar la actividad de comunicaciones en la subcapa MAC (Media Access Control

- Control de Acceso al Medio).

Nivel de enlace

- LLC (Lógico Link Control)
- MAC (Media Access Control)

Un driver MAC es el device driver situado en la subcapa MAC. Este driver es también conocido como el driver de la tarjeta de red. Proporciona acceso de bajo nivel a los adaptadores de red proporcionando soporte de transmisión de datos y algunas funciones básicas de administración del adaptador.

Un protocolo MAC determina qué ordenador puede usar el cable de red si varios están intentándolo usar simultáneamente. CSMA/CD, el protocolo 802.3, permite a los ordenadores transmitir datos si no hay otro ordenador transmitiendo. Si dos hosts transmiten simultáneamente, ocurre una colisión.

El protocolo detecta la colisión y detiene todas las transmisiones hasta que el cable queda limpio. Entonces, cada ordenador comienza a transmitir de nuevo después de esperar un periodo aleatorio de tiempo.

Los Protocolos Más Comunes

En esta sección se ven los protocolos más usados:

- TCP/IP
- NetBEUI

- X-25
- Xerox Network System (XNS)
- IPX/SPX yNWLink
- APPC
- AppleTalk
- OSI protocol suite
- DECnet

Protocolos TCP/IP

Vamos a explicar como se envía unos datos desde un ordenador a otro mediante el protocolo TCP/IP (Transmission Control Protocol / Internet Protocol) analizando como se transforman los datos iniciales antes de ser enviados por la red y como son transformados en la computadora destino

El **protocolo TCP** se encarga de dividir los paquetes antes de su envío y de su agolpamiento una vez recibidos

El **protocolo IP** se encarga del tráfico de los paquetes entre computadoras

Ejemplo: Queremos transmitir una cierta cantidad de datos desde el computadora 1 a la 9



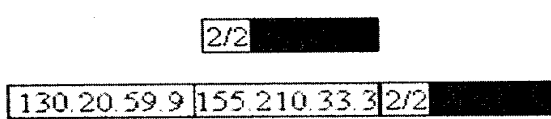
@IP: 130.20.59.9
 @NIC:
 0F:8A:5E:20:1B:35

@IP: 155.210.33.3
 @NIC:
 0F:8A:5E:20:1B:3B

Computadora 1: Nivel de Transporte

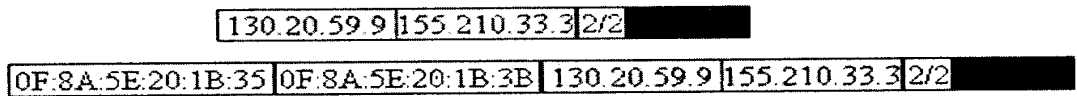


Se dividen los datos en tantas partes como sean necesarias para que pueda ser transmitida cada parte de una sola vez y se incluye información en cada una de las partes sobre el número total de partes y que orden ocupa cada una de ellas



Computadora 1: Nivel de Red
 Se forman los **paquetes**: En cada parte se incluye la **dirección IP** origen y destino

Computadora 1: Nivel de Enlace



Se forman las **tramas**: En cada paquete se incluye la **dirección física**



Computadora 1: Nivel físico, son transmitidos los **bits** de cada trama

Computadora 9: Nivel físico, son recibidos los **bits** de cada trama

Además TC/IP Transmisión Control Protocol / Internet Protocol (TCP/IP) es una suite de protocolos estándar de la industria proporcionando comunicaciones en un entorno heterogéneo. TCP/IP es un protocolo rutable, para interconectar redes entre empresas y acceder a Internet y sus recursos.

Ha llegado a ser el protocolo estándar usado para interoperatividad entre distinto y tipos de ordenadores. Esta interoperatividad es una de las principales ventajas de TCP/IP. La

mayoría de las redes soportan TCP/IP como protocolo. También soporta enrutamiento y es usado comúnmente como protocolo de internet working.

Con motivo de su popularidad, TCP/ IP ha llegado a ser el estándar de facto para Internet working

Con motivo de su popularidad, TCP/ IP ha llegado a ser el estándar de facto para internet working.

Otros protocolos escritos específicamente para la suite TCP/IP son:

- SMTP (simple mail transfer protocol) e-mail.
- FTP (file transfer protocol) para intercambiar ficheros entre ordenadores ejecutado TCP/IP.
- SNMP (simple networks manegement protocol). Administración de redes.

Históricamente, había 2 desventajas principales de TCP/IP: su tamaño y velocidad

TCP/IP es un stack de protocolos relativamente grande que puede causar problemas en clientes basados en Ms-Dos. Sin embargo en sistemas operativos basada en interface gráfica del usuario (GUI), como Windows 95 ó NT, el tamaño no es inconveniente y la velocidad es más o menos la misma que IPX.

Net BEUI. Es un protocolo del nivel de Transporte pequeño, rápido y eficiente que es proporcionado con todos los productos de red de Microsoft.

XNS (Seros Network System)

Xerox Network Systems (XNS) fue desarrollado por Xerox para sus LANs Ethernet. Fue ampliamente usado en los 80, pero ha sido lentamente desplazado por TCP/IP. Es un protocolo grande y lento, produce muchos broad casts, causando mucho tráfico de red.

IPX/SPX y NWLink

Intenetwork packet exchange /sequenced packet exchange es un stack de protocolo que se usa en las redes Novell. Como Net BEUI, es un protocolo relativamente pequeño y rápido en una LAN. Pero, no como Net BEUI, soporta routing (enrutamiento). IPX/SPX es una derivación de XNS (Xerox).

Microsoft provee NWLink como su versión de IPX/SPX. Es un protocolo de transporte y es ruteable.

APPC

Advanced Program to Program communication, es un protocolo de transporte IBM desarrollado como parte de su arquitectura de sistemas de red (SNA). Fue diseñado para habilitar a los programas de aplicación ejecutándose en distintos ordenadores para comunicarse e intercambiar datos directamente

Apple Talk

Es un stack de protocolo propiedad de Apple diseñado para que los Apple Macintosh compartieran ficheros e impresoras en un entorno de red.

SI Protocol Suite

Es un stack de protocolo completo. Cada protocolo mapea directamente un micro nivel del modelo OSI. La suite OSI incluye protocolos de enrutamiento y transporte, protocolos de la serie IEEE 802, un protocolo del nivel de Sesión, uno del nivel de Presentación y varios del nivel de Aplicación diseñados para proporcionar completa funcionalidad de networking, incluyendo acceso de ficheros, impresión y emulación de terminal.

DECnet

Es un stack de protocolo propiedad de Digital.

Es un conjunto de productos hardware y software que implementan la Digital Network Architecture (DNA). Define la comunicación en red, sobre LAN Ethernet, fiber distributed data interface metropolitan área networks (FDDI MANs), y WANs que usan facilidades de transmisión de datos publicas o privadas.

DECnet puede usar también los protocolos a TCP/IP y la suite OSI tan bien como sus propios protocolos. Es un protocolo ruttable.

DECnet puede usar también los protocolos a TCP/IP y la suite OSI tan bien como sus propios protocolos. Es un protocolo ruttable.

DECnet ha sido actualizado varias veces. Cada una se denomina fase. La actual es la fase V, y los protocolos usados son propiedad de Digital y una completa implementación de la-suite OSI.

1.5.4 Protocolo Data Socket

Data Socket es una tecnología que simplifica el intercambio de datos entre aplicaciones, archivos, servidores de FTP, y servidores de Web. Proporciona un API común a varios protocolos de comunicación diferentes.

Data Socket, es una tecnología y un grupo de herramientas, que facilita el intercambio de datos e información entre una aplicación y un número fuentes y bancos de datos diferentes. Estas fuentes y bancos incluyen archivos, los servidores de HTTP/FTP, servidores OLE para el Control de proceso (OPC), y servidores Datasocket de National Instruments, para publicar los datos vivos entre las aplicaciones. A menudo, se localizan estas fuentes y blancos en una computadora diferente. Usted puede especificar

las fuentes y blancos de DataSocket (conexiones) usando URLs (el localizador del recurso uniforme).

DataSocket usa datos mejorado la estructura por intercambiar los datos de la medida, así como los atributos de los datos. El datos atribuye podría incluir la información como una proporción de adquisición, nombre de operador de prueba, estampa de tiempo, y calidad de datos.

La Fuente de datos

Una fuente de datos esta localizada en el DataSocket lector que se desea para conectar y recuperar los datos. Usted especifica una fuente de datos con un URL. Como su URL usa un navegador Web, el localizador de la fuente de datos pueden apuntar a muchos tipos diferentes de fuentes que dependen de un prefijo. El prefijo es llamado el esquema del URL. DataSocket soporta varios esquemas:

- dstp: (Protocolo transferencia DataSocket)
- http: (el protocolo de traslado de hipertexto)
- ftp: (el protocolo de traslado de archivo)
- opc: (OLE para el Control de proceso)
- entre otros

DSTP

DataSocket Transfer Protocol (Protocolo transferencia DataSocket). Es un protocolo basado en TCP/IP a través del cual los datos son pasados entre DataSocket clientes conocidos como Lector y aplicaciones o Escritor del Escritor usando el Servidor de DataSocket.

Usted conecta a un Servidor de DataSocket desde un Lector y Escritor usando el esquema DSTP URL, como se demuestra en el siguiente ejemplo:

Lo siguiente el URL conecta el data item nombrado la wave al Servidor de DataSocket que corre en la computadora local:

el `dstp://localhost/wave`

El Banco de datos

Un banco de datos es una localización a que se quiere conectar el Escritor de DataSocket y escribir los datos. Se especifica un banco de los datos con un URL. Como su URL usa un navegador Web, el localizador de la fuente de datos pueden apuntar a muchos tipos diferentes de fuentes que dependen de un prefijo. El prefijo es llamado el esquema del URL. DataSocket soporta varios esquemas:

- `dstp`: (Protocolo transferencia DataSocket)
- `http`: (el protocolo de traslado de hipertexto)
- `ftp`: (el protocolo de traslado de archivo)
- `opc`: (OLE para el Control de proceso)
- entre otros

LabVIEW

Es un lenguaje de programación grafico para el diseño de diseño de adquisición de datos, instrumentación, y control. Además nos permite diseñar interfaces de usuario mediante una consola interactivo basado en software. Los programas en **LabVIEW**

Son llamados instrumentos virtuales o VI's, debido a su apariencia y operación ilimitada de instrumentos físicos, tales como osciloscopios y multímetros.

Cada VI utilizan funciones que manipulan entradas desde la interfase del usuario u otras fuentes y presenta esa información o la envía a otros archivos o computadores.

Se pueden diseñar dichas interfaces, especificando el sistema funcional, el diagrama de bloques o una notación de diseño de ingeniería.

LabVIEW es a la vez compatible con herramientas de desarrollo similares y pueden trabajar con programas de otra área de aplicación.

Características

Una de las principales características de LabVIEW es su modularidad, es decir, la capacidad de utilizar bloques funcionales para la definición de la especificación

LabVIEW permite contactarse con otras aplicaciones mediante un intercambio de datos como Active X, librerías dinámicas, base de datos, Excel, protocolos de comunicación como Data Socket. TCP/IP UDC RS-232, entre otras

LabVIEW también puede ser un programa en tiempo real en donde la aplicación trabaja sin la necesidad de otro sistema operativo, este programa denominado LabVIEW RT viene con su propio Kernel que se encarga de la administración de las tareas.

Componentes

Un VI contiene los siguientes componentes:

- Panel Frontal.- Sirve como interface de usuario

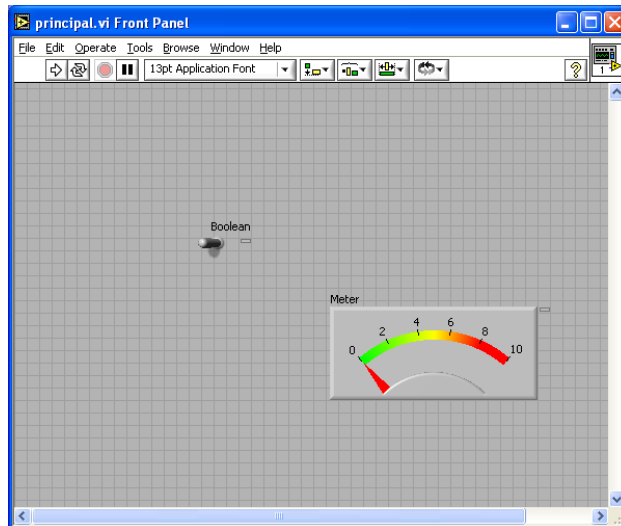


Fig. 1.27 Panel Frontal

- Diagrama de Bloques.- contiene los códigos de fuente gráficos que defienden la funcionalidad del VI

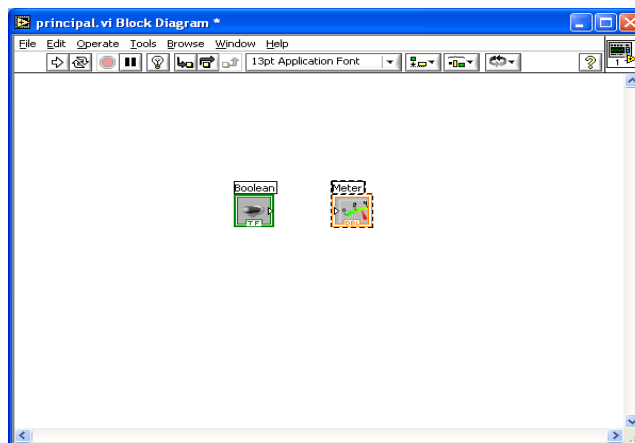


Fig. 1.35 icono y conector

- Icono y Conector .- Identifica el VI tanto como pueda usar un VI en otro VI. Un VI dentro de otro VI es llamado un SubVI correspondiente a una subrutina en el lenguaje de programación basado en texto.

1.6 Direcciones IP

Las direcciones IP (Internet Protocol) nacieron con Internet, como medio para identificar a las diferentes computadoras.

IP utiliza una dirección numérica para definir cada nodo de la red. Cada dirección comprende una serie de cuatro números separados por un punto, llamándose a cada número **octeto** (llamados así porque en su forma binaria contienen ocho bits). Cada octeto solo puede valer entre 0 y 255, límite impuesto por los 8 bits.

Una típica dirección IP es 211.155.76.12

La dirección IP más baja es 0.0.0.0 y la más alta es 255.255.255.255

Cuando varias computadoras pertenecen a la misma red deben tener parte de la dirección común. Esto ha obligado a los organismos encargados de asignar direcciones IP a crear cinco tipos de direcciones, ya que algunas organizaciones necesitarán más direcciones dentro de su red que otras. Desde una empresa media que puede necesitar 150 direcciones IP, por ejemplo, hasta el gobierno de EEUU que pueden necesitar millones de direcciones, hay que cubrir racionalmente todas las necesidades de forma que los distintos enrutadores de la red sepan si se trata de la misma o distinta red.

Los cinco tipos de direcciones son:

-TIPO A: Solo utiliza el primer octeto para designar la dirección de la red, utilizándose los tres últimos octetos para identificar los distintos nodos de la red. Solo existen 128 direcciones de red diferentes, pero cada una de las redes dispone de 16.777.216 hosts o nodos diferentes. Estas direcciones son utilizadas por los gobiernos y grandes instituciones. Su rango va de 0.0.0.0 a 127.255.255.255. Ejemplo: la dirección 122.144.133.3 corresponde a la computadora con dirección 144.133.3 incluida en una red de dirección 122

- TIPO B: Utilizan los dos primeros octetos para designar la dirección de la red y los dos restantes para definir los hosts. De ésta forma existen más direcciones de red de este tipo, 16.575, teniendo cada una de ellas un máximo de 65.536 nodos posibles. Su rango va de 128.0.0.0 a 191.255.255.255. Ejemplo: la dirección 150.210.33.3 corresponde a la computadora con dirección 33.3 incluida en una red de dirección 150.210

-TIPO C: Utilizan los tres primeros octetos como dirección de red, siendo posibles 2.210.850 direcciones de red diferentes, cada una de ellas con 254 nodos diferentes. Su rango va de 192.0.0.0 a 223.255.255.255

-TIPO D: Son direcciones multicast. Su rango va de 224.0.0.0 a 239.255.255.255

-TIPO E: Son direcciones reservadas para el futuro. Su rango va de 240.0.0.0 a 247.255.255.255

1.6.1 Creación de Direcciones Propias

Cuando en una red utilizamos el protocolo TCP/IP debemos definir una dirección IP para cada una de las computadoras. Estas direcciones pueden ser elegidas casi al azar, pero entonces no podremos utilizar la conexión a Internet, ya que estaríamos saltándonos las normas de asignación de direcciones IP en Internet.

1.6.2 Grupos de Direcciones IP: Máscaras de Red

Existe una notación estándar para grupos de direcciones IP, a veces llamada «dirección de red». Igual que un número de teléfono puede ser separado en prefijo de área y el resto, podemos separar una dirección IP en el prefijo de red y el resto. Antes se hablaba de «la red 1.2.3», refiriéndose a todas las 256 direcciones de la 1.2.3.0 a la 1.2.3.255. O si no bastaba con esa red, se hacía referencia a «la red 1.2», que implica todas las direcciones desde la 1.2.0.0 a la 1.2.255.255. Normalmente no escribimos «1.2.0.0 -

1.2.255.255». En su lugar, lo abreviamos como «1.2.0.0/16». Esta extraña notación «/16» (se llama «netmask» - máscara de red) precisa de alguna explicación.

Cada número entre los puntos en una dirección IP se compone de 8 dígitos binarios (00000000 a 11111111): los escribimos en la forma decimal para hacerlos más legibles. El «/16» significa que los primeros 16 dígitos binarios constituyen la dirección de red, o en otras palabras, «1.2.» es la parte de la red (recuerde: cada dígito representa 8 binarios). Esto significa que cualquier dirección IP que comience por «1.2.» es parte de la red: «1.2.3.4» y «1.2.3.50» lo son, y «1.3.1.1» no. Para hacer la vida más fácil, solemos usar redes que acaban en «/8», «/16» y «/24». Por ejemplo, «10.0.0.0/8» es una gran red que contiene las direcciones desde la 10.0.0.0 a la 10.255.255.255 (alrededor de 24 millones de direcciones). 10.0.0.0/16 es más pequeña, y sólo contiene las direcciones IP de la 10.0.0.0 a la 10.0.255.255. 10.0.0.0/24 es aún más pequeña, y sólo contiene las direcciones 10.0.0.0 a 10.0.0.255.

Para terminar de hacerlo confuso, hay otras maneras de escribir máscaras de red. Podemos escribirías como direcciones IP: 10.0.0.0/255.0.0.0 Cabe señalar que la IP más alta de cualquier red está reservada para la dirección de multidifusión, que se puede usar para enviar un mensaje a todas las máquinas de la red a la vez.

1.6.3 Mascara de Red

Tabla 1.4 **Mascaras de red**

Forma Corta	Forma Completa	Máximo número maquinas	Comentarios
/8	/255,000,000	16,777,215	se llama clase A
/16	/255,255,000	65,535	se llama clase B
/17	255,255,128,0	32,767	
/18	/255,255,192,0	16,383	
/19	/255,255,224,0	8,191	
/20	/255,255,240,0	4,095	
/21	/255,255,248,0	2,047	
/22	/255,255,252,0	1,023	
/23	/255,255,254,0	511	
/24	/255,255,255,0	255	
/25	/255,255,255,128	127	
/26	/255,255,255,192	63	

CAPÍTULO II

Implementación de la Red LAN

2.1 Estudio del lugar

Lo primero a efectuar antes de realizar cualquier operación previa, es comprobar toda la instalación sobre lo cual se va a efectuar el montaje de la red.

La instalación total comprende:

- 4 ordenadores
- 3 tarjetas de adquisición de datos
- Conexión de Internet

Una vez estudiada las diferentes conexiones y determinando el número de ordenadores que se va a instalar se procede a determinar el material que se va a necesitar para la instalación de la red

Para esta red se necesitaron:

- Switch de 16 puertos
- Conectores RJ45
- Cable UTP
- Conectores aéreos macho RJ45
- Material diverso para la instalación

2.2 Características del lugar.

Primeramente se crea un plano (vista desde arriba) del donde se va a montar la red. Para poder determinar el lugar correcto donde se va a instalar todo el sistema de cableado y conexiones a los puestos de los ordenadores.

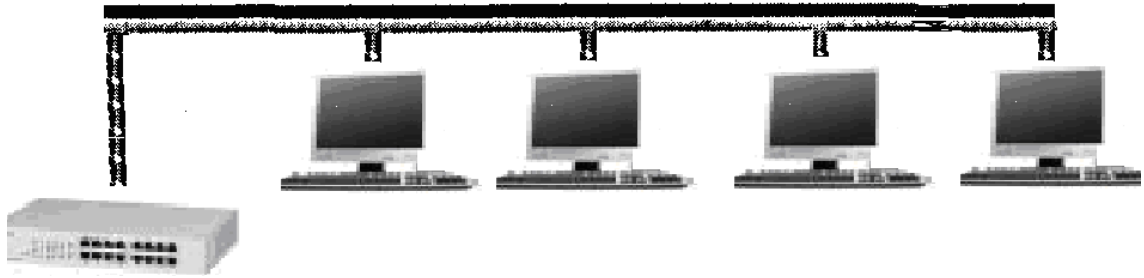


Fig 2.1 Análisis de la Red

Este esquema presenta la colocación de los ordenadores y como podemos ver la mejor colocación para el cableado, de esta manera se puede evitar las complicadas conexiones de cables ya que no pueden estar en lugares que molesten o que impidan el paso para las personas.

2.3 Conexión del Switch

Para la conexión del switch se colocó en un lugar donde se pueda conectar a la corriente eléctrica y donde sea fácil desconectarlo cuando no se lo utilice la red.

Como todos los cables tienen que ir conectados al switch debe tener un sitio específico para lo cual no tenga ninguna complicación u ocasione algún desperfecto.

2.4 Conexión de las computadoras

Se debe conectar cada una de las computadoras al switch, conectando un extremo del cable al conector de la tarjeta de red de cada una de las computadoras y el otro extremo del cable a un conector del switch.

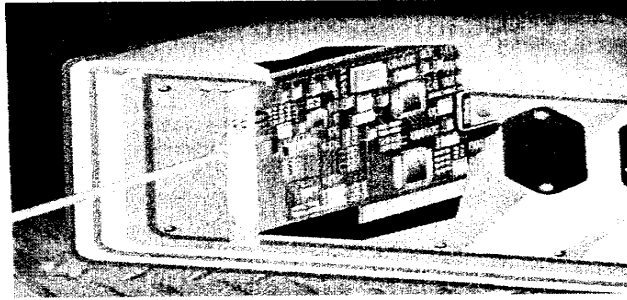


Fig 2.2 Conexión de computadoras

2.5 Construcción del cableado.

En la fotografía que aparece ahora, se puede ver un rollo de cable tipo UTP categoría 5 utilizando para montar en canaletas desde el RJ45 del ordenador al RJ45 del switch

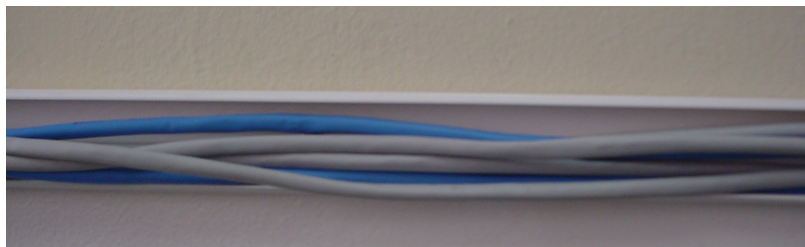


Fig 2.3 Cable pasado por la canaleta

Dicho cable se instala por el interior de la canaleta en este caso por el interior de la mesa donde van los ordenadores.

En el intermedio de la canaleta encontramos todos los cables de cada uno de los ordenadores de la red que van hacia el switch o concentrador para realizar la instalación de la red.



Fig 2.4 Ubicación del Switch en el laboratorio

Puede observar un cable conectado al switch proviene de una clavija de pared RJ45, cada uno de los cables que lleguen a través de la canaleta hacia el switch ocuparan los conectores del switch como muestra la figura 2.5.

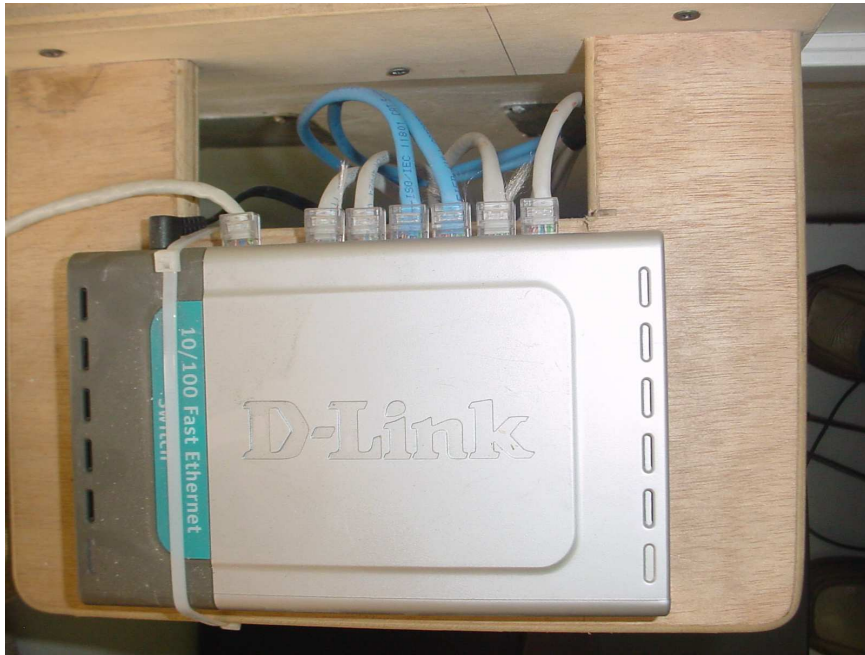


Fig 2.5 Conexión de los cables al switch

2.6 Instalación de las tarjetas

En la figura que aparece ahora se puede observar un ordenador sin su tapa, donde se encuentra instalada la tarjeta de red

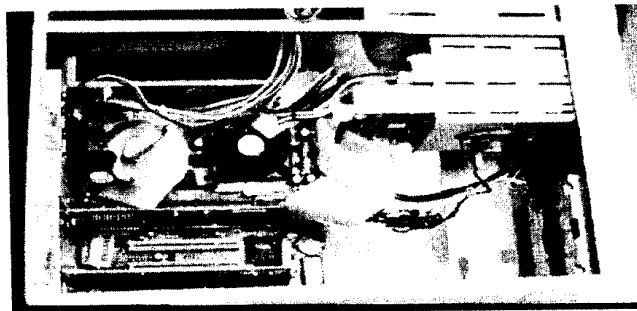


Fig 2.6 Implementación de las tarjetas

Como puede observar en la zona inferior izquierda hay una ranura blanca (PCI) libre para poder conectar una tarjeta de red tipo Ethernet como la que muestra la figura 2.7



Fig 2.7 Llanura para la tarjeta Ethernet

Una vez montada la tarjeta, la parte posterior del ordenador presenta la clavija que tiene la tarjeta de red que se acaba de instalar para poder conectar el cable de red presente en el cajetín ubicado en la pared.

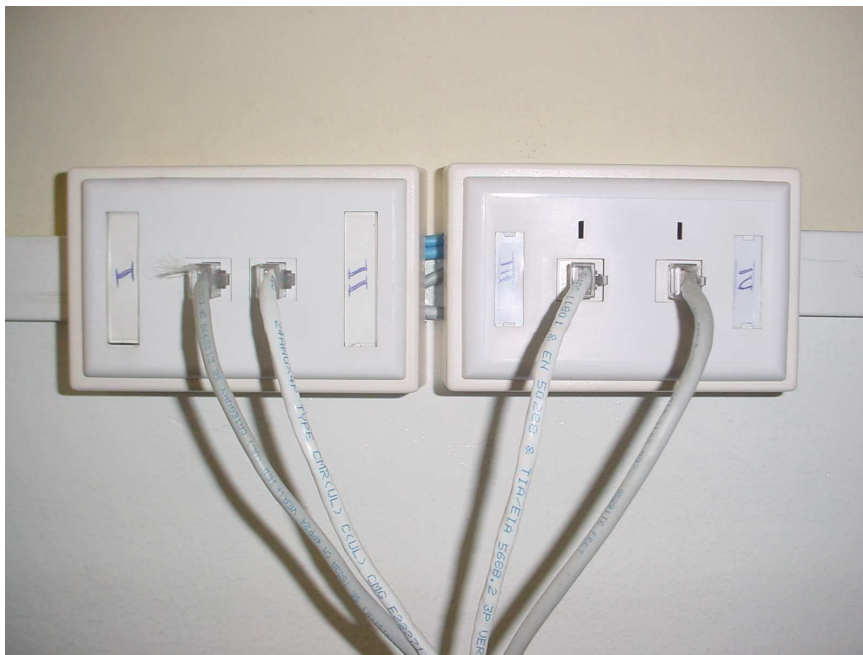


Fig 2.8 Cajetines

2.7 Implementación de controladores de la tarjeta de red.

Cuando se encienda las computadoras se puede instalar los controladores de la tarjeta que se encuentran en el CD o disquete que acompaña a la tarjeta, siguiendo las indicaciones de Windows

Una vez realizada la instalación se deberá reiniciar la computadora.

2.8 Configuración de la red.

En cada una de las máquinas se tiene que realizar lo siguiente:

En el icono de red del escritorio: botón derecho-propiedades e ingresamos a ver la figura 2.9

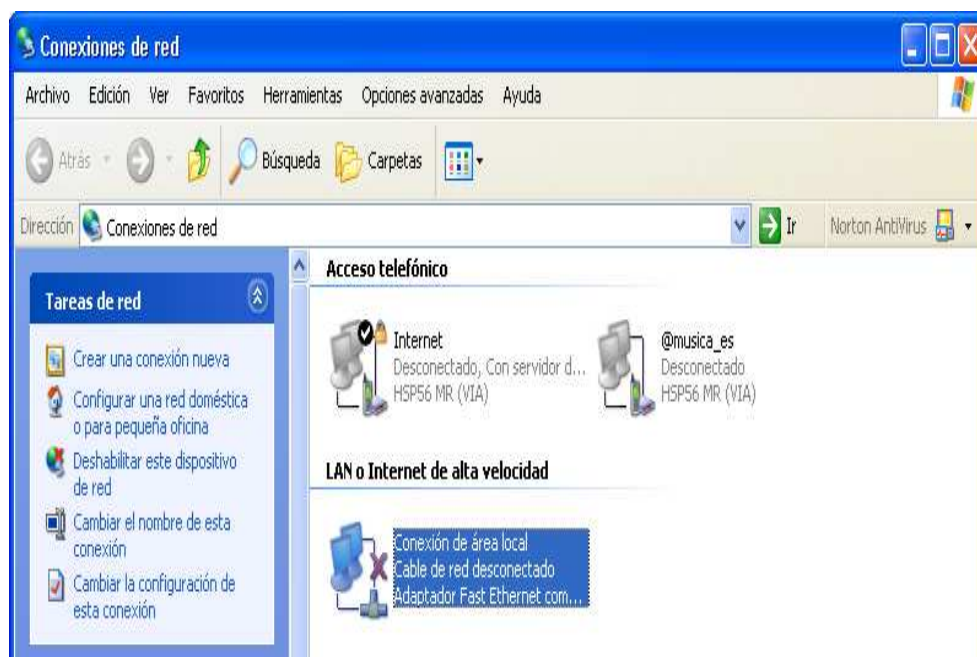


Fig 2.9 Configuración de Red

En el icono conexión de área local: botón derecho-propiedades e ingresamos a ver la figura 2.10.



Fig 2.10 Configuración de conexión de la red

Damos un clic en Procolo Internet (TCP/IP), y luego en propiedades, nos aparece la figura 2.11

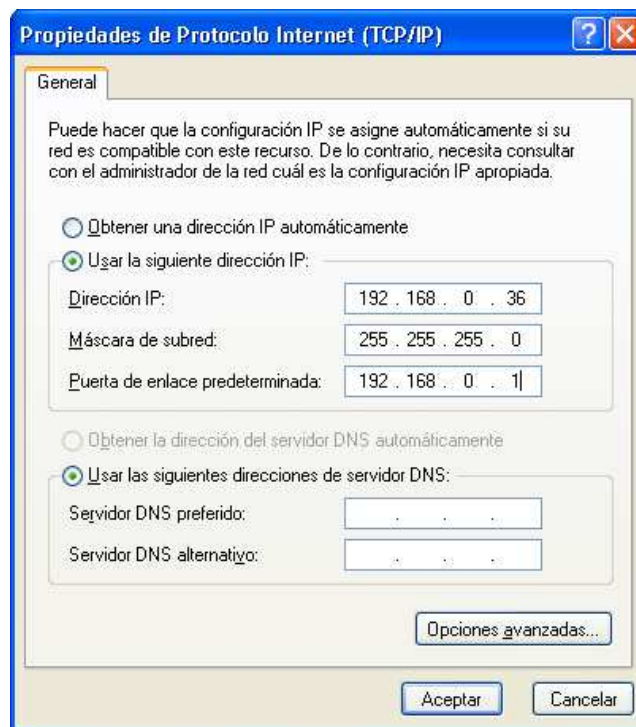


Fig 2.11 Configuración de direcciones IP y mascarar

En esta ventana colocamos la dirección IP de cada máquina con su correspondiente máscara y puerta de enlace.

CAPITULO III

Análisis Económico

3.1 COSTO DE ACCESORIOS EMPLEADOS

Para la realización de este proyecto se han empleado diferentes equipos como dispositivos los mismos que detallan a continuación.

Tabla 3.1. Costo total del Proyecto

ELEMENTOS	VALOR \$
Tarjetas de Red	80
Switch	90
Cascadas	30
Cablea	470
Armario	20
Alquiler de Equipo Electrónico (chequeo)	15
TOTAL	705

CAPITULO IV

Conclusiones y Recomendaciones

4.1 Conclusiones

A lo largo del desarrollo de este proyecto se alcanzado los objetivos planteados inicialmente, lo que ha permitido determinar las siguientes conclusiones:

- No se realizó un estudio de alternativas en cuanto a redes porque existe en el instituto una red LAN, lo único que se hizo es conectar la Intranet que se realizó en el laboratorio al la red LAN del instituto.
- En la elaboración de este proyecto sirve para comprender un poco más acerca de los nuevos protocolos que están apareciendo con la tecnología actual como en este caso del Protocolo DataSocket logrando así la Implementación de la Red en el Laboratorio de Instrumentación Virtual para el estudio de dicho protocolo con todas sus herramientas virtuales y guías del usuario.
- Durante este estudio se pudo conseguir una información detallada de todos los equipos y medios que fueron utilizados, escogiendo los más idóneos para este proyecto.
- La información acerca del Protocolo DataSocket fue de mucha importancia, ya que permitió conocer y comprender el funcionamiento y operación del mismo con la interpretación de cada una de sus funciones.

- El presente estudio también permitió aplicar los conocimientos adquiridos sobre la implementación de una red LAN.
- El Laboratorio de Instrumentación Virtual ha sido equipado con una Red LAN para poder trabajar con el Protocolo DataSocket, esta será un recurso muy importante para la enseñanza en el instituto.
- Para realizar este trabajo se lo hizo en una forma práctica con todos los equipos e instrumentos existentes en dicho laboratorio.

4.2 Recomendaciones

Todos los equipos necesitan de algunas normas para tener una buena conservación, es decir aquí se proponen algunas de ellas para asegurar el buen desempeño de cada uno de ellos:

- Para tener un Protocolo DataSocket en línea este deberá estar encendido el Server Data Socket para empezar a trabajar en cualquier ejercicio.
- Se recomienda que para un mejor entendimiento del Protocolo DataSocket tenga conocimientos acerca de dicho Protocolo y LabVIEW de la National Instruments
- Para un mejor manejo del protocolo se recomienda usar todas las herramientas como los pasos a seguir detallado en la guía del usuario.

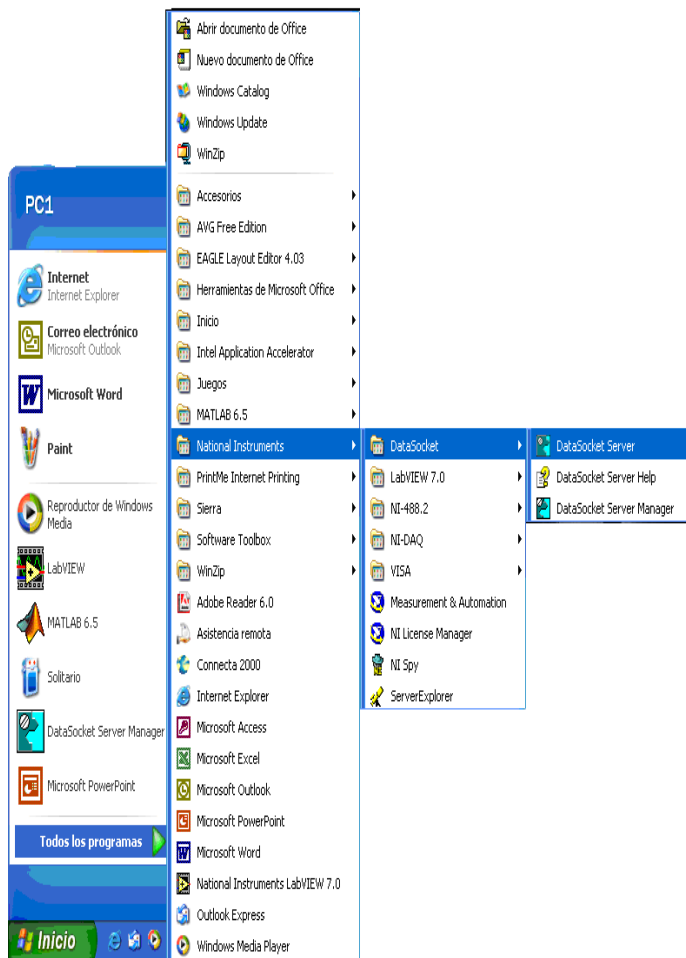
Guía del usuario



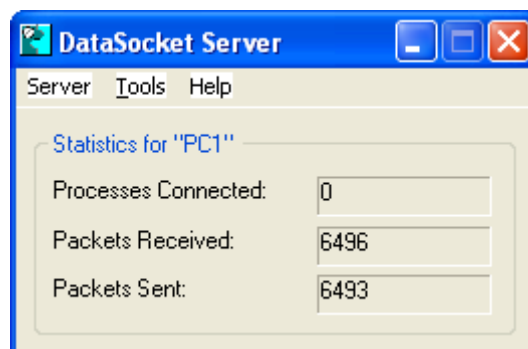
Este es un proyecto diseñado como un recurso de ayuda en el proceso de enseñanza para el personal docente por lo cual es de fácil manejo, con los conocimientos básicos de dicho proyecto.

Para el Encendido

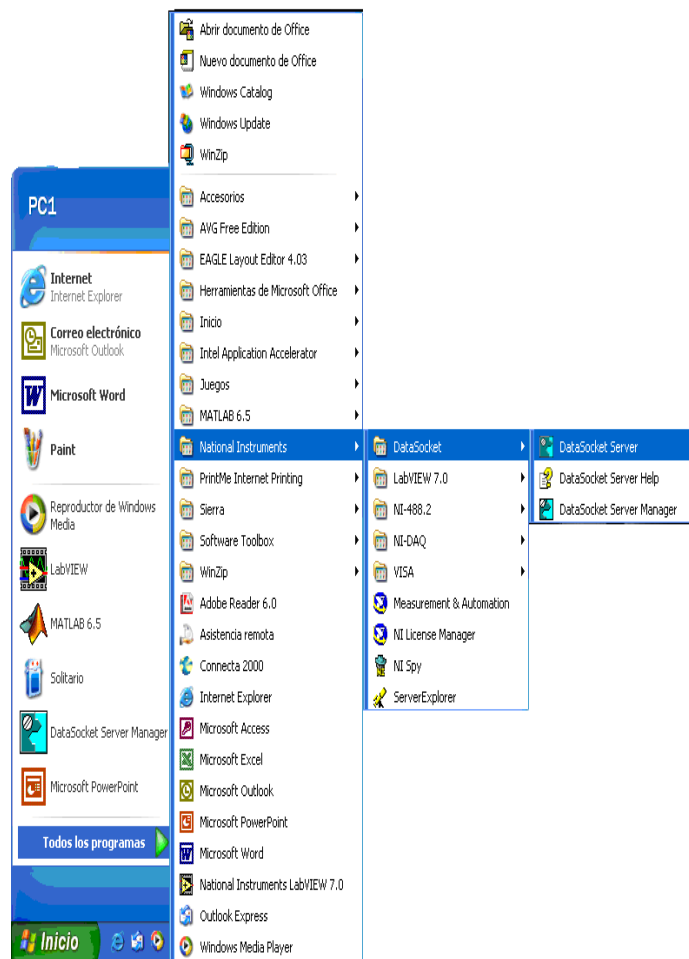
1. Encendemos los ordenadores del Laboratorio y verificamos que se encuentren en red
2. Hacemos click en inicio y vamos al servidor del Protocolo Data Socket



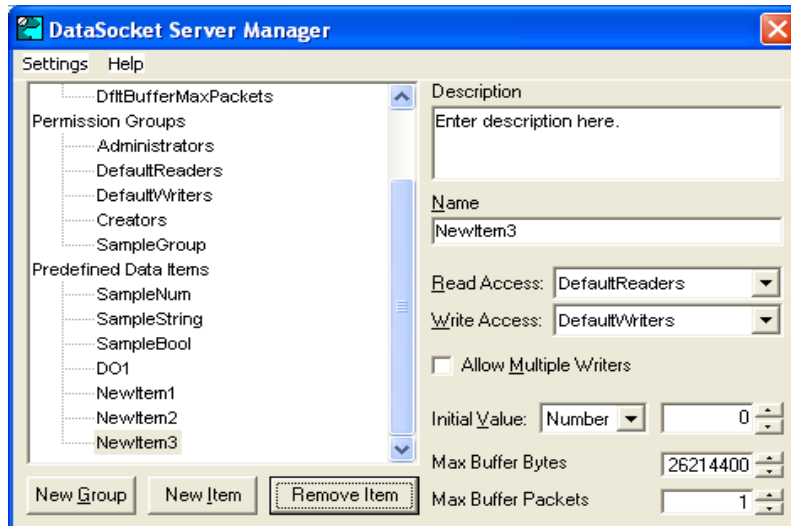
3. Lo cual nos aparecerá esta ventana



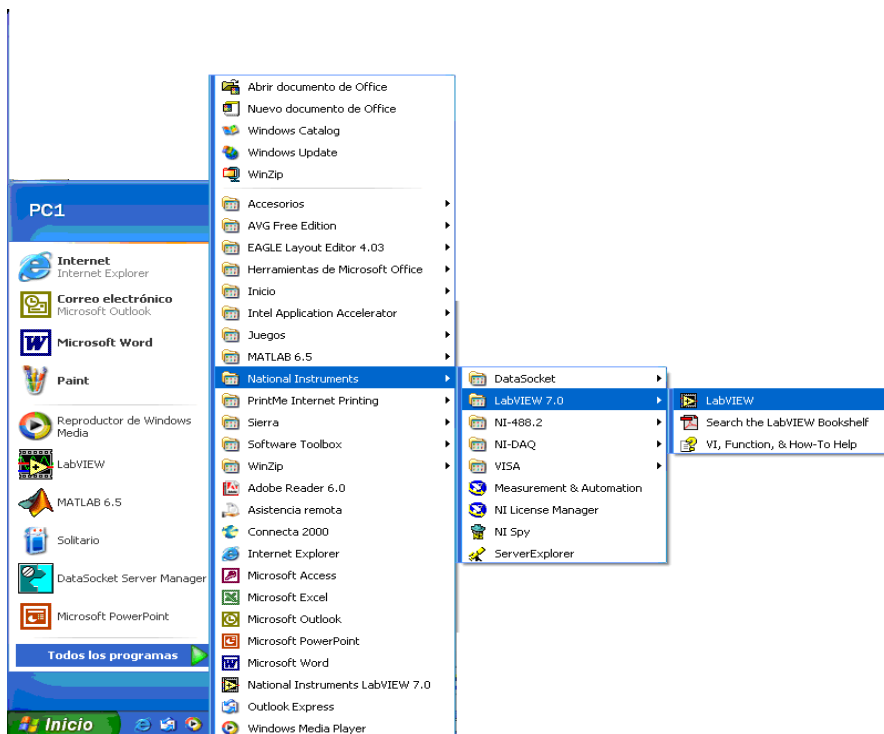
4. Igualmente procedemos hacer click en inicio y vamos al servidor manejador



5. Lo cual nos aparecerá esta figura, en el cual crearemos un DO1 como se mira en el Server manager.



6. Procedemos a abrir el programa **LabVIEW**

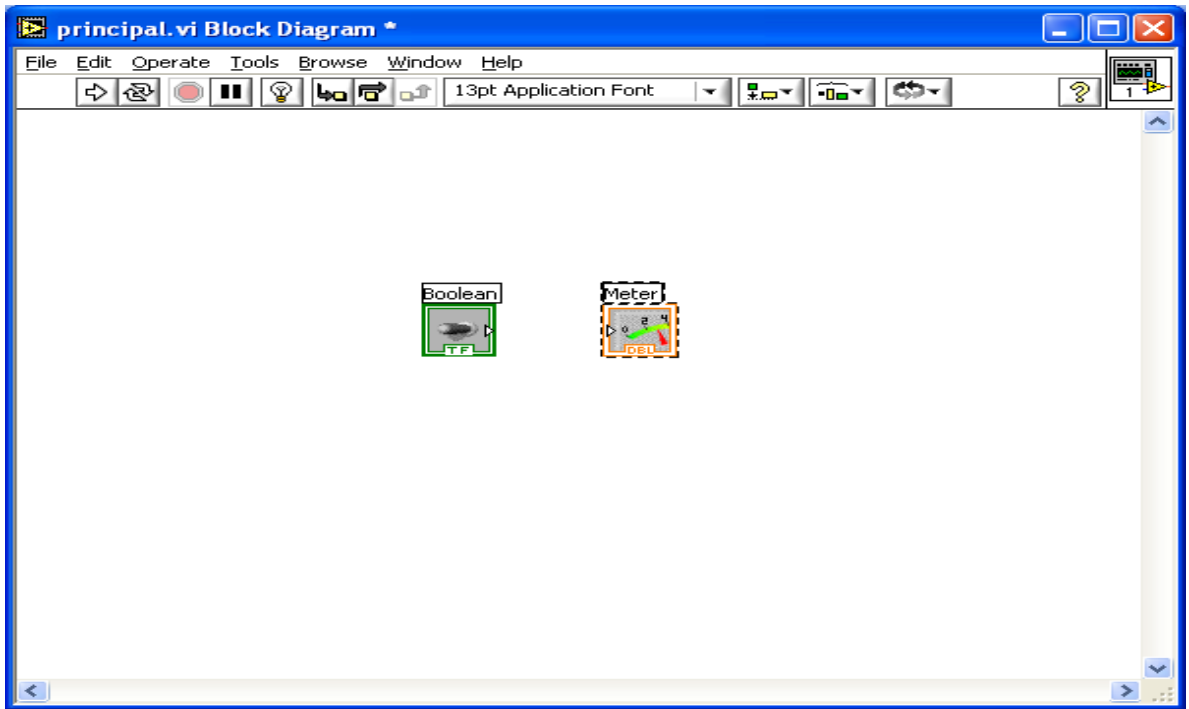


7. Lo cual nos aparecerá esta figura, Hacemos click en New si queremos realizar un nuevo ejercicio o hacemos click en Open si queremos seguir trabajando en un ejercicio que se lo guardo.

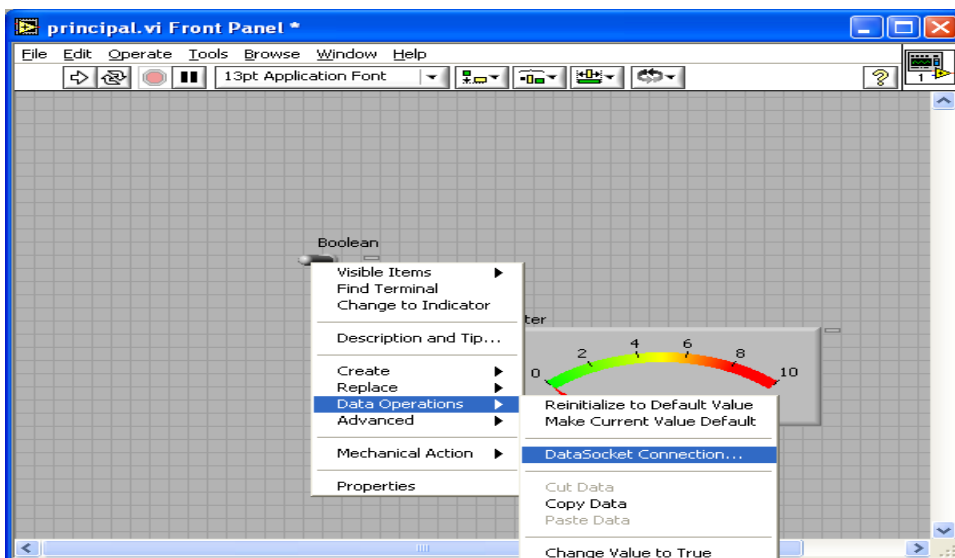


8. Posteriormente se nos abrirá un panel frontal donde ingresaremos algunos elementos como en este caso colocamos un indicador numérico y un control booleano

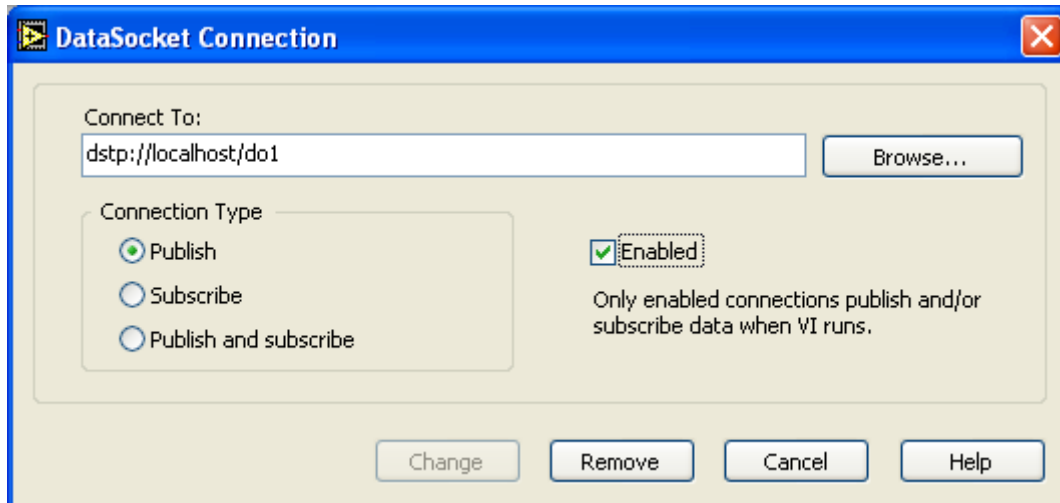
9. En el diagrama de bloques únicamente nos aparece los símbolos gráficos de los controles e indicadores colocados en el panel frontal



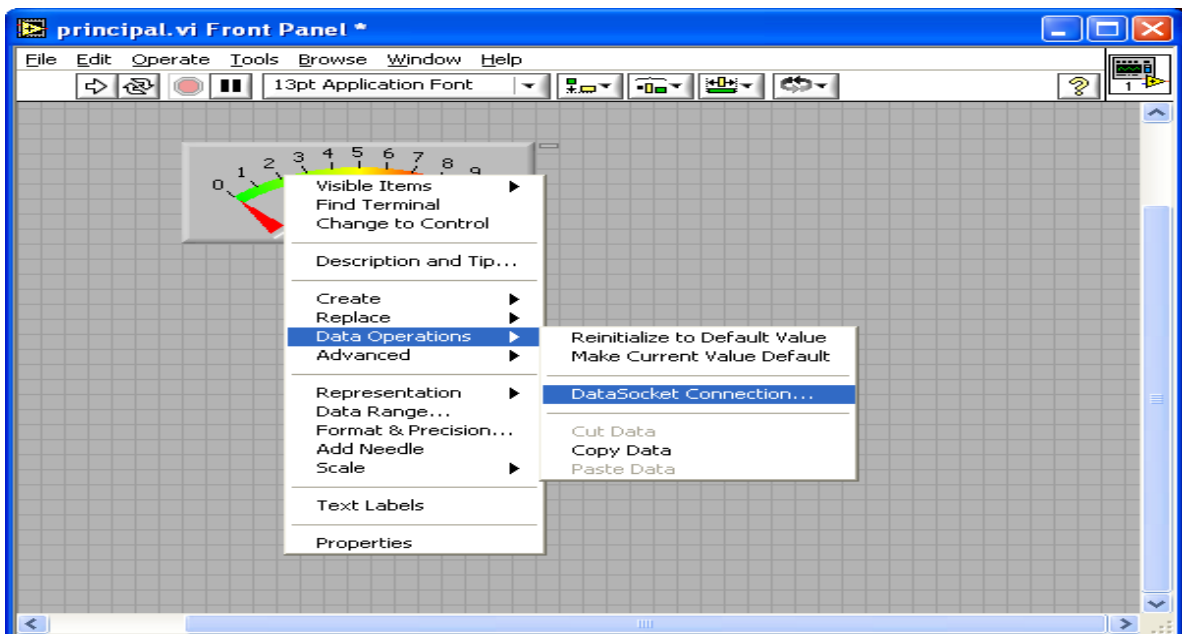
10. En el siguiente paso damos un click derecho en uno de los elementos para configurarlo, en este caso en el control booleano, nos aparecerá una ventana secundaria del control, damos un click Data Operación, y luego en DataSocket Connection



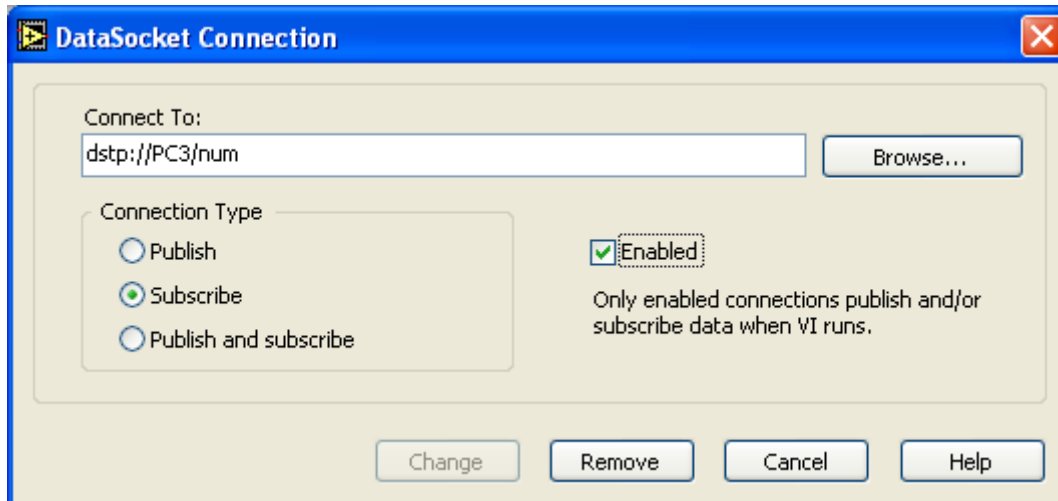
11. A continuación nos aparece es ventana, donde seleccionamos el item DO1 creado en DataSocket Server Manager, en tipo de conexión escogemos Publish; es decir vamos a publicar este dato en el servidor DataSocket para que este accesible a cualquier Lector de DataSocket.



12. Para la configuración del otro elemento, haremos click derecho como nos indica la figura



13. En este caso ya no es localhost, sino PC3 la dirección; es decir vamos a leer el item num creado en la máquina PC3, para ello seleccionamos Subscribe



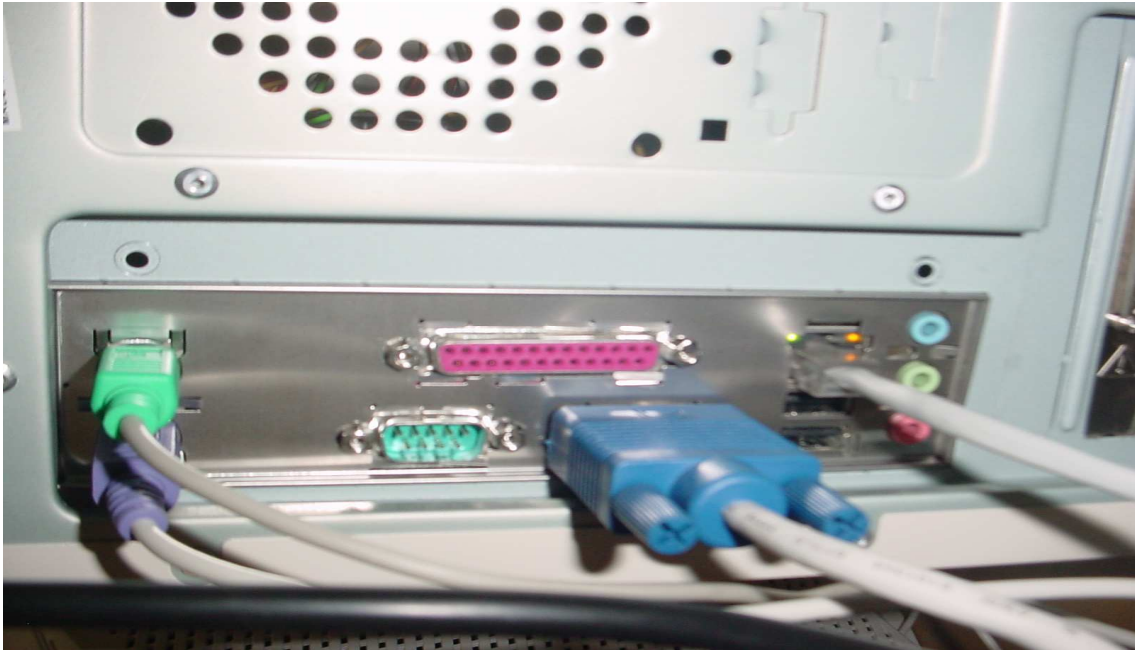
14. Para poder correr el ejercicio debe estar encendido el servidor DataSocket en las dos máquinas utilizadas para este ejercicio, como es: localhost o PC1 y la Pc3.

ANEMOS

ANEXO A: Red del Laboratorio de Instrumentación Virtual



ANEXO B: Tarjeta de Red



ANEXO C: Conectores RJ 45



GLOSARIO DE TERMINOS

- **10 BASE 2:** Implementacion de Ethernet de 10 Mgbyte en cable coaxial delgado
- **10 Base T:** Estándar de transmisión de Ethernet sobre MIT a 10 Mgbt
- **Address:** En redes la palabra dirección se refiere a un distintivo unico para cada nodo de la red
- **Administrador:** Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor.
- **Ancho de Banda:** Relación de velocidad para la transmisión de datos medidos en Kilobaudios por segundo que representa la capacidad del canal de comunicación para transportar datos.
- **Api:** Pequeños programas desarrollados para apoyar la interacción del sistema principal con las aplicaciones específicas.
- **Arpa:** Agencia militar de EE.UU encargada de proyectos tecnológicos como las redes computacionales militares.
- **Arpanet:** Proyecto del Departamento de los EE.UU que utiliza protocolos tipo x.25 donde la cantidad de información no es fija.
- **Ascii:** Código utilizado para representar los caracteres de escritura en formato binario (7bits para 128 caracteres o el modo extendido de 8 bits para 256)
- **Asincronica:** Forma de transmisión de datos donde no se necesita señal de información de reloj, la señal contiene la información de cuando cambia cada dato.

- **ATM:** tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad con tecnología de paquetes retrazados que se le considera al arquitectura del futuro en comunicaciones digitales.
- **Backbone network:** red de infraestructura que actúa como conductor primario del trafico de datos casi siempre recibe y manda información a otras redes
- **Bios:** Porción de Firwarded de una computadora que maneja el flujo de señales entre el sistema principal y los dispositivos periféricos
- **Bridge:** Puente dispositivo que pasa todos los mensajes de una red a otra sin distinguir a que red pertenece el destino del mensaje
- **Broadcast:** Transmisión abierta mensajes que se manda sin destino especifico.
- **Buffer:** Espacio físico de memoria destinados a guardar datos temporalmente
- **Bus:** Circuito de interconexión eléctrica para transmitir información
- **Cache:** Memoria mas cercana al CPU. Utilizada como buffer entre el CPU principal y el resto de la computadora, es la memoria mas rápida fina y cara por ser la que más se ocupa.
- **Cliente:** Producto o presentación de front end directamente con el usuario, no realiza los proceso ni los cálculos, eso se los deja a los programas de backup.
- **Driver:** Manejador es el programa que contiene el algoritmo de manejo de un tercer elemento para poder manejarlo como otro dispositivo
- **E3:** Gama de comunicación digital de 34 mgbits el mas veloz del mercado
- **EISA:** Estándar de intercomunicación entre CPU y tarjetas secundarias, dispositivos de I/o
- **Emulación:** Imitación de la forma de comportarse de un equipo, emita el comportamiento de una terminal de red.

BIOGRAFIA

- **Instalación y Administración de redes (Mc. Graw Hill)**
- **Topología de Redes (Manual Politécnica Nacional)**
- **Direcciones IP (Proyecto 8002 del IEEE)**
- **Instalaciones de Redes Domesticas (Mc. Graw Hill)**
- **Redes Lan (Ing. Pablo Cuichan)**
- **Fundamentos de Redes y Cableado Estructurado
(Microsoft)**
- **Diseño de Redes con fibra Optica (Microsoft)**
- **Seguridad en Redes de Datos (Microsoft)**
- **Manual de DataSocket de National Instruments**

HOJA DE VIDA

DATOS PERSONALES

APELLIDOS:	AGUAS NIETO
NOMBRES:	LUIS OSWALDO
FECHA DE NACIMIENTO:	15 DE NOVIEMBRE DE 1980
EDAD:	24 AÑOS
ESTADO CIVIL:	CASADO

ESTUDIOS REALIZADOS

PRIMARIO:	ESCUELA PARTICULAR SALESIANA DOMINGO SAVIO
------------------	---

SECUNDARIA:	COLEGIO PARTICULAR FRANCISCO DE ORELLANA
--------------------	---

SUPERIOR:	INSTITUTO TECNOLOGICO SUPERIOR AERONAUTICO
------------------	---

CURSOS:

SUFICIENCIA EN INGLES	INSTITUTO TECNOLOGICO SUPERIOR AERONAUTICO
------------------------------	---

TELECOMUNICACIONES Y REDES	UNIVERSIDAD DE ESPECIALIDADES "ESPIRITU SANTO"
-----------------------------------	---

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR:

CBOS. AGUAS NIETO LUIS OSWALDO

CI: 171543090-4

DIRECTOR DE CARRERAS I.T.S.A

ING. GUILLERMO TRUJILLO J.

LATACUNGA,