

# Manual de Redes



**Martín Vargas**  
Cordinación RPC y Redes



# Curso de Redes

## Índice:

### ***Bolilla 1***

Introducción	2
¿Qué es una red informática?	2
Cliente-servidor.	2
Clasificación De Redes	3
Medio Físico	5
Protocolos de Comunicaciones	9
Protocolos de Red	11
Clasificación de las Redes	12
Hardware de Red	14
El Modelo OSI	17
Comparación entre Protocolos OSI e Internet	20
Conectores RJ-45	21
Configuración de una Red	22
Comandos	24
Configuración de un Routers WAN-LAN	27
Redes Inalámbrica	34

### ***Anexo I***

Windows NT Server	38
Windows 2000 Server	38
Dominios y Relaciones de Confianza	40
Definición de Dominios	41
Concepto Básico Sobre Cuentas de Usuario	44
El Entorno de Usuario	45
Planificación de la Seguridad	46

### ***Anexo II***

Realizando un cableado estructurado	49
Que es La Categoría 5	50
Distancias permitidas.	50
Componentes del cableado estructurado	52



## **Introducción**

### **¿Qué es una red informática?**

Se puede definir una red informática como un conjunto de equipos conectados entre sí con la finalidad de compartir información y recursos

La finalidad de una red es que los usuarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la organización. Así las organizaciones obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- **Mayor facilidad de comunicación.**
- **Mejora de la competitividad.**
- **Mejora de la dinámica de grupo.**
- **Reducción del presupuesto para proceso de datos.**
- **Reducción de los costos de proceso por usuario.**
- **Mejoras en la administración de los programas.**
- **Mejoras en la integridad de los datos.**
- **Mejora en los tiempos de respuesta.**
- **Flexibilidad en el proceso de datos.**
- **Mayor variedad de programas.**
- **Mayor facilidad de uso. Mejor seguridad.**

Para la prestación de los servicios de red se requiere que existan sistemas en la red con capacidad para actuar como servidores. Los servidores y servicios de red se basan en los sistemas operativos de red.

Un sistema operativo de red es un conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios. Estos programas interceptan las peticiones de servicio de los usuarios y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red, le permite a ésta ofrecer capacidades de multiproceso y multiusuario. Según la forma de interacción de los programas en la red, existen dos formas de arquitectura lógica:

### **Cliente-servidor**

Este es un modelo de proceso en el que las tareas se reparten entre programas que se ejecutan en el servidor y otros en la estación de trabajo del usuario. En una red cualquier equipo puede ser el servidor o el cliente. El cliente es la entidad que solicita la realización de una tarea, el servidor es quien la realiza en nombre del cliente. Este es el caso de aplicaciones de acceso a bases de datos, en las cuales las estaciones ejecutan las tareas del interfaz de usuario (pantallas de entrada de datos o consultas, listados, etc) y el servidor realiza las actualizaciones y recuperaciones de datos en la base. En este tipo de redes, las estaciones no se comunican entre sí.



Las ventajas de este modelo incluyen:

- Incremento en la productividad.
- Control o reducción de costos al compartir recursos.
- Facilidad de administración, al concentrarse el trabajo en los servidores.
- Facilidad de adaptación.

Redes de pares (peer-to-peer).

Este modelo permite la comunicación entre usuarios (estaciones) directamente sin tener que pasar por un equipo central para la transferencia. Las principales ventajas de este modelo son:

- Sencillez y facilidad de instalación, administración y uso.
- Flexibilidad. Cualquier estación puede ser un servidor y puede cambiar de papel, de proveedor a usuario según los servicios.

### **Clasificación De Redes**

Se pueden configurar las redes en base a diferentes puntos, por ejemplo:

#### **Tecnología de transmisión**

• **Broadcast.** Un solo canal de comunicación compartido por todas las máquinas. Un “paquete” mandado por alguna máquina es recibido por todas las otras.

• **Point-to-point.** Muchas conexiones entre pares individuales de máquinas.

Los paquetes de A a B pueden atravesar máquinas intermedias, entonces se necesita el ruteo (*routing*) para dirigirlos.

#### **Por el tamaño**

- **LAN (local area network)**
- **MAN (metropolitan area network): 10 km**
- **WAN (wide area network): 100 km a 10.000 km**

#### ***Lan***

Normalmente usan la tecnología de broadcast: un solo cable con todas las máquinas conectadas. El tamaño es restringido a una misma área física.

Velocidades típicas son de 10 a 100 Mbps (megabits por segundo; un megabit es 1.000.000 bits)



### *MAN*

Una red de área metropolitana es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, pertenecientes a la misma organización propietaria de los equipos y utilizando medios de enlace de diferentes características.

### *WAN*

Consisten en una colección de *hosts* (máquinas) o LANs de hosts conectados por una *subred*. La subred consiste en las líneas de transmisión y los *ruteadores*, que son PC's dedicados a cambiar de ruta. Se mandan los paquetes de un ruteador a otro. Se dice que la red es *packet-switched* (paquetes Ruteados) o *store-and-forward* (guardar y reenviar).

## **Topología**

La topología o forma lógica de una red es la forma en que se construye el cableado que comunica a cada computador con el servidor, esto puede ser en:

- Anillo.
- Estrella.
- Bus.
- Árbol.
- Trama.

### *Anillo.*

Es una de las tres principales topologías de red. Las estaciones están unidas una con otra formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo.

Una variación del anillo que se utiliza principalmente en redes de fibra como FDDI es el doble anillo.

### *Estrella.*

Es otra de las tres principales topologías. La red se une en un único punto, normalmente con control centralizado, como un concentrador de cableado.

### *Bus.*

Es la tercera de las topologías principales. Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo



### *Árbol.*

Esta estructura de red se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

### *Trama*

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (Lan). Los nodos están conectados cada uno con todos los demás.

## **Medio físico**

El medio físico es el medio sobre el que se envían las señales eléctricas (BITS) para realizar la transmisión de la información.

Los *cables de cobre* utilizados para transmisión son conductores clásicos que en ocasiones no son de este metal, sino aleaciones que mejoran las características eléctricas del cable. Los más utilizados son:

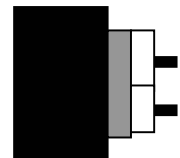
### *Coaxial.*

El término *coaxial* quiere decir eje común ya que un cable coaxial está formado por un conductor central rodeado de una capa de material aislante o *dieléctrico*, rodeada a su vez por una malla de hilos conductores cubierta por una funda de material aislante y protector, Formado así cuatro capas concéntricas, como se ve en la figura:



### *Twinaxial.*

Este tipo de cable es una variación del coaxial que dispone de dos conductores centrales, envueltos cada uno en un aislante. Se utiliza en instalaciones de redes de tipo TOKEN RING.



*Par trenzado apantallado (STP, Shielded Twisted Pair).*

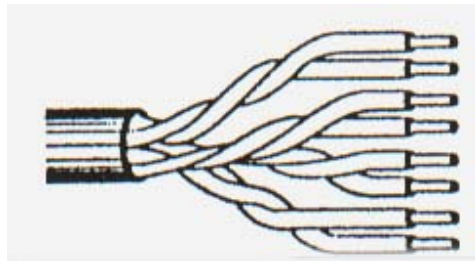


Este tipo de cable está formado por grupos de dos conductores cada uno con su propio aislante trenzados entre sí y rodeados de una pantalla de material conductor, recubierta a su vez por un aislante. Cada grupo se trenza con los demás que forman el cable y, el conjunto total se rodea de una malla conductora y una capa de aislante protector. Esta

disposición reduce las interferencias externas, las interferencias entre pares y la emisión de señales producidas por las corrientes que circulan por el cable. Un uso común de este tipo de cables es la conexión de los trancéptores insertados en el coaxial de una red 10base5 con la NIC de una estación.

*Par trenzado sin pantalla (UTP, Unshielded Twisted Pair).*

En este tipo de cable, los conductores aislados se trenzan entre sí en pares y todos



los pares del cable a su vez. Esto reduce las interferencias entre pares y la emisión de señales. Estos cables se utilizan, sobre todo, para los sistemas de cableado integral, combinando telefonía y redes de transmisión de datos, principalmente 10baseT. Se han definidos estándares para la instalación y cableado del cable UTP que trabajan con las redes 10 BASE-T. El estándar define las

siguientes categorías de cable:

- Categoría 1: Cable telefónico de par trenzado sin apantallar, apto para voz pero no para datos.
- Categoría 2 Cable de par trenzado sin apantallar para transmisiones de hasta 4 Mbits/seg.
- Categoría 3 Soporta velocidades de transmisión de hasta 16 mbits/seg, se utiliza en 10baseT Ethernet 10Mbits, el cable es de 3 pares.
- Categoría 4 Certificado para velocidades de no mas de 20 Mbits/seg, tiene 4 pares.
- Categoría 5 Define un cable de 4 pares de 100 ohmios que puede transmitir hasta 100 Mbits/seg.

## Fibra óptica



La fibra es un medio de transmisión de información analógica o digital. Las ondas electromagnéticas viajan en el espacio a la velocidad de la luz.

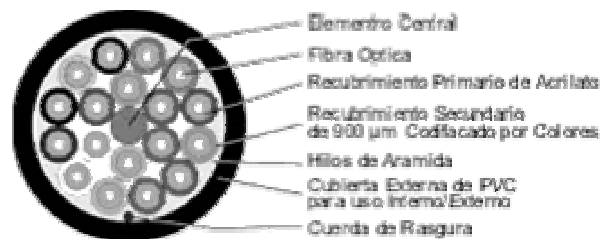
Básicamente, la fibra óptica está compuesta por una región cilíndrica, por la cual se efectúa la propagación, denominada núcleo y de una zona externa al núcleo y coaxial con él, totalmente necesaria para que se produzca el mecanismo de propagación, y que se denomina envoltura o revestimiento.

La capacidad de transmisión de información que tiene una fibra óptica depende de tres características fundamentales:

a) *Del diseño geométrico de la fibra.*

b) *De las propiedades de los materiales empleados en su elaboración. (diseño óptico)*

c) *De la anchura espectral de la fuente de luz utilizada. Cuanto mayor sea esta anchura, menor será la capacidad de transmisión de información de esa fibra.*



El peso del cable de fibras ópticas es muy inferior al de los cables metálicos, redundando en su facilidad de instalación.

La mayoría de las fibras ópticas se hacen de arena o sílice, materia prima abundante en comparación con el cobre. Con unos kilogramos de vidrio pueden fabricarse aproximadamente 43 kilómetros de fibra óptica. Los dos constituyentes esenciales de las fibras ópticas son el núcleo y el revestimiento. El núcleo es la parte más interna de la fibra y es la que guía la luz.

La F.O. presenta un funcionamiento uniforme desde -550 C a +125C sin degradación de sus características.

Las microcurvaturas y tensiones se determinan por medio de los ensayos de:

- **Tensión:** cuando se estira o contrae el cable se pueden causar fuerzas que rebasen el porcentaje de elasticidad de la fibra óptica y se rompa o formen microcurvaturas.
- **Compresión:** es el esfuerzo transversal.
- **Impacto:** se debe principalmente a las protecciones del cable óptico.
- **Enrollamiento:** existe siempre un límite para el ángulo de curvatura pero, la existencia del forro impide que se sobrepase.
- **Torsión:** es el esfuerzo lateral y de tracción.





### Comparación con los Cables Coaxiales

Características	Fibra Óptica	Coaxial
Longitud de la Bobina (mts)	2000	230
Peso (kgs/km)	190	7900
Diámetro (mm)	14	58
Radio de Curvatura (cms)	14	55
Distancia entre repetidores (Kms)	40	1.5
Atenuación (dB / km) para un Sistema de 56 Mbps	0.4	40

#### VENTAJAS

- La fibra óptica hace posible navegar por Internet a una velocidad de dos millones de bps.
- Acceso ilimitado y continuo las 24 horas del día, sin congestiones.
- Video y sonido en tiempo real.
- Es inmune al ruido y las interferencias.
- Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.
- Carencia de señales eléctricas en la fibra.
- Presenta dimensiones más reducidas que los medios preexistentes.
- El peso del cable de fibras ópticas es muy inferior al de los cables metálicos.
- La materia prima para fabricarla es abundante en la naturaleza.
- Compatibilidad con la tecnología digital.

#### INCONVENIENTES

- Sólo pueden suscribirse las personas que viven en las zonas de la ciudad por las cuales ya esté instalada la red de fibra óptica.
- El coste es alto en la conexión de fibra óptica, las empresas no cobran por tiempo de utilización sino por cantidad de información transferida al computador, que se mide en megabytes.
- El coste de instalación es elevado.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.



## **Protocolos De Comunicaciones**

Los protocolos de bajo nivel controlan el acceso al medio físico, a través de la tarjeta de red, lo que se conoce como *MAC (Media Access Control)*.

Los tipos de protocolos más utilizados son los siguientes:

### **ETHERNET**

El protocolo de red Ethernet fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Es el método de conexión más extendido en la actualidad.

La velocidad de transmisión de datos en Ethernet es de 10/100 Mbits/s. En este tipo de protocolos todas las terminales comparten el ancho de banda disponible.

#### **Existen cuatro tipos de Ethernet:**

##### *10Base2:*

Puede transmitir datos a 10mbps pudiendo llegar el cableado hasta 185 metros. Se utiliza cable coaxial RG-58. Un mismo segmento de cable puede soportar hasta 30 computadoras aproximadamente. Es el más utilizado y recomendado para redes pequeñas. Utiliza la topología local bus, donde un mismo cable recorre todas y cada una de las computadoras.

##### *10Base5:*

Transmite datos a 10mbps puede alcanzar 500 metros. El cableado es grueso y es utilizado principalmente para largas oficinas o hasta todas las computadoras de un edificio. Del cable principal (backbone) salen cables usualmente Par Trenzado que se conectan directamente a cada una de las computadoras. Se pueden conectar hasta 100 computadoras con este cableado en un mismo segmento.

##### *10BaseT:*

Transmite datos entre 10mbps y 100 mbps por Banda Base y utiliza un Hub (concentrador) desde el cual con cable Par Trenzado se conecta cada una de las computadoras quedando en forma de estrella. El Hub queda en el centro de la estrella y funciona como "repetidor". El cable desde el Hub hasta la computadora no debe de medir más de 100 mts.



### *10baseF:*

Es la especificación Ethernet sobre fibra óptica. Los cables de cobre presentan el problema de ser susceptibles tanto de producir como de recibir interferencias. Por ello, en entornos industriales o donde existen equipos sensibles a las interferencias, es muy útil poder utilizar la fibra. Normalmente, las redes Ethernet de fibra suelen tener una topología en estrella.

### *Token Ring*

Las redes basadas en protocolos de paso de tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbits/s.

Existen redes token ring de 16 Mbits/s, pero no están definidas en ninguna especificación de IEEE. Es una topología inventada por IBM para sus equipos del tipo Main Frame. Las estaciones conectadas al anillo transfieren paquetes a sus vecinos, de esta manera cada estación actúa como un repetidor. Las placas de token ring de IBM existen en versiones de 4 Mbits y de 16 Mbytes por segundo. El máximo de estaciones en un anillo es 260 para cable apantallado.

### *Frame Relay (Paso de tramas)*

Es un protocolo que define conexiones a una red pública de datos, brindando rapidez y eficiencia. La comunicación se realiza a través de una línea dedicada, el tráfico se envía por esta línea al proveedor de frame relay y se conmuta a través de la red. Estas redes transmiten normalmente a velocidades de 1.5 Mbits/seg. de datos.

### *ATM (Asynchronous Transfer Mode - Modo de transferencia asíncrono).*

Es la especificación más reciente y con mayor futuro. Permite velocidades de a partir de 156 Mbits/s llegando a superar los 560 Mbits/s. Se basa en la transmisión de pequeños paquetes de datos de 56 bytes, con una mínima cabecera de dirección que son conmutados por equipos de muy alta velocidad. La gran ventaja de esta especificación es la capacidad que tiene para transmitir información sensible a los retardos como pueden ser voz o imágenes digitalizadas combinada con datos, gracias a la capacidad de marcar los paquetes como posibles de ser eliminados, para que los equipos de conmutación puedan decidir que paquetes transmitir en caso de congestión de la red.



## **Protocolos de Red**

Un *protocolo* es el elemento esencial que permite que programas de diferentes fabricantes, escritos en distintos lenguajes y ejecutándose en máquinas muy dispares puedan "hablar" entre sí.

El protocolo de red determina el modo y organización de la información (tanto datos como controles) para su transmisión por el medio físico con el protocolo de bajo nivel.

Los protocolos de red más comunes son.

- IPX/SPX.
- TCP/IP.
- AppleTalk.
- NetBEUI.

IPX/SPX.

***Internetwork Packet eXchange/Sequenced Packet eXchange.*** Es el conjunto de protocolos punto a punto utilizado por el sistema operativo de red **Netware** de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

TCP/IP.

Este no es un protocolo, si no un conjunto de protocolos, que toma su nombre de los dos más conocidos: **TCP** (*Transmission Control Protocol*, protocolo de control de transmisión) e **IP** (*Internet Protocol*). Esta familia de protocolos es la base de la red Internet, la mayor red de PC's del mundo. Por lo cual, se ha convertido en el más extendido.

TCP/IP es un protocolo de red independiente del nivel físico y que soporta múltiples sesiones entre múltiples PC's.

TCP/IP está construido en capas, lo que permite adaptarlo a nuevas tecnologías y requerimientos sin necesidad de modificar el conjunto.

TCP/IP soporta sesiones confirmadas, asegurando que los datos llegan a su destino, y lo hacen en el mismo orden en que se enviaron.

La arquitectura abierta de TCP/IP permite construir sobre él protocolos de aplicación de muy diversa índole y funcionalidad, muchos de los cuales son estándares muy conocidos.



## Direccionamiento IP

Todos los nodos de una red necesitan de una dirección numérica de 4 bytes (32 bits) llamados octetos, con este número se identifica cada nodo de la red.

Algunos protocolos de aplicación fueron construidos bajo el conjunto de protocolos TCP.

- FTP (Transferencia de archivos entre estaciones de una red.
- SMTP (Protocolo para la transferencia de mensajes electrónicos)
- IP (Protocolo para la Internet)

## Clasificación de las Redes

Existen 3 clases de redes, denominadas A, B y C cada clase permite un número limitado de direcciones de red y de host. Las redes de clase A permiten definir hasta 126 redes y una cantidad ilimitada de host, mientras que las redes de clase C definen una cantidad casi ilimitada de redes pero solo 255 host por red. Cuando se instalan los servicios TCP/IP también será necesario especificar la máscara de subred, la cual identifica la parte del identificador de host de la dirección basada en la clase de red.

*CLASE A:* El primer Byte es un número del 1 al 127. Los últimos 3 bytes identifican host en la red. La máscara de la subred 255.0.0.0

*CLASE B:* El primer byte es un número del 128 al 191. El segundo byte es parte de la dirección de red, el 3 y 4 bytes solo identifican host en la red, Máscara de subred: 255.255.0.0

*CLASE C:* El primer byte es un número de 192 al 254. El segundo y tercer byte son parte de la dirección de red, el 4 byte solo identifica hasta 255 host. Máscara de subred 255.255.255.0.

## Máscara de Subred

Una máscara de subred es el principal modo en que TCP/IP limita el número de posibles direcciones con que tenga que tratar una máquina en un momento dado.

La máscara de red es una manera de enmascarar o esconder unas partes de la red de otras.

La máscara de red para su dirección determina cuántos de los números que componen la dirección IP serán vistos en realidad por otras máquinas como una dirección local de la red.

Por eso es importante que las computadoras en una misma parte local de la red usen la misma máscara de subred.



### AppleTalk.

Este protocolo está incluido en el sistema operativo del computador Apple Macintosh desde su aparición y permite interconectar PC's y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Existen tres formas básicas de este protocolo:

### LocalTalk.

Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida pero es adecuada para los servicios que en principio se requerían de ella, principalmente compartir impresoras.

### Ethertalk.

Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita aplicaciones como la transferencia de ficheros.

### Tokenalk.

Es la versión de Appletalk para redes Tokenring.

### NETBEUI.

**NetBIOS Extended User Interface** (Interfaz de usuario extendido para NetBIOS). Es la versión de Microsoft del **NetBIOS** (Network Basic Input/Output System, sistema básico de entrada/salida de red), que es el sistema de enlazar el *software* y el *hardware* de red en los PCs. Este protocolo es la base de la red de Microsoft Windows para Trabajo en Grupo.

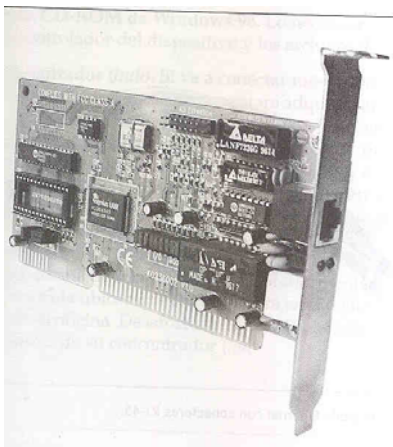


## HARDWARE DE RED

- NIC (Tarjeta de red).
- HUB/SWITCHES.
- Bridges.
- Gateways.(Software)
- Routers.

Estos son los elementos necesarios más comunes para armar una red entre dos o más PC's, los cuales analizaremos a continuación:

### NIC (Tarjeta de red).



**Network Interface Card** (Tarjeta de interfaz de red) o **Medium Access Card** (Tarjeta de acceso al medio). Es el dispositivo que conecta la estación (computador u otro equipo de red) con el medio físico. Se suele hablar de tarjetas en el caso de los PC's, ya que la presentación suele ser como una tarjeta de ampliación de los mismos, diferente de la placa de CPU, aunque cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporado.

A veces, es necesario, además de la tarjeta de red, un **transceptor**. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10base5) o porque el medio sea distinto del que utiliza la tarjeta.

### HUB / SWITCHES (CONCENTRADORES)



Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo *concentradores* de cableado, pero cada vez disponen de mayor número de capacidades, como aislamiento de tramos de red, capacidad de conmutación de las salidas para aumentar la capacidad de la red, gestión remota, etc. Los concentradores se pueden clasificar en tres grupos principales:

- Grupos de trabajo
- Intermedios
- Empresa.



## BRIDGES

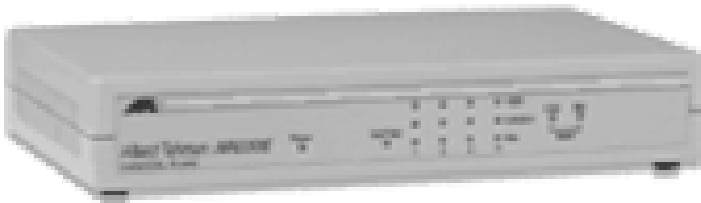
Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones.

Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

### Los bridges ofrecen las siguientes ventajas y funciones:

- Puede ampliar la distancia o numero de nodos de toda la red
- Puede dividir una red sobrecargada en dos segmentos, mejorando el rendimiento
- Los bridges son independientes del protocolo.

## ROUTERS



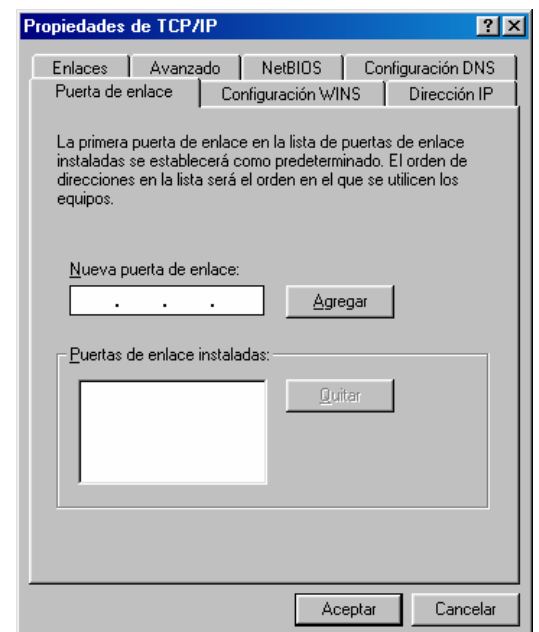
Son equipos de interconexión de redes que actúan a nivel de la red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Se encarga de encontrar el camino mas corto entre wan y Wan.

Los routers son conmutadores de paquetes dependientes del protocolo. Estos leen la información definida en el nivel de Red, esta información contiene las direcciones de red origen y destino.

Como funcionan, supongamos que una estación (nodo 1) desea enviar un paquete a una estación (nodo 2) en una red distante. Solo necesitamos enviar el paquete del nodo 1 a su router, que a su vez envía el paquete al router de la red de destino (nodo2)

## GATEWAYS

Son puertas de enlace que permiten comunicar una red con otra red a nivel de protocolos de red. Es donde se le dice a la red por donde debe enviar la información. A través de las direcciones de red.





## UTILIZACIÓN DE BRIDGES, ROUTERS Y HUBS

Los *repetidores, bridges, routers*, son dispositivos que pueden usarse para ampliar la red o interconectar redes.

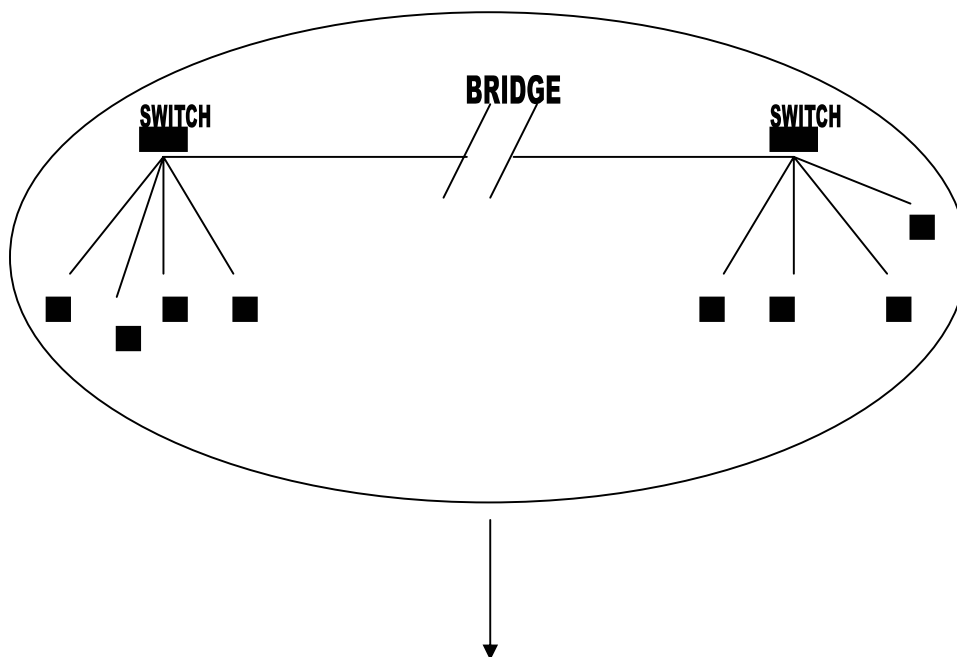
Cuando la red se sobrecarga de tráfico y el rendimiento comienza a bajar, se puede solucionar con una de estas opciones:

- Dividir la red y enlazarla a través de bridges o routers.
- Utilizar una topología más rápida.

Cuando se divide una red se puede filtrar o bloquear la transmisión para evitar que se transmita a toda la red.

Si se utiliza un BRIDGE para dividir una red existente en dos segmentos de red, continúa teniendo la misma dirección, pero se puede filtrar el tráfico para reducir la carga de ambos lados de la red.

Si en cambio se quiere interconectar subredes deberá utilizar un ROUTERS, cada una de las subredes deberá tener su propia dirección, estos dispositivos gestionan todo el tráfico entre redes.



*Un mismo sistema de red, dividido en dos sectores por un bridge.*



## **El Modelo OSI**

### **Redes Divididas en Niveles**

Las redes se dividen normalmente en niveles. El objetivo de estos niveles es tratar la información para pasarla a los niveles adyacentes, el número de niveles varía según la red.

Para normalizar las redes estructuradas en niveles la Organización Internacional de Estándares (ISO) propuso su Modelo de Referencia OSI (Interconexión de sistemas abiertos).

El sistema OSI tiene 7 niveles que son:

### **Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación.**

Cada uno de estos niveles es realizado por una parte de hardware y/o software del sistema.

#### *Nivel Físico*

Es prácticamente todo hardware y define el medio de comunicación (tipo de cable y conectores), los niveles eléctricos de la señal, velocidad de la transmisión con el fin de que un bit enviado con un determinado valor (0 ó 1) sea reconocido en el extremo receptor.

#### *Nivel de Enlace de datos*

Se refiere a la conexión física entre máquinas. Debe asegurar la transmisión y recepción sin errores, para ello divide los datos emitidos en tramas. Este nivel asegurará la recepción sin problemas. El bridge actúa en este nivel y por tanto solo son capaces de encaminar paquetes entre nodos de la misma red física.

#### *Nivel de Red*

Se encarga de encaminar los paquetes desde su origen a su destino. Define protocolos para la transmisión de paquetes en redes interconectadas mediante router, son responsables del encaminamiento de los paquetes enviados en la red.

#### *Nivel de Transporte*

Realiza una conexión extremo a extremo entre los niveles de transporte de las máquinas origen y destino. Los protocolos de los tres niveles inferiores trabajan entre máquinas adyacentes y los paquetes pasan por esos niveles de todas las máquinas de la ruta.

En una comunicación, solo se ven involucrados los niveles de transporte del origen y destino sin intervenir los de las máquinas intermedias.



En una comunicación a través de varios nodos puede suceder que se pierdan las tramas de asentimiento con lo que el nodo que ha enviado la trama volverá hacerlo creyendo que se ha perdido por lo que tendremos tramas duplicadas en la red. Además, si empleamos un encaminamiento dinámico utilizando diferentes rutas puede ser que una trama enviada más tarde de un mismo conjunto de datos llegue antes que las enviadas anteriormente. El nivel de transporte será el encargado de eliminar las tramas repetidas y ponerlas todas en el orden correcto. El nivel de transporte será la encargada de subsanar las posibles deficiencias del nivel de red. Los protocolos SPX y TCP trabajan en la conexión del nivel de transporte.

#### *Nivel de Sesión*

Gestiona el control de diálogo entre los usuarios de diferentes máquinas mejorando los servicios entre ellos permitiendo que el tráfico vaya en un solo sentido o evitando que ambos extremos ejecuten una misma operación a la vez. También realiza tareas de sincronización. Por ejemplo el nivel de sesión en una transferencia de archivo va insertando puntos de verificación. Si tenemos una red insegura cada vez que exista una interrupción de las comunicaciones el nivel de sesión se encargará de proseguirlas a partir del último punto de verificación.

#### *Nivel de Presentación*

Se ocupa de los aspectos de representación de la información. Por ejemplo se ocupa del tipo de codificación de los datos previamente establecido. También se ocupa de la compresión de los datos y de su encriptación.

#### *Nivel de Aplicación*

Se ocupa de emulación de terminales, transferencia de ficheros, correo electrónico y otras aplicaciones.

### **Modo de Comunicación de Datos en el Modelo OSI**

Los datos que se desean enviar de una máquina a otra son llevados al nivel de aplicación. Ahí se le añade la cabecera de aplicación CA delante de los datos y entonces el tren de bits es pasado al nivel de presentación. Esta transforma toda la información recibida – cabecera y datos – y la pasa al nivel de sesión y así sucesivamente. De esta forma todos los niveles transforman el tren de bits que les viene del nivel superior en bloque sin importarles que parte sean las cabeceras de los niveles anteriores y que parte sean los datos y posteriormente añaden su propia cabecera.

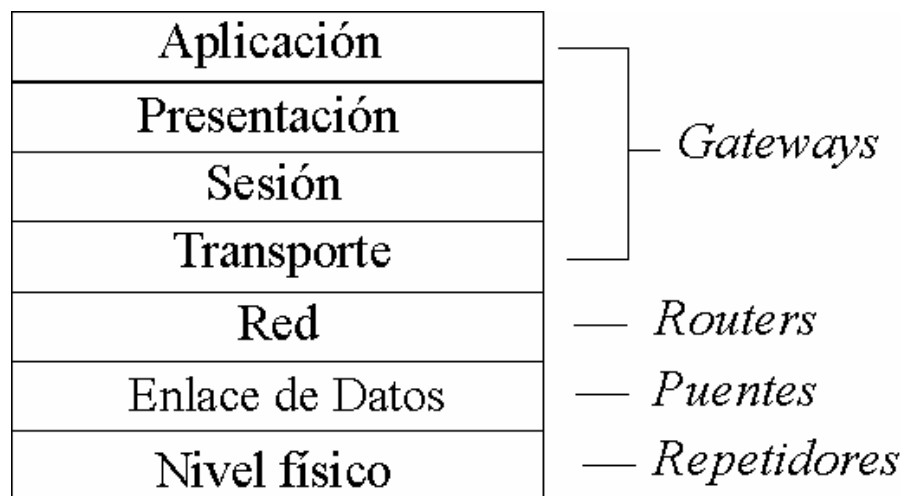
Así llegan al nivel físico que coloca los paquetes que le llegan en el medio de transmisión y los envía a la máquina receptora. Allí los paquetes seguirán el proceso contrario: cada nivel quita su cabecera correspondiente y realiza la transformación inversa a la realizada por el nivel equivalente, llegando al nivel de presentación que entrega al proceso receptor el tren de bits del proceso emisor.



En los nodos intermedios solo los otros tres niveles inferiores habrán tenido que tratar la información observando en la cabecera correspondiente a su nivel si el paquete iba dirigido a ellos, y viendo que no, reenviándolo hacia el receptor.

El resultado para los cuatro niveles superiores es como si hubieran recibido de su nivel equivalente directamente la información.

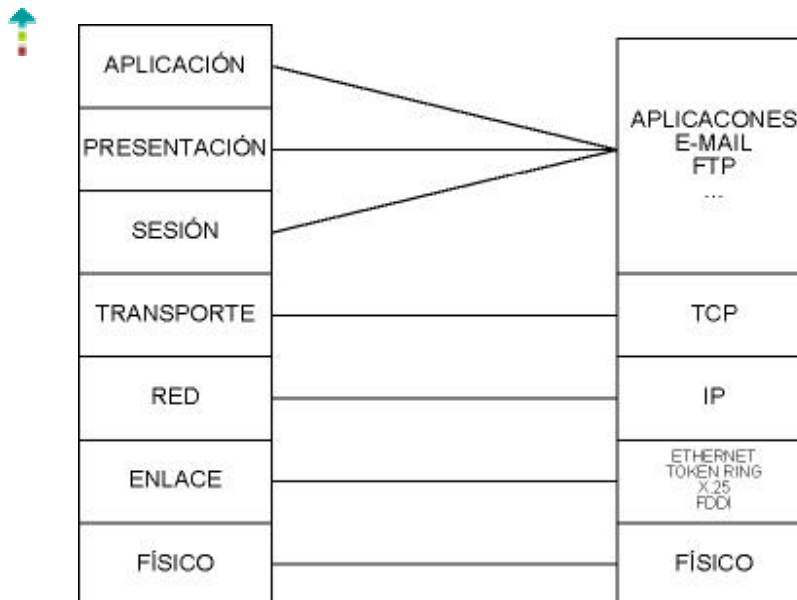
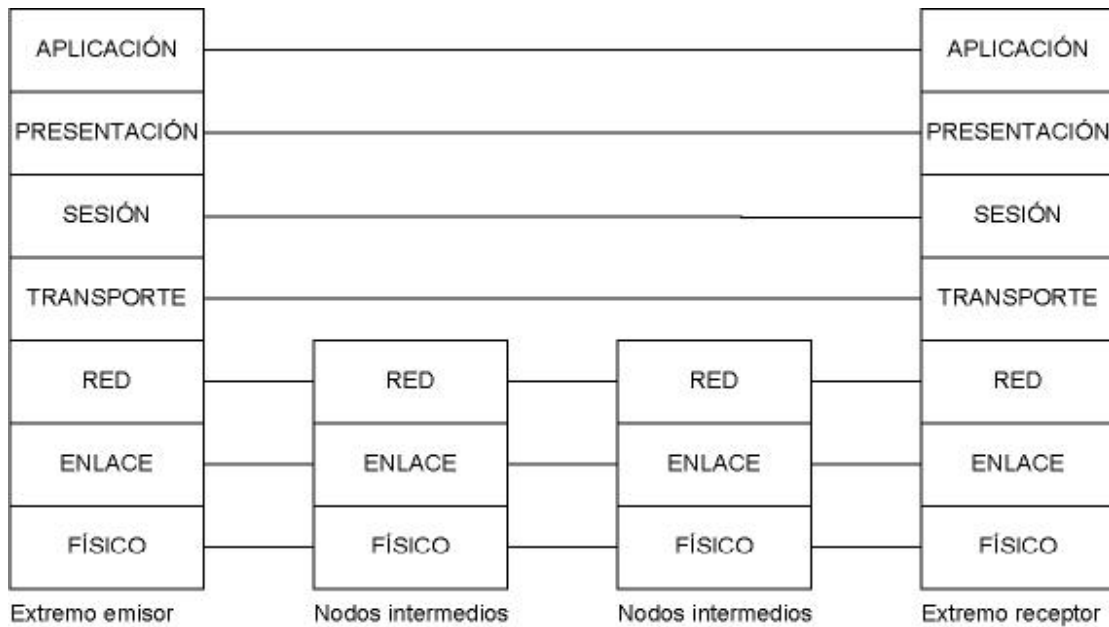
Por ello los niveles superiores se denominan protocolos de extremo a extremo. En la figura podemos ver un esquema de transmisión de modelo OSI.



### Comparación entre Protocolos OSI e Internet

Aunque el modelo OSI estaba pensado para que fuera seguido por la mayoría de las redes futuras el auge de Internet ha hecho que la pila de protocolos basada en TCP/IP sea la más utilizada en la actualidad.

En la figura podemos ver la comparación entre ambos modelos.





### Armado de Conectores RJ-45 Según la Norma

El cable UTP (**par trenzado no blindado**) es de 4 pares (8 hilos), normalmente de los siguientes colores:

- Naranja
- Verde
- Azul
- Marrón

Si esta usando 568A:

<b>1-Blanco-Verde</b>
<b>2-Verde</b>
<b>3-Blanco-Naranja</b>
<b>4-Azul</b>
<b>5-Blanco-Azul</b>
<b>6-Naranja</b>
<b>7-Blanco Marrón</b>
<b>8-Marrón</b>

Si esta usando 568B:

<b>1-Blanco Naranja</b>
<b>2-Naranja</b>
<b>3-Blanco Verde</b>
<b>4-Azul</b>
<b>5-Blanco-Azul</b>
<b>6-Verde</b>
<b>7-Blanco Marrón</b>
<b>8-Marrón</b>

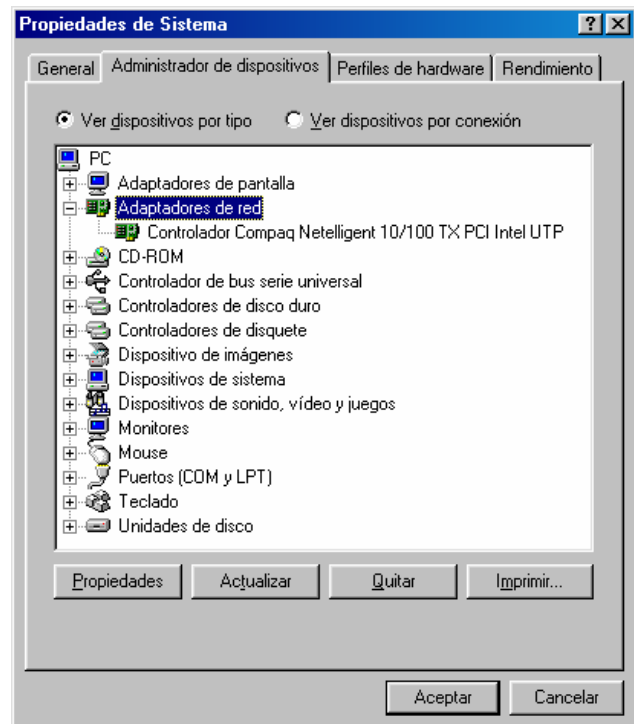
Si se desea hacer un **CROSS OVER**, un patch cord cruzado, se debe colocar en un extremo del cable un conector en norma 568 A y en el otro un conector en norma 568 B



## Pasos para la Configuración de una Red Bajo El Sistema Operativo Windows 98

Antes de iniciar la configuración de la red, es necesario haber instalado los controladores de nuestro adaptador de red, según se muestra en la fotografía adjunta

Es importante no confundir el “Adaptador de acceso telefónico a redes” con la tarjeta de red.

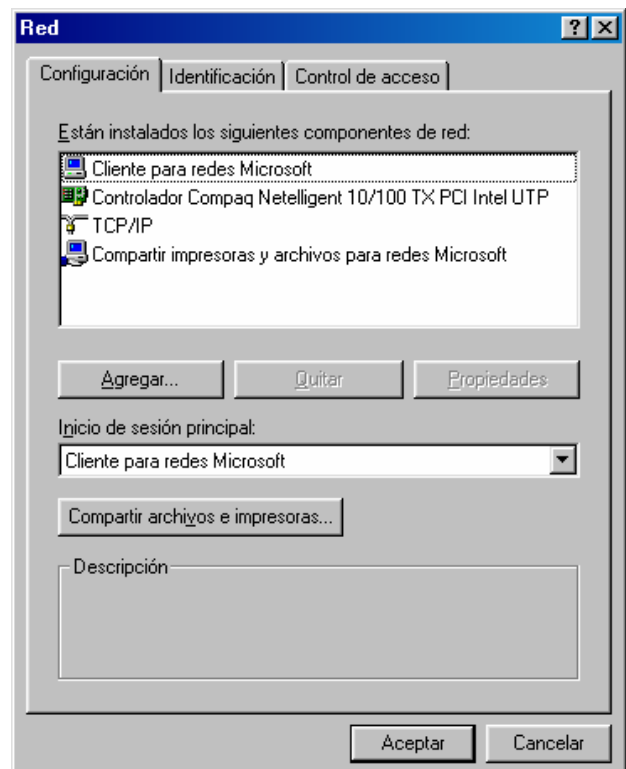


Luego con el botón derecho se debe presionar sobre el icono de “entorno de red” el cual nos despliega la siguiente pantalla:

En esta pantalla se pueden observar los diferentes protocolos de red que se deben configurar en nuestro equipo para transformarlo en un nodo de la red.

Seleccione la opción TCP/IP, en donde deberá configurar el protocolo según el siguiente detalle: Donde aparece la dirección IP debe escribir lo siguiente 192.168.0.x (donde x será el número único de cada PC) el rango de este valor es de 1 a 254.

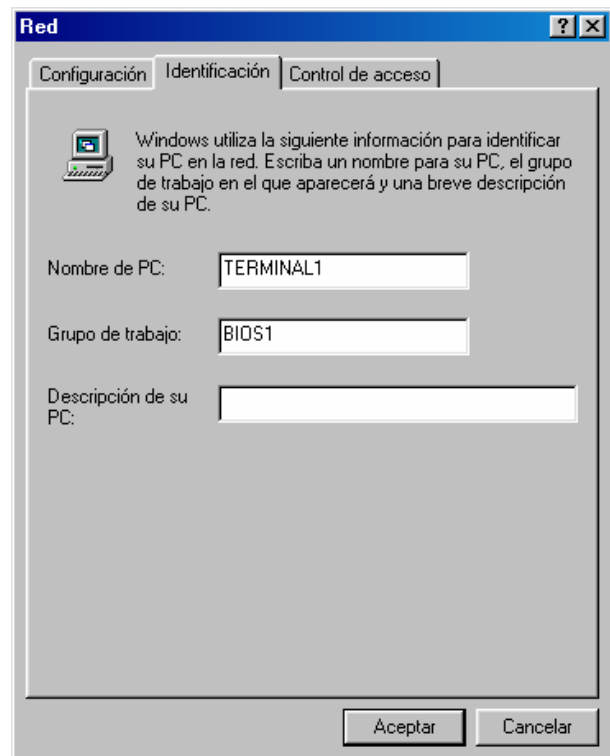
En la opción Mascara de Red debe introducir el valor 255.255.255.0



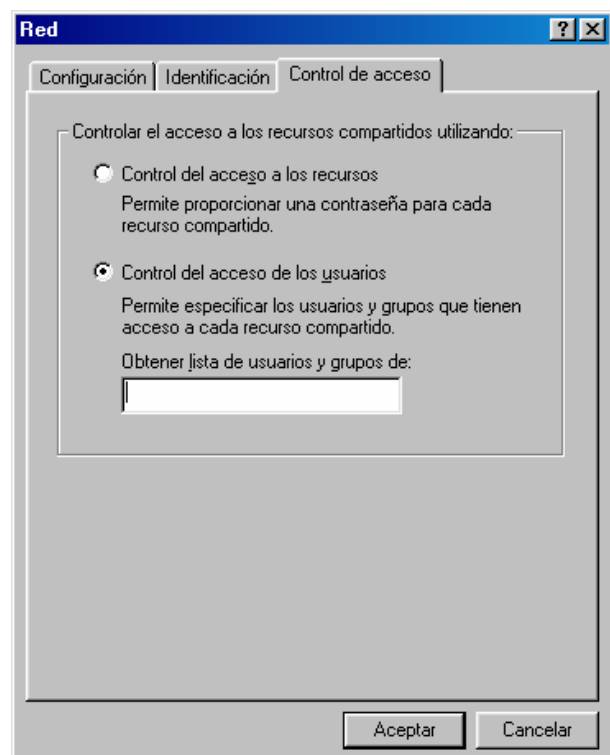


En esta ventana identificamos a nuestra PC, es decir, el nombre con que el equipo aparecerá en la red y será visto por otros usuarios.

También es necesario generar un grupo de trabajo, debido a que toda red necesita tener grupos de afinidad. Ese nombre deberá repetirse en cada nodo de la red.



Las opciones del “CONTROL DE ACCESO”, nos permite dar ciertos permisos a otros equipos o usuarios, si trabajamos con servidores, para que puedan ingresar en nuestros recursos compartidos, disco duro e impresora.

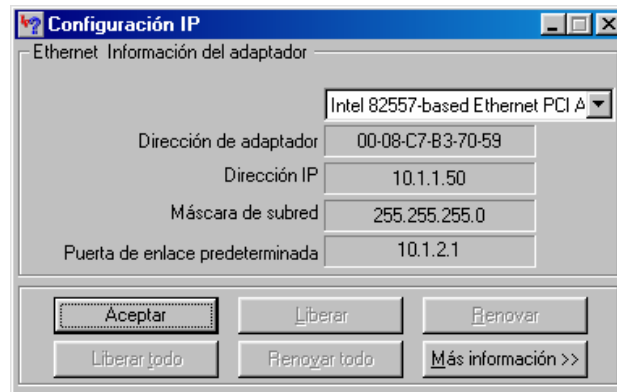






Si queremos chequear la correcta configuración del adaptador de red (NIC) y el de la IP seleccionada, debemos ir al menú Inicio, opción Ejecutar y escribir lo siguiente:

### WINIPCFG.



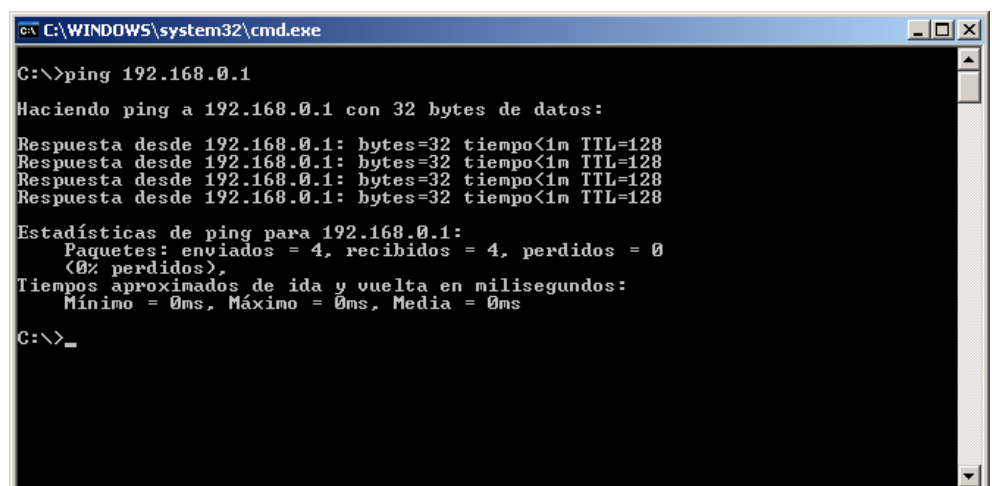
Otros comandos:

### Ping:

Permite el envío de paquetes informáticos una dirección IP especificada esta nos puede dar algunos de los siguientes mensajes:

Ej: Ping a la dirección de nuestro PC:

Si la respuesta es positiva (como lo muestra la imagen) la teoría indica que la instalación del Protocolo es correcta, de lo contrario se deberá de instalar nuevamente el protocolo.





En este caso la respuesta es negativa. Esta respuesta si se diese cuando ejecutamos el mismo comando pero a la dirección IP de otro PC nos daría la señal de que tenemos problemas de conexión, posiblemente el otro PC este apagado o desconectado, para descartar deberíamos de

buscar un tercer PC a quien realizarle un PING. En tanto si nos diera el mensaje mostrado en la figura anterior diríamos que hay una excelente conexión entre los PC's.

Otra variante del comando Ping es la -t que envía ininterrumpidamente paquetes a la dirección IP especificada, de esta forma nos permite ver y establecer si es buena la conexión y estable.

Para ver mas variantes del comando Ping ejecute "Ping /?".

## IPCONFIG

Este comando nos permite ver desde consola (WINIPCFG funciona solo para Windows 98) la configuración de la o las tarjetas de red.

La variante "pconfig/renew" permite renovar la configuración si esta basada en una configuración bajo DHCP. Por mas opciones ejecute "pconfig/?"

```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.0.10

Haciendo ping a 192.168.0.10 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.10:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos),
C:\>
```

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local        :

    Sufixo de conexión específica DNS :
    Dirección IP. . . . . : 192.168.0.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada :
C:\>_
```



## Tracert

Muestra los saltos de redes necesarios para llegar a una dirección IP especificada. En la primera imagen la dirección IP pertenece a la misma red que el PC que ejecuta el comando.

```
C:\WINDOWS\system32\cmd.exe

C:\>tracert 192.168.0.1

Traza a 192.168.0.1 sobre caminos de 30 saltos como máximo.

 1    <1 ms    <1 ms    <1 ms    192.168.0.1

Traza completa.

C:\>
```

En la segunda imagen se muestra los saltos necesarios para llegar una dirección IP perteneciente a Internet, pasando por todos los Routers y servidores necesario para llegar a la dirección especificada. Este comando es muy útil en redes grandes la cual se

```
C:\WINDOWS\system32\cmd.exe

C:\>tracert biosuruguay.com

Traza a la dirección biosuruguay.com [209.25.160.212]
sobre un máximo de 30 saltos:

 1    45 ms    59 ms    49 ms    pucen2bras1.antel.net.uy [200.40.19.9]
 2    59 ms    49 ms    49 ms    gcentro-2-acc.antel.net.uy [200.40.19.34]
 3    49 ms    49 ms    59 ms    ibb2cen2-adinet.antel.net.uy [200.40.0.202]
 4    59 ms    59 ms    59 ms    ibb2agu2-1-3.antel.net.uy [200.40.16.81]
 5    *        *        *        Tiempo de espera agotado para esta solicitud.
 6   199 ms    200 ms    207 ms    sl-st20-mia-8-12.sprintlink.net [144.223.245.209]
 7   200 ms    200 ms    200 ms    sl-bb20-mia-11-0-0.sprintlink.net [144.232.2.194]
 8   240 ms    240 ms    239 ms    sl-bb24-fw-9-0.sprintlink.net [144.232.20.41]
 9   240 ms    240 ms    240 ms    sl-bb25-fw-14-0.sprintlink.net [144.232.11.94]
10   270 ms    360 ms    270 ms    sl-crs1-ana-0-8-0-2.sprintlink.net [144.232.18.3]
11   270 ms    280 ms    280 ms    sl-bb21-sj-8-0.sprintlink.net [144.232.18.55]
12   280 ms    280 ms    270 ms    sl-st20-sj-13-0.sprintlink.net [144.232.9.58]
13   270 ms    280 ms    280 ms    144.223.242.122
14   280 ms    280 ms    280 ms    oc48-pos4-0.sj-mkp2-dis-1.peer1.net [216.187.88.174]
15   270 ms    280 ms    280 ms    216.187.88.174
16   280 ms    280 ms    280 ms    VLAN3.FMT6509-1.maxim.net [66.40.24.106]
17   280 ms    280 ms    290 ms    host212.maxim.net [209.25.160.212]

Traza completa.

C:\>_
```

encuentra dividida es sub-redes menores.



## Configuración de un Router WAN-LAN

En esta configuración tomaremos de ejemplo un Router de marca SOHO, lo cual no indica que este tenga alguna preferencia para nosotros en la instalación, la configuración de los mismos se realizan de forma muy similar.

Para iniciar la configuración deberemos de iniciar el navegador de Internet de nuestra preferencia, en donde indicamos la página a visitar digitaremos la dirección IP del Router, con esto nos pedirá nombre de usuario y contraseña para ingresar, veamos las opciones de configuración básicas que estos presentan.

En la primera pantalla “SETUP” tenemos:

Nombre del equipo

Zona Horaria

Dirección IP Interna

Dirección IP Externa

Nombre de Usuario y Contraseña

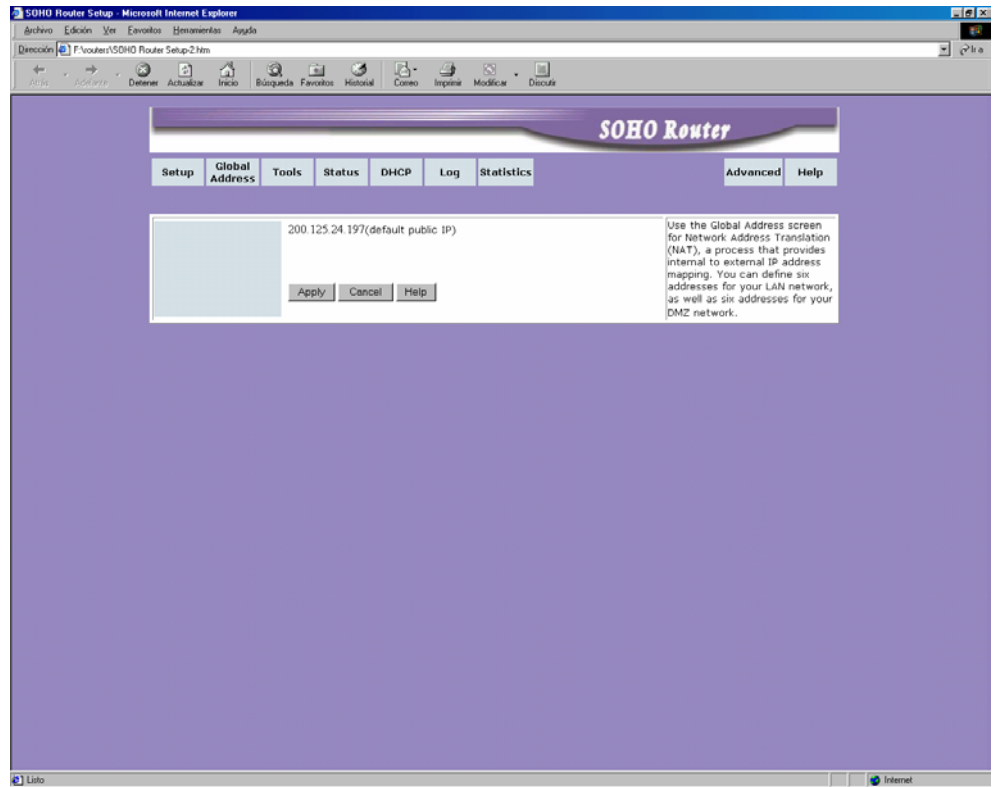
Conexión por Demanda

Destacamos en esta pantalla, el nombre del equipo, la zona horaria y uno de los valores mas importantes es la dirección IP interna que debe de pertenecer al rango de direcciones IP de nuestra red, de esta forma los demás equipos podrán generar un enlace entre los equipos, cabe de destacar que esta dirección será la Puerta de Enlace (Gateway) de los PC's de la red, por otro lado la dirección IP externa será asignada al momento de conectarnos de forma automática y por ultimo deberemos de indicar el nombre de usuarios y contraseñas que se nos asigne al contratar el Servicio.



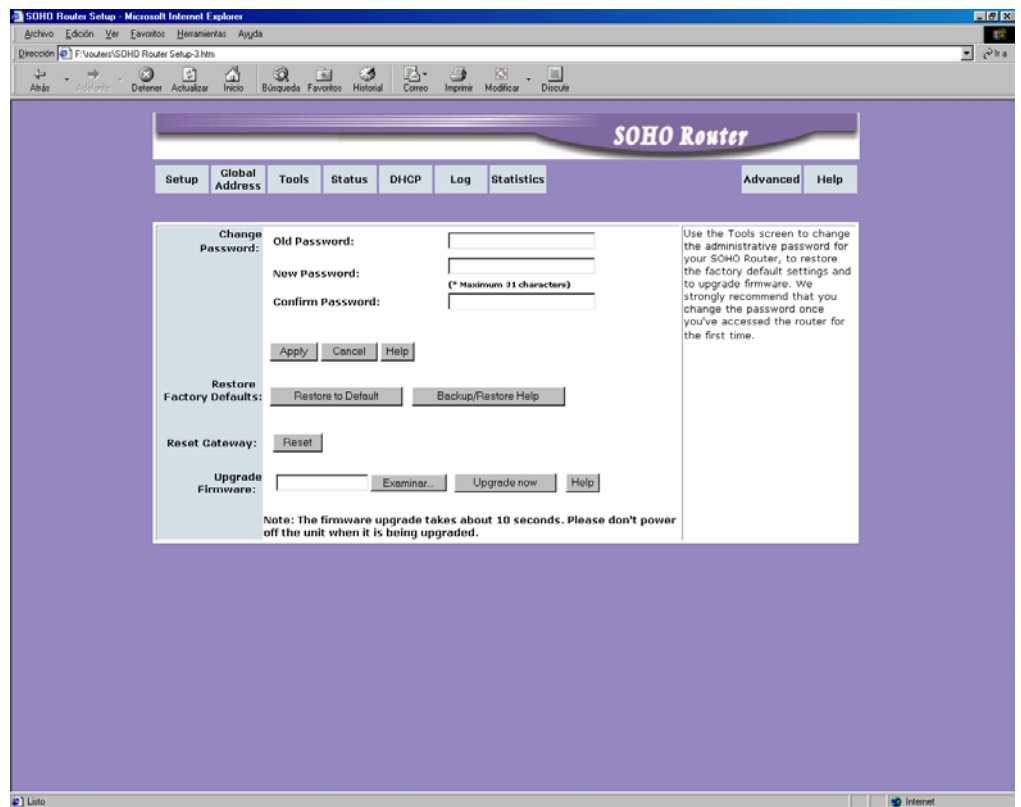
En la siguiente imagen vemos la dirección IP pública asignada en esta conexión.

Para llegar a esta opción realizamos clic en “Global Address”



“Tools – Herramientas”

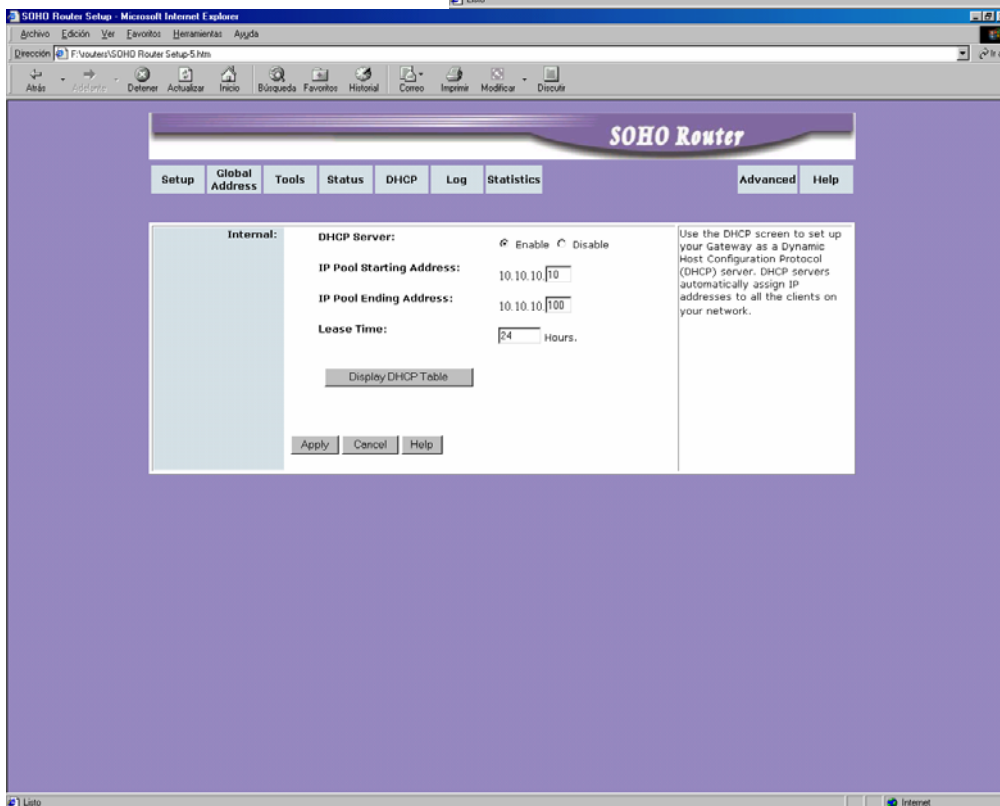
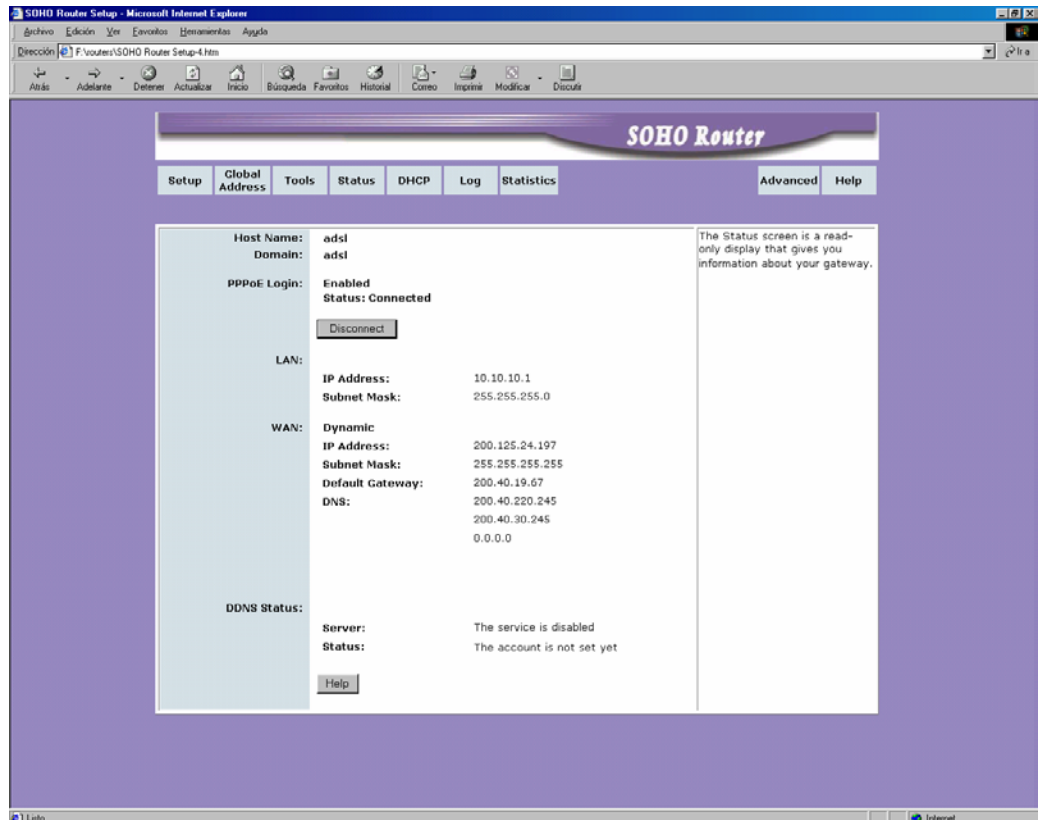
Esta opción nos permite cambiar la contraseña de ingreso al Router, cosa que deberemos realizar para aumentar nuestra seguridad en los cambios de la configuración, adicionalmente podremos realizar actualizaciones del sistema.





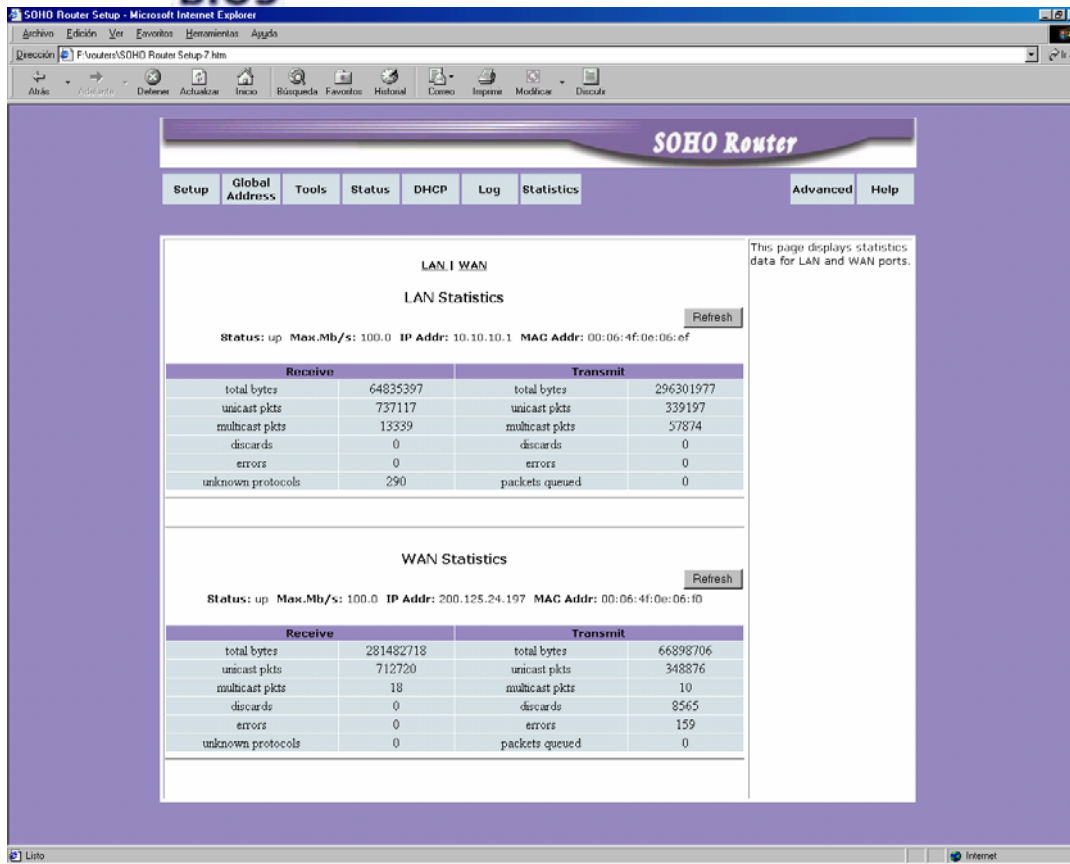
### “Status – Estado”

Esta opción nos muestra el estado de conexión o no, y la configuración de las direcciones IP interna y externa.



“DHCP” Aquí podemos habilitar el servicio DHCP y seleccionamos el rango de direcciones que estarán destinadas a esos efectos, de esta forma convertimos al Routers en un servidor DHCP, en esta imagen se aprecia que solo 90 direcciones se dejan para ser asignadas con DHCP.





Por ultimo para destacar en esta opciones básicas esta “Statistics” Estadísticas, que nos muestra la cantidad de datos recibidos y enviados en cada red, y con la cantidad de errores, de haber en este ultimo un numero importante deberemos de verificar la instalación y configuración de nuestra red, así como la conexión externa.

Pasamos a las opciones avanzadas, y destacamos algunas de ellas que nos pueden dar utilidades de control en nuestra red.

IP/URL – Block:  
Aquí podemos indicar las direcciones IP o paginas Web que deseamos impedir el ingreso a nuestros usuarios.

The screenshot shows the 'IP/URL Block' configuration screen in the SOHO Router Setup interface. It includes a table for configuring IP blocks, with columns for IP Block Starting Address and IP Block Ending Address. The table has 6 rows for configuring different IP blocks. Below the table are buttons for 'Apply', 'Cancel', 'Clear All', and 'Help'. A sidebar on the right provides instructions on how to use the screen to create and apply filters.

	IP Block Starting Address	IP Block Ending Address
1	0 . 0 . 0 . 0	0 . 0 . 0 . 0
2	0 . 0 . 0 . 0	0 . 0 . 0 . 0
3	0 . 0 . 0 . 0	0 . 0 . 0 . 0
4	0 . 0 . 0 . 0	0 . 0 . 0 . 0
5	0 . 0 . 0 . 0	0 . 0 . 0 . 0
6	0 . 0 . 0 . 0	0 . 0 . 0 . 0

Use this screen to create and apply filters that can selectively block traffic to pass in and out of your network according to the IP addresses.



Veamos las mismas configuraciones pero en un Router de otra marca que agrega además ser inalámbrico, veremos que no hay grandes cambios, simplemente buscar la opción correcta en el lugar justo.

The screenshot shows the 'LAN > LAN settings' page of a Belkin router's web utility. The interface is in Spanish and includes a sidebar with navigation options like LAN Setup, Internet WAN, Wireless, Firewall, and Utilities. The main content area displays the following settings:

- IP Address >**: 192 . 168 . 2 . 1
- Subnet Mask >**: 255 . 255 . 255 . 0
- DHCP server >**: On (radio button selected)
- IP Pool Starting Address >**: 192 . 168 . 2 . 2
- IP Pool Ending Address >**: 192 . 168 . 2 . 100
- Lease Time >**: Forever
- Local Domain Name >**: Belkin

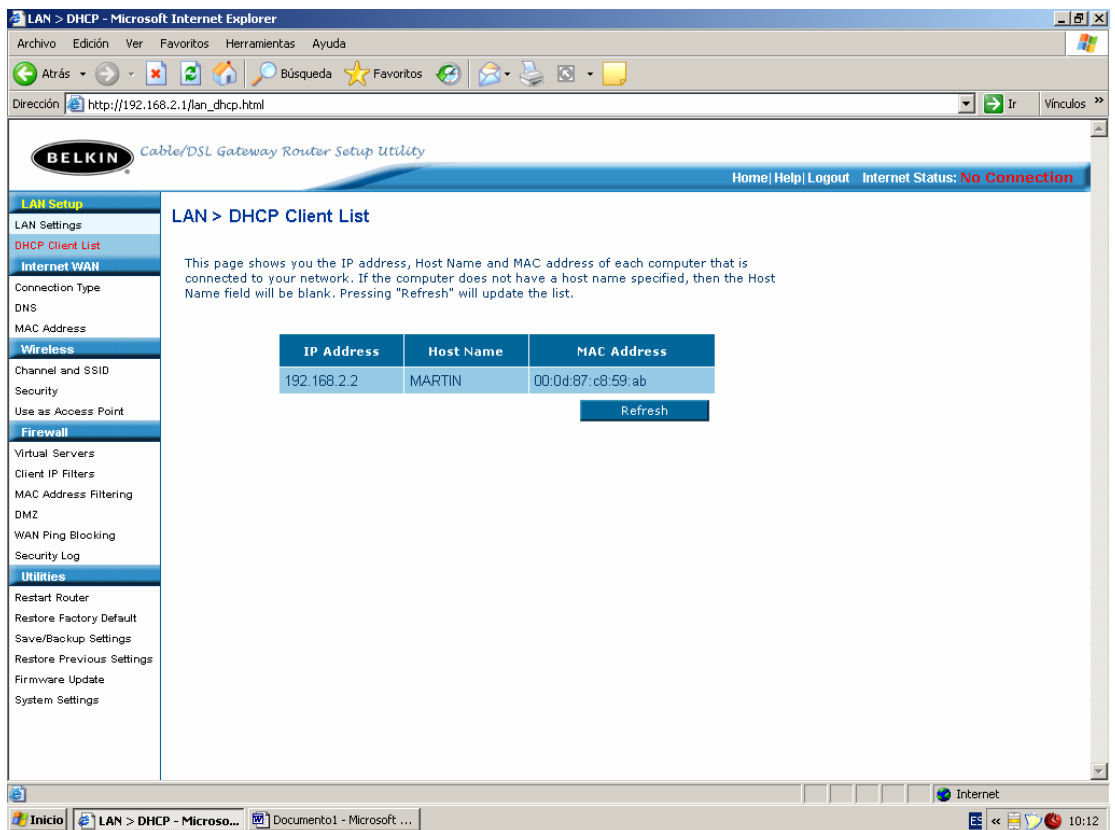
At the bottom of the settings area are two buttons: 'Clear Changes' and 'Apply Changes'. The browser's address bar shows 'http://192.168.2.1/login.cgi'.

En esta imagen se aprecia: En primera instancia la dirección IP que tendrá el Router, en segunda su máscara, luego la configuración del Servicio DHCP y el rango de dirección IP reservadas, el tiempo de duración de la asignación de la dirección IP y finalmente el nombre del dominio.

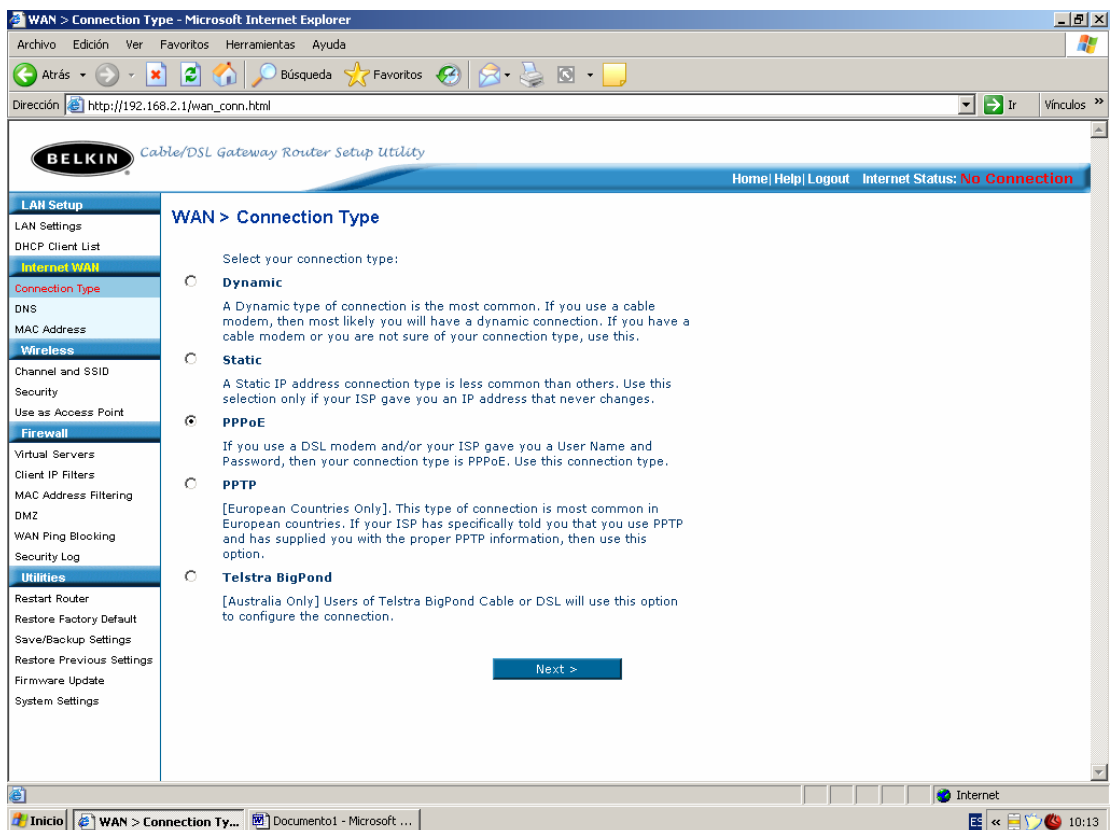




En esta ventana se muestra el listado de direcciones IP asignadas por el servicio DHCP y el nombre del equipo que tiene tal IP.



En esta imagen seleccionamos el tipo de conexión hacia internet, opción PPPoE es para aquellos que tengan ADSL y tienen que ingresar su nombre de usuario y contraseña, Static para aquellos que tienen una IP Fija y Dynamic los que cambian la IP pero no





tiene nombre de usuario ni contraseña, por ejemplo los que se conectan con la empresa “DEDICADO”.

Al seleccionar PPEoE la ventaja que se muestra es la imagen que vemos y en ella configuramos el nombre de usuario y la contraseña.

WAN > Connection Type > PPPoE - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección [http://192.168.2.1/wan\\_ppoe.html](http://192.168.2.1/wan_ppoe.html)

**BELKIN** Cable/DSL Gateway Router Setup Utility

Home | Help | Logout Internet Status: **No Connection**

**LAN Setup**

- LAN Settings
- DHCP Client List
- Internet WAN**
- Connection Type
- DNS
- MAC Address
- Wireless
- Channel and SSID
- Security
- Use as Access Point
- Firewall
- Virtual Servers
- Client IP Filters
- MAC Address Filtering
- DMZ
- WAN Ping Blocking
- Security Log
- Utilities
- Restart Router
- Restore Factory Default
- Save/Backup Settings
- Restore Previous Settings
- Firmware Update
- System Settings

**WAN > Connection Type > PPPoE**

To enter your PPPoE settings, type in your information below and click "Apply changes". [More Info](#)

User Name >

Password >

Retype Password >

Service Name (Optional) >

MTU (1440-1454) >

Do not make changes to the MTU setting unless your ISP specifically requires a different setting than 1454. [More Info](#)

☐ Disconnect after  minutes of no activity.

[More Info](#)

En esto otro caso solo deberemos de ingresar el nombre del puesto.

WAN > Connection Type > Dynamic IP - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección [http://192.168.2.1/wan\\_dyna.html](http://192.168.2.1/wan_dyna.html)

**BELKIN** Cable/DSL Gateway Router Setup Utility

Home | Help | Logout Internet Status: **No Connection**

**LAN Setup**

- LAN Settings
- DHCP Client List
- Internet WAN**
- Connection Type
- DNS
- MAC Address
- Wireless
- Channel and SSID
- Security
- Use as Access Point
- Firewall
- Virtual Servers
- Client IP Filters
- MAC Address Filtering
- DMZ
- WAN Ping Blocking
- Security Log
- Utilities
- Restart Router
- Restore Factory Default
- Save/Backup Settings
- Restore Previous Settings
- Firmware Update
- System Settings

**WAN > Connection Type > Dynamic IP**

To enter your Dynamic IP settings, type in your information below and click "Apply changes". [More Info](#)

Host Name >

Host Name = A name that some Internet Service Providers require for connection to their system.

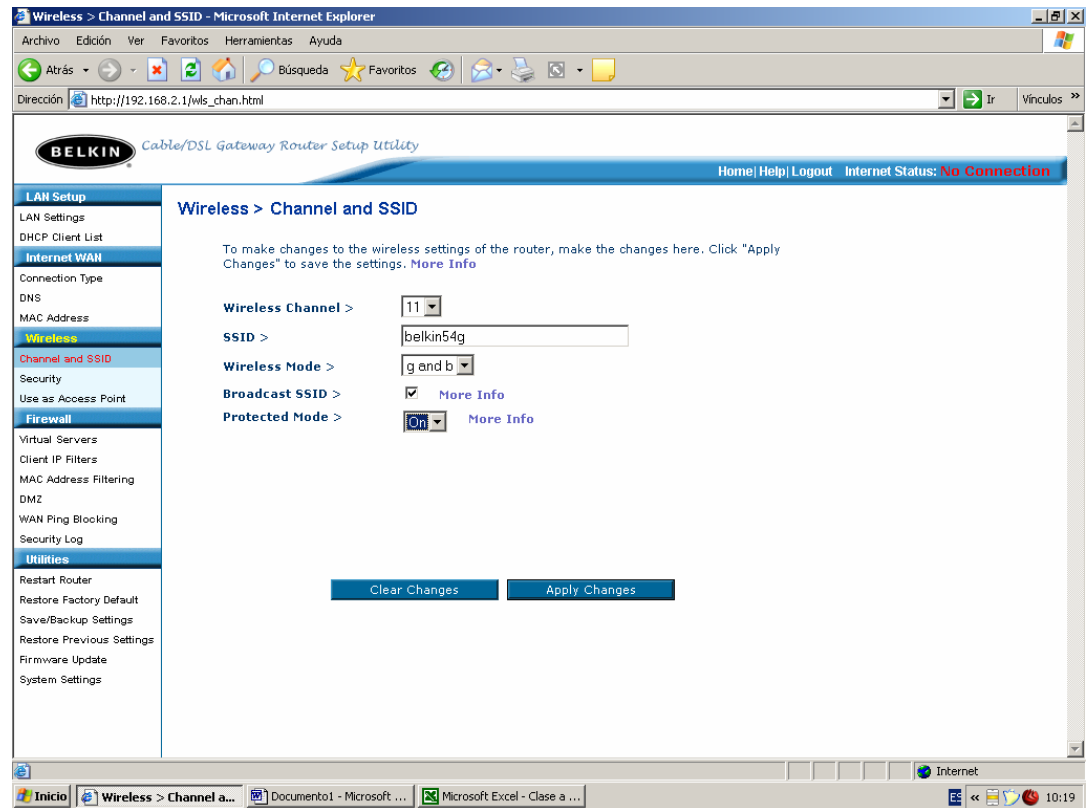
[Change WAN MAC Address](#)



Entremos en la configuración inalámbrica de la Red

“Wireless Channel”

Canal Inalámbrico, este será el canal por donde se transmitirá la señal de red, en caso de tener otra red inalámbrica o artefactos inalámbricos que puedan afectar a la red deberemos de cambiar este canal por otro, tenemos 11 canales posibles para la transmisión.



“SSID” Este será el identificador de la Red, el nombre con que las tarjetas inalámbricas podrán ver a la red.

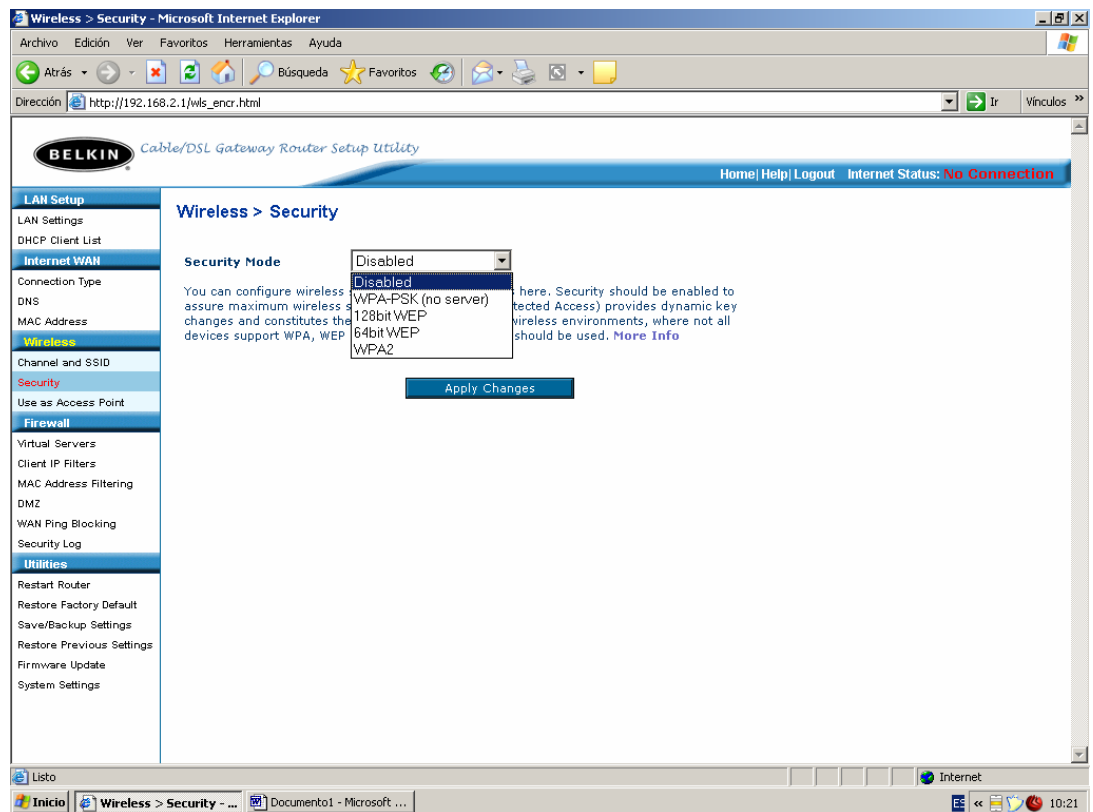
“Wireless Mode” Modo de trabajo, estos pueden ser tres g y b, solo b o solo g, la diferencia esta en la velocidad de transferencia que tienen estas normas, donde la g llega a los 54Mbps, y la b solo 24Mbps, de esta forma al seleccionar la combinada g y b nos aseguramos que cualquier tarjeta de red se pueda conectar a nuestra red inalámbrica.

“Broadcast SSID” de no estar tildada esta opción la red no podrá ser “vista” de forma automática.

“Protectec Mode” Esta poción mejora los rendimientos en redes con mucho trafico o interferencias.



En esta pantalla donde optaremos por el sistema de seguridad al ingreso de nuestra red inalámbrica, las opciones son:



Disabled (Deshabilitado) Esta opción no genera ningún tipo de restricción al ingreso de la red, por lo tanto cualquiera que tenga una tarjeta de red inalámbrica y se encuentre en el radio de cobertura del Routers podrá ingresar a nuestra red, por supuesto nada segura de muy fácil instalación.

WPA-PSK: Usa solo lo que se conoce como una clave pre-establecida como la clave de red. Una clave de red es básicamente una contraseña que tiene entre 8 y 63 caracteres. Puede ser una combinación de letras, números o caracteres. Cada cliente utiliza la misma clave de red para acceder a la red. Esta es la modalidad que se utiliza típicamente en un ambiente domestico.

128BitWep: Debido a las deficiencias potenciales de seguridad de WEP de 64 bits, se desarrollo un método de encriptación más seguro de 128 bits. La encriptación de 128 bits incluye un largo de clave de 104 bits, mas 24 bits adicionales de datos generando por el sistema (128 bits en total). Algunos fabricantes de hardware se refieren a la encriptación de 128 bits por el nombre de encriptación de 104 bits. La mayoría de los equipos inalámbricos nuevos disponibles en el mercado en la actualidad, soportan encriptación de 64 bits y de 128 bits.

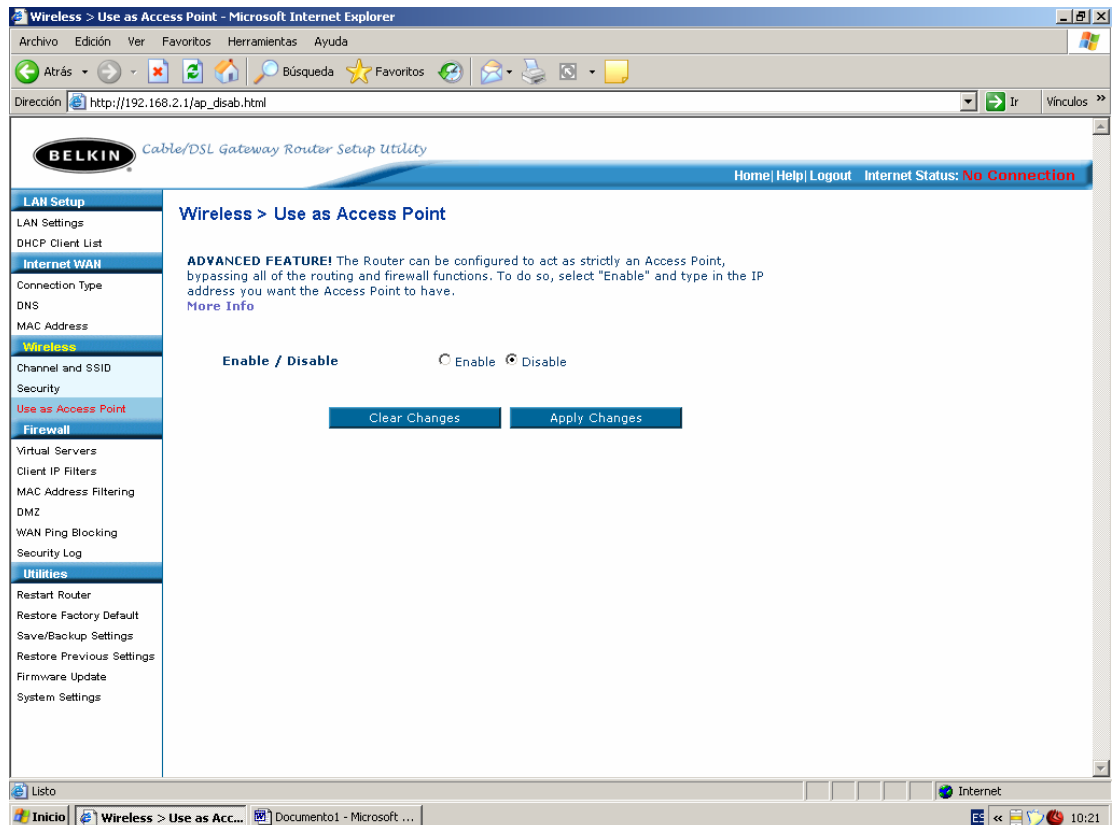
64bitWep: Se introdujo con la encriptación de 64 bits, que incluye un largo de clave de 40 bits, más 24 bits adicionales de datos generados por el sistema (64 bits en total). Algunos fabricantes de hardware se refieren a la encriptación de 63 bits por el nombre de



encriptación de 40 bits. Poco después de lanzarse al mercado la tecnología, los investigadores determinaron que la encriptación de 64 bits era muy fácil de decodificar.

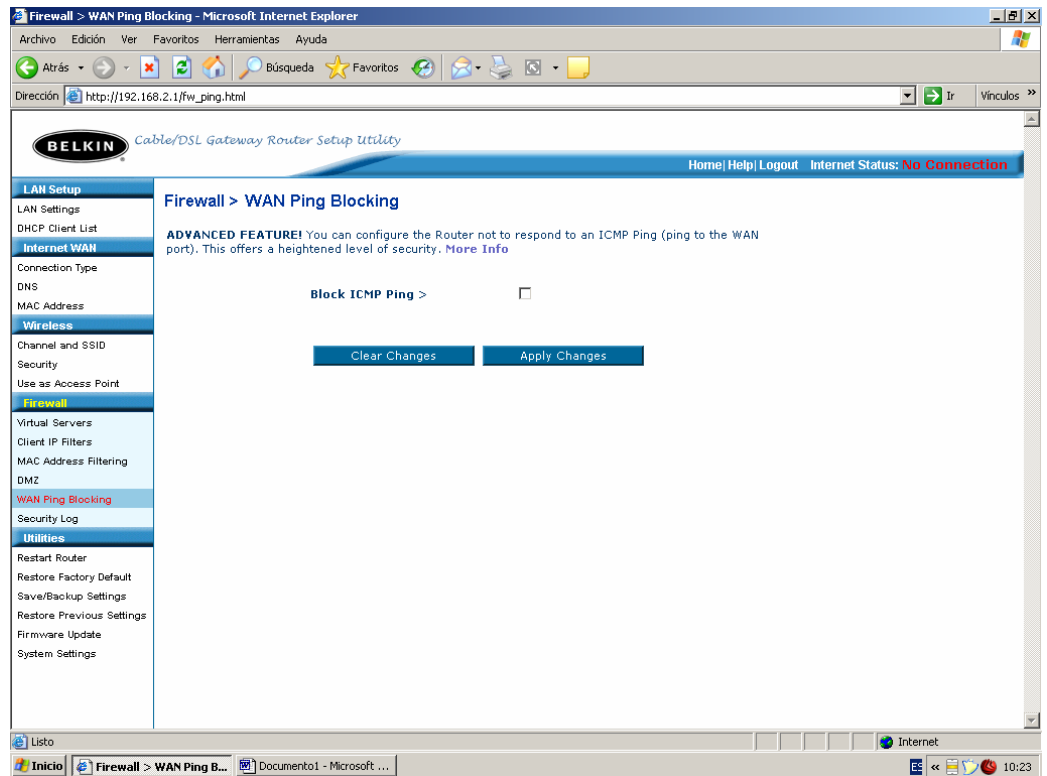
WPA2: Es un estándar Wi-Fi destinado a mejorar las características de seguridad de WEP. Para usar la seguridad WPA, es necesario actualizar los controladores y el software de sus equipos inalámbricos para que soporte WPA.

En esta pantalla logramos tener deshabilitadas las funciones del routers y este cumplir como un simple punto de acceso para los puestos de red inalámbricos, las funciones de DHCP y Routers son deshabilitadas.





El tildado de esta opción configura al router para no contestar comandos como el PING, considerados la principal herramienta de búsqueda de equipos informáticos por los Hackers.



Las ventanas que restan están directamente relacionadas con el Firewall que la mayoría de estos equipos cuentan y que muchas de estas serán discutidas en el Seminario de “Introducción a la seguridad Informática”.



## **Anexo I**

### Windows NT Server como Servidor de Aplicaciones.

La versión 4 de Windows NT Server es un flexible sistema operativo de red que puede utilizarse en diferentes formas:

1. Como un único servidor de archivos, con clientes que almacenan sus datos en un solo almacén central.
2. Como un sistema operativo subyacente de un servidor de base de datos, tal como Microsoft SQL SERVER 7.0, que funciona como un servicio de Windows NT Server manteniendo las bases de datos y procesando información de los clientes.
3. Como un servidor de aplicaciones, proporcionando la capacidad de ejecutar aplicaciones del servidor, bien en un modo simple de servicio de archivos o como el actual sistema cliente servidor donde el funcionamiento de la red se comparte entre el cliente y el servidor, cada uno teniendo la responsabilidad de una parte de la aplicación.

### Windows NT Server como Servidor de Aplicaciones.

Windows NT Server cuenta con un servicio de duplicación de archivos, que asegura que todo el mundo esta trabajando con la misma información al mismo tiempo. Además la duplicación de archivos puede ayudar a equilibrar la carga del servidor.

### **SYSTEM MANAGEMENT SERVER**

System Management Server de Microsoft forma parte del BACKOFFICE, el paquete que ayuda administrar más fácilmente la red en todos sus aspectos. Disponible también para Windows 2000.

### **WINDOWS 2000 SERVER DESCRIPCIÓN GENERAL**

Gran parte de la velocidad adquirida por la interconexión de computadoras se ha debido al rápido crecimiento de Internet. Windows NT reclama el 56 por 100 de los servidores de INTERNET en el mundo, y el 80 por 100 de los de INTRANET...

Los servicios de información de Internet están incluidos en Windows 2000 y vienen con muchas mejoras incluidas a los proveedores de servicios de Internet, quienes ofrecen servicios de hospedajes de paginas, entre otras mejoras ya permiten compresión HTTP, cuotas de procesador del servidor virtual y contabilidad de procesos.

La mayoría de los usuarios se sienten poco interesados con los sistemas operativos y más curiosos con el software de aplicación.

La tecnología responsable de atraer muchos desarrolladores es el modelo de componentes de Microsoft (COM) se encuentra implícito en cada aspecto del propio



software del sistema operativo de MICROSOFT, sus herramientas de desarrollo y sus aplicaciones. COM beneficia tanto a administradores y desarrolladores porque permiten que sus aplicaciones estén distribuidas en una red y se actualicen de manera centralizada.

El elemento adicional de Windows 2000 es el directorio activo, permite que cualquier usuario o aplicación pueda utilizar un recurso disponible en la red.

Guarda algo más que la localización de los objetos, almacena información crítica para el objeto.

Windows 2000 consigue que los servidores de archivos sean aun más fiables y eficientes que antes, con el nuevo sistema de archivos distribuidos de Microsoft (Dfs), dicho sistema permite compartir elementos entre los servidores de archivos y que los clientes puedan elegir el servidor más cercano.

Al final Dfs reducirá el tráfico de la red, aumentando el tiempo de disponibilidad y mejorando la distribución de la carga entre los servidores. A su vez se incorporan mejoras al utilizar el sistema de archivos NTFS 5.

La administración de una red con Windows 2000 será mas sencilla y rápida que nunca gracias a la consola de gestión de Microsoft (MMC – Microsoft Management Console).

MMs Le otorga control de herramientas y computadoras, permitiendo personalizar la administración de todo el sistema.

La configuración de los entornos de escritorios será más sencilla gracias a la política de grupo y al directorio activo. Se pueden configurar los escritorios y las aplicaciones de manera de restringir todos los accesos que sean necesarios.

Seguridad: Este es un tema candente en el mundo informático y esencialmente vital en las redes, WIN 2000 incorpora uno de los sistemas de seguridad más importantes hasta el momento llamado KERBEROS.

Se han extendido las capacidades de conectividad de manera que Windows 2000 esta preparado para telefonía sobre IP, tecnología que permite mezclar voz y datos por una red, manejando L2TP: Protocolo de entunelado en capa 2 y PPTP: Protocolo de entunelado punto a punto e Ipsec: Protocolo de seguridad de Internet.

Las funciones de conmutación permiten que Windows 2000 tenga un nuevo papel, el de enrutador de red. Ya es fiable la tecnología de medios por flujos, gracias al nuevo soporte de los estándares de calidad de servicios (QoS) y la integración de los servicios de medios de Windows, (Windows Media Services).

Esta el sistema operativo soporta DNS dinámico y Wins con replicación persistente de conexiones y mejora de la redundancia.





El protocolo de configuración dinámica del host esta integrado al protocolo de actualización dinámica DNS y ahora los clientes DHCP pueden arrancar incluso en ausencia de servidor DHCP.

### Dominios y Relaciones de Confianza

El concepto de dominio, es el principio estructural subyacente en una red Microsoft Windows NT 4.0, el concepto de confianza, la base de relaciones entre dominios en una red de Windows NT Server nacieron de la creciente demanda de sofisticación de los sistemas de red.

Microsoft introdujo el concepto de **trabajo en grupo**, un grupo de trabajo es un agrupamiento lógico de varios usuarios de computadoras cuyas necesidades de información o actividades laborales están relacionadas y que quieren compartir sus recursos de archivos con los demás. Normalmente todas las computadoras en un grupo de trabajo son iguales: no hay computadora central.

Por eso se refiere a estas instalaciones como redes igualitarias.

Las redes de trabajo en grupo son atractivas porque son fáciles de instalar y mantener.

Los usuarios individuales administran la utilización en común de los recursos determinando qué se compartirá y quién tendrá acceso.

El tamaño por si mismo puede limitar la eficacia de un grupo de trabajo. Cuando hay muchos usuarios y el lógico incremento correspondiente al número de recursos, los usuarios podrán difícilmente encontrar los recursos en redes grandes.

También la naturaleza informal de los grupos hace que no haya administración o control central.

En un grupo grande la administración resulta ardua y desalentadora



## Planificación de la Red

### Definición de Dominios

La unidad básica de Windows NT es el dominio, es un grupo de computadoras que comparten una base de datos y tienen una política de seguridad en común.

Un dominio consiste en una computadora que funcione como controlador principal de dominio (PDC), al menos una computadora que funcione como controlador de dominios de reserva (BDC) y al menos una estación de trabajo. Puede haber controladores de dominio de reserva adicionales y servidores como así también estaciones de trabajo.

Una red de Windows NT puede estar conformada por un único dominio o puede consistir en muchos dominios interconectados, como una red a nivel de corporación que tenga miles de estaciones de trabajo repartidas por todo el mundo

### Ventajas de un Modelo de Dominio Único

- Configuración de diseño flexible
- Administración de red centralizada
- Flexibilidad en la adición de nuevos usuarios y en el cambio de restricciones de acceso
- Una base de datos únicos para cuentas de usuarios.
- Un sistema de seguridad unificado para el dominio completo.
- Adecuado control de acceso a directorios y archivos.

### El Controlador Principal de Dominio

El controlador principal de dominio es el computador más importante en un dominio, impone las políticas de seguridad para el dominio y es el principal depósito de la base de datos de las cuentas. También podría ser el principal poseedor de los recursos compartidos del dominio.

Los cambios en la base de datos de cuentas de usuario se hacen sólo en el controlador principal de dominio y después se propagan automáticamente a los controladores de dominio de reserva, donde se mantienen copias de lectura de la base datos.

La herramienta que se utiliza para la administración de cuentas de usuarios es el administrador de usuarios para dominios. (USRMGR)

Si el controlador principal de dominios no esta presente en la red, los usuarios continúan siendo capaces de conectarse a la red si se han creado uno a mas controladores de dominio de reserva y sí al menos uno de ellos esta presente.



En cualquier caso, no se podrían hacer cambios en las cuentas de usuarios y grupos en los dominios, añadir nuevos usuarios o grupos a los dominios hasta que el controlador principal de dominio no este nuevamente funcionando o hasta que se cambie algunos de los controladores de dominio de reserva a controlador principal de dominio

### El Controlador de Dominio de Reserva

El dominio de Windows NT SERVER puede y en la mayoría de los casos debe, tener uno o más controladores de dominio de reserva.

Cada controlador de dominio de reserva contiene una copia fiel de la base de datos de las cuentas y puede validar a los usuarios cuando inician una sesión en el sistema y autorizar el acceso a los usuarios a los recursos.

Esto hace bastante fácil proporcionar una redundancia a recursos compartidos críticos en el sistema, en caso de que falle el controlador principal de dominio.

### Estaciones de Trabajo

Las estaciones de trabajo pueden ejecutar MSDOS, OS2, Microsoft Windows 3.x. Windows 95, 98. Microsoft Windows NT Workstation y Macintosh OS.

Los requisitos de Hardware son menores para Windows 95 que para Workstation...

Las estaciones con Workstation se verán mejoradas en estabilidad y redundancia en caso de tener que trabajar en red.

### Relaciones de Confianza

En una red que consista en dos o más dominios, cada dominio actúa como una red por separado con su propia base de datos de cuentas, incluso en la organización más rígidamente estratificada, algunos usuarios de un dominio necesitan utilizar algunos o todos los recursos del otro dominio.

La solución usual para la configuración de niveles de acceso de usuario entre dominios es lo que se llama relaciones de confianza.

Windows NT proporciona todas las herramientas necesarias para instalar una red de múltiples dominios con relaciones de confianza entre los controladores de dominios que protejan las áreas de recursos sensibles, mientras que libere a los usuarios de la carga de tener que tratar con procedimientos detallados y múltiples contraseñas.



### Relaciones de Dominios sin Confianza

Es ciertamente posible tener múltiples dominios sin confianza. Por ejemplo, un usuario individual puede tener una cuenta separada para cada dominio en una red de múltiples dominios

La dificultad con este método es que un usuario que desee acceder a mas de un dominio normalmente necesita un acceso simultáneo, lo que no es posible en esta configuración.

### Modelos de Dominio

Windows NT Server tiene 4 modelos de relaciones de confianza entre dominios.

Analicemos cada uno de estos modelos, las situaciones de negocios que mejor se adaptan y las ventajas y desventajas de cada una.

Estos son los modelos que se pueden utilizar:

- **Dominio único.**
- **Dominio maestro único.**
- **Múltiples dominios maestros.**
- **Dominios con confianza total.**

#### Ventajas de un dominio único.

Es el modelo más simple, todos los servidores están dentro de un único dominio.

Grupos locales y grupos globales son lo mismo y todos los administradores pueden administrar todos los servidores.

Con un dominio único no hay relaciones de confianza que administrar.

#### Modelo de dominio maestro único

El modelo de dominio, maestro único proporciona administración de usuarios junto con agrupamientos lógicos de recursos departamentales.

Es modelo incluye uno o más dominios a nivel departamental (dominios secundarios) donde cada uno confía en el mismo dominio maestro.

#### Modelos de múltiples dominios maestros con confianza total

El modelo de múltiples dominios maestro con confianza total tiene sentido si se prefiere administración distribuida de usuarios y recursos pero la organización tiene la estructura administrativa fuerte y centralizada



Cada dominio confía en todos los demás y una cuenta de usuario se crea en el dominio en el que el usuario inicia la sesión por defecto.

El dominio donde esta localizada una cuenta de usuario se conoce como dominio base.

Los dominios secundarios son los responsables de la administración de sus propios usuarios y grupos globales y se accede a estos usuarios y grupos globales a través de una red.

El modelo de múltiples dominios maestros con confianza total tiene sentido en organizaciones relativamente pequeñas que hayan crecido por encima del dominio único.

En el modelo con confianza total: todas las relaciones de confianza son bidireccionales.

#### Concepto Básico Sobre Cuentas de Usuario.

Cualquiera que utilice una red de Windows NT SERVER debe tener una cuenta de usuario en algún dominio.

Si la cuenta de usuario no esta en el dominio al que el o ella sé este intentando conectarse, sólo se permitirá el acceso al dominio si este tiene una relación de confianza con el dominio donde este almacenada la cuenta de usuario.

Una cuenta de usuario incluye nombre y contraseña y restricciones sobre como puede el usuario utilizar la red.

La cuenta se crea con un identificador de seguridad llamado SID (identificador único en la red).

#### Administración de Usuarios como Grupos

Windows NT SERVER viene con un conjunto de grupos globales y locales incorporados que proporcionan un excelente punto de partida para la administración de usuarios en la red.

Se puede administrar un gran número de usuarios de una vez aprovechando esta función de grupo de usuarios.

Hay básicamente dos tipos de grupos de usuarios locales y globales.

El grupo local existe y mantiene sus permisos solo dentro del dominio en el que fue creado.



El grupo global reside en un dominio, pero mantiene sus permisos a lo largo de todos los dominios que confíen.

Se pueden crear fácilmente grupos clientes locales y globales que tengan un conjunto de permisos que se quiera y necesite.

Una vez que se ha creado un grupo y los necesarios permisos para el grupo, se pueden añadir rápidamente nuevos usuarios o ajustar los permisos para el grupo.

Una estructura de grupo bien meditada puede ahorrar mucho tiempo y administración.

### El Entorno de Usuario

#### Perfiles de Usuario.

Un perfil de usuario solo se puede utilizar en una computadora que ejecute Windows NT Server 4.0 o Windows NT Workstation, el mismo comienza como una copia de usuario predeterminado, un perfil en cada computadora que ejecute Windows NT SERVER 4.0.

Cuando un usuario inicia una sesión en una estación de trabajo por primera vez, Windows NT crea un perfil de usuario mediante el registro de cualquier cambio hecho a los ajustes del perfil durante esa sesión y su almacenamiento en el perfil de usuario local de esa persona.

El administrador de la red puede elegir instalar un perfil de usuario móvil para el usuario que viajara con él o ella cuando inicie la sesión en otra máquina y mostrará el perfil de escritorio del usuario de esa máquina.

#### Ventajas de los perfiles de usuarios móviles.

Cuando un usuario inicia una sesión en su computadora, los ajustes y el escritorio son los mismos que cuando se desconecta por última vez.

Varias personas pueden utilizar la misma computadora y cada una tendrá su propio escritorio personalizado.

Se puede almacenar un perfil de usuario como perfil de usuario móvil en un servidor, de manera que el entorno sea el mismo para ese usuario en cualquier computadora NT en la red.

Los perfiles también pueden ofrecer las siguientes ventajas como administrador

Puede crear perfiles de usuario especiales que proporcionen un entorno consistente

A los usuarios que se confundan con facilidad. Perfiles fáciles de entender.

Puede crear un perfil de usuario y asignarlo entonces a un grupo de usuarios.



Puede asignar perfiles obligatorios de manera que los usuarios no puedan modificar los ajustes de escritorio.

Puede asignar recursos inaccesibles a cualquiera asignado a un perfil en particular

Para conseguir objetivos de seguridad específicos.

Puede hacer un nuevo recurso o aplicación disponible a un número de usuarios en un paso, si todos comparten el mismo perfil obligatorio.

#### Tipos de Perfiles

1) Perfil Local: Este perfil esta disponible sólo en la maquina del usuario. Su aspecto y ajustes los determina el usuario sin ninguna restricción impuesta por el administrador.

2) Personal de usuario móvil: Este perfil se almacena en un servidor y está disponible para el usuario en cualquier máquina Windows NT en la red. Los ajustes los establece el usuario sin ninguna restricción impuesta por el administrador.

3) Obligatorio de usuario móvil: El perfil se almacena en el servidor y está disponible desde cualquier computadora. Windows NT en la red. Algunos o todos los ajustes están determinados por el administrador. Y no los puede cambiar el usuario.

Se pueden utilizar uno o todos estos perfiles dependiendo de la organización

#### Planificación de la Seguridad.

##### Administración Central

Es un modelo de administración central, una persona, grupo o departamento que administra toda la red, usuarios, recursos, servicios etc.

##### Administración Distribuida

En un modelo de administración distribuida, la red se administra a nivel departamental o grupo de trabajo.

Aunque la administración a nivel local puede facilitar respuestas rápidas a las necesidades de los usuarios, este tiempo de respuesta se consigue a menudo al precio de la seguridad de la red.

Con varios administradores a nivel de grupo o departamento los criterios diferirán de uno a otro.



Cuanto más grupos en un sistema existan más relaciones de confianza se requerirán, lo que aumenta las tareas administrativas.

### Seguridad de Usuarios

La seguridad de usuarios tiene 2 aspectos:

- 1) Facilitación del acceso de los usuarios a los recursos que se necesiten
- 2) Mantener fuera del alcance aquellos recursos que no se quieren compartir

### Seguridad de Archivos

Hay dos aspectos para mantener la seguridad de un archivo:

- 1) Control del acceso al archivo
- 2) Protección de la integridad del archivo.

Tanto los archivos de datos como los archivos de documento contienen datos en un formato estructurado, pero los archivos de documentos son normalmente legibles para las personas.

Mientras que los archivos de datos deben interpretarlos los programas.

Windows NT SERVER versión 4 permite controlar el acceso a los usuarios tanto a nivel de archivo, como de carpeta.

Por lo tanto es posible que alguien tenga total acceso a una carpeta y no a un archivo dentro de esa carpeta o viceversa.

Esto solo es posible, si se ha elegido instalar el sistema de archivo NTFS.

### Permisos

El primer permiso se aplica al directorio mismo, el segundo permiso se aplica al archivo.

Bajo Windows NT, los permisos son combinaciones de atributos que pueden asignarse a cualquier archivo.

Estos son los atributos de archivos individuales.

- LEER
- ESCRIBIR
- EJECUTAR
- BORRAR





- CAMBIAR PERMISOS
- TOMAR POSESIÓN

También deberá considerarse archivos sensibles a la auditoria o confidenciales.

Para asegurarse que nadie intente un acceso no autorizado.

#### Permisos para Directorios y Archivos NTFS.

Sin acceso (Ninguno): El usuario no puede tener acceso de ningún modo al directorio

Lista (RX): El usuario puede listar los archivos y subdirectorio de este directorio, y puede cambiar a un subdirectorio de este directorio, el o ella no puede tener acceso a los archivos creados en el directorio por otros.

Leer: El usuario puede leer el contenido de los archivos y puede ejecutar aplicaciones del directorio.

Agregar: (WX) (Sin especificar) El usuario puede añadir archivos al directorio pero no puede leer el contenido de los archivos actuales o cambiarlos.

Agregar y Leer: (RWX) El usuario puede leer o añadir archivos y puede cambiar el contenido de los archivos actuales.

Cambiar: (RWXD): El usuario puede leer y añadir archivos y puede cambiar el contenido de los archivos actuales.

Control Total: (TODO) El usuario puede añadir, leer y cambiar archivos: puede cambiar los permisos para el directorio y sus archivos; y puede tomar posesión del directorio y de sus archivos.

#### Permisos de Archivos

Sin acceso: (Ninguna): El usuario no puede obtener acceso de ninguna manera incluso aunque él o ella sea miembro del grupo al que en su conjunto, le haya sido concedido acceso al archivo.

Leer (RX): El usuario puede leer el contenido del archivo y puede ejecutarlo si es una aplicación.

Cambiar (RWXD): El usuario puede leer, cambiar, borrar el archivo.

Control total (Todo): El usuario puede leer, cambiar, borrar, establecer permisos para el archivo y tomar posesión de él.



## Anexo II

### REALIZANDO UN CABLEADO ESTRUCTURADO

Un sistema de cableado estructurado es la infraestructura de cable destinada a transportar las señales que emite un emisor hasta el correspondiente receptor. Es un sistema pasivo y está diseñado para soportar, sin degradación de las señales, transmisiones de voz, datos, imágenes, dispositivos de control, de seguridad, detección de incendios, etc. Toda esta gama de señales se transmiten a través de un mismo tipo de cable.

Para que se comporte como un verdadero sistema, una instalación de cableado estructurado debe contar con toda la línea de productos (desde el tipo de cable a utilizar hasta los adaptadores terminales) que aseguren la conectividad y operación de cualquier tipo de aplicación. Se entiende por aplicación, al diseño de ingeniería que define que tipo de cable es el más adecuado para conectar al cableado un equipo o sistema, qué adaptadores o “baluns” se deben colocar para asegurar que las señales mantengan sus características técnicas, determinar las distancias máximas a las cuales se pueden conectar los equipos terminales, etc.

Otra característica importante es que sea un sistema abierto. Esto quiere decir que puedan conectar y poner en operación, cualquier sistema de dato sin importar quien es su fabricante

Un sistema de cableado debe cumplir con las normas y estándares definidos por la ANSI/EIA/TIA indicadas en sus boletines 568, 568A, 569, 570. Así mismo debe soportar los diferentes estándares de la industria como son IEEE 802.5, IEEE 802.3, por ejemplo.

Generalmente, una instalación de cableado estructurado está compuesto por diferentes tipos de cable, de acuerdo con la instalación requerida, se debe seleccionar el tipo de cable adecuado.

El cable de par trenzado sin blindaje - UTP - se clasifica según su categoría (algunos fabricantes lo llaman nivel). Este cable UTP (Unshield Twisted Pair) permite la transmisión de grandes volúmenes de información. Estas propiedades están dadas por varios factores: el cobre con que está fabricado el conductor, el material de recubrimiento, tanto de cada conductor como del cable total y finalmente en trenzado de cada par (número de vueltas por pie). Estas características hacen que el cable no requiera de blindajes, que mantenga la señal limpia y transporte grandes volúmenes de información.

Se fabrican en Categorías 3, 4 o 5. El cable categoría 3 permite transportar hasta 10 Mb/seg. Con esta capacidad se cubren aplicaciones de redes (10BaseT, a 4 MB/seg.), aplicaciones de voz (sistemas telefónicos), transmisión de señales en aplicaciones con equipos multiusuario, aplicaciones de video, aplicaciones de seguridad y control, etc. El cable categoría 4 soporta las mismas aplicaciones de la anterior categoría más aplicaciones que requieran hasta 20 Mb/seg. Finalmente la categoría 5 transporta hasta 100 Mb/seg. Esta capacidad cubre las mencionadas anteriormente y adicionalmente pueden correr



aplicaciones de redes a esa velocidad, ATM, TP-PMD, etc. Algunos fabricantes, en categoría 5, llegan a soportar hasta 155 Mb/seg.

En cable UTP existen también dos clases de cables denominados Plenum y No-Plenum. El cable Plenum es un cable en el que sus recubrimientos están fabricados con componentes resistentes al fuego y con un bajo nivel de toxicidad en los gases que emite al someterse a fuego. Estos cables se utilizan en instalaciones que no van dentro de tuberías o bandejas. En instalaciones en las cuales se distribuirá en cable a través de ductos o tuberías se utiliza el cable No-Plenum

### Que es La Categoría 5

El cableado estructurado en categoría 5 es el tipo más común en la actualidad, como vimos anteriormente se refiere a la velocidad de transmisión de los componentes de un cableado basado en UTP.

#### Distancias permitidas.

- El máximo de distancia permitida por norma es de 99 metros.
- El límite para el cableado fijo es de 90 mts.
- El límite para los Patch Cord en la Patchera es de 6 mts
- El límite para los Patch Cord en la conexión del terminal es de 3 mts, máximo.

#### Beneficios de un Sistema de Cableado Estructurado

##### Plan de distribución integrado:

Desde la concepción misma del proyecto se analizan y diseñan las opciones que permiten un manejo integrado de todas las diferentes señales y servicios que se tendrán disponibles. Al integrar aplicaciones, se pueden utilizar un solo medio de distribución para llevar todos los cables que habilitarán las señales en cada salida de información.

##### Arquitectura Abierta:

Sin Importar quien es el proveedor de los PC's, Hubs, Conmutadores, etc. el cableado ofrece la misma conectividad y capacidad de transmisión.

##### Solución integrada y modular:

Las interconexiones entre armarios de piso y en el piso mismo, permiten muy fácilmente llevar una señal hasta el sitio deseado sin que esto implique una remodelación del área en la cual se pondrá a funcionar dicho servicio.



#### Total funcionalidad y flexibilidad:

El cableado estructurado conecta cada salida de información desde los armarios de piso hasta el puesto mismo de trabajo. Esto implica que cada recurso que se asigna a una salida está perfectamente definido y configurado para prestar el servicio adecuadamente. Con sistemas de cableado, se realiza una verdadera labor de planeación pues los servicios que se asignan están estudiados y analizados desde mucho tiempo antes de instalarse en la realidad, facilitando así su crecimiento posterior.

El proceso de asignación de un servicio a una salida de información está basado en la reconexión de cables (puente) en los tableros de piso. Esto facilita la asignación de los mismos recursos a la persona que por cualquier razón debe cambiar de ubicación física dentro del edificio. Siempre tendrá la misma extensión telefónica, la misma dirección de red, las mismas salidas de video, etc. sin importar que se encuentre hoy en el 1er. piso y que mañana sea trasladado al 6°. piso.

#### Topología de red tipo estrella:

Por su concepción, el cableado estructurado está diseñado de manera tal que permite instalar, conectar y poner en servicio inmediatamente, una red de PC's en una topología de estrella. Esta topología es la más segura y flexible de todas las topologías existentes, además de tener un alto grado de confiabilidad y seguridad en su funcionamiento. Sin embargo, el cableado estructurado permite sin ningún inconveniente, conectar cualquier tipo de red o de sistema de cómputo que tenga el usuario.

#### Fácil administración del sistema por parte del Administrador del Sistema:

Una vez que se ha instalado el sistema y ha sido capacitado el administrador, él directamente y sin dependencia alguna con el proveedor del cableado, puede reasignar los servicios que se encuentran disponibles en cada una de las salidas de información. Una vez terminada la instalación, se deja totalmente identificada y documentada con planos y manuales. El administrador no requiere de conocimientos técnicos especializados en el tema.

#### Crecimiento manejable y administrable:

Todo el crecimiento que la organización va a tener a sido planeada con anticipación de manera que cuando realmente se vaya a crecer ya existen los ductos con capacidad de recibir nuevas ampliaciones cuando ya se haya agotado la capacidad adicional instalada en el momento inicial. Así mismo evita que se hagan instalaciones adicionales NO controladas que descompensen los sistemas o que generen interferencias o errores. El crecimiento en los tableros es modular. Esto significa que adicionando bloques o paneles de conexión, se va ampliando el sistema sin interferir con lo ya instalado.



Fácil control y acceso a la administración de la red del sistema por parte del administrador:

Las redes de datos se pueden administrar muy fácilmente, especialmente si la topología adoptada es de estrella. Cuando un usuario se mueve de su ubicación física a otra, no se requiere reconfigurar su estación de red por cuando, al redireccionar su conexión se conservan vigentes todos los parámetros de configuración del equipo. Por otra parte, la topología en estrella evita que la red se caiga cuando una de las estaciones presenta problemas.

Soporta: Voz, Datos, Imágenes, Sonido, Video, Sensores y Detectores, etc. en un mismo sistema:

El mismo tipo de cable tiene la capacidad de transportar señales de cualquier tipo. Esto implica que solamente tenemos que manejar un único tipo de inventario de material, las compras se simplifican al manejar una única referencia y es posible negociar precios preferenciales por compra en volumen. La capacidad del cable utilizado permitirá conectar y poner en servicio las nuevas tecnologías de comunicación que actualmente se encuentran en proceso de desarrollo y que se encontrarán en el mercado en los próximos 10 años.

## **COMPONENTES DEL CABLEADO ESTRUCTURADO**

### ROSETA:

Se trata de una pieza plástica de soporte que se amura a la pared y permite encastrar hasta dos conectores RJ 45.-

### FRENTE PARA CONECTOR:

Se trata de una tapa plástica de una caja estándar de electricidad embutida de 5 x 10 cm, que permite conectar hasta 2 conectores RJ45.

### CABLE UTP (SÓLIDO)

El cable de estas características posee 4 pares bien trenzados entre sí, se puede presentar en cajas de 1000' (305 mts), es un cable que permite una mejor manipulación, debido a que no se enrosca y viene marcado con números que marcan las distancias de cada tramo.

### PATCH PANEL

Están formados por un soporte, usualmente metálico y de medias ajustadas al estándar de los rack de 19".

De un lado se colocan los conectores RJ 45 y del otro los conectores IDC para block tipo 110. Se fabrican en capacidades de 12 bocas.

### PATCH CORD

Están contruidos con cables UTP de 4 pares, clase 5, tipo flexible con un conector tipo RJ45 en cada extremo del cable, el largo máximo recomendado no puede exceder los 3 mts.

### CONECTOR RJ 45

Conector similar al telefónico RJ 11 pero posee 8 contactos bañados en oro, lo que asegura una mejor comunicación.

### CONEXIÓN A UNA CAJA RJ 45

