Tecnología de Redes

INDICE DE CONTENIDO

Tema 1

Comunicación

En esta lección, nos introduciremos en el mundo de las redes, también veremos los gastos que supone montar una red en un espacio, donde el traspaso de información es primordial.

Índice

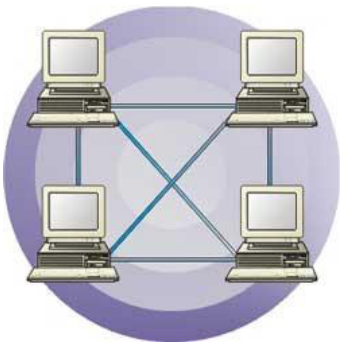
01 Orígenes

En el año 1981, IBM creó la primera computadora personal (PC), dirigida a aquellas personas que deseaban disponer de su propio equipo informático.

En breve, dichos equipos se iban conectando uno a uno hasta formar grupos de redes, alrededor de 1985 las redes se extendieron, y se hicieron tan grandes y complejas que el control lo tomaron los departamentos de informática.

En la actualidad, cada ordenador o nodo, se halla conectado a una gran red, y cada vez, un mayor número de redes se interconectan entre sí. Por lo cual, se incrementan los usuarios conectados detrás de *ese cablecito*, que promete maravillas y a veces sólo trae frustraciones.

Una red es simplemente un conjunto de nodos, capaces de intercambiar información, unidos mediante un enlace físico.



En los inicios del procesado de información, con la informática sólo se facilitaban los trabajos repetitivos y monótonos del área administrativa. La automatización de esos procesos trajo como consecuencia directa una disminución de los costos y un incremento en la productividad.

En la informática convergen los fundamentos de las ciencias de la computación, la programación y metodologías para el desarrollo de software, la arquitectura de computadores, las redes de computadores, la inteligencia artificial y ciertas cuestiones relacionadas con la electrónica. Se puede entender por informática a la unión sinérgica de todo este conjunto de disciplinas. Esta disciplina se aplica a numerosas y variadas áreas del conocimiento o la actividad humana, como por ejemplo: gestión de negocios, almacenamiento y consulta de información, monitorización y control de procesos, industria, robótica, comunicaciones, control de transportes, investigación, desarrollo de juegos, diseño computarizado, aplicaciones/herramientas multimedia, medicina, biología, física, química, meteorología, ingeniería, arte, etc. Puede tanto facilitar la toma de decisiones a nivel de una empresa como permitir el control de procesos críticos. Actualmente es difícil concebir un área que no use, de alguna forma, el apoyo de la informática. Ésta puede cubrir un enorme abanico de funciones, que van desde las más simples cuestiones domésticas hasta los cálculos científicos más complejos.

Entre las funciones principales de la informática se cuentan las siguientes:

- Creación de nuevas especificaciones de trabajo
- Desarrollo e implementación de sistemas informáticos
- Sistematización de procesos
- Optimización de los métodos y sistemas informáticos existentes
- facilita la automatización de datos

Podríamos decir que la informática va en aumento, y que las comunicaciones son auténticas *ciudades virtuales*.

02 Red de computadoras

Una **red de computadoras**, también llamada **red de ordenadores**, **red de comunicaciones de datos** o **red informática**, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

Componentes básicos de las redes

Para poder formar una red se requieren elementos: **hardware**, **software** y **protocolos**. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (*hosts*) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los dispositivos de red son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es la de interconectar los componentes hardware de una red, y por tanto, las computadoras individuales, también denominados *hosts*, a los equipos que ponen los servicios en la red, los servidores, utilizando el cableado o tecnología inalámbrica soportada por la electrónica de red y unidos por cableado o radiofrecuencia. En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea ésta parte de un ordenador, de un conmutador, de una impresora, etc. y sea de la tecnología que sea (ethernet, Wi-Fi, Bluetooth, etc.).

Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red, o NIC (*Network Card Interface*), con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, ceros y unos). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (*Media Access Control*), que consta de 48 bits. Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

El trabajo del adaptador de red es el de convertir las señales eléctricas que viajan por el cable (ej: red Ethernet) o las ondas de radio (ej: red Wi-Fi) en una señal que pueda interpretar el ordenador.

Estos adaptadores son unas tarjetas PCI que se conectan en las ranuras de expansión

del ordenador. En el caso de ordenadores portátiles, estas tarjetas vienen en formato PCMCIA o similares. En los ordenadores del siglo XXI, tanto de sobremesa como portátiles, estas tarjetas ya vienen integradas en la placa base.

Adaptador de red es el nombre genérico que reciben los dispositivos encargados de realizar dicha conversión. Esto significa que estos adaptadores pueden ser tanto Ethernet, como wireless, así como de otros tipos como fibra óptica, coaxial, etc. También las velocidades disponibles varían según el tipo de adaptador; éstas pueden ser, en Ethernet, de 10, 100, 1000 Mbps o 10000, y en los inalámbricos, principalmente, de 11, 54, 300 Mbps.

03 Clasificación de las redes

Una red puede recibir distintos calificativos de clasificación en base a distintas taxonomías: alcance, tipo de conexión, tecnología, etc.

Por alcance

- **Red de área personal**, o PAN (*Personal Area Network*) en inglés, es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.

- **Red inalámbrica de área personal**, o WPAN (*Wireless Personal Area Network*), es una red de computadoras inalámbrica para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, móviles, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella. El medio de transporte puede ser cualquiera de los habituales en las redes inalámbricas pero las que reciben esta denominación son habituales en Bluetooth.

- **Red de área local**, o LAN (*Local Area Network*), es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización. No utilizan medios o redes de interconexión públicos.

- **Red de área local inalámbrica**, o WLAN (*Wireless Local Area Network*), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas.

- **Red de área de campus**, o CAN (*Campus Area Network*), es una red de computadoras de alta velocidad que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, una base militar, hospital, etc. Tampoco utiliza medios públicos para la interconexión.

- **Red de área metropolitana** (*metropolitan area network* o *MAN*, en inglés) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica más extensa que un campus, pero aún así limitado. Por ejemplo, un red que interconecte los edificios públicos de un municipio dentro de la localidad por medio

de fibra óptica.

- **Redes de área amplia**, o WAN (*Wide Area Network*), son redes informáticas que se extienden sobre un área geográfica extensa utilizando medios como: satélites, cables interoceánicos, Internet, fibras ópticas públicas, etc.

- **Red de área de almacenamiento**, en inglés SAN (*Storage Area Network*), es una red concebida para conectar servidores, matrices (*arrays*) de discos y librerías de soporte, permitiendo el tránsito de datos sin afectar a las redes por las que acceden los usuarios.

- **Red de área local virtual**, o VLAN (*Virtual LAN*), es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física. Este tipo surgió como respuesta a la necesidad de poder estructurar las conexiones de equipos de un edificio por medio de software, permitiendo dividir un conmutador en varios virtuales.

Por tipo de conexión

Medios guiados

- El **cable coaxial** se utiliza para transportar señales electromagnéticas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo y uno exterior denominado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes; los cuales están separados por un material dieléctrico que, en realidad, transporta la señal de información.

- El **cable de par trenzado** es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes. Dependiendo de la red se pueden utilizar, uno, dos, cuatro o más pares.

- La **fibra óptica** es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Medios no guiados

- **Red por radio** es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

- **Red por infrarrojos**, permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala. No disponen de gran alcance y necesitan de visibilidad entre los dispositivos.

- **Red por microondas**, es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. Los protocolos más frecuentes son: el IEEE 802.11b y transmite a 2,4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo);

el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11a; el IEEE 802.11n que permite velocidades de hasta 600 Mbps; etc.

Por relación funcional

- **Cliente-servidor** es la arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

- ***Peer-to-peer***, o red entre iguales, es aquella red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Por tecnología

- Red ***Point-To-Point*** es aquella en la que existe multitud de conexiones entre parejas individuales de máquinas. Este tipo de red requiere, en algunos casos, máquinas intermedias que establezcan rutas para que puedan transmitirse paquetes de datos. El medio electrónico habitual para la interconexión es el conmutador, o *switch*.

- Red ***broadcast*** se caracteriza por transmitir datos por un sólo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo. Los equipos unidos por un concentrador, o *hub*, forman redes de este tipo.

Por topología física

Topologías físicas de red.

La **red en bus** se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o *backbone*) al cual se conectan los diferentes dispositivos.

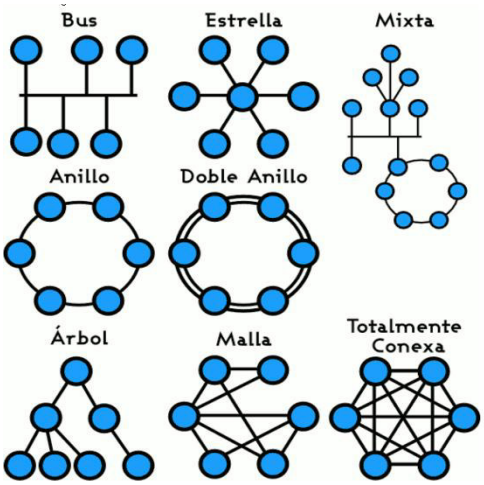
- En una **red en anillo** cada estación está conectada a la siguiente y la última está conectada a la primera.

- En una **red en estrella** las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

- En una **red en malla** cada nodo está conectado a todos los otros.

- En una **red en árbol** los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.

- En una **red mixta** se da cualquier combinación de las anteriores.



Por la direccionalidad de los datos

- Simplex o unidireccional: un equipo terminal de datos transmite y otro recibe.
- *Half-duplex*, en castellano semidúplex: el método o protocolo de envío de información es bidireccional pero no simultáneobidireccional, sólo un equipo transmite a la vez.
- *Full-duplex*, o dúplex: los dos equipos involucrados en la comunicación lo pueden hacer de forma simultánea, transmitir y recibir.

Por grado de autentificación

- **Red privada**: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.
- **Red de acceso público**: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

Por grado de difusión

- Una **intranet** es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.
- **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

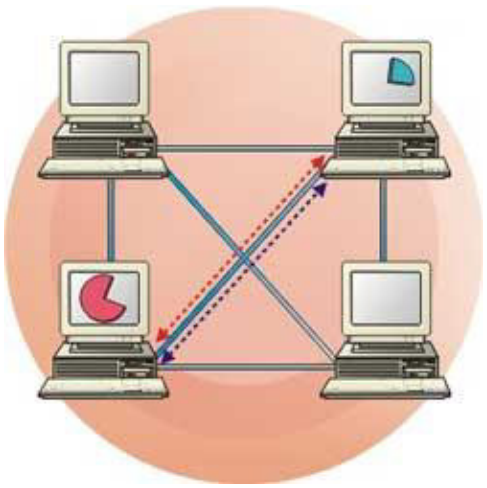
Por servicio o función

- Una **red comercial** proporciona soporte e información para una empresa u organización con ánimo de lucro.
- Una **red educativa** proporciona soporte e información para una organización educativa dentro del ámbito del aprendizaje.
- Una **red para el proceso de datos** proporciona una interfaz para intercomunicar equipos que vayan a realizar una función de cómputo conjunta.

04 Ventajas de las redes

Gracias a las redes, podemos comunicar los diferentes puestos de trabajo, así como:

- **Compartir recursos software**: Es más barato comprar una aplicación para 50 ordenadores, que comprar 50 aplicaciones para cada nodo.
- **Compartir recursos hardware**: Es más barato comprar un par de impresoras o escáneres para 50 ordenadores, que comprar una impresora o un escáner para cada uno.
- **Compartir una base de datos**: Cualquier usuario conectado a la red, podrá tener acceso a cualquier modificación en la base de datos que haya realizado otro usuario. Por Ej.: Todos los usuarios de un mismo banco podrán acceder a la misma base de datos desde cualquier nodo conectado a la red.



05 Objetivos de las redes

El objetivo genérico perseguido por una red, es conseguir una serie de ventajas en la interconexión de sistemas informáticos respecto de otros mecanismos o medios empleados. Algunas de ellas son:

- **Reducción de costes**: Nos será más barato utilizar una red, en una empresa donde la información viaje constantemente, que emplear otra forma de difusión. La infraestructura invertida en el montaje de la red se va recuperando progresivamente.
- **Flexibilidad**: Podemos desplazarnos a cualquier sitio del mundo sin importar en ello la distancia.
- **Fiabilidad y seguridad**: Por ejemplo: En una red, todo personal que no esté autorizado no podrá beneficiarse de los recursos disponibles (Impresoras, escáner, etc.).
- **Velocidad**: Logramos transmitir una determinada información de una manera segura e inmediata.
- **Compartición de recursos**: Podemos utilizar en una misma red un DVD de otro equipo.
- **Compatibilidad**: Logramos utilizar redes mayores sin ninguna complejidad.
- **Simplicidad**: Para enlazar equipos o nodos a un medio, no se requiere gran cantidad de cableado, conectándose de una forma utilizada también por otros medios como, teléfono, TV, etc.

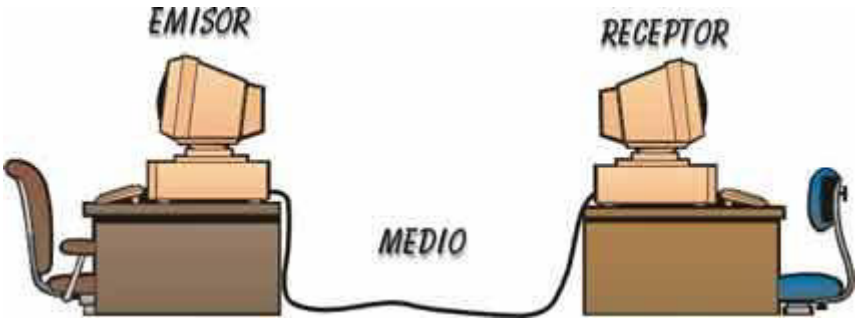
06 Telemática

La **telemática** cubre un campo científico y tecnológico de una considerable amplitud, englobando el estudio, diseño, gestión y aplicación de las redes y servicios de comunicaciones, para el transporte, almacenamiento y procesado de cualquier tipo de información (datos, voz, vídeo, etc.), incluyendo el análisis y diseño de tecnologías y sistemas de conmutación. Su objeto de estudio son las llamadas TICs (Tecnologías de la información y la comunicación). La Telemática abarca entre otros conceptos los siguientes planos funcionales:

- El plano de usuario, donde se distribuye y procesa la información de los servicios y aplicaciones finales;
- El plano de señalización y control, donde se distribuye y procesa la información de control del propio sistema, y su interacción con los usuarios;
- El plano de gestión, donde se distribuye y procesa la información de operación y gestión del sistema y los servicios, y su interacción con los operadores de la red.

Se denomina telemática a la ciencia que estudia la unión de dos campos, Telecomunicaciones e informática, encargada de la comunicación de nodos. Este estudio recae en tres partes principales:

- **Emisor o Fuente**: Es aquel nodo que transmite la información.
- **Medio**: Es el camino por el cual viaja la información.
- **Receptor o Colector**: Es aquel nodo que recibe la información.



La comunicación está dividida en tres grandes grupos, dependiendo del tipo de transmisión:

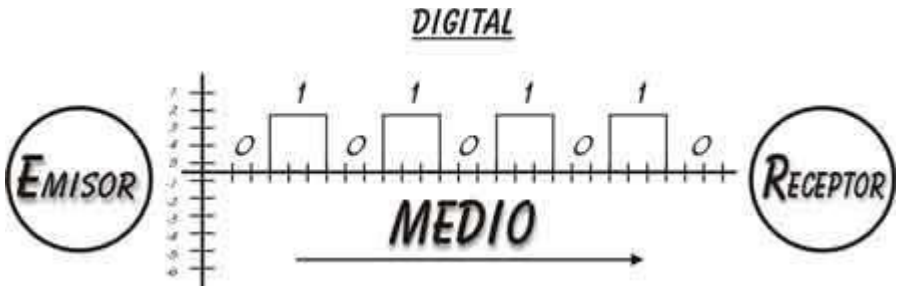
1. Simplex: Sistema en el que sólo se puede transmitir por un sentido, por ejemplo las antenas de TV.
2. Semidúplex: Sistema en que se puede transmitir la información en ambos sentidos, pero alternativamente, por ejemplo las emisoras de radiofrecuencias.
3. Dúplex: Sistemas en los que se pueden transmitir información en las dos direcciones simultáneamente, por ejemplo el teléfono.

Para que el emisor y el receptor se puedan comunicar, deben tener unas reglas o normas. A estas *reglas o normas*, se les denominan Protocolos.

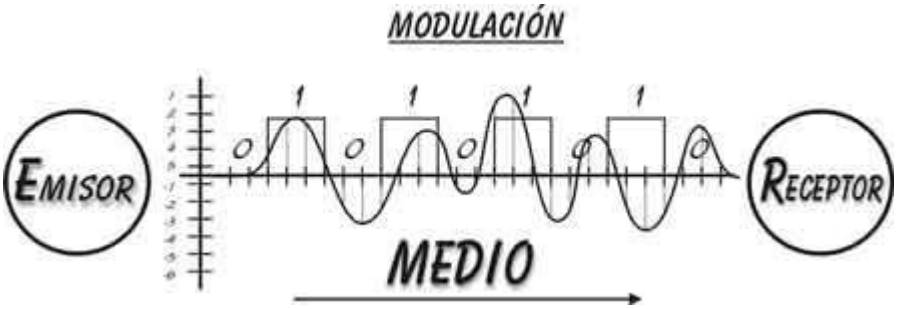
La información que se transmite por el medio puede ser de tres tipos:

- **Analógica**: Esta señal se propaga por el medio a través de valores alternos.

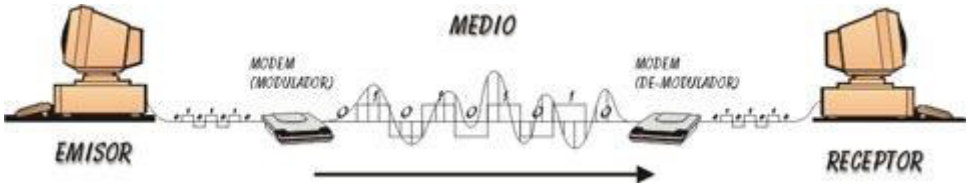
- **Digital**: Esta señal se propaga por el medio mediante impulsos.



- **Modulación**: Ambas señales pueden ser superpuestas en casos concretos como, por ejemplo, la portadora, en la que la señal analógica transporta la señal digital.



La utilidad del **MÓDEM** es el ejemplo más claro. Cuando queremos transmitir una determinada información, el modulador recoge la señal digital y la transporta al sitio de destino. Cuando llega al receptor, éste la de-modula y le quita la señal analógica dejando operativa sólo la señal digital.



Tema 2

Teoría de Redes

Esta lección nos dará a conocer los distintos tipos de transmisión, así como el modo de transmitir. También estudiaremos la distribución de los nodos conectados en red, y cómo se comunican entre ellos.

Las características de una red pueden variar dependiendo de la forma de conexión, la técnica de acceder a la red, el cable por el que viaja la información, y su arquitectura.

Índice

01 Redes conmutadas

Consiste en un conjunto de nodos interconectados entre sí, mediante el medio físico (el cable,...), encaminando la información del nodo origen al nodo destino, pasando por nodos intermedios. Estos últimos son los encargados de encauzar los datos para que llegue a su destino.

Dentro de las redes conmutadas podemos distinguir dos grupos:

- **Conmutación de paquetes**: Cuando un nodo quiere enviar una información a otro nodo, la divide en paquetes, esto hace controlar la información que se va enviando. Si se pierde un paquete por el camino, simplemente el nodo receptor avisa al nodo emisor qué número de paquete ha fallado, y éste lo vuelve a enviar.

Sigamos los mismos pasos que recorre la información desde que un nodo emisor envía la información hasta que el nodo receptor la recoge:

1. El nodo emisor *trocea* la información en pequeños *paquetes* que irán numerados.

2. El primer paquete pasará por el nodo intermediario (aquel nodo que esté en la trayectoria entre el emisor y el receptor), y lee la cabecera, ésta contendrá la dirección del destino.

3. Al no ser el nodo intermediario el destino, éste le añade a la cabecera otra más pequeña, que servirá para remediar alguna pérdida o deterioro de algún paquete.

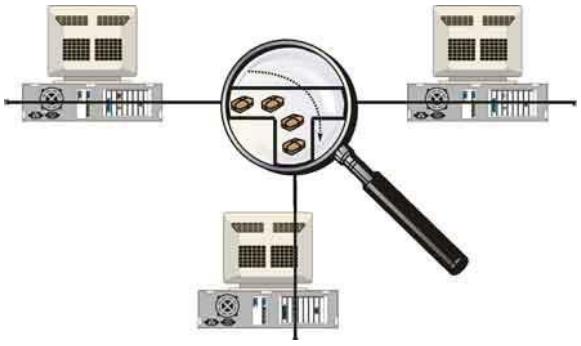
El nodo intermediario (que puede ser uno o varios) puede llegar a mantener una cola de paquetes, que saldrán a su destino según el orden de importancia sometido a criterios de preferencia, por ejemplo: En una empresa, el departamento de investigación y desarrollo tiene más prioridad en recibir los datos que el departamento de marketing.

Cuando el primer paquete llega a su destino, éste lee su cabecera y al comprobar que la información va dirigida hacia él, la recoge.

Existen dos técnicas de envío dentro de los tipos de conmutación:

-**Técnicas de datagramas**: Esta técnica envía los paquetes a medida que se van dividiendo. El inconveniente de esta técnica es, por ejemplo, que puede llegar el paquete 5, antes que el paquete 1, puesto que los paquetes van buscando los caminos hasta llegar a su destino.

-**Técnicas de circuitos virtuales**: Esta técnica envía un paquete de control el cual asignará un camino lógico por donde viajarán todos los demás paquetes. El paquete de control contendrá la información de cuántos paquetes se enviarán. Esto nos servirá para informar al receptor qué paquetes se han perdido.



- **Conmutación de circuitos**: En esta comunicación no existen nodos intermediarios, simplemente hay una comunicación nodo a nodo (nodo emisor, nodo receptor), mediante un medio físico (el cable,..). Esta conexión permanece hasta que termina la transmisión. Un ejemplo claro de conmutación de circuitos es la telefonía.

Seguiremos los pasos de la información, desde que el emisor comienza a transmitirla información, hasta que le llega por completo al receptor.

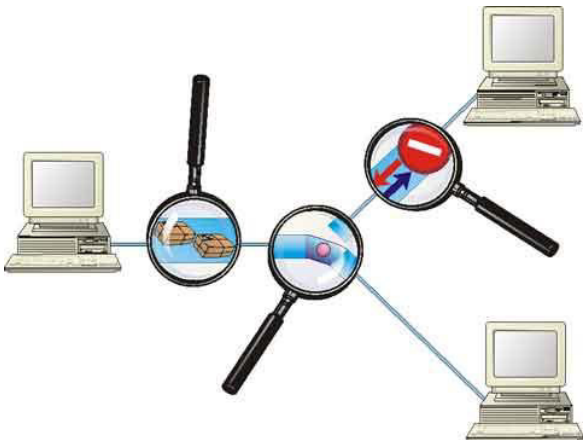
Cuando la información empieza a salir, ésta pasa por tres etapas de conexión:

- **Establecimiento del circuito**: El emisor solicita una conexión con el receptor mediante los nodos intermediarios, que actuarán como uniones exclusivas del emisor-receptor.

- **Transferencia de datos**: Una vez creada la conexión, los dos nodos empezarán la transmisión de datos de emisor a receptor sin ninguna espera, ya que estos dos nodos tienen el canal reservado para ellos solos.

- **Desconexión del circuito**: Cuando se termina la comunicación o la transferencia de datos, el nodo emisor o receptor avisa a los demás nodos que han intervenido, para realizar la conexión exclusiva, que liberen el canal utilizado.

Esta comunicación es bastante ineficiente pues los canales quedan reservados para el uso exclusivo de una comunicación. Sin embargo, la transmisión de voz, en este tipo de comunicación, es la más usada, ya que llega en tiempo real, a pesar de sus pequeñas *pérdidas.*



02 Ventajas y desventajas de las técnicas de envío

Técnicas de datagramas

- Para la transmisión de pocos paquetes, la técnica de datagrama es la más rápida, puesto que no necesita un paquete de control.

- La técnica de datagrama es más segura, de modo que, si un nodo tiene algún problema al recibir los datos, sólo perderá el paquete con el que está trabajando, pero sin embargo, la técnica de circuitos virtuales, si pierde el paquete de control, fallará la transmisión perdiendo, por tanto, toda la información.

Técnicas de circuitos virtuales

- Para mayor cantidad de datos, la técnica de circuitos virtuales es más rápida, puesto que todos los paquetes llegan más rápido a su destino.

- En la técnica de circuitos virtuales, todos los paquetes llegan en el mismo orden en el que salen.

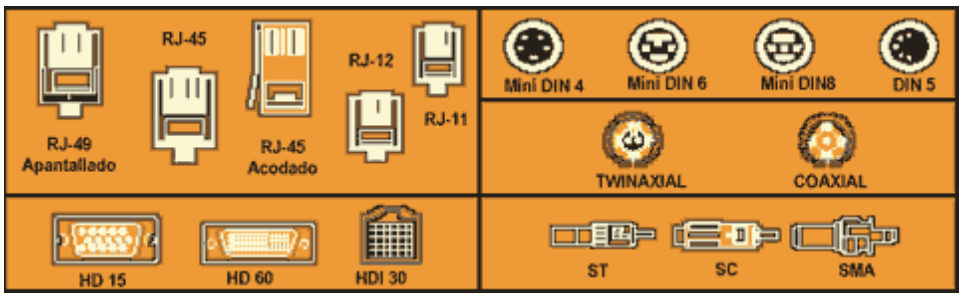
- En la técnica de circuitos virtuales, cuando a un nodo le llega un paquete erróneo, éste avisa al nodo anterior para que se lo vuelva a mandar antes de seguir transmitiendo.

03 Medios de transmisión

El medio de transmisión define las características de interconectar varios nodos en una red.

Los medios físicos más utilizados han sido por excelencia: el cable de par trenzado (el del teléfono) y el coaxial (la antena del TV), aunque éste último prácticamente ha desaparecido

En contrapartida, aparecen las nuevas alternativas, que son: la fibra óptica y las ondas de radio.



En la siguiente tabla, vamos a comparar los tipos de medios existentes en el mercado y cómo responden mediante la distancia:

Tabla de Medios físicos					
Medio	Capacidad	Pérdidas	Longitud típica	Coste	Flexibilidad
Coaxial grueso (Parecido a la antena de TV)	Alta	Baja	500 m	Medio	Baja
Coaxial fino	Alta	Baja	200 m	Muy bajo	Media
Par trenzado sin apantallar (UTP)	Media Alta	Media	De 20 m a 30 m	Muy bajo	Alta
Par trenzado apantallado (STP)	Media	Media	100 m	Bajo	Alta
Fibra óptica	Muy Alta	Casi ninguna	500 m	Muy alto	Baja
Radio	Media Alta	Media	De 10 m a 10 Km	Alto	Muy alta
Infrarrojos	Media	Media	20 m	Alto	Muy alta
Láser	Alta	Media / Alta	1 – 5 Km	Alto	Media

Tipos de cableado:

Los principales tipos de cable que nos vamos a encontrar son:

- **Coaxial**: Este tipo de cable consiste en un hilo conductor central, rodeado por un aislante. Dicho aislante, separa el hilo conductor central de una malla protectora, esta malla evita las injustas interferencias, causantes de las pérdidas de datos. Este tipo de cable es más caro que el par trenzado y ya está en desuso.

- **Cable de par trenzado**: Es un cable formado por un par de hilos de cobres aislados y enrollados entre sí. La utilización del trenzado tiende a disminuir la interferencia. Los conectores utilizados en los extremos son los RJ-45.

Físicamente este cable se puede dividir en dos tipos:

- **STP** (Shielded twisted pairs o par trenzado apantallado): Cada par va cubierto por una malla que actúa como protector contra las interferencias.

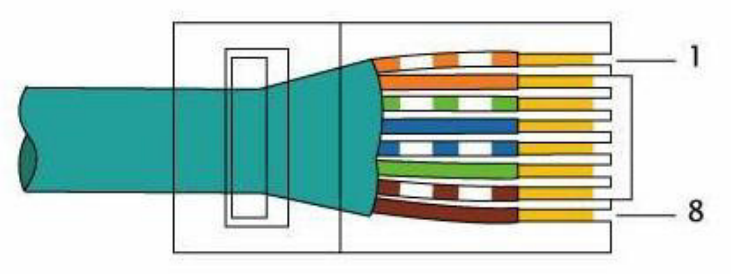
- **UTP** (Unshield twisted pairs o par trenzado sin apantallar): Cada par va desnudo y la única protección contra las interferencias es su trenzado.

Las velocidades en este tipo de medio pueden variar según la categoría del cable utilizado. La categoría de estos cables va desde la 1 hasta la 6, ya no es habitual encontrar cables de categoría menor a categoría 5 y no se aconseja su utilización, por lo que empezamos la clasificación en esta categoría:

- **Categoría 5**: Puede transmitir información hasta 100 Mbps.
- **Categoría 5e** (enhanced): Puede transmitir información hasta 1000 Mbps.
- **Categoría 6**: No se aconseja otro tipo para instalar una red nueva, permite transmitir a la misma velocidad que el cable de categoría 5e pero con mayor tolerancia ruido y a interferencias externas

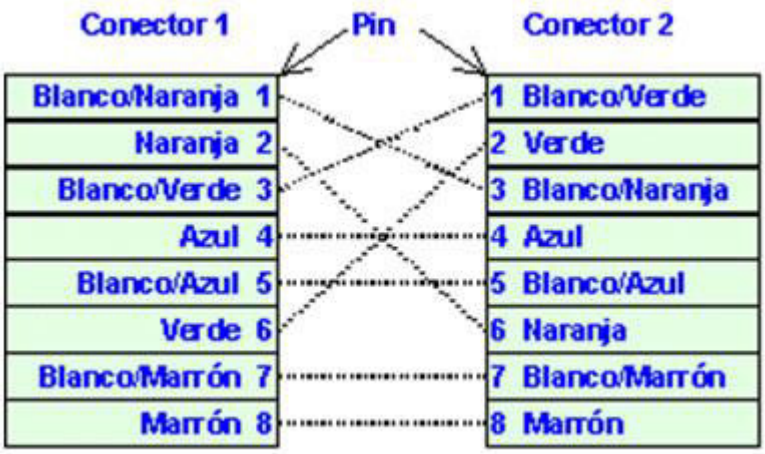
Estos cables están formados por 8 cables trenzados a pares y estos pares están a su vez trenzados entre sí, cada cable se identifica por un color o combinación de colores y para conseguir que su funcionamiento sea óptimo, se aconseja que estén colocados en los conectores en un orden concreto:

- Blanco/naranja
- Naranja
- Blanco/verde
- Azul
- Blanco/azul
- Verde
- Blanco/Marrón
- Marrón



Es muy importante que los cables lleguen al fondo del conector, y que en ambos extremos el orden sea el mismo. Una vez tengamos los cables introducidos en el conector, debemos cerrarlo usando una **crimpadora**.

- **Cable cruzado**: El cable de par trenzado que hemos visto, es el indicado para conectar un PC a un switch o a un router, no obstante, si quisiéramos conectar dos dispositivos similares entre sí (como dos switches o dos PCs), necesitaríamos un cable cruzado. Este es un cable en el que un extremo lleva el orden de cables normal y en el extremo contrario se intercambian los cables de las posiciones 1 y 3 y las de 2 y 6.



- **Fibra óptica**: Este tipo de medio es frágil y muy fino, conduce energía de naturaleza óptica. Su forma es parecida a la de un cilindro, y se divide en tres partes: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico, dichas fibras están revestidas del mismo material que el núcleo pero con diferentes propiedades. Inmediatamente después y rodeando al núcleo, nos encontramos la cubierta, su misión es aislar al núcleo de posibles aplastamientos, abrasiones e incluso de la humedad.

Este medio es muy apropiado para largas distancias, aunque precisa equipos caros y complejos para realizar las conexiones de los nodos.

Los beneficios de la fibra óptica son:

- Permite un mayor ancho de banda, es decir, mayor cantidad de datos.

- Menor atenuación, con lo que puede transportar la información sin sufrir ninguna modificación.

- Aislamiento electromagnético, es decir, las interferencias no le influyen.

- Mayor separación de repetidores, al ser un medio de luz, puede alcanzar una gran distancia antes de que la señal se atenúe.

.

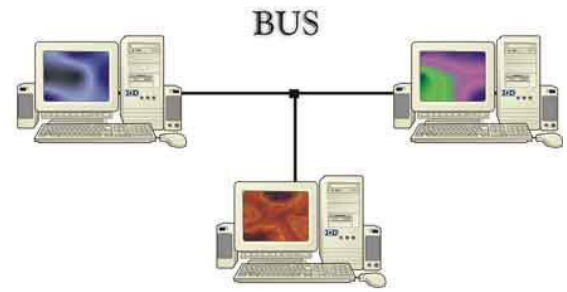
04 Topologías

Se llaman **topologías** a las relaciones de interconexión entre nodos, es decir, la forma de unión entre los distintos dispositivos de una red, o mejor dicho, la organización del cableado.

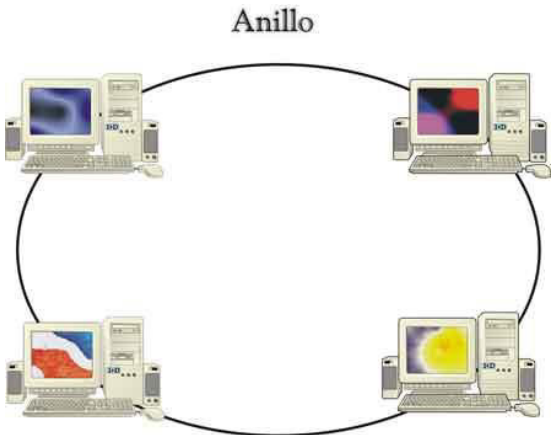
Las topologías más usadas entre las redes informáticas son:

- **Bus**: La característica principal de esta topología es su enlace multipunto, lo que hace que las estaciones o nodos se conecten a lo largo de un único medio.

La denominada *estrella pasiva*, aunque geométricamente parezca una estrella, desde el punto de vista topológico se designa Bus, esta supuesta *estrella pasiva* tiene las mismas propiedades, ya que su característica principal es el multipunto.



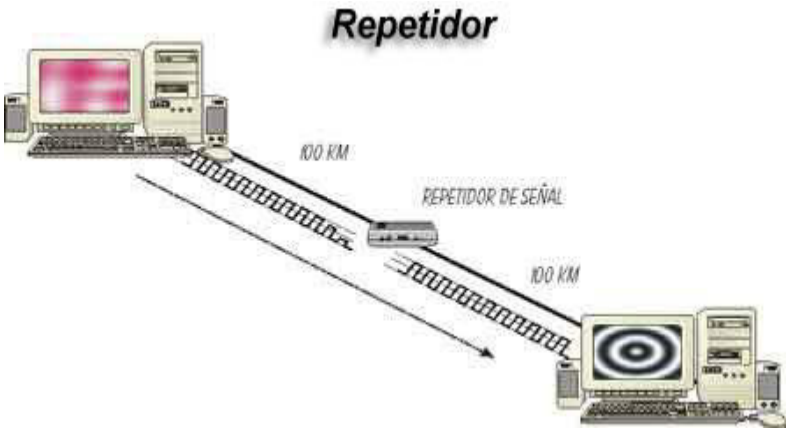
- **Anillo**: Las estaciones o nodos están unidas unas con otras formando un círculo a través de un medio común (cable, láser, etc.) La información circula en un solo sentido alrededor del círculo. El problema de esta topología es la fiabilidad, ya que, el fallo de un nodo implica la caída de toda la red. Para evitar algunos problemas, se utiliza el puenteo y el doble anillo.



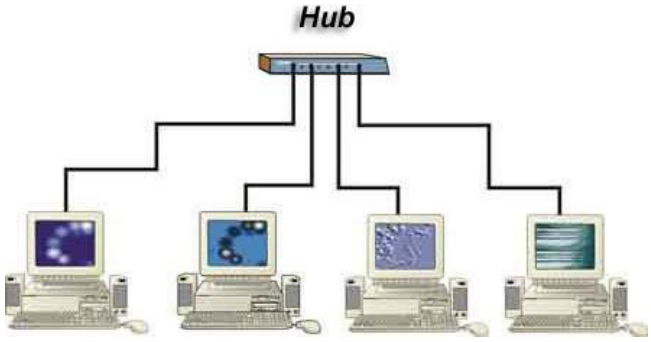
- **Estrella**: En esta topología, encontramos todas las estaciones conectadas a un nodo (controlador), dicho nodo se conecta a los demás mediante un enlace punto a punto. La ventaja de esta topología es la facilidad de localizar las averías, puesto que si se rompe el medio, sólo se pierde la conexión con el nodo al que está conectado. Dos de los inconvenientes son el alto coste que implica el montaje de una red con esta topología y la gran cantidad de cableado. No obstante, es la topología más extendida actualmente ya que las anteriores están en desuso.

05 Dispositivos

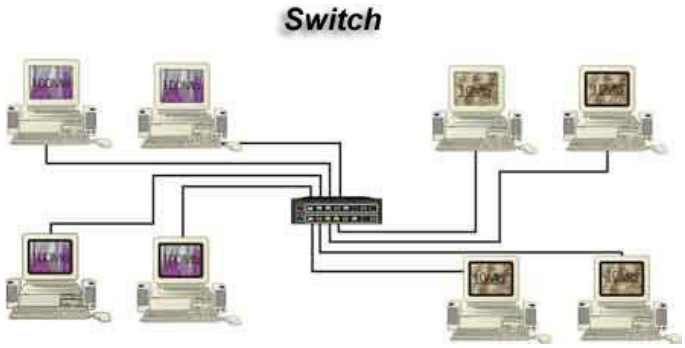
Repetidores: Un repetidor es un dispositivo pasivo cuya misión consiste en recoger señales del medio y regenerarlas, amplificándolas principalmente, hacia otro lado de la red que conecta. El repetidor se utiliza en redes iguales, que estén separas por distancias elevadas.



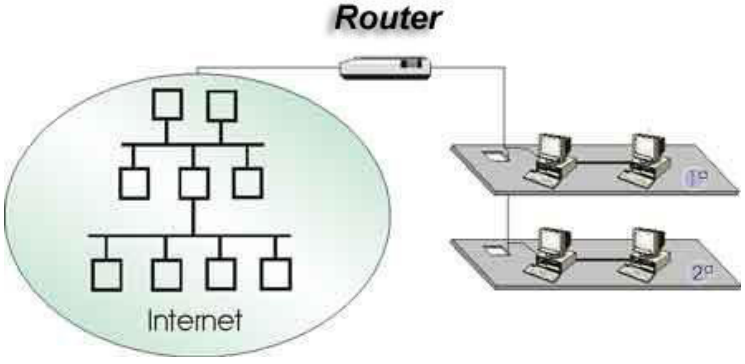
Hub: Las redes bus de pares trenzados se constituyen físicamente como redes en estrella pasiva. Cada nodo de dicha red se conecta a este dispositivo central, conocido como repetidor multipuerto. Este punto de conexión amplifica las señales recogidas por uno de los puertos y la inyecta por la red. Son dispositivos antiguos que ya están en desuso.



Switch: Son parecidos a los Hub, con la gran diferencia de poder cambiar la velocidad de cada puesto de conexión. Además es capaz de enviar el tráfico sólo al puerto donde está conectado el dispositivo de destino en lugar de inyectarlo hacia toda la red. Con este dispositivo, podemos personalizarla red y aprovechar su máximo rendimiento.



Encaminadores o routers: Estos módulos enlazan redes que utilizan el mismo protocolo pero distinta técnica de acceso. Este unidad realiza una selección dinámica de las rutas mediante listas, y pueden elegir la más óptima tendiendo a un conjunto de factores como la capacidad, la velocidad, etc. El router tiene como su primera ventaja encontrar un camino alternativo y adecuado a través de grandes redes.



Firewall: Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial

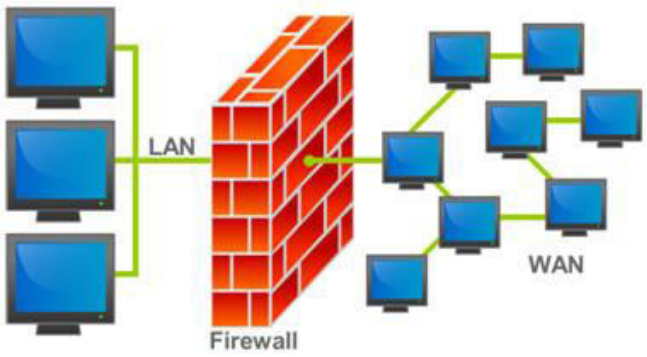
Un firewall es simplemente un filtro que analiza el tráfico entre las redes y en función de las reglas que tenga definidas, permite o deniega su paso. Básicamente los parámetros que analiza y en los que podemos basar las reglas a configurar son:

- Origen: Desde qué red/host/dispositivo se ha iniciado el tráfico de datos.
- Destino: Hacia qué red/host/dispositivo va dirigido el tráfico de datos.
- Entrante o saliente: En qué interfaz de red está el destino (LAN, Internet, etc.).
- Puerto de origen: Qué puerto del host origen está originando los datos.
- Puerto de destino: Hacia qué puerto del host destino van dirigidos los datos (p ej. Puerto 80 si es a un servidor WEB, puerto 25 si es a un servidor de correo, etc.).
- Fecha y hora: En muchos dispositivos es posible condicionar nuestras reglas en base al tiempo (p ej. No permitir la navegación hacia ciertas páginas en horario laborable)

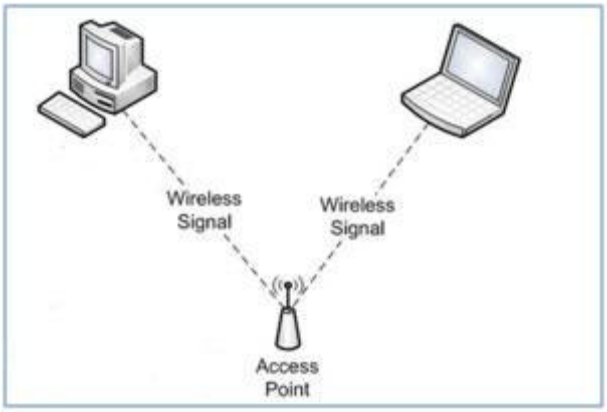
De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en una máquina con una conexión a cada una de las redes que queramos separar.

Desde hace varios años, hay sistemas operativos que disponen de una aplicación de Firewall integrada, esta aplicación no está destinada a proteger dos redes distintas, sino a proteger el propio ordenador donde se instala contra el tráfico malicioso que pueda venir por la red, sea esta de cualquier tipo (LAN, WAN, Internet, etc.).



Punto de acceso: El accesspoint o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.



Actualmente es muy común, sobre todo en instalaciones domésticas, disponer de un router ADSL que engloba en un solo dispositivo las funciones de router, switch, firewall y punto de acceso.

01 Práctica: Montar cable normal

Montaje de un cable Ethernet con RJ-45

Con este ejercicio, vamos a crear nuestro medio de comunicación. Una vez terminado, podemos probarlo conectando un equipo a nuestro switch o router.

Pasos a seguir:

El material necesario para la práctica es el siguiente:

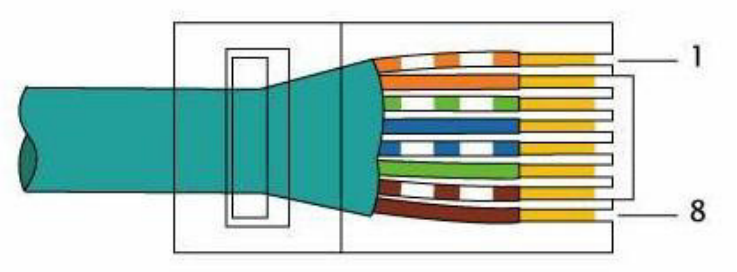
- Cable UTP categoría 5 o superior.
- Dos terminales RJ-45.
- Crimpadora para RJ-45.

Primero, vamos a proceder a desenfundar el cable de par trenzado cuidando de no dañar los hilos de cobre ni sus fundas individuales.

Seguidamente, introduciremos los hilos del medio de par trenzado en el terminalRJ-45.

Como podemos observar, los hilos son de diferentes colores, como Rojo, Rojo-Blanco, Verde, Verde-Blanco, etc. E irán colocados de una forma determinada. A continuación, veremos la combinación que debe seguirse en ambos extremos:

1. Blanco/naranja
2. Naranja
3. Blanco/verde
4. Azul
5. Blanco/azul
6. Verde
7. Blanco/Marrón
8. Marrón



Cuando hayamos introducido los hilos, los fijaremos al terminal con la herramienta mencionada anteriormente.

Por último, probaremos el cable en una red que haya funcionado previamente.

02 Práctica: Montar cable cruzado

Montaje de un cable cruzado Ethernet con RJ-45

Con este ejercicio, vamos a crear un cable que nos servirá para conectar 2 dispositivos del mismo tipo, como por ejemplo 2 PCs sin necesidad de utilizar un router o switch.

Pasos a seguir:

El material necesario para la práctica es el siguiente:

- Cable UTP categoría 5 o superior.
- Dos terminales RJ-45.
- Crimpadora para RJ-45.

Primero, vamos a proceder a desenfundar el cable de par trenzado cuidando de no dañar los hilos de cobre ni sus fundas individuales.

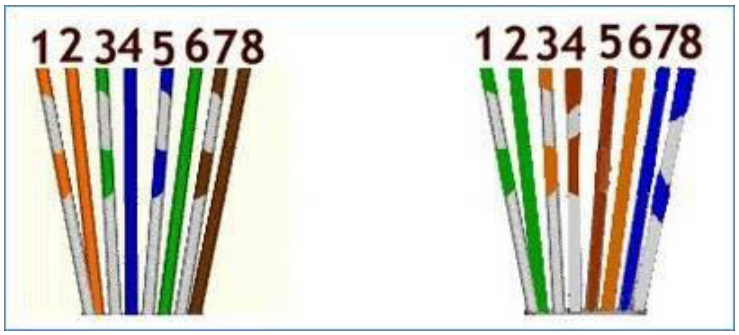
Seguidamente, introduciremos los hilos del medio de par trenzado en el terminalRJ-45.

Como podemos observar, los hilos son de diferentes colores, como Rojo, Rojo-Blanco, Verde, Verde-Blanco, etc. E irán colocados de una forma determinada. A continuación, veremos la combinación que debe seguirse en un extremo.

1. Blanco/naranja
2. Naranja
3. Blanco/verde
4. Azul
5. Blanco/azul
6. Verde
7. Blanco/Marrón
8. Marrón

En cambio, en el extremo contrario deberemos intercambiar el orden de algunos cables (intercambiamos el 1 por el 3 y el 2 por el 6), de manera que quede:

1. Blanco/verde
2. Verde
3. Blanco/naranja
4. Azul
5. Blanco/azul
6. Naranja
7. Blanco/Marrón
8. Marrón



Cuando hayamos introducido los hilos, los fijaremos al terminal con la herramienta mencionada anteriormente.

Por último, probaremos el cable conectando cada extremo a un equipo, les asignaremos una dirección TCP/IP a cada uno (por ejemplo 192.168.0.1 y 192.168.0.2 ambas con máscara 255.255.255.0) y haremos un ping entre ellos.

Tema 3

Clasificación y Normalización

En esta lección vamos a clasificar las redes según su ámbito, sabiendo que la distancia es un factor problemático. También estudiaremos, las normas que se han creado para mantener un acuerdo, entre el fabricante de componentes informáticos y el usuario de la red.

Índice

01 Clasificación de redes según su ámbito geográfico

La longitud de una red puede alcanzar hasta todo un planeta, pero existen tres áreas principales:

- **Red de área Local**, también llamada **LAN**: Es aquélla que suele abarcar una distancia aproximada que va desde una habitación a un edificio completo.

- **Red de área Media**, también llamada **MAN**: Es aquélla que puede alcanzar desde uno a varios edificios dentro de una misma ciudad.

- **Red de área extensa**, también llamada **WAN**: Es aquélla que alcanza varias ciudades de uno o varios países.

A continuación, explicaremos cada una de ellas detenidamente.

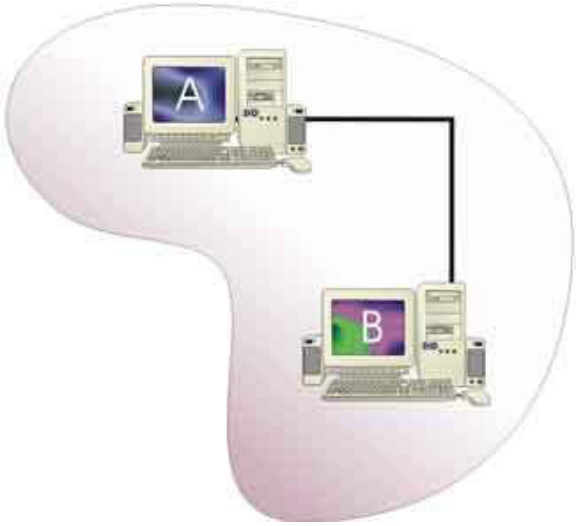
02 Redes LAN

El significado de las siglas de este tipo de área es red de ámbito local (Local Area Networks). Una **red de área local**, **red local** o **LAN** es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

Este tipo de red es la más utilizada por pequeñas empresas. El diámetro que puede alcanzar una red de este tipo, es menor a 5 Km de longitud, teniendo una capacidad entre 5 y 1024 Mbps; pudiendo conectar desde 2 a 50 nodos en un mismo medio.

La información que puede transportar sin ninguna limitación son: los datos, gráficos, mientras que la voz, audio y video sí presentan limitaciones, debido a la necesidad de altas capacidades de transporte.

La velocidad y capacidad es muy alta, puesto que la información no viaja distancias largas. Esta distancia va en proporción al medio que utilicemos, es decir, un coaxial grueso, tendrá más desventajas frente a un medio de fibra óptica.



Ventajas

En una empresa suelen existir muchas computadoras conectadas entre sí, las cuales necesitan de su propia impresora, los datos almacenados en uno de los equipos es muy probable que sean necesarios en otros, por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de dos usuarios, la ocupación de los recursos de almacenamiento en disco se multiplican, las computadoras que trabajen con los mismos datos deberán de tener los mismos programas para manejar dichos datos, etc. La solución a estos problemas es una red de área local, que *permite compartir bases de datos, programas y periféricos* como puede ser un módem, una tarjeta RDSI, una impresora, etc. Poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.

Además, una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de banda ancha compartida por varias computadoras conectadas en red.

03 Redes MAN

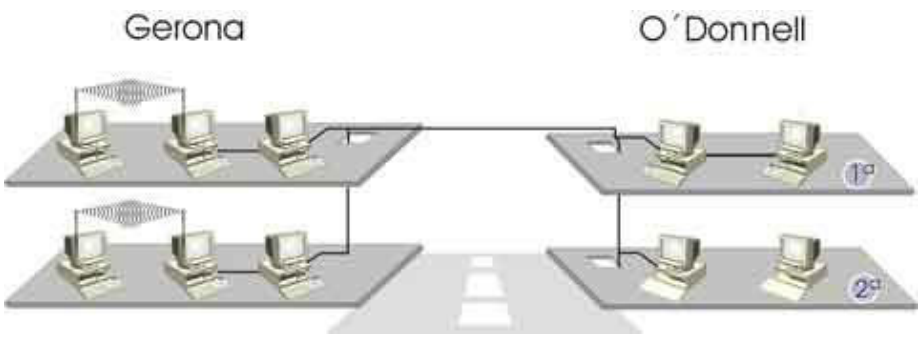
El significado de estas siglas es red de área metropolitana (Metropolitan Area Networks). Este tipo de redes, tiene una longitud de entre 10 y 150 Km aproximadamente, teniendo una capacidad de transmisión de datos de 50 a 622 Mbps

Una **red de área metropolitana** es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50 ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10 Mbps, 20 Mbps, 45 Mbps, 75 Mbps, sobre pares de cobre y 100 Mbps, 1 Gbps y 10 Gbps mediante Fibra Óptica.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores 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.

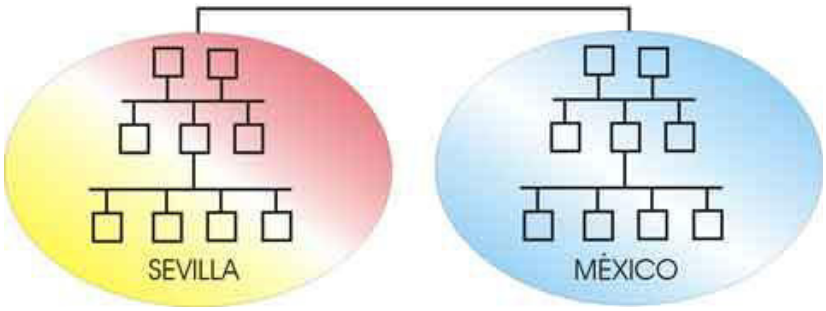
Este tipo de redes es una versión más grande que la LAN y que normalmente se basa en una tecnología similar a esta, La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione, que equivale a la norma IEEE.

Las redes **Man** también se aplican en las organizaciones, en grupos de oficinas corporativas cercanas a una ciudad, estas no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Estas redes pueden ser públicas o privadas.



04 Redes WAN

WAN hace referencia a redes de largo alcance. Esta red puede cubrir todo el planeta y soportar cualquier tipo de datos, el inconveniente es la velocidad.



Una **red de área amplia**, con frecuencia denominada **WAN**, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros.

Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de internet para proveer de conexión a sus clientes.

Hoy en día, Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente, mientras que las redes privadas virtuales que utilizan cifrado y otras técnicas para hacer esa red dedicada, aumentan continuamente.

Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

05 Normalización

Debido a la cantidad de fabricantes y al uso de sus equipos informáticos, se crearon secciones en los organismos de normalización, que se encargaron de establecer unas normas para hacer posible la conexión de los diferentes nodos.

Los organismos más importantes de normalización son dos: ISO (International Organization Standarization) y IEEE (Institute of Electrical and ElectronicEngineers).

- **ISO (International Organization Standarization u Organización Internacional de Normalización)**

Esta organización voluntaria fue fundada en 1946, compuesta por las organizaciones nacionales de normalización, formada por 89 países, entre los que destacan EE.UU. y Alemania.

En relación con las redes, desarrolló el modelo OSI (Open Systems Interconection o Interconexión de Sistemas Abiertos).

- **IEEE o IE3 (Institute of Electrical and Electronic Engineers o Instituto de Ingeniería Eléctrica y Electrónica)**

Es la organización profesional más grande del mundo, entre sus actividades destacan las normas en el área de ingeniería eléctrica y computación. El grupo de normas más importantes en redes de ámbito local, es la 802.x. Estas mismas normas han sido adoptadas por la ISO con el nombre de 8802.x.

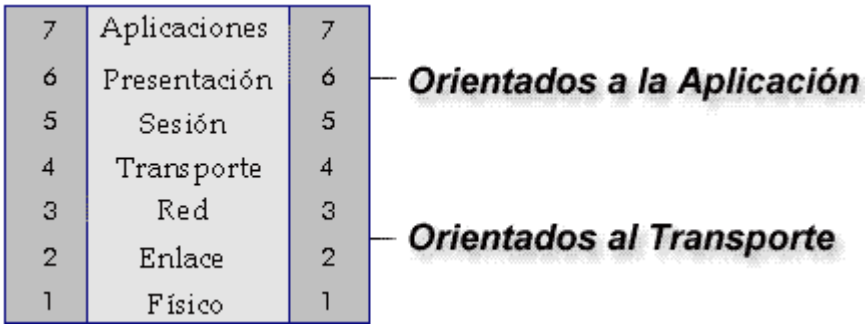
06 El modelo OSI

Este modelo, derivado del modelo ISO, fue aprobado en 1983, y consta de siete niveles, por donde la información debe pasar antes de que el receptor recoja la información.

Los cuatro primeros niveles son los que se encargan del inicio y el control de la comunicación, y se dice que están orientados al transporte.

Los tres últimos niveles son los encargados de facilitar empleo de las aplicaciones, y están orientados a éstas.

Cada uno de los niveles se encarga de resolver los problemas de los niveles inferiores.



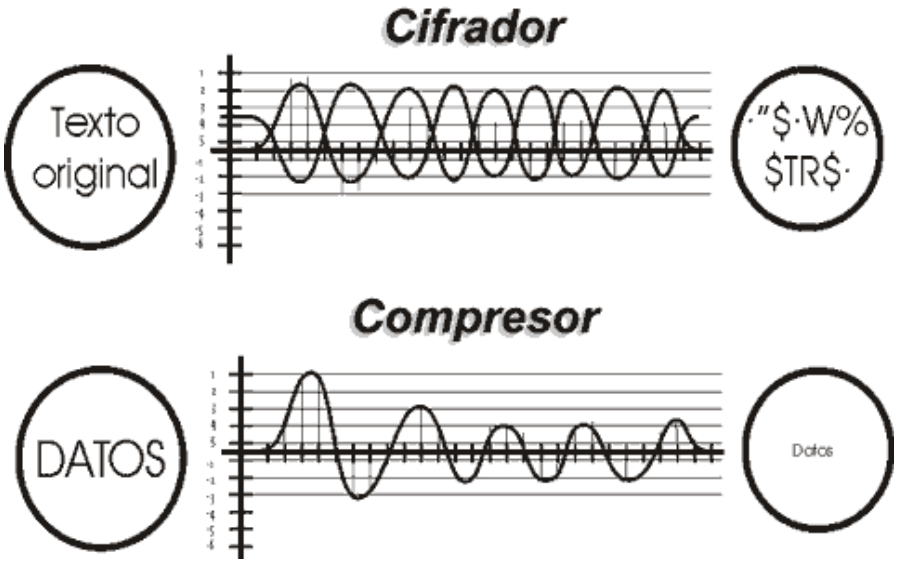
Cada uno de los niveles desempeña una función que más tarde será procesada por el nivel superior. A continuación, veremos la función que desempeñan los siete niveles:

7	Aplicaciones	Semántica de datos
6	Presentación	Representación de datos
5	Sesión	Diálogo ordenado
4	Transporte	Extremo a extremo
3	Red	Encaminamiento
2	Enlace	Punto a Punto
1	Físico	Eléctrico y Mecánico

Ahora vamos a observar, el proceso que sigue una información desde que el nodo emisor envía una determinada información al nodo receptor.

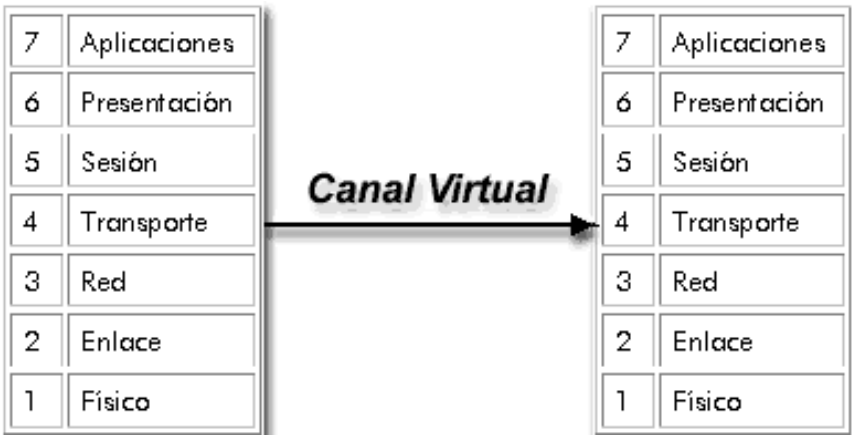
La información sale de su **proceso**, y viaja al nivel de **Aplicación**, el cual le añade una **cabecera** (AH), y se lo pasa al siguiente nivel. El nivel de **Aplicación** contiene los programas del usuario y entre sus funciones se encuentra, acceso a ficheros, transferencia de ficheros, comunicación entre tareas, etc.

El nivel de **Presentación** lo recoge y le añade otra cabecera (PH), cuando termina se lo pasa al siguiente nivel. Es este nivel el encargado de llevar a cabo funciones de uso común, como, aceptar los tipos de datos transferidos del nivel de aplicación y negociar una presentación con el nivel del otro extremo. Este nivel también se encarga de la compresión de datos y **encriptación** de la seguridad.

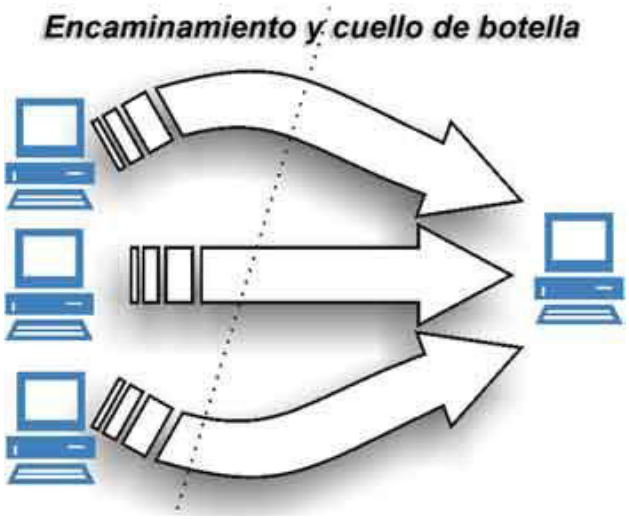


El nivel de **Sesión** lo recibe y le añade otra cabecera (SH), que a su vez, pasa la información al siguiente nivel. Este nivel establece el tráfico de información, que puede ser en ambas direcciones o en una sola. Otras de las funciones de este nivel es la sincronización. El nivel de sesión proporciona una forma de insertar puntos de verificación en el flujo de los datos, de forma que si se produce una pérdida de datos, se puede recuperar gracias al punto de verificación añadido.

El nivel de **Transporte** le añade otra cabecera (TH), y lo pasa al siguiente nivel. Este nivel es el encargado de dividir la información en pequeños paquetes. Normalmente, este nivel crea una conexión de red por cada conexión de transporte, sin embargo, puede crear múltiples conexiones dividiendo los datos entre éstas. Se puede considerar que el nivel de transporte es el primer nivel ISO de extremo a extremo (origen-destino) puesto que los demás niveles restantes son entre máquinas.



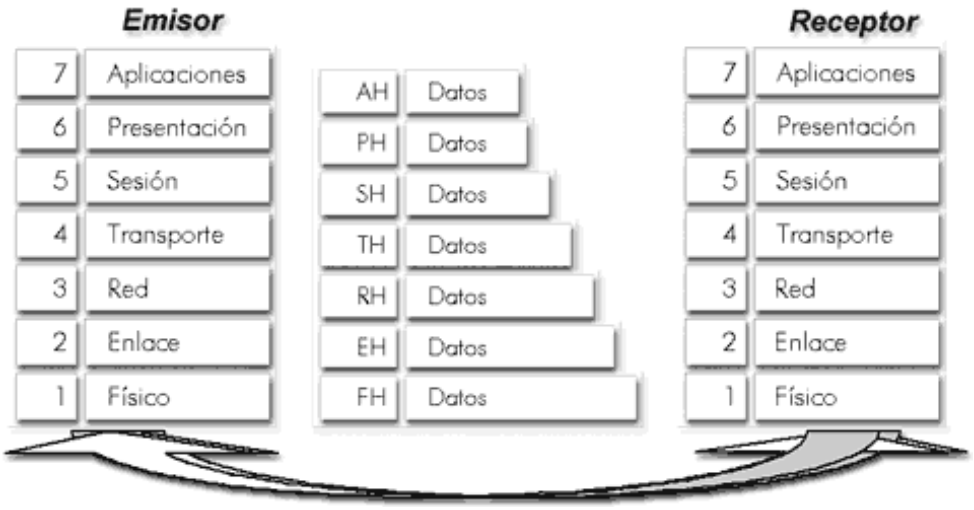
En el nivel de **Red** se agrega otra cabecera (RH), y lo traspasa al siguiente nivel. Este nivel se encarga del encaminamiento, es decir, por dónde enviar los paquetes de información para que lleguen a su destino. Un problema que debe solucionar, es la congestión (si hay demasiados paquetes en un mismo canal da lugar a un cuello de botella). Además, deberá contar los paquetes para poder generar la información de **facturación**.



En el nivel de **Enlace**, cuando recibe la información le añade otra cabecera (EH). Este nivel es el encargado de transformar los **paquetes** de datos en tramas. Al nivel de enlace le corresponde el control de errores, pérdida, duplicación de datos, retardo de transmisión, etc.; además se encarga de que lleguen las tramas en el orden en el que han salido del emisor.

Por último, el nivel **Físico** que le añade la cabecera (FH) y lo dirige por el medio. La tarea principal de este nivel es que lleguen los datos exactamente igual que como se han enviado, es decir, si el emisor envía un Bit con valor 1, se debe recibir en el receptor el mismo valor. Los problemas a considerar en este nivel son el medio, la tarjeta de red, etc.

Cuando la información llega al receptor, vuelve a pasar por los mismos niveles, pero esta vez se van suprimiendo las cabeceras según vayan pasando por el nivel adecuado.



Como podemos observar, los datos van aumentando de capacidad, según van pasando por los siete niveles, ya que cada nivel le va añadiendo una cabecera

El modelo ISO en el Hardware: Como ya sabemos, las funciones de un sistema están divididas en siete capas. El modelo OSI define el hardware, como el esqueleto o soporte físico, constituido por cables, y dispositivos de conexión. Este hardware se corresponde con el nivel 1 (Físico) y nivel 2 (Enlace). El resto de los niveles servirán para la correcta información, tratamiento, y utilización de aplicaciones necesarias.

Por tanto, el hardware de una LAN, está constituida por elementos físicos que permiten transportar información entre nodos conectados a la red. Estos elementos serán: el medio, la tarjeta, el adaptador, los repetidores de señal, etc. Para otras conexiones, se utilizarán dispositivos. Como puentes o Bridges, encaminadores o routers y pasarelas o gateways.

07 Modelo IEEE 802.x

El instituto de ingenieros estableció varios subcomités con el fin de desarrollar un estándar para las redes locales. Este estándar define el número y tipo de dispositivos que se pueden conectar. Los requisitos más importantes son:

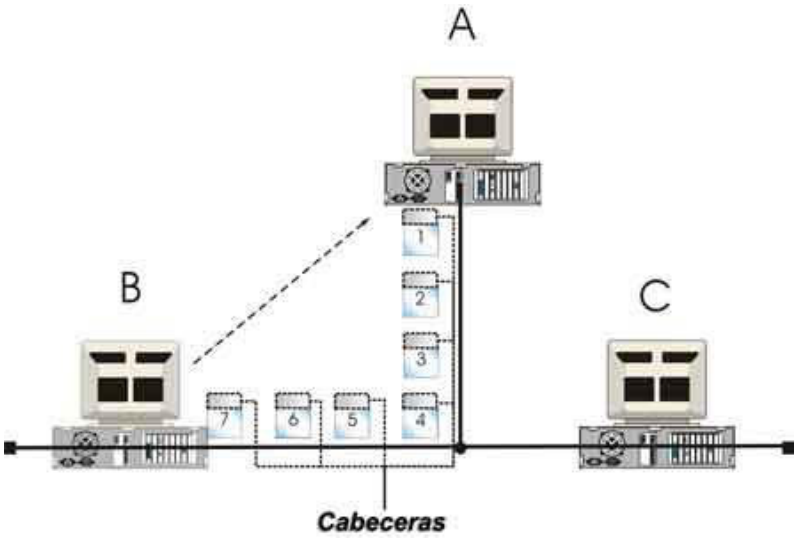
Tamaño	La red deberá soportar al menos 200 nodos y cubrirá un mínimo de 2 Km de diámetro.
Velocidad de transmisión	Los datos se deberán poder transmitir a una velocidad comprendida entre 2 y 20 Mbps.
Funciones de transmisión de datos	Las funciones deberán incluir, como mínimo, transferencias de ficheros, base de datos, correo electrónico y transmisión de voz.
Dispositivos conectados	Todo aquel nodo conectado deberá podrá incluir, dispositivos diferentes.
Servicios	La red deberá soportar varios procesos en curso
Ampliación	Añadir y reducir dispositivos
Reparto de recursos	Cuando un nodo comparte un recurso, debe ser compatible con los demás miembros de la red.
Fiabilidad	En la red, sólo debe ocurrir un error por año. (Para este requisito, podríamos añadir, que la teoría, siempre, se aleja de la práctica.)

Cuando los científicos empezaron a desarrollar el estándar, se dieron cuenta que no existía ninguna tecnología que reuniese todos los requisitos. Debido a esto, el proyecto 802.x fue dividido en diferentes comités. Asignándole el nombre de Redes Locales IEEE802.

Norma	Función
802.1 Niveles de Gestión (HILI)	Este comité no desarrolla estándares, si no que se encarga de los temas comunes de los demás comités.
802.2 Control de Enlace (LLC)	Se encarga de las comunicaciones entre los dispositivos.
802.3 Bus CMSA/CD	Se encarga de desarrollar una red en Bus, utilizando el método de contienda CMSA/CD.
802.4 Token Bus	Se encarga de definir la red lógica en anillo mediante la técnica del paso de testigo.
802.5 Token Ring	Se encarga de definir la red de paso de testigo en una topología en estrella.
802.6 Redes MAN	Esta norma se encarga del uso de las redes metropolitanas.
802.7 Redes LAN (Banda ancha)	Esta norma proporciona asesoramiento técnico en sistemas con banda ancha.
802.8 Fibra óptica	Asesoramiento técnico en fibra óptica.
802.9 Redes integradas, voz y datos	Se encarga del manejo de la información, durante la transmisión de datos en el medio de par trenzado.
802.10 Seguridad	Está encargada de la protección de la información en la red.
802.11 Redes inalámbricas	Esta norma, se encargada de las redes de transmisión inalámbricas.

Veamos ahora cuáles son los modelos más utilizados.

- **IEEE 802.3** (Ethernet): Este modelo relaciona la técnica CSMA/CD, con topologías en BUS. Como ya sabemos, las estaciones o nodos se conectan directamente al mismo medio para transmitir datos, estos datos, según IEEE 802.3, se encapsulan en grupos de una trama, y le añaden la dirección del destino mediante una cabecera, después de esto, lo transmite al medio.



- **IEEE 802.3u** (Fast Ethernet): Este módulo se conoce como 100 Base T, y mantiene la misma técnica de acceso CSMA/CD. Este módulo soporta los siguientes medios: -100 Base TX cable de 2 pares; de categoría 5.

  -100 Base T4 cable de 4 pares; de categoría 3 ó 4. -100 Base FX cable de fibra óptica.

  Beneficios:

  -Mantiene la técnica CSMA/CD
  -Pueden integrarse fácilmente en las redes Ethernet 10Mbps, ya que las antiguas versiones quedarán a salvo.
  -Es respaldada por multitud de fabricantes.

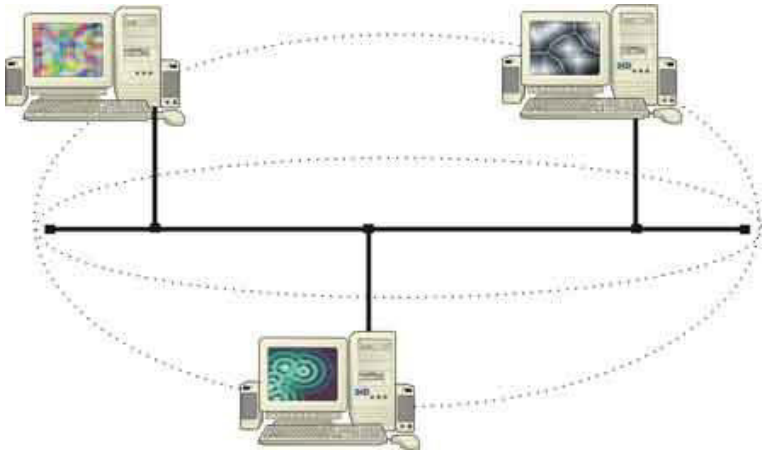
  Características principales:

  -Es el tipo de redes más extendido.
  -Se pueden conectar estaciones sobre la marcha sin la necesidad de reiniciar la red.
  -Las estaciones no tienen que esperar al testigo, debido a ello, transmiten directamente.
  -No ofrece una gestión de prioridades.
  -En situaciones de elevada carga, la presencia de colisiones llega a hacerse importante y puede limitar el rendimiento.

- **IEEE 802.4** (Token Bus): Este modelo de la IE3 se especializa en la normativa del paso a testigo en la topología en Bus. Estudia su comportamiento, así como, sus ventajas y desventajas.

  Como ya sabemos, la topología en Bus se compone de un medio, del cual, todos los nodos se sostienen. Una de sus mejores ventajas, es su sencilla instalación, el reducido coste, y la facilidad de añadir y quitar nodos. Sin embargo, la desventaja principal, es la dificultad de localizar los errores, cuando éstos se produzcan.

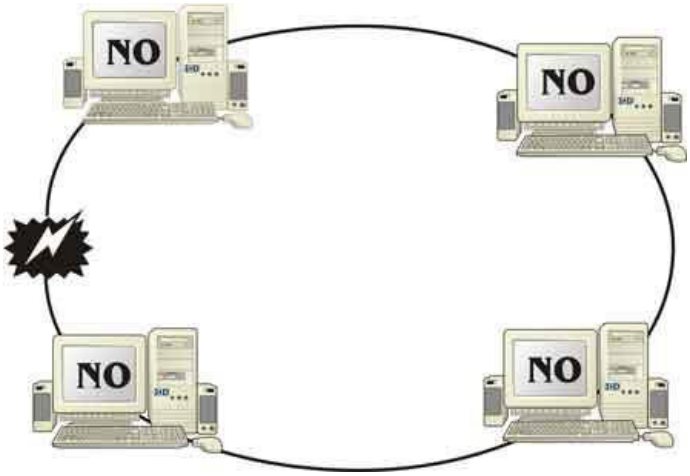
  Cuando hablamos del anillo lógico, estamos haciendo mención al recorrido que realiza el testigo al pasar por las estaciones. Veamos un ejemplo claro de un anillo lógico:



- **IEEE 802.5** (Token Ring): Este modelo hace referencia al Token ring, el cual se basa en la topología en anillo y la técnica pasó a testigo. Sabemos que esta topología con esta técnica de acceso tiene un inconveniente: si falla un nodo, la red se cae, es decir, no funciona y sería muy difícil encontrar la localización exacta de la avería.

  Ventajas e Inconvenientes:

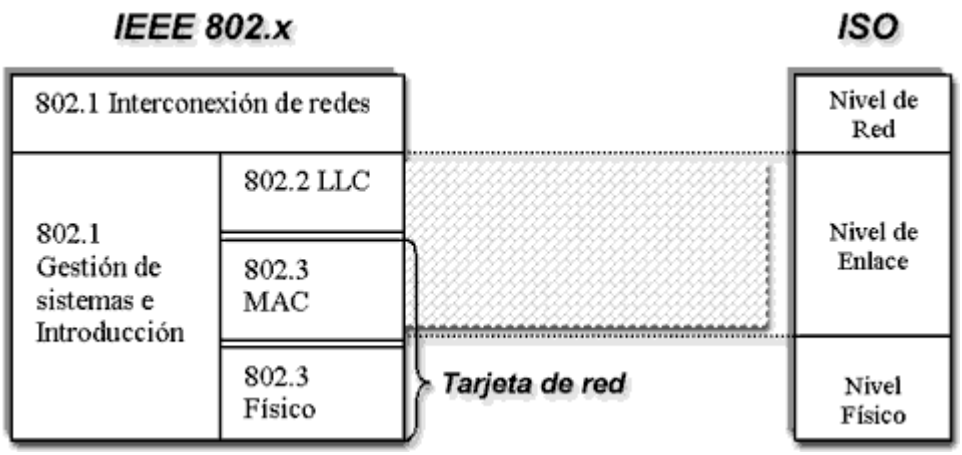
  -Tiene conexiones punto a punto y se puede usar cualquier tipo de medio.
  -Es posible manejar prioridades.
  -Tiene prestaciones de alta capacidad.
  -El problema del tiempo se hace notar, puesto que se ha de esperar al testigo.



08 La ISO y la IEEE 802x

Estas dos organizaciones establecieron un mutuo acuerdo para poder realizar con éxito la relación de normativas.

IEEE puso especial interés en la compatibilidad entre estos dos organismos, y aceptó las especificaciones de la OSI. Ésta, por su parte, aceptó las normas de la IEEE 802 dando lugar a la organización OSI 8802.



Como podemos ver en la figura anterior, el nivel de enlace del modelo OSI está dividido en 2 subniveles en el modelo IEEE. Estos son:

- **Nivel de control de enlace de datos LLC** (Logic Link Control): Este subnivel, únicamente actúa como interface entre el nivel MAC y el nivel de Transporte.

- **Nivel de control de acceso al medio MAC** (Media Access Control): Es el más cercano al nivel Físico, y se encarga de independizar a los niveles superiores del tipo de red que se esté utilizando, así como, de empaquetar en tramas los datos del subnivel LLC.

Tema 4

Redes Wireless

En los últimos años se han hecho muy comunes las redes Wireless o WIFI, la comodidad de no tener que disponer de cables físicos y el ahorro que supone no instalar dichos cables físicos a lo largo de una red hace que cada vez más gente opte por su utilización.

Índice

01 Punto de Acceso

Los **puntos de acceso**, también llamados APs o wireless accesspoint, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El *accesspoint* o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.
Los puntos de acceso utilizados en casa o en oficinas, son generalmente de tamaño pequeño, componiéndose de un adaptador de red, una antena y un transmisor de radio.

Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes "*ad-hoc*" o modo *peer-to-peer,* las cuales solo utilizan las tarjetas de red para comunicarse.

Las redes más usuales que veremos son en modo estructurado, es decir, los puntos de acceso harán de intermediario o puente entre los equipos wifi y una red Ethernet cableada. También harán la función de escalar a más usuarios según se necesite y podrá dotar de algunos elementos de seguridad.

Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de Router. Son los llamados Wireless Routers los cuales soportan los estándar 802.11a, 802.11b y 802.11g.

Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a él se llama “celda”. Usualmente se hace un estudio para que dichas celdas estén lo más cerca posible, incluso solapándose un poco. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red.

Los puntos de acceso antiguos, solían soportar solo a 15 a 20 usuarios. Hoy en día los modernos APs pueden tener hasta 255 usuarios con sus respectivos ordenadores conectándose a ellos.

Si conectamos muchos *Access Point* juntos, podemos llegar a crear una enorme red con miles de usuarios conectados, sin apenas cableado y moviéndose libremente de un lugar a otro con total comodidad.

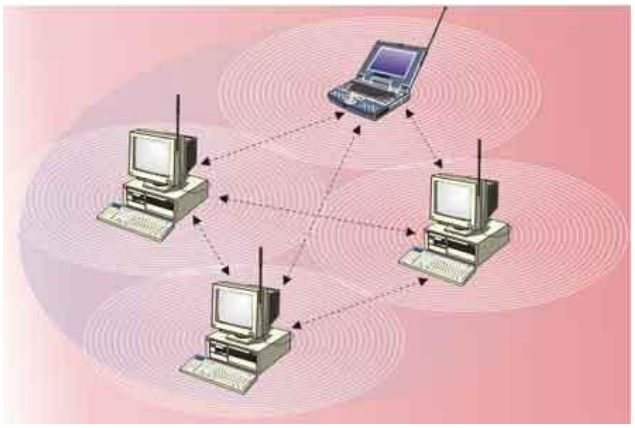
A nivel casero y como se ha dicho, los puntos de acceso inalámbricos nos permitirán conectar varias conexiones Ethernet o Fast Ethernet, y a su vez conectar varios clientes sin cable Existen varias especificaciones de redes WIFI dentro del estándar IEEE 802.11, para usar uno de estos estándares de conexión, tanto el punto de acceso como el dispositivo cliente deben admitirlo.

Estándares de la familia IEEE 802.11 (Wi-Fi)			
Protocolo	**Año**	**Frecuencia de operación**	**Velocidad máxima**
• 802.11	1997	2.4-2.5 GHz	2 Mbit/s
• 802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	54 Mbit/s
• 802.11b	1999	2.4-2.5 GHz	11 Mbit/s
• 802.11g	2003	2.4-2.5 GHz	54 Mbit/s
• 802.11n	2008	2.4 GHz o 5 GHz bands	540 Mbit/s

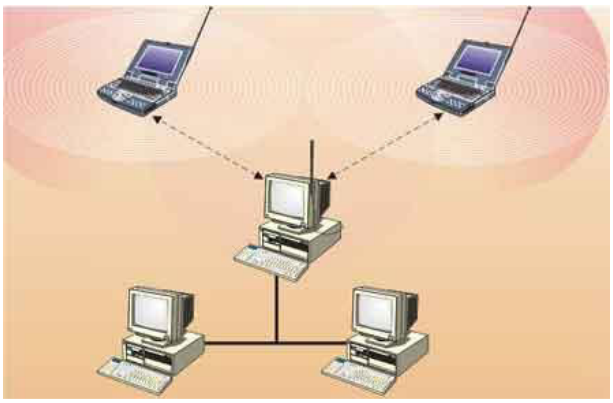
02 Tipo de configuraciones

En este apartado, vamos a tratar las posibles conexiones que se pueden realizar con varias redes, ya sean, sólo por medio físico, por medio de radio o por medios híbridos.

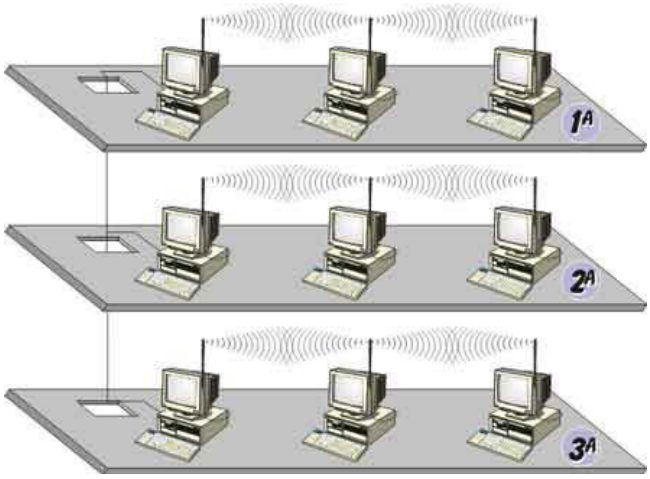
- **Peer to Peer**: También llamado cliente a cliente, esta configuración es la más básica y se realizan las conexiones entre dos estaciones, que están equipadas con tarjetas adaptadoras para WLAN. Esta red es independiente y sólo puede comunicar o compartir los recursos de cada uno, siempre y cuando no se salgan del área que cubre cada estación.



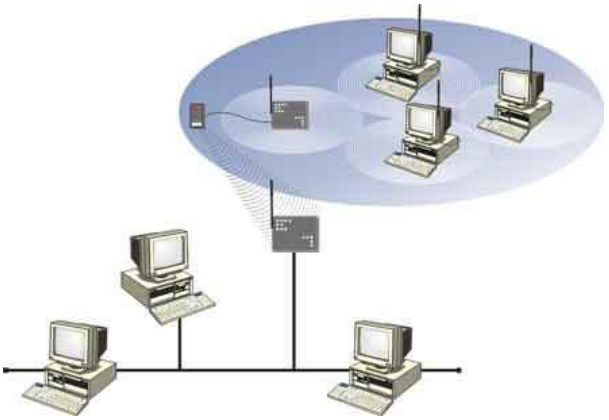
- **Cliente y punto de acceso:** El punto de acceso (APs) se conecta a la red de medió físico y cualquier cliente tiene acceso a los recursos del servidor. Además, actúan como mediadores en el tráfico de la red.



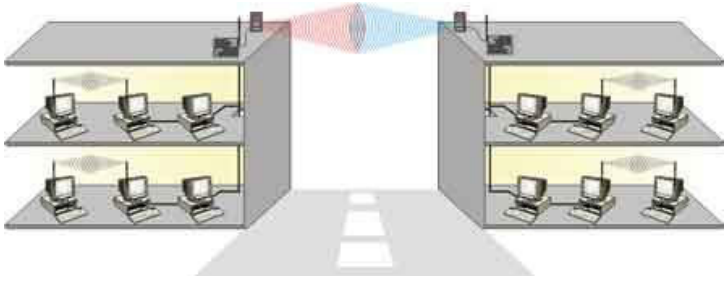
- **Múltiples puntos de acceso y Roaming**: Los puntos de acceso tienen un radio de cobertura comprendida entre los 150m en lugares cerrados, y los 300m en lugares abiertos. Las zonas muy extensas necesitan varios puntos de acceso. La finalidad de estos puntos es permitir que los clientes puedan moverse sin cortes de transmisión entre los puntos. A esto se le ha denominado Roaming.



- **Uso de un punto de extensión**: Para resolver algunos problemas de determinadas topologías, un diseñador de la red puede usar puntos de extensión (Eps), como por ejemplo, para aumentar el número de puntos de acceso. Los puntos de extensión, como su propio nombre indica, extienden el rango de la red transmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión.



- **Utilización de antenas direccionales**: Uno de los componentes a considerar en una red WLAN, es la antena direccional. Por ejemplo, si queremos unir dos edificios que están en una distancia bastante remota, instalaremos una antena direccional a cada edificio con una línea de visión directa. Dichas antenas estarán conectadas a un punto de acceso, y éste, a su vez, conectará la parte de red inalámbrica con la parte de red instalada bajo medio físico.



03 Seguridad en Redes Wireless

Uno de los grandes inconvenientes de estas redes es que al no poder aislar el medio físico de transmisión (las ondas por transmitidas por el aire), resulta más difícil garantizar la seguridad de la red que en un medio cableado.

La forma más habitual y sencilla de hacer segura una red WIFI es configurando una clave de acceso que cifre el tráfico entre los dispositivos clientes y el punto de acceso. Además esta clave será necesaria para poder establecer la conexión inicial.

El cifrado puede ser de los siguientes tipos:

- **WEP**: Es uno de los tipos más básicos. WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Este cifrado se puede hacer de 64 o 128. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.

Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales y 5 o 13 dígitos alfanuméricos.

Por supuesto es mucho más recomendable la clave larga que proporcione un cifrado de 128 bits, no obstante como la clave de cifrado siempre es la misma, un usuario malintencionado podría acceder a nuestra red con un programa denominado de “fuerza bruta” que lo que hace es probar diversas combinaciones de letras números y palabras continuamente hasta que da con la clave adecuada.

A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.

- **WPA:** Emplea el cifrado de clave dinámico, lo que significa que la clave de cifrado está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal.

- **WPA2:** Es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. La principal diferencia entre WPA original y WPA2 es que la segunda necesita un método de cifrado mucho más evolucionado y complejo de WPA.

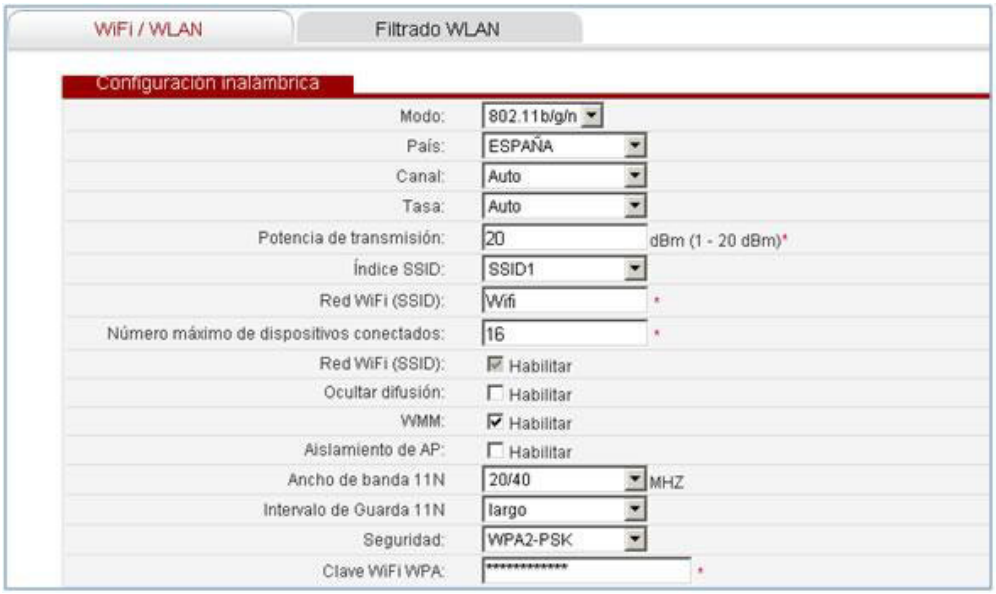
Siempre que sea posible, se recomienda combinar el cifrado más complejo disponible con una aplicación de seguridad por filtros MAC.

01 Práctica: Configurar Wifi

Configurar Wifi

En esta práctica vamos a realizar las tareas necesarias para configurar una red Wifi, al no disponer de un mismo interfaz en todos los puntos de acceso o routers inalámbricos, vamos a dar los pasos generales a seguir, pero la forma de realizar estos pasos dependerá del dispositivo utilizado:

- Accedemos a la administración web del dispositivo, si es un router ADSL, lo normal es que su dirección corresponda a la dirección que el PC tenga configurada como puerta de enlace, podemos verla ejecutando el comando IPCONFIG.
- Si nos pide usuario/contraseña de administrador y no disponemos de estos datos, podemos investigar en Internet cuales son los usados por defecto para nuestro dispositivo.
- Hay que accederá la configuración de WIFI o WLAN y realizar las siguientes operaciones:
    - Cambiar el SSID o nombre de la red
    - Modificar el tipo de seguridad a WPA o WPA2
    - Fijar una nueva contraseña de acceso WIFI
    - Probar desde un dispositivo WIFI que podemos ver la nueva red y que accedemos utilizando la nueva contraseña.



Tema 5

Protocolos

En esta lección veremos el concepto de protocolo y sus características generales. Enumeraremos los tipos de protocolos y conoceremos más sobre las direcciones IP.

Índice

01 Características generales

Un protocolo como un conjunto de normas que definen los múltiples aspectos que intervienen en una comunicación, por ejemplo: dos personas de distintos continentes no podrán comunicarse a no ser que establezcan una comunicación en común, como los signos.

Las propiedades generales que definen los protocolos son:

- **Sintaxis**: Formato, codificación y niveles de señalización de datos.

- **Semántica**: Información de control y gestión de errores.

- **Temporización**: Coordinación y velocidad en el orden de los datos.

Cada protocolo tiene unas características generales, que definimos a continuación.

• **Directo/Indirecto**: El enlace entre las estaciones puede ser, punto a punto (Directo) o mediante un nodo intermedio (Indirecto).

• **Monolítico/estructurado**: El significado de monolítico hace referencia a la comunicación en una sola capa, mientras que estructurado hace referencia a varias capas.

• **Simétrico/asimétrico**: Aquí se hace relación a las características de cada nodo, por ejemplo: si dos estaciones son idénticas, serían simétricas, si no lo son, serían asimétricas.

• **Normalizado/no Normalizado**: Se llama no normalizado a la utilización de protocolos expresamente para medios particulares, sin embargo, el empleo de protocolos generalizados se llama normalizados.

02 Funciones

Las funciones de los protocolos hacen referencia a unas capas creadas según la ISO, son:

• **Capa de Aplicación**: Proporciona comunicación entre nodos distintos.

• **Capa de Transporte**: Encargada de proporcionar seguridad y efectividad en el transporte.

• **Capa de Internet**: La finalidad asignada a esta capa es guiar la información a otras redes o redes intermedias.

• **Capa de Red**: Esta capa establece una conexión directa entre la red y la interfaz.

• **Capa Física**: Encargada de la codificación y señalización en el medio.

Las funciones más importantes de los protocolos se definen en los siguientes puntos:

- **Segmentación**: En la comunicación, habitualmente es necesario dividir los módulos de información en unidades más pequeñas e iguales para su mejor tratamiento. A este proceso se denomina segmentación o también DPU (Unidad de Datos de Protocolos).

- **Encapsulado**: Esta función se encarga de adjuntar una información de controlar segmento de datos. Esta información llevará la dirección del receptor, el código de detección de errores, etc.

- **Control de conexión**: Este control realiza las medidas oportunas para llevar un recuento de los DPU enviados y recibidos.

- **Entrega ordenada**: El envío de DPU puede producir varios problemas, si existen varios caminos posibles, como por ejemplo, pérdidas, reenvío de datos y datos repetidos. Para que esto no ocurra, esta función se encarga de que los datos lleguen al receptor, en el mismo orden en el que salieron de emisor.

- **Control de flujo**: Esta función se encarga de evitar todas las saturaciones producidas en cualquier capa.

- **Control de errores**: Este control utiliza un temporizador para saber si la información ha llegado correctamente, si después de dicho tiempo no se recibe ninguna respuesta del receptor, este control reenvía de nuevo los DPU.

- **Direccionamiento**: Esta función se encarga del enrutamiento de los DPU.

- **Multiplexación**: Las conexiones entre capas se pueden establecer de dos formas: desde una capa superior a una capa inferior y viceversa.

- **Servicios de transmisión**: Esta función desempeña otras dos sub-funciones importantes: la prioridad y seguridad.

03 Tipos de Protocolos

Cada protocolo opera en distinta capa del modelo **OSI**. Veamos con la siguiente tabla, dónde trabajan algunas aplicaciones y algunos de los principales protocolos:

<table>
<tr><td>Aplicación</td><td rowspan="3">TELNET</td><td rowspan="3">FTP</td><td rowspan="3">SMTP</td><td rowspan="3">DNS</td><td rowspan="3">NTP</td><td rowspan="3">SNMP</td><td rowspan="3">ICMP</td><td rowspan="3">HTTP</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td colspan="4">TCP</td><td colspan="4">UDP</td></tr>
<tr><td>Red</td><td colspan="4">IP</td><td colspan="4">ICMP</td></tr>
<tr><td>Liga de datos</td><td colspan="2">802.3</td><td colspan="2">802.5</td><td colspan="2">802.8</td><td colspan="2" rowspan="2">Línea síncrona</td></tr>
<tr><td>Física</td><td colspan="2">Ethernet</td><td colspan="2">Token Ring</td><td colspan="2">FDDI</td></tr>
</table>

Capa de aplicación, Presentación y Sesión

En estas capas, podemos encontrar los distintos tipos de protocolos y sus aplicaciones.

A continuación se muestran los más usados:

• **TELNET**: Está diseñado para proporcionar el servicio de conexión remota, es decir, mediante este protocolo y con una aplicación adecuada, podemos acceder a una estación situada en la misma red, como si estuviésemos operando en la misma estación local.

• **FTP** (File Transfer Protocol): Permite acceder a los servidores de una red para realizar tareas como, descargar ficheros, copiar archivos, etc. FTP proporciona dos modos de transferencia de ficheros: ASCII y Binario. El modo ASCII se utiliza para transmitir archivos de texto; mientras que el modo Binario se utiliza para el resto de los archivos.

• **SMTP**: Es utilizado para el correo electrónico, ya que puede unir tanto mensajes de texto (ASCII), como de datos (Binario). Generalmente, los mensajes transmitidos no son enviados directamente a la estación receptora, sino que son enviados a un servidor de correo, que los almacena y, posteriormente, los envía a su destino.

• **DNS** (Domain Name Service): Muchos usuarios prefieren utilizar un nombre quesea más fácil de recordar, que usar una dirección numérica. Más adelante lo veremos más en profundidad

• **NTP** (Network Time Protocol): Sincroniza el reloj de los servidores con una precisión de Nanosegundos.

• **SNMP** (Simple Network Management Protocol): Se utiliza para administrar múltiples redes físicas de diferentes fabricantes. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar las uniones con las demás capas.

• **ICMP** (Internet Control Message Protocol): Internet es un sistema que no dispone de ningún control central y este protocolo proporciona el medio adecuado para que se pueda comunicar el software entre el servidor y el cliente.

• **HTTP** (Hyper Transfer Protocol): Es un protocolo de transferencia de hipertexto utilizado en Internet.

Capa de Transporte

Esta capa mantiene la comunicación entre el emisor y el receptor, asegurándose de que los datos lleguen sin errores y con una plena coordinación.

• **UDP** (User Datagrama Protocol): Este protocolo puede llegar a sustituir al protocolo TCP, siempre y cuando, el protocolo UDP se utilice para enviar pequeños paquetes de información. Suele utilizarse para aplicaciones en tiempo real como transmisión de video o de voz.

• **TCP** (Protocolo de Control de Transporte): Sus principales funciones se dividen en cuatro partes:

- **Servicios de conexión**: Los datos que salen del emisor llegan al receptor con la misma secuencia.

- **Conexión virtual**: Se denomina conexión virtual a una conexión que realiza el emisor con el receptor, para verificar que los datos transmitidos sean correctos y no haya ningún problema.

- **Flujo no estructurado**: Posibilidad de enviar datos de control junto a datos de información.

- **Conexión full Dúplex**: Permite una transferencia en ambas direcciones, y reduce el tráfico de la red.

Capa de Red

• **ICMP** (Internet Control Message Protocol): Este protocolo es actualmente, el encargado de llevar el control de Internet, y sus características son similares al del protocolo UDP.

• **IP** (Internet Protocol): El Protocolo IP tiene como única misión dirigir la información al destino. Este protocolo es el más utilizado por otros protocolos y tiene la responsabilidad de llevar todos los paquetes, sin errores, sin duplicados y sin pérdidas. Este protocolo también es el encargado de asignar la ruta por donde circularán los datos. Las direcciones IP hacen que el envío sea efectivo y eficaz. Las direcciones IP tienen 32 bits y separados por puntos en grupos de 8 bits. Cada grupo puede tener un valor comprendido entre 0 y 255.

Se pueden clasificar según sus clases:

CLASE A	Dirección de red (7 Bits)	Dirección de nodo (24 Bits)	0			
CLASE B	Dirección de red (14 Bits)	Dirección de nodo (16 Bits)	1	0		
CLASE C	Dirección de red (21 Bits)	Dirección de nodo (8 Bits)	1	1	0	
CLASE D	Multicast (28Bits)		1	1	1	0

Clase A

Corresponde a redes extensas y con muchas estaciones, las combinaciones decimales pueden ser desde 0.1.0.0 hasta 126.0.0.0, permitiendo 1.6 millones de nodos. En estas direcciones el primer byte tiene un valor comprendido entre 0 y 126, ambos inclusive, quedando los tres últimos, para identificar al host.

Clase B

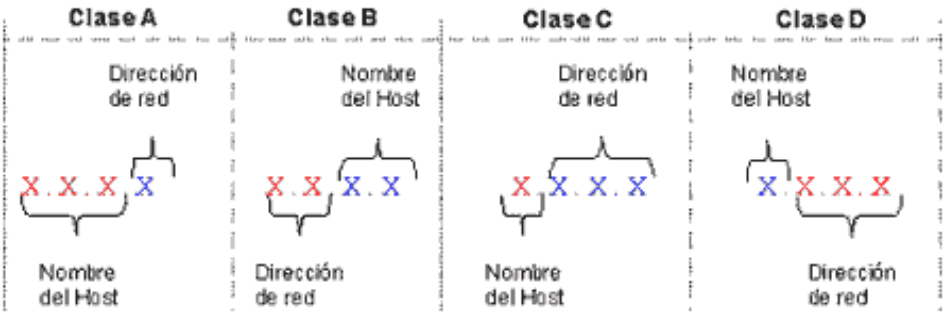
Concierne a redes de tamaño intermedio y el rango de direcciones del primer byte puede ser entre 128 y 191, y del segundo byte, entre 1 y 254, quedando los dos últimos valores para el host. Esta clase permite 64.516 conexiones de nodos en la misma red.

Clase C

En este caso, el valor del primer byte tendrá que estar comprendido entre 192 y 223, el segundo entre 1 y 254, y el tercero entre 1 y 254, quedando el último byte para el host. Esta clase permite 254 conexiones.

Clase D

Esta clase reserva todas las direcciones para el multidestino (Multicast), es decir, un nodo determinado puede enviar un mensaje a un grupo especificado de nodos. Las direcciones comprendidas son 224.0.0.0 y 239.255.255.255.



04 Principales Protocolos de una red

NetBios

Es un conjunto de protocolos definidos por IBM y retocado por Microsoft, el cual lo denomina Netbeui. Este protocolo sólo se utiliza en redes de área local o de área metropolitana, ya que sus capacidades de enrutamiento son limitadas.

IPX/SPX (Internet Packet eXchange/Sequencial Packet eXchange)

(Intercambio de paquetes entre redes/Intercambio de paquetes secuencial). Este conjunto de protocolos que fue definido por la compañía NOVELL como soporte de sus redes de área local. Es un protocolo plenamente enrutable, pero presenta ciertos problemillas de congestión durante el tráfico de información.

TCP/IP (Transmision Control Protocol/Internet Protocol)

Aunque pocos usuarios saben a ciencia cierta lo que es el TCP/IP, todos lo emplean y lo confunden en un solo protocolo. Este protocolo apareció en el mercado antes de quela ISO se normalizara. Es el más usado actualmente, tanto en Internet como en redes privadas.

En 1973, un grupo de investigadores en tecnología de comunicación inició un proyecto basado en la transmisión de paquetes de información a través de las redes. De este proyecto surgieron dos grandes redes:

- **ARPANET**: Creada para la investigación mundial, llamándose después, INTERNET.
- **MILNET**: Creada para uso militar.

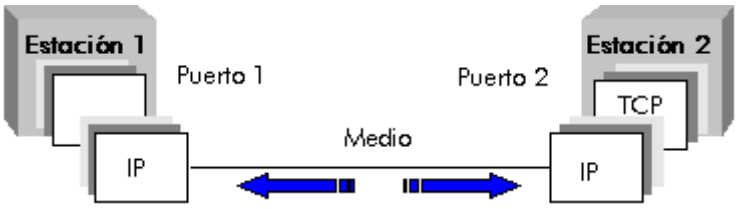
Para relacionar estas dos extensas redes, se unieron varios protocolos: el protocolo de Internet (IP) y los protocolos de control de transmisión (TCP), dando lugar al TCP/IP.

Cada vez que se habla de un protocolo de red determinado, estamos usando un conjunto de protocolos, por ejemplo, cuando usamos el TCP/IP, estamos usando los protocolos FTP, SMTP, TELNET, etc.

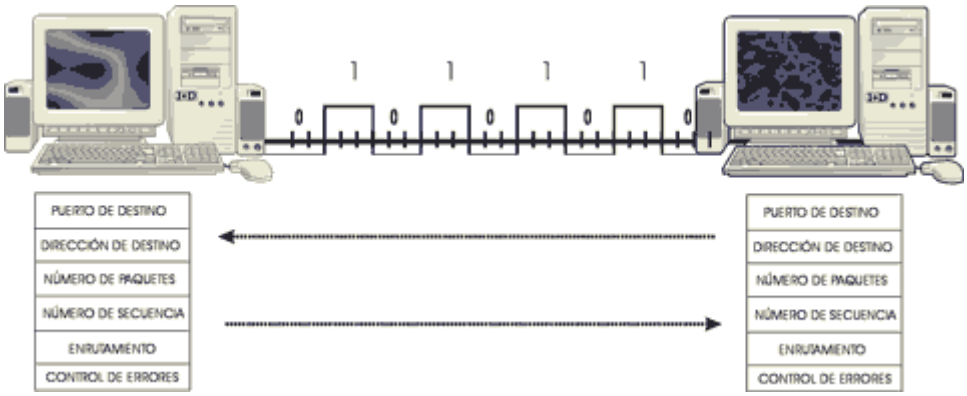
El protocolo IP se encarga de retransmitir datos desde una estación a otra, pasando por todos los dispositivos necesarios.

El protocolo TCP se encarga de suministrar al protocolo IP, los paquetes de datos, y comprobar que han llegado a su destino.

Cada estación debe tener una dirección de red, además debe tener un puerto o dirección local para que el TCP entregue los datos a la aplicación adecuada.



Por ejemplo: La Estación 1 desea enviar una información con puerto 1 a una aplicación con puerto2 en la estación 2; el TCP de la estación 1 pasa los datos a su IP, y éste la encamina hacia la dirección de la estación 2, pero antes de llegar a ella, los pasos a seguir son los siguientes: de la IP, se traslada a la TCP, finalizando en el puerto 2 de la misma estación.



Cuando pasa la información por el TCP de la estación emisora, éste le añade una serie de cabeceras como: puerto de destino, número de secuencia, control de errores, etc. mientras que el IP, adjunta datos como: dirección del receptor, el encaminamiento a seguir, etc.

05 Direcciones IP

Según las clases vistas anteriormente, las direcciones IP pueden soportar una cantidad determinada de estaciones de trabajo. A continuación, explicaremos uno de los procesos que existen para determinar qué cantidad de nodos soporta una determinada dirección de red:

- Considerando una dirección al azar: IP: 201.222.5.120

- Y una **MASK** (máscara de subred): MASK: 255. 255.248.0

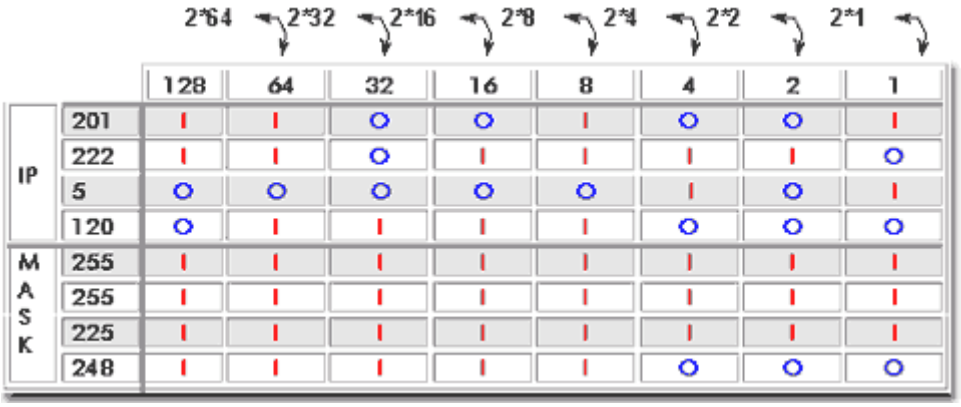
Sabiendo que, su combinación en binario es:

- **IP**: 201.222.5.120 11001001.11011110.00000101.01111000

- **MASK**: 255.255.248.0 11111111.11111111.11111111.11111000

Para pasar un número a binario, existen varios métodos. En este apartado utilizaremos uno de ellos.

El método que vamos a usar es la suma de múltiplos, es decir, colocamos una fila de números, de derecha a izquierda, que sean múltiplos de 2. El primer número que colocaremos será el 1, el segundo a la izquierda sería el 2, el tercero el 4, y así, sucesivamente.



Cuando hayamos pasado a binario las direcciones IP y las Máscaras de Subred, realizaremos la siguiente operación:

1. Colocaremos las direcciones, una encima de otra, en modo binario.

- IP: 201.222.5.120 11001001.11011110.00000101.01111000
- MASK: 255.255.248.0 11111111.11111111.11111111.11111000

2. Realizaremos una operación, que sólo afecta a la última palabra, en la que compararemos los dígitos de arriba con los dígitos de abajo. El resultado de la comparación será:

a. Por ejemplo, si el primer dígito de la dirección IP coincide con el primer dígito de la máscara de subred, su resultado daría el mismo valor, es decir, si en la dirección IP es 1 y en la dirección de la Máscara de Subred es 1, el resultado sería 1; ocurriría lo mismo si el valor fuese 0.

b. Pero, si las comparaciones son distintas, es decir, si el cuarto dígito de la dirección IP es un 1, y el cuarto dígito de la dirección de la Máscara de Subred es 0, el resultado será 0; ocurriría lo mismo si fuese al contrario.

Ahora realizaremos la operación del ejemplo creado anteriormente:

- **IP**: 201.222.5.120 11001001.11011110.00000101.01111000
- **MASK**: 255.255.255.248 11111111.11111111.11111111.11111000

Dirección de Subred 201.222.5.120 11001001.11011110.00000101.01111000

Esta dirección nos informa de cuántos nodos soportan la red.

Una vez obtenido el resultado, contaremos los bits en valor 0 que estén en la última palabra de la subred. En nuestro ejemplo son tres, por lo cual, para saber el número de nodos que soporta la subred, tenemos que multiplicar el número dos, que es la potencia utilizada para la conversión a binario, por el número de ceros de la última palabra de la subred, es decir:

- 2 que es el número de conversión en binario, elevado al Nº de ceros que haya en la última palabra de la subred.

- Obteniendo como resultado final 8, este número será la cantidad de nodos o equipos que podrán soportar la red, siempre y cuando, utilicemos la dirección IP y la máscara de subred del ejemplo.

201.222.5.120	
201.222.5.121	1º Ordenador
201.222.5.122	2º Ordenador
201.222.5.123	3º Ordenador
.....	.....
.....	.....
201.222.5.127	Último Ordenador

06 Direcciones IP públicas o privadas

Dentro de las direcciones IP que ya hemos visto, hay que diferenciar claramente entre dos tipos:

- **Direcciones públicas**: Son aquellas que se asignan a cualquier dispositivo conectado directamente a Internet como por ejemplo un router ADSL, un servidor web de Internet o un teléfono 3G, cada dirección es única y no se podrá repetir en ninguna parte del mundo en ese momento. Las asignan los proveedores de Internet (también llamados ISPs) generalmente de manera dinámica, por lo que no se puede asignar una sin ser el "propietario" legal de esa dirección.
- **Direcciones privadas**: Son aquellas que se utilizan para los dispositivos que no están conectados directamente a Internet, sino que (en caso de tener acceso a Internet) deben conectarse mediante un Router o algún dispositivo que les haga de pasarela, son de uso libre dentro de redes LAN o WAN.

Son las direcciones que van de los rangos:

- **Clase A**: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
- **Clase B**: 172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- **Clase C**: 192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Router ADSL: Actualmente la mayoría de routers domésticos cumplen 3 funciones bien distintas:

- **Router**: Para comunicar la red interna con la red externa (Internet).
- **Switch**: Para comunicar entre sí 2 o más dispositivos conectados a la red interna.
- **Punto de acceso**: Proporcionan acceso WiFi a la red interna.

De esta manera, si tomamos como ejemplo un router ADSL doméstico con 3 ordenadores conectados, veremos que los ordenadores conectados podrían tener las direcciones IP privadas 192.168.1.10, 192.168.1.11 y 192.168.1.12.

En cambio, el router ADSL tendría 2 direcciones distintas, una privada para su conexión LAN interna (por ejemplo 192.168.1.1) y otra pública (por ejemplo 84.77.83.80) asignada directamente por la compañía de teléfonos donde se haya contratado la línea que será además propietaria de esa dirección a nivel mundial.

Cuando veamos la configuración IP de uno de los ordenadores, resultará que la dirección de su puerta de enlace será la de la conexión interna del Router (192.168.1.1), esto significa que cuando este ordenador quiera acceder a una dirección IP que no es

de su mismo rango (como la de un servidor de Internet), dirigirá la petición al router quien a su vez encaminará la petición hacia la conexión ADSL y por tanto hacia Internet

En cambio, si un ordenador quiere comunicarse con otro ordenador de la misma red, la petición no irá a través de la puerta de enlace, sino que viajará a través del dispositivo que cumple las funciones de switch que, en este caso, resultará ser el mismo router, pero este tráfico nunca se enviará a la conexión ADSL del Router, se gestionará internamente.

Cuando solicitamos un servicio dentro de una red, lo hacemos cursando una petición a una dirección IP y a un puerto determinado por el cual el receptor estará "escuchando" la llegada de peticiones, por ejemplo, todo el tráfico web que vemos en un navegador se está dirigiendo por defecto al puerto 80, el envío de correos electrónicos se dirige al puerto 25 o la transmisión de ficheros con un FTP se hace a través del puerto 21.

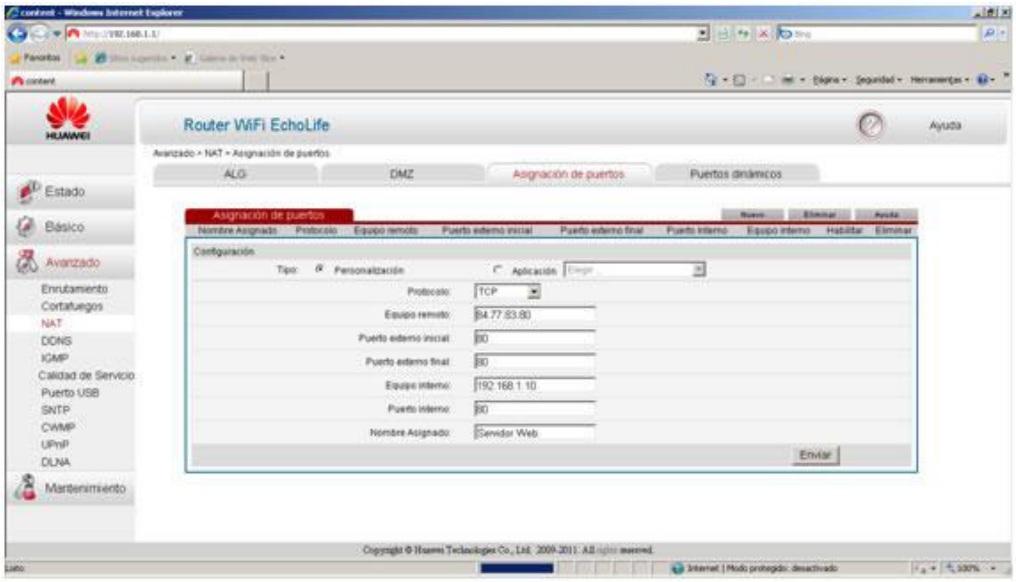
Otra capacidad que tienen muchos routers es la de hacer NAT (Network AddressTranslation) que consiste en que todas las peticiones que vengan de Internet hacia la IP pública a un puerto determinado, se redirijan a un equipo de la red interna hacia un puerto donde se esté escuchando peticiones.

Por ejemplo:

Imaginemos que en el equipo con la dirección 192.168.1.10se ha instalado un servidor Web que funciona por el puerto 80. Desde un PC conectado a la red, la página web sería visible poniendo la siguiente dirección en un navegador: http://192.168.1.10

No obstante, queremos que esta página web sea accesible desde un equipo de Internet ajeno a nuestra red local. Para ello configuraríamos un NAT en el router que dijera que las peticiones a http://84.77.83.80 se dirijan a la dirección http://192.168.1.10 (ambos casos hacia el puerto 80)

El interfaz de administración de cada router es distinto y por lo tanto es imposible explicar a ciencia cierta cómo son las pantallas en cada caso. Aquí se muestran unas pantallas de ejemplo sobre un router Huawei HG532c, para cada caso habrá que investigarlo o leer el manual de funcionamiento del router en cuestión.



07 IPv6

Para comprender los problemas de direccionamiento IP que enfrentan los administradores de red en la actualidad, hay que tener en cuenta que el espacio de direcciones de IPv4 proporciona aproximadamente 4 294 967 296 direcciones únicas. De éstas, sólo es posible asignar 3700 millones de direcciones porque el sistema de direccionamiento IPv4 separa las direcciones en clases y reserva direcciones para multicast, pruebas y otros usos específicos.

En la última década, la comunidad de Internet ha analizado el problema del agotamiento de las direcciones IPv4 y se han publicado enormes cantidades de informes. De hecho, las direcciones IPv4 disponibles para todo el mundo se agotaron en Septiembre de 2012.

El conjunto de números disponibles se ha reducido significativamente en los últimos años por los siguientes motivos:

- Crecimiento de la población: la población de Internet está creciendo. En noviembre de 2005, se estimó que había aproximadamente 973 millones de usuarios. Desde entonces, esta cifra se ha duplicado. Además, los usuarios permanecen conectados durante más tiempo, lo que hace que reserven direcciones IP durante períodos más prolongados.

- Usuarios móviles: la industria ha colocado más de mil millones de teléfonos móviles. Se han vendido más de 20 millones de dispositivos móviles habilitados para IP, incluidos los asistentes digitales personales (PDA, Personal Digital Assistants), pen tablets, blocs de notas y lectores de código de barras. Cada día se conectan más dispositivos habilitados para IP. Los teléfonos antiguos no necesitaban direcciones IP, pero los nuevos sí las necesitan.

- Transporte: Los modelos más recientes de coches están habilitados para IP, para permitir el monitoreo remoto y proporcionar mantenimiento y asistencia con rapidez. Lufthansa ya brinda conectividad a Internet en sus vuelos. Más empresas de transporte, incluido el transporte marítimo, proporcionarán servicios similares.

- Productos electrónicos para los consumidores: los dispositivos para el hogar permiten la supervisión remota mediante la tecnología IP. Las grabadoras de video digital (DVR, Digital Video Recorders) que descargan y actualizan guías de programas de Internet son un ejemplo. Las redes domésticas pueden conectar estos dispositivos.

La posibilidad de expandir las redes para exigencias futuras requiere un suministro ilimitado de direcciones IP y una mayor movilidad que no se pueden satisfacer sólo con DHCP y NAT. IPv6 satisface los requisitos cada vez más complejos del direccionamiento jerárquico que IPv4 no proporciona.

Actualmente el uso de las direcciones IPv6 está principalmente ligado a las direcciones públicas asignadas directamente por los ISPs, pero se espera que pronto todas las redes internas (LAN y WAN) empiecen a utilizar únicamente este protocolo estándar y abandonen IPv4.

IPv6 debería proporcionar una cantidad de direcciones suficiente para las necesidades de crecimiento futuras de Internet durante muchos años más.

La cantidad de direcciones IPv6 disponibles permiten asignar a cada persona del planeta un espacio de direcciones de Internet equivalente al espacio total de IPv4.

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales (valores numéricos y de la A a la F).

Por ejemplo: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 es una dirección IPv6 válida.

Se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000"). Por ejemplo,

2001:0db8:85a3:0000:1319:8a2e:0370:7344 se puede escribir como
2001:0db8:85a3::1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

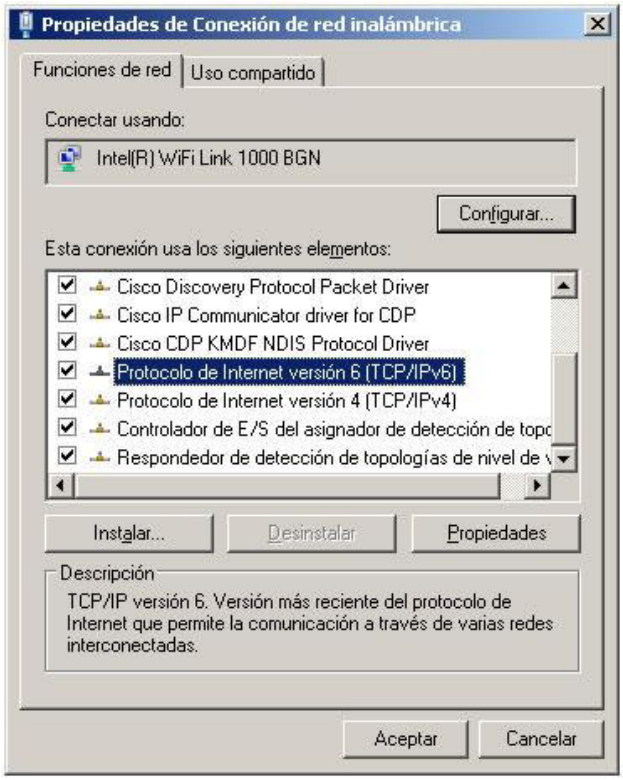
2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab

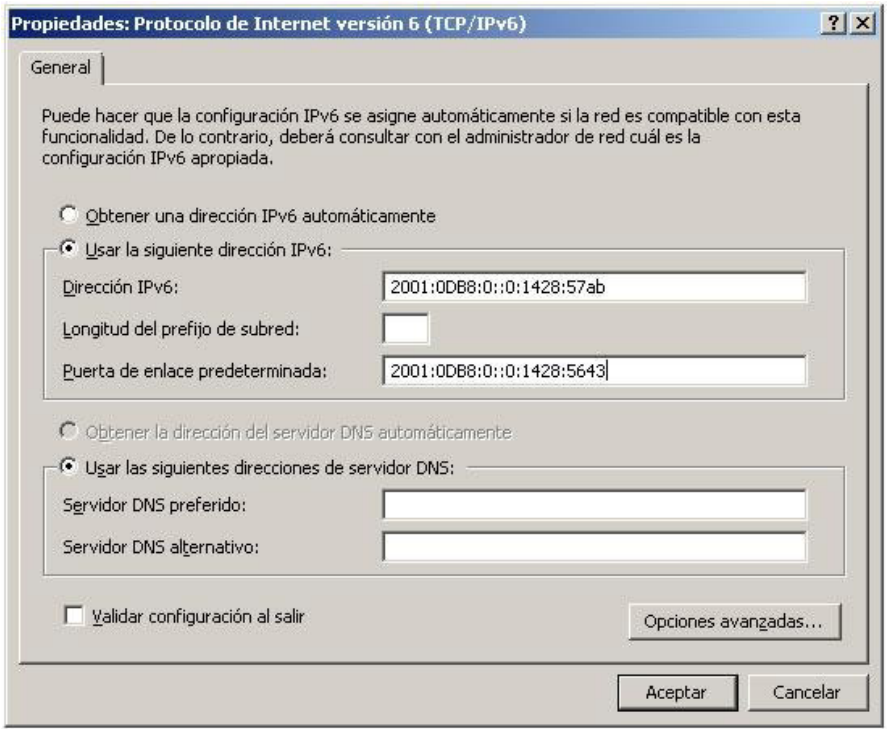
Son todas válidas y significan lo mismo, pero

2001::25de::cade

No es válida porque no queda claro cuántos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo también se pueden omitir.


Propiedades de Conexión de red inalámbrica
Funciones de red
Uso compartido
Conectar usando:
Intel(R) WiFi Link 1000 BGN
Configurar...
Esta conexión usa los siguientes elementos:
Cisco Discovery Protocol Packet Driver
Cisco IP Communicator driver for CDP
Cisco CDP KMDF NDIS Protocol Driver
Protocolo de Internet versión 6 (TCP/IPv6)
Protocolo de Internet versión 4 (TCP/IPv4)
Instalar...
Desinstalar
Propiedades
Descripción
TCP/IP versión 6. Versión más reciente del protocolo de Internet que permite la comunicación a través de varias redes interconectadas.
Aceptar
Cancelar


Propiedades: Protocolo de Internet versión 6 (TCP/IPv6)
General
Puede hacer que la configuración IPv6 se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IPv6 apropiada.
Obtener una dirección IPv6 automáticamente
Usar la siguiente dirección IPv6:
Dirección IPv6:
2001:0DB8:0::0:1428:57ab
Longitud del prefijo de subred:
Puerta de enlace predeterminada:
2001:0DB8:0::0:1428:5643
Obtener la dirección del servidor DNS automáticamente
Usar las siguientes direcciones de servidor DNS:
Servidor DNS preferido:
Servidor DNS alternativo:
Validar configuración al salir
Opciones avanzadas...
Aceptar
Cancelar

08 DHCP

DHCP significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, pero desde sus inicios se diseñó como un complemento del protocolo BOOTP (Protocolo Bootstrap), que se utiliza, por ejemplo, cuando se instala un equipo a través de una red (BOOTP se usa junto con un servidor TFTP donde el cliente encontrará los archivos que se cargarán y copiarán en el disco duro). Un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host.

Funcionamiento del protocolo DHCP

Primero, se necesita un servidor DHCP que distribuya las direcciones IP. Este equipo será la base para todas las solicitudes DHCP por lo cual debe tener una dirección IP fija. Por lo tanto, en una red puede tener sólo un equipo con una dirección IP fija: el servidor DHCP.

El sistema básico de comunicación es BOOTP (con la trama UDP). Cuando un equipo se inicia no tiene información sobre su configuración de red y no hay nada especial que el usuario deba hacer para obtener una dirección IP. Para esto, la técnica que se usa es la transmisión: para encontrar y comunicarse con un servidor DHCP, el equipo simplemente enviará un paquete especial de transmisión (transmisión en 255.255.255.255 con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local. Cuando el DHCP recibe el paquete de transmisión, contestará con otro paquete de transmisión (no olvide que el cliente no tiene una dirección IP y, por lo tanto, no es posible conectar directamente con él) que contiene toda la información solicitada por el cliente.

Se podría suponer que un único paquete es suficiente para que el protocolo funcione. En realidad, hay varios tipos de paquetes DHCP que pueden emitirse tanto desde el cliente hacia el servidor o servidores, como desde los servidores hacia un cliente:

- **DHCPDISCOVER** (para ubicar servidores DHCP disponibles)
- **DHCPOFFER** (respuesta del servidor a un paquete DHCPDISCOVER, que contiene los parámetros iniciales)
- **DHCPREQUEST** (solicitudes varias del cliente, por ejemplo, para extender su concesión)
- **DHCPACK** (respuesta del servidor que contiene los parámetros y la dirección IP del cliente)

- **DHCPNAK** (respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea)
- **DHCPDECLINE** (el cliente le anuncia al servidor que la dirección ya está en uso)
- **DHCPRELEASE** (el cliente libera su dirección IP)
- **DHCPINFORM** (el cliente solicita parámetros locales, ya tiene su dirección IP)

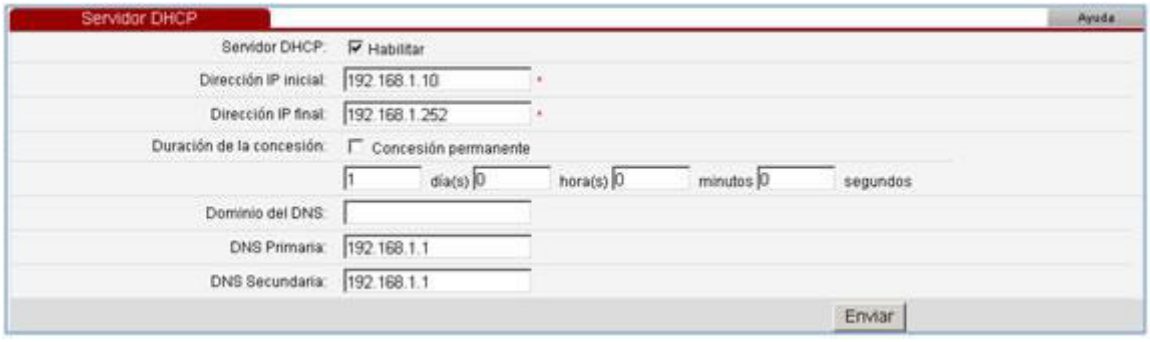
El primer paquete emitido por el cliente es un paquete del tipo DHCPDISCOVER. El servidor responde con un paquete DHCPOFFER, fundamentalmente para enviarle una dirección IP al cliente. El cliente establece su configuración y luego realiza un DHCPREQUEST para validar su dirección IP (una solicitud de transmisión ya que DHCPOFFER no contiene la dirección IP) El servidor simplemente responde con un DHCPACK con la dirección IP para confirmar la asignación. Normalmente, esto es suficiente para que el cliente obtenga una configuración de red efectiva, pero puede tardar más o menos en función de que el cliente acepte o no la dirección IP...

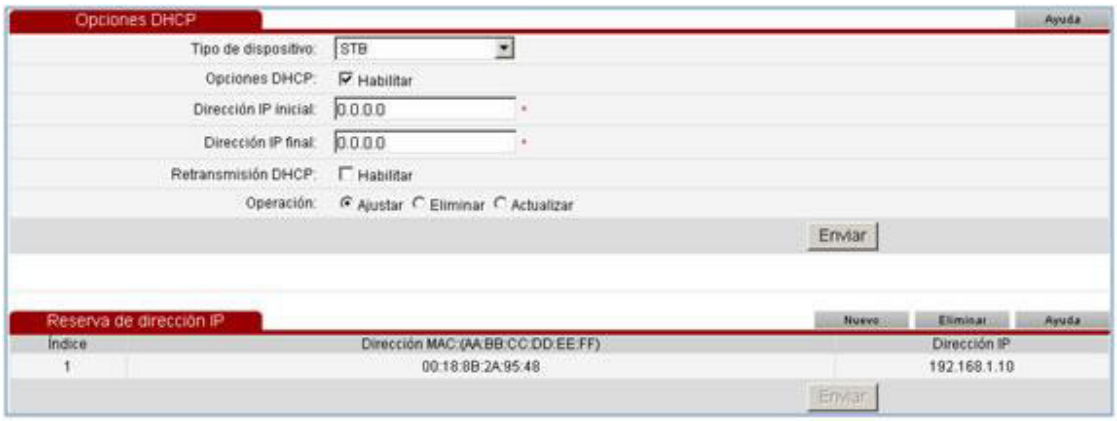
Concesiones:

Para optimizar los recursos de red, las direcciones IP se asignan con una fecha de inicio y de vencimiento para su validez. Esto es lo que se conoce como "concesión". Un cliente que detecta que su concesión está a punto de vencer, puede solicitarle al servidor una extensión de la misma por medio de un DHCPREQUEST. Del mismo modo, cuando el servidor detecta que una concesión va a vencer, enviará un DCHPNAK para consultarle al cliente si desea extenderla. Si el servidor no recibe una respuesta válida, convertirá la dirección IP en una dirección disponible.

Esta es la efectividad de DHCP: se puede optimizar la asignación de direcciones IP planificando la duración de las concesiones. El problema es que si no se liberan direcciones, en un momento determinado no se podrá cumplir con nuevas solicitudes DHCP debido a que faltarán direcciones que puedan distribuirse.

En una red en la cual muchos equipos se conectan y desconectan permanentemente (redes de escuelas o de oficinas de ventas, por ejemplo), es aconsejable ofrecer concesiones por períodos cortos. En cambio, para una red compuesta principalmente por equipos fijos que se reinician rara vez, las concesiones por períodos largos son más que suficientes. No se olvide que DHCP trabaja principalmente por transmisión y que puede ocupar ancho de banda en redes pequeñas con alta demanda.





09 DNS

DNS (Domain Name Service) es un servicio que se da en Internet y en multitud de redes LAN y WAN, es el servicio encargado de traducir las direcciones convencionales como nombres de equipos, páginas web o servicios a direcciones IP que puedan ser alcanzables en una red.

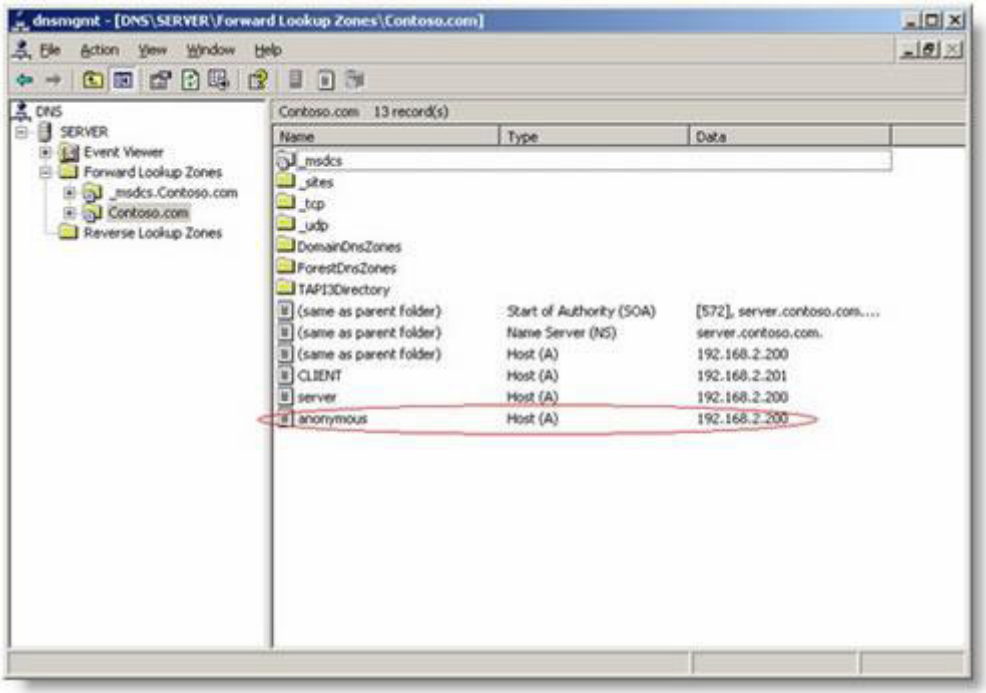
De esta manera, un servidor DNS de Internet será el encargado de decirle al navegador, que la dirección http://www.google.es es en realidad la dirección IP 173.194.34.24, con lo que si en un navegador escribimos http://173.194.34.24, accederíamos a la misma página.

Por lo tanto, podemos afirmar que un servidor DNS es como una "guía telefónica" de direcciones IP, este servicio es fundamental para que Internet funcione tal como lo conocemos.

Además de en Internet, un servicio DNS puede estar localizado dentro de una LAN, una MAN o una WAN, imaginemos una red de una empresa con 500 ordenadores y/o servidores distribuidos en 5 o 6 oficinas, si un ordenador de una oficina necesita acceder a un servidor de otra oficina, deberá preguntarle al servidor DNS más cercano sobre la dirección IP de dicho servidor, ya que posiblemente el usuario no conozca más que el nombre del servidor o del servicio que presta (por ejemplo: http://intranet.miempresa.com).

A diferencia del DHCP, servidores DNS puede haber tantos como se necesiten en una misma red, pero para que la información que devuelvan esté actualizada en todos ellos, es necesario que uno de ellos sea el propietario de la "zona DNS" y que la comparta con los demás servidores. De esta manera, este servidor DNS será el único capaz de realizar cambios en sus registros y los otros servidores solo serán de consulta.

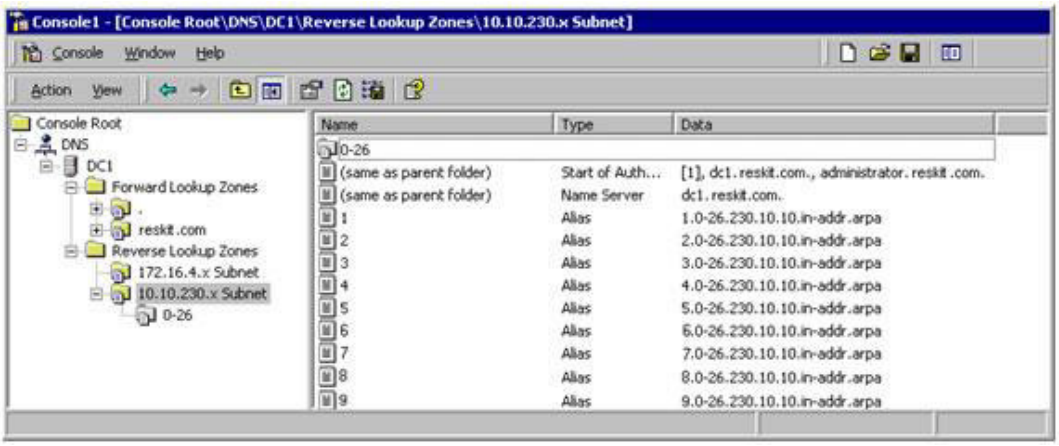
Una zona DNS es la que engloba a todos los registros que comparten el mismo sufijo o dominio (por ejemplo: miempresa.com).



Búsquedas DNS inversas

Al igual que en un servidor DNS tenemos las búsquedas directas en las zonas (a partir de un nombre el servidor busca su dirección IP correspondiente), también existen las zonas de búsqueda inversa, donde se mantiene un listado ordenado por direcciones IP de manera que si un equipo quiere saber a qué nombre o servicio corresponde una IP determinada, el servidor buscará en esta zona inversa hasta encontrar el resultado.

No obstante, en Internet son varios los servicios y servidores que tienen deshabilitada esta opción ya que tenerla habilitada se considera una forma de facilitar el trabajo a los hackers.



Tipos de registro DNS

Los registros que almacena un servidor DNS pueden ser de varios tipos, dependiendo del tipo de servicio al que hagan referencia:

- **Tipo A** – Devuelve una dirección IPv4 de 32-bit, es el más utilizado para ubicar nombres de host independientemente del servicio que presten.
- **Tipo AAAA** – Igual que el anterior pero con direcciones IPv6 de 128-bits.
- **Tipo MX** - Asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio, de esta manera, si se envía un correo a juan@miempresa.com, el servidor de correo emisor buscará en su servidor DNS el registro MX con el nombre "miempresa.com" y a ese servidor de correo es al que entregará el mensaje.
- **Tipo CNAME** - (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio. Es usado cuando se están corriendo varios servicios en un servidor con una sola dirección ip. Cada servicio tiene su propia entrada de DNS (como http://intranet.miempresa.com y ftp.miempresa.com). Esto también es usado cuando se ejecutan múltiples servidores http, con diferentes nombres, sobre el mismo host.
- **Tipo SOA** - (Autoridad de la zona) Proporciona información sobre el servidor DNS primario de la zona, como el correo electrónico del administrador del dominio, el número serial del dominio, y los tiempos de refrescado o actualización.
- **Tipo PTR** –Son los registros de búsqueda inversa.
- **Tipo SPF** - Sender Policy Framework - Ayuda a combatir el Spam. En este registro se especifica qué hosts están autorizados a enviar correo con un dominio específico. El servidor que recibe, consulta el SPF para comparar la IP desde la cual le llega, con los datos de este registro.

10 Direcciones MAC

Todas las tarjetas de red Ethernet, tienen una pequeña memoria en la que alojan un dato único para cada tarjeta de este tipo. Se trata de la dirección MAC, y está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis parejas (cada pareja se separa de otra mediante dos puntos ":" o mediante guiones "-"). Por ejemplo, una dirección MAC podría ser F0:E1:D2:C3:B4:A5.

MAC son las siglas de Media Access Control y se refiere al control de acceso al medio físico. O sea que la dirección MAC es una dirección física (también llamada dirección hardware), porque identifica físicamente a un elemento del hardware, según los estándares no puede haber en el mundo 2 tarjetas de red con la misma dirección MAC.

La mitad de los bits de la dirección MAC son usados para identificar al fabricante de la tarjeta, y los otros 24 bits son utilizados para diferenciar cada una de las tarjetas producidas por ese fabricante.

A un nivel de enlace, la transmisión de datos se hace entre las direcciones MAC, los switches crean unas tablas llamadas ARP donde identifican qué direcciones MAC están conectadas a cada uno de sus puertos.

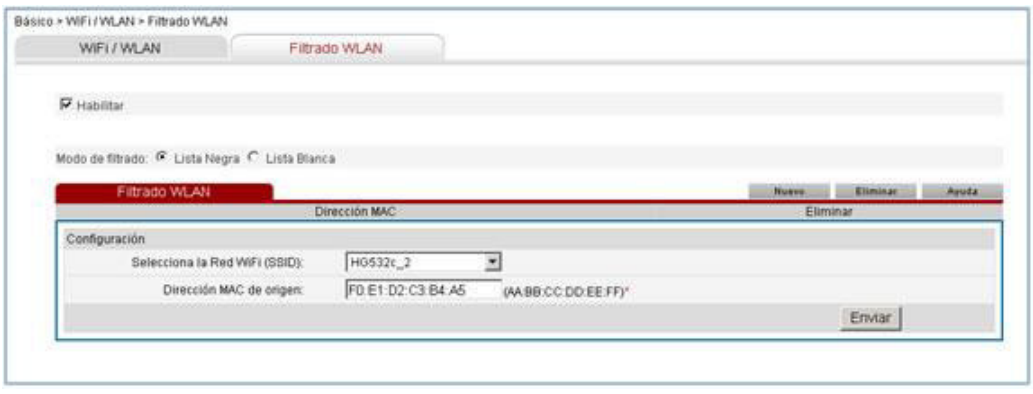
FILTRO POR MAC

En switches avanzados, en muchos puntos de acceso WIFI e incluso en bastantes routers ADSL WIFI caseros, es bastante común disponer de una aplicación de filtro por MAC.

Esta aplicación facilita que sólo puedan conectarse a la red aquellos dispositivos cuya dirección MAC hemos declarado previamente y autorizado a ello.

De la misma manera, podemos especificar aquellos dispositivos con dirección MAC a los que queremos denegar el acceso explícitamente, por ejemplo aquellos que se hayan conectado alguna vez a nuestra red WIFI sin permiso.

En una empresa, con los switches adecuados, esto constituye una muy buena medida de seguridad, ya que se protege individualmente cada punto de red evitando que se puedan conectar dispositivos intrusos que comprometan la seguridad de nuestra red.

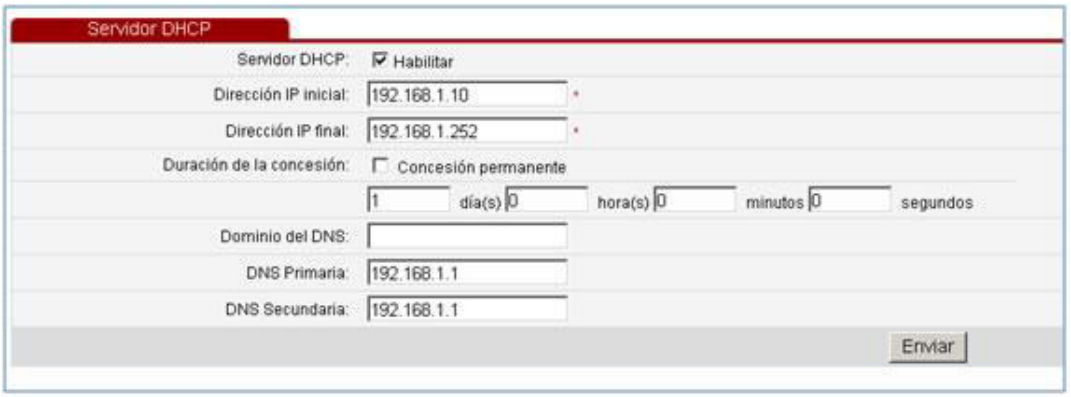


01 Práctica: Configurar DHCP en router

En esta práctica vamos a configurar el servicio DHCP de nuestro router ADSL, para ello debemos acceder al apartado DHCP dentro de la administración.

Debemos cambiar los siguientes apartados:

- Desactivar DHCP y comprobar que al arrancar el PC no es capaz de ver la red porque no se le asigna dirección IP.
- Volver a activarlo y comprobar que el PC ya tiene dirección IP.
- Cambiar la dirección IP inicial del DHCP, que empiece a dar direcciones desde la 10 (por ejemplo 192.168.1.10).
- Reiniciar el equipo y comprobar que la nueva dirección que se le asigna es superior a la inicial fijada en el punto anterior.



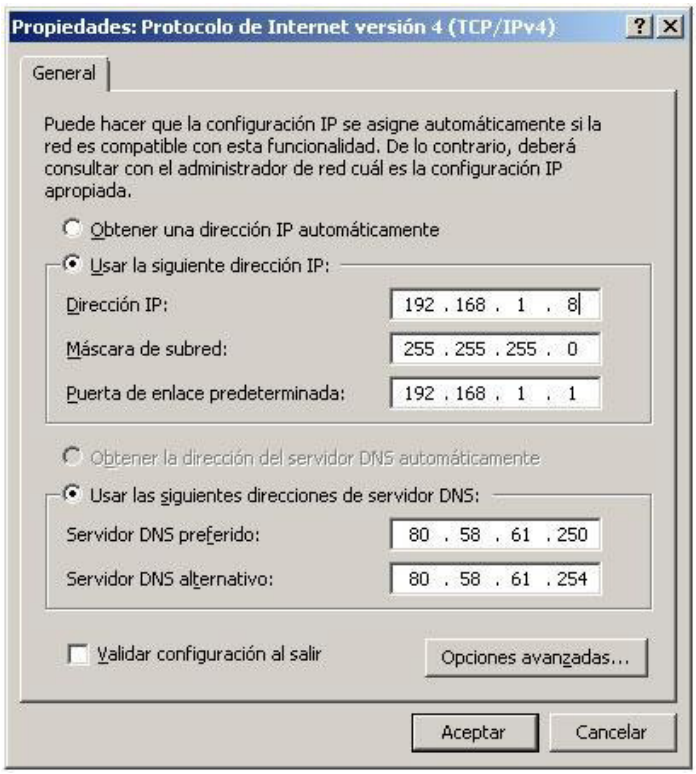
- Algunos routers permiten reservar una dirección DHCP determinada para una dirección MAC, comprobar nuestra dirección MAC con IPCONFIG /ALL e intentar prefijar una cualquiera. Reiniciar y comprobar que funciona.

02 Práctica: Configurar 2 equipos sin DHCP

Siguiendo con la práctica anterior, vamos a configurar 2 equipos distintos conectados a la misma red con 2 direcciones IPs que se encuentren fuera del rango DHCP.

Debemos configurar todos los apartados igual que los pondría el DHCP (IP, Mascara, Puerta de enlace, DNS). Para verificar los datos podemos obtenerlos con un IPCONFIG /ALL en un equipo que aún conserve la dirección asignada por DHCP.

Comprobar mediante el comando PING que la configuración es correcta.



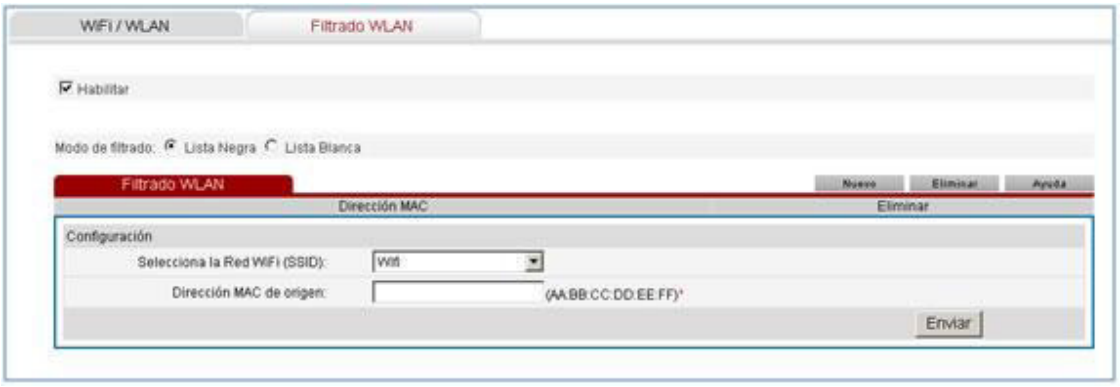
03 Práctica: Poner filtro por Mac

En esta práctica vamos a configurar un filtro por MAC para que sólo los equipos declarados en este filtro puedan conectarse a la red.

Generalmente se aplica solo al entorno WIFI por lo que es posible que necesitemos dispositivos que se conecten por esta vía.

Los pasos a seguir son:

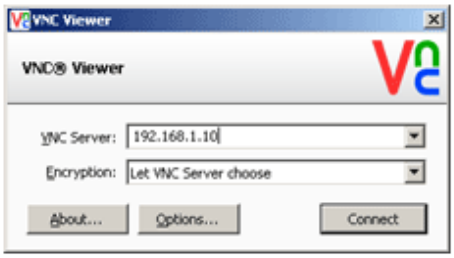
- Obtener la dirección MAC de un equipo con el comando IPCONFIG /ALL
- Buscar el apartado de filtro por MAC e incluir la MAC obtenida como dispositivo autorizado.
- Probar con otro dispositivo que tenga conexión WIFI que no podemos conectar a la red.
- Deshabilitar la seguridad WIFI (dejar la red desprotegida y sin contraseña) y comprobar que el segundo dispositivo sigue sin poder conectar.
- Algunos routers permiten la creación de un filtro contrario, es decir, crear una lista con los dispositivos que no se pueden conectar a nuestra red WIFI. Investigarlo y probarlo.

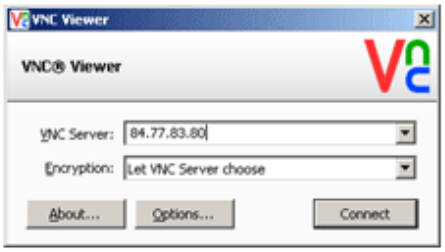


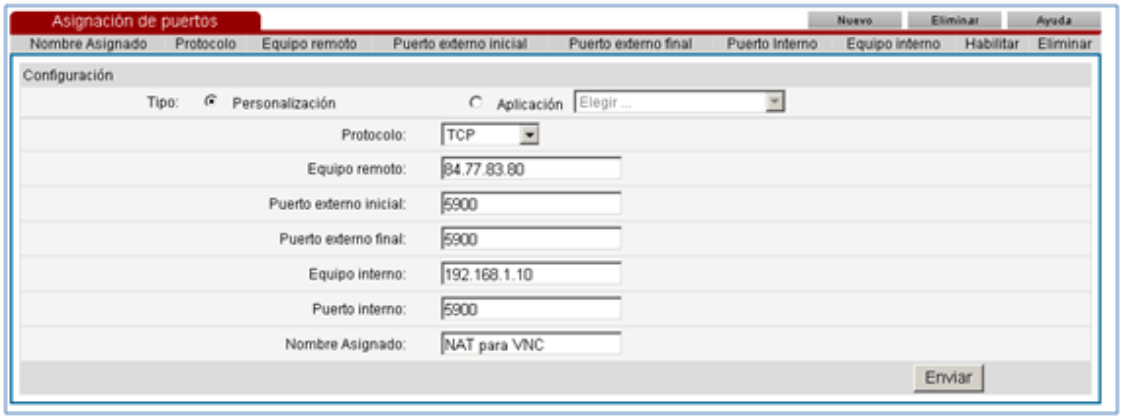
04 Práctica: Hacer NAT para VNC

Esta es la práctica más complicada pero también la más completa, vamos a instalar un software de control remoto en nuestro PC y a configurar NAT para poder controlar nuestro PC desde cualquier equipo de Internet.

- Descargar el programa gratuito RealVNC desde la página http://www.realvnc.com/download/vnc/ e instalarlo.
- Configurar una contraseña de acceso
- Buscar el fichero vncviewer.exe y copiarlo a otro equipo de la misma red, ejecutarlo, poner la dirección IP del primer equipo y comprobar que con la contraseña podemos tomar control del 1º equipo desde el 2º equipo.
- Entrar en la configuración del router, buscar el apartado de redireccionamiento de puertos o NAT y hacer que las peticiones a la IP pública al puerto 5900 se redirijan a la dirección IP del 1º equipo al mismo puerto (5900)
- Entrar a la página http://www.cualesmiip.com/ y averiguar cuál es la IP pública (externa) de nuestro router.
- Desde un equipo conectado a Internet pero desde una red distinta, ejecutar vncviewer.exe, introducir la IP pública de nuestro router y comprobar que con la contraseña podemos tomar control del 1º equipo.







Tema 6

Nociones sobre Internet

La lección que vamos a tratar ahora, está relacionada con el principio de las redes. En esta lección, daremos un breve repaso de los hitos más importantes de la historia de la Red de Redes, desde sus orígenes con ARPANET, hasta nuestros días.

ÍNDICE

01 Historia y Evolución

No se hablaba de Internet antes de que surgiera el proyecto ARPANET del departamento de los Estados Unidos. Denominada hoy como el gran invento del siglo. De hecho, nadie podía predecir en los años 60, el éxito que tendría la red en nuestros días.

A lo largo de casi 30 años, la red deja de ser de uso exclusivo de investigaciones convirtiéndose en un medio de comunicación para el usuario en general y la empresa.

Orígenes militares

Podríamos decir que Arpanet, o poco después Internet, se creó tras haber contestado a dos preguntas importantes:

¿Cómo comunicarse después de una supuesta guerra nuclear?

¿Cómo se controlaría y se administraría la comunicación?

1964: Propuesta de RAND Corporation

- La idea era que si parte de una red se veía atascada, el conjunto debería seguir funcionando.

- En principio, se asume como una red no fiable.

- Todos los nodos (supercomputadoras de alta velocidad) con las mismas características.

- La transmisión de modo paquete; cada paquete se encamina de forma independiente por la red.

- Una frase importante en la creación de ésta, fue: El caos hace la red robusta.

Año 1969

- El primer nodo se instala en UCLA (Universidad de California en los Ángeles).

- En seguida se conectan otros host en el SRI (StandfordResearchInstitute) y la UCSB (Universidad de California en Santa Bárbara).

- En diciembre, con la Universidad de UTA, se cuenta ya con cuatro nodos.

- Se da a conocer públicamente la red, a la que se le da el nombre de ARPANET (ARPA era la agencia de proyectos de Investigación Avanzada del Departamento de Defensa.)

Entre el año 1971 y el año 1972

- Entre estos años se habían instalado aproximadamente, unos 52 nodos.

- El propósito de ARPANET fue el desarrollo de técnicas y experiencia sobre la interconexión de computadoras.

Entre el 1980 hasta el 1992

- Los empresarios ven como una forma de trabajo el uso de ordenadores en las empresas.

- Los usuarios individuales empiezan por interesarse en la informática en red, y utilizan los ordenadores para mejorar los recursos humanos.

Entre 1994 y 1995

- Se forma Netscape Communications Corporation.

- Comienza la era de Internet.

- Aparece JAVA (Sun Microsystems).

Entre 1996 y 1998

- Más de 150 países, 10 millones de ordenadores.

- Aparece InfoVía.

- Se crea en España el punto neutro de interconexiones.

- Se estudia la forma de utilizar una red inalámbrica (WLAN).

Del 2000 en adelante

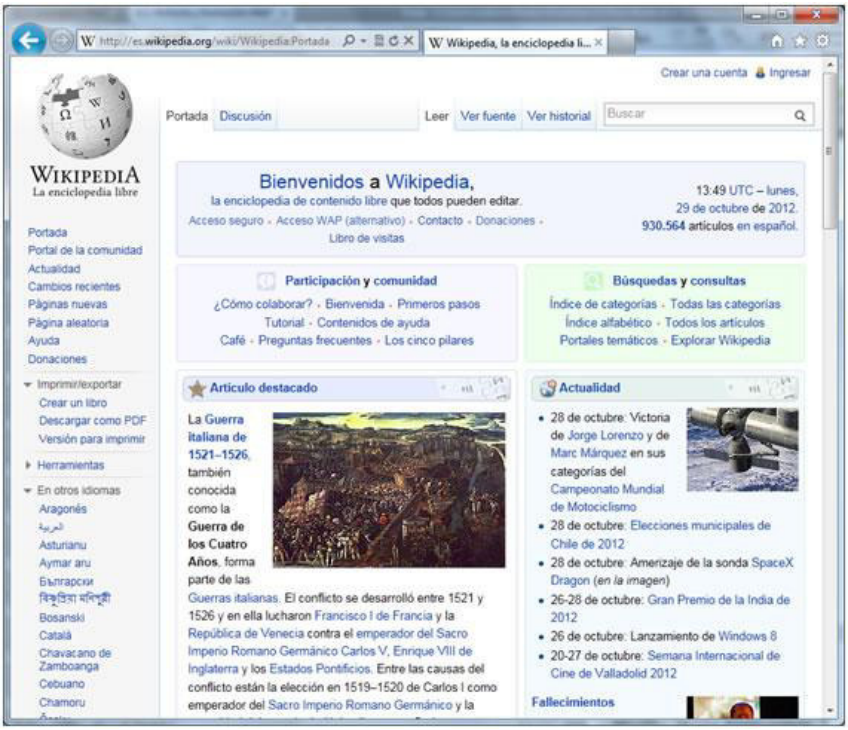
- Comienzan a crease nuevos servidores de Internet.

- Se piensa en utilizar una nueva clase de dirección IP, la clase E.

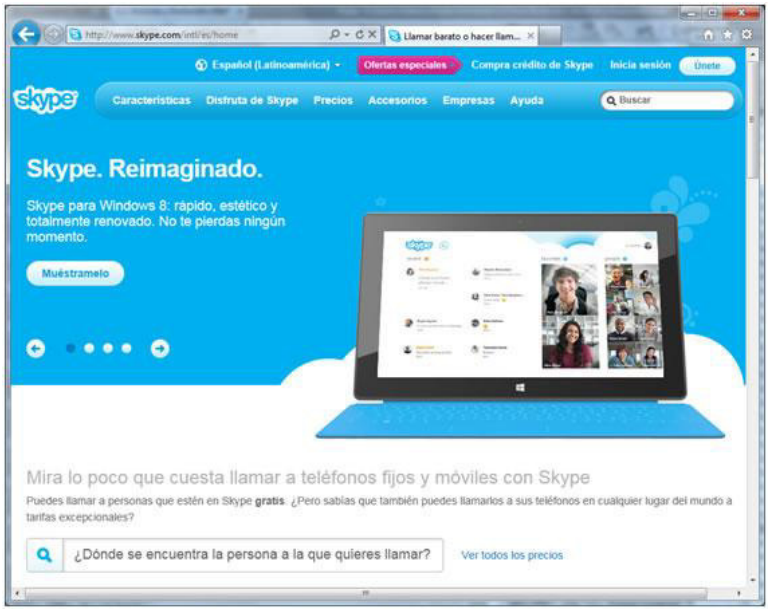
- Gran parte de las empresas utilizan redes inalámbricas (WLAN).

- Existen aproximadamente 200 millones de usuarios de Internet en todo el mundo, de los cuales 114 millones utilizan WWW (World Wide Web), cifra que va aumentando cada día. La tasa anual de crecimiento de usuarios es del 65%.

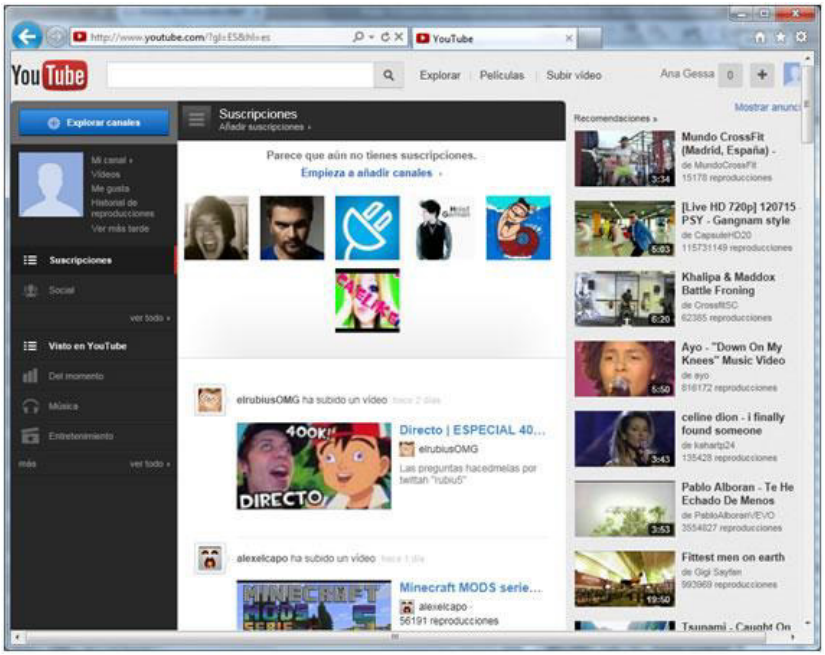
- En 2001 se lanza Wikipedia.



- En 2003 aparece el VoIP (Voice over IP) con el lanzamiento de Skype.



- En 2005 comienza el servicio YouTube que populariza el streaming de vídeo.



- En 2007 se lanza el primer iPhone y se revitaliza el interés por la Web Móvil.

02 Conceptos

El término **Internet** proviene de Internetting o interconexión de redes. Es una red descentralizada que interconecta otras muchas redes de muy diversas arquitecturas. De ahí que a Internet se le conozca también con el nombre de Red de Redes.

La mayoría de los servicios que ofrece Internet, como los servicios Web, FTP, E-mail, etc., se basan en un modelo de arquitectura software conocido con el nombre de Cliente–Servidor. Esto quiere decir, que tales servicios son ofrecidos por máquinas, generalmente remotas, denominadas servidores.

Los usuarios acceden a estos servidores a través de unas aplicaciones, que serían clientes de una aplicación servidora. Por ejemplo: un programa de correo electrónico, como Outlook Express, puede ser cliente de una aplicación como Exchange Server que se ejecuta en un servidor Windows remoto.

Existen ocasiones en las que cliente y servidores realizan en una misma máquina. El cliente se comunica con el servidor mediante un protocolo específico del servicio en cuestión (siguiendo el mismo ejemplo, el protocolo utilizado sería SMTP).

Internet, Intranet y Extranet

Una Intranet es una simulación de Internet realizada a pequeña escala, mientras que Extranet, admite redes de diferentes ámbitos.

- **Intranet**: Es la implantación de tecnologías de Internet como HTML, Java, navegadores web, sistemas de correo electrónico POP3 (en una LAN).

Mediante una Intranet se intenta compartir datos y aplicaciones dentro del ámbito interno de la empresa, utilizando el medio propio de Internet.

- **Extranet**: Aquí ya no podemos hablar puramente de Intranet o de Internet, ya que se comparten datos con redes totalmente externas.

Servicios de Internet

A través de la red, Internet ofrecen una serie de servicios a todos los usuarios conectados a la misma. Los principales servicios son los siguientes:

• **Correo electrónico** (E-mail): Es uno de los más útiles y atractivos de Internet, ya que permite la comunicación mediante mensajes entre sus usuarios. Cada uno de los usuarios está identificado por una dirección de correo electrónico, constituida mediante el identificador de usuario, seguido por el símbolo @ y por el nombre del dominio al que pertenece el usuario.

• **Transferencia de ficheros** (FTP): Los programas que utilizan este servicio, sirven para transportar ficheros.

• **Gopher**: Es un sistema de intercambio de documentos. Estos documentos pueden ser de cualquier tipo, desde imágenes, texto, sonidos e incluso vídeo. El Gopher se desarrolló en la Universidad de Minnesota a mediados del año1992 y debe su nombre a la mascota de esta Universidad.

• **Chats en Internet** (IRC): IRC (Internet Relay Chat) es un sistema de charla multiusuario donde las personas dialogan en unos salones virtuales. Para poder entrar en uno de estos canales, es necesario un programa cliente IRC que conecte con un servidor IRC en la red.

Los dominios son parte de un sistema de direcciones por nombre. Como ya hemos visto, estos dominios se resuelven a partir de servidores DNS.
Cuando se creó el Sistema de Nombres de Dominio en los años 80, el espacio de nombres se dividió en dos.

El primero incluye los dominios, basados en los dos caracteres de identificación de cada territorio de acuerdo a las abreviaciones del ISO-3166. (Ej. *.es, *.uk) y se denomina ccTLD (Dominio de nivel superior de código de país o Country Code Top level Domain).

Los segundos, incluyen un grupo de siete dominios de primer nivel genéricos, (gTLD), que representan una serie de nombres y multi-organizaciones: GOV, EDU, COM, MIL, ORG, NET e INT.

El crecimiento de Internet ha implicado la creación de nuevos dominios gTLD,a mayo de 2012, existen 22 gTLD y 293 ccTLD.

Tema 7

Configuración de una red con Windows

Aunque existen múltiples sistemas operativos, el más utilizado en todo el mundo sigue siendo Windows de Microsoft.

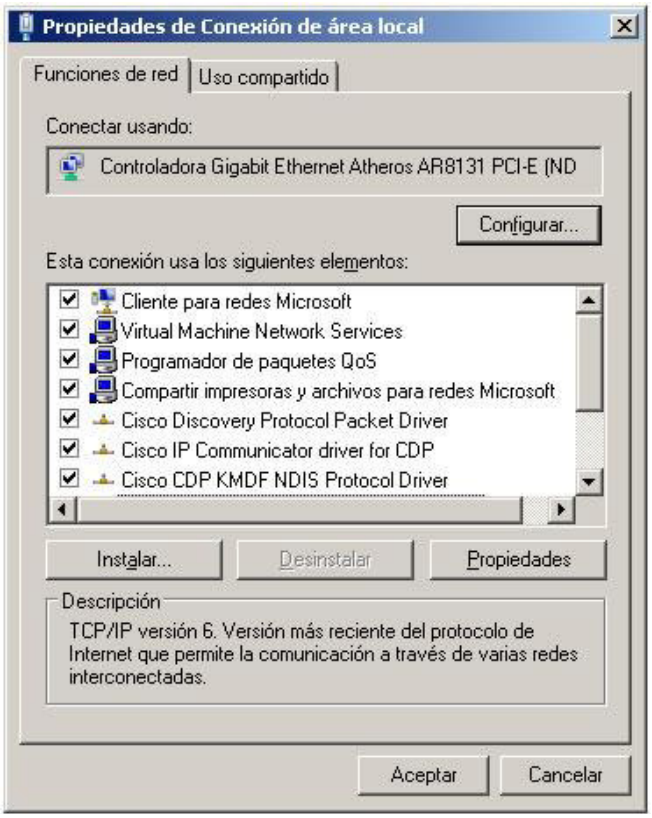
Por este motivo, vamos a aprender los pasos para configurar una red con este sistema operativo, concretamente con la versión Windows 7.

Índice

01 Introducción

Aunque en Windows 7 por defecto ya vienen instalados todos los clientes, protocolos y servicios de red típicos que se van a utilizar, es posible que necesitemos instalar alguno nuevo este un caso concreto.

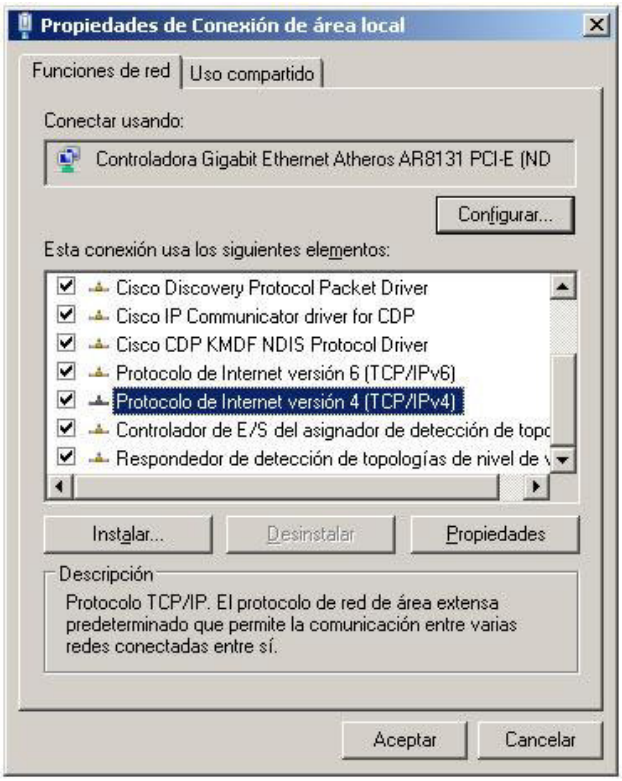
Para ello, es necesario acceder a las propiedades de la conexión de red que queramos modificar y seleccionar el botón **Instalar**.



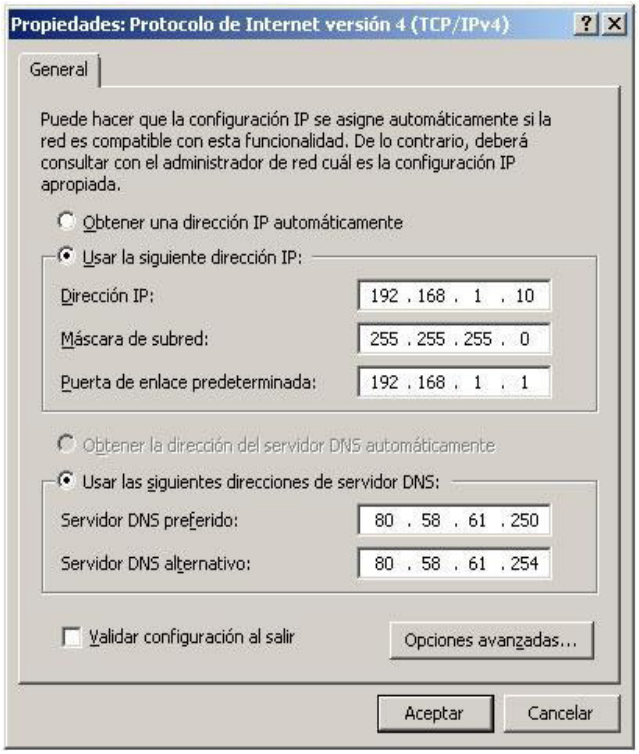
Al hacerlo aparecerá una ventana donde debemos seleccionar el tipo de elemento a instalar y, posteriormente, nos solicitará la ubicación de los ficheros de configuración desde donde queremos instalar el componente.

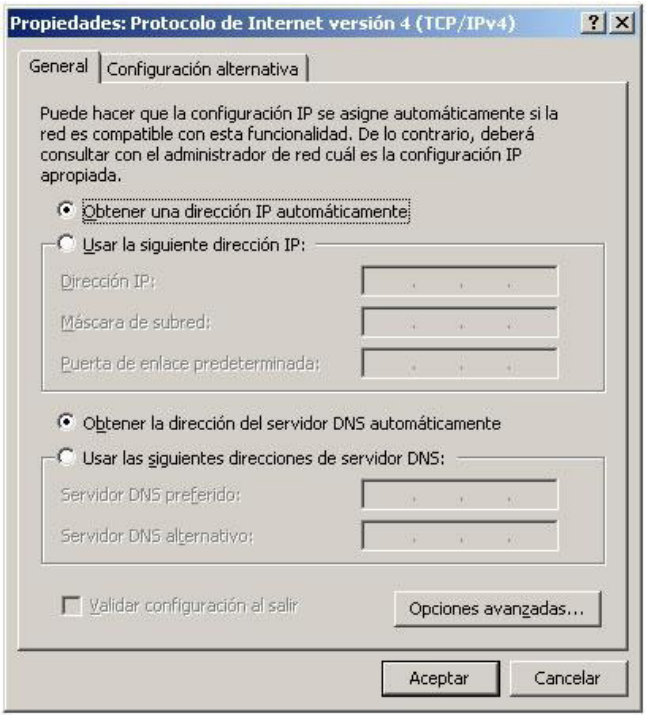
02 Configurar TCP/IP

Dentro de esta pantalla de propiedades del adaptador, la tarea más común es configurar las propiedades del protocolo TCP/IP para este adaptador, para ello seleccionamos el protocolo y pinchamos en el botón **Propiedades**.

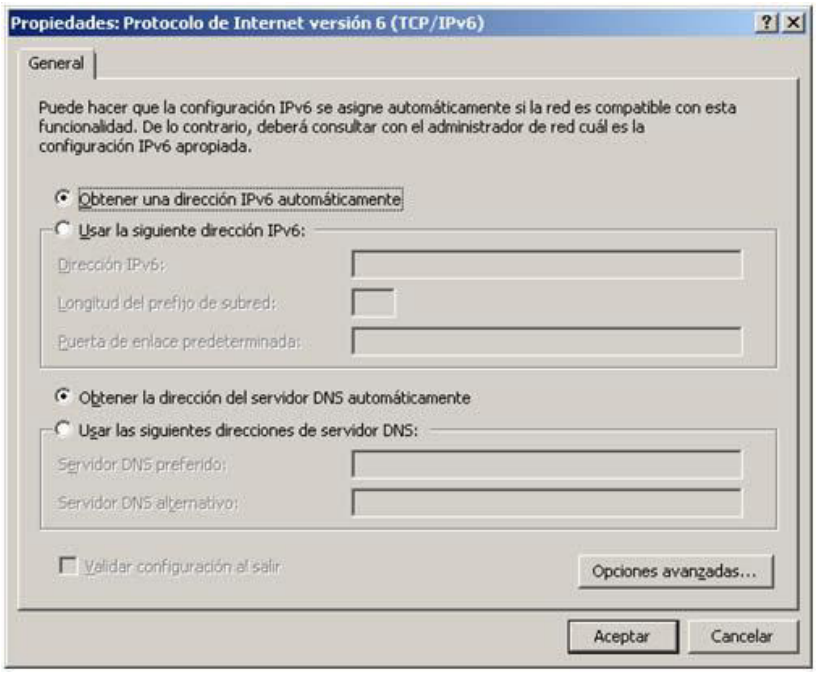


A continuación, aparecerá una ventana donde debemos seleccionar si queremos que la dirección IP se obtenga de forma automática, generalmente mediante DHCP, o si queremos especificarla nosotros manualmente. Las mismas opciones aparecen para los servidores DNS.





Si en lugar del protocolo TCP/IP versión 4 seleccionamos el protocolo TCP/IP versión 6, se muestra una pantalla similar para configurar las propiedades de este protocolo.



03 Seleccionar ubicación de red

La primera vez que un equipo se conecta a una red, debemos elegir una ubicación de red. De esta forma, la configuración apropiada de firewall y seguridad se define automáticamente para el tipo de red donde hemos conectado. De esta manera podemos asegurar que nuestro equipo está correctamente protegido en todo momento.

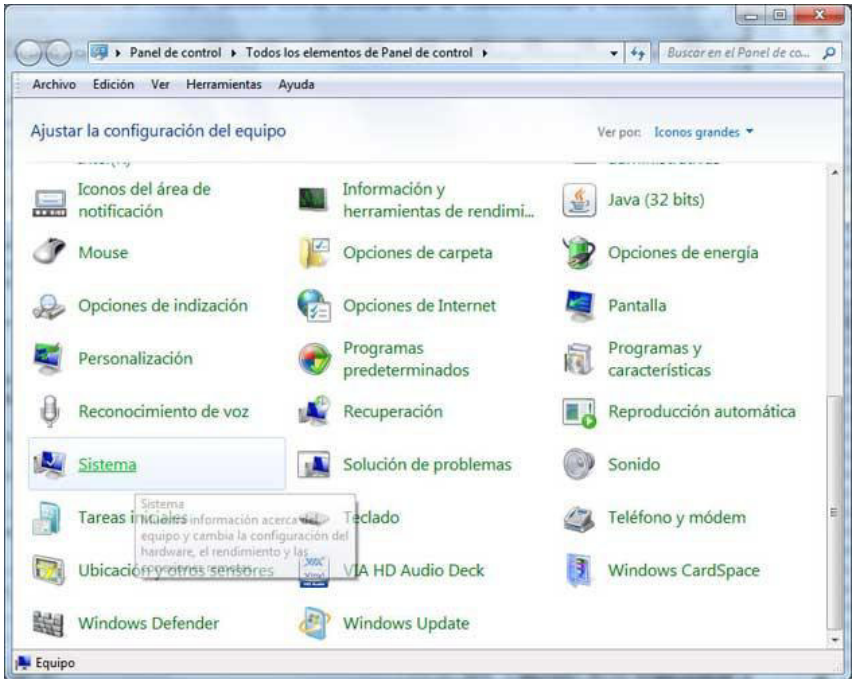
Existen cuatro ubicaciones de red:

- **Red doméstica** para redes domésticas o cuando conozcamos y confiemos en los usuarios y dispositivos de la red. Los equipos de una red doméstica pueden pertenecer a un grupo en el hogar. La detección de redes está activada para las redes domésticas, lo que permite ver otros equipos y dispositivos de la red y que otros usuarios de la red vean el equipo.
- **Red de trabajo** para oficinas pequeñas u otras redes del lugar de trabajo. La detección de redes, que permite ver otros equipos y dispositivos de la red y que otros usuarios de la red vean su equipo, está activada de forma predeterminada, pero no podremos crear un grupo en el hogar ni unirnos a él.
- **Red pública** para las redes de lugares públicos (por ejemplo, cafeterías o aeropuertos). Esta ubicación se ha diseñado para evitar que el equipo sea visible para otros equipos y ayudará a proteger el equipo de software malintencionado de Internet. Grupo Hogar no está disponible en redes públicas, y la detección de redes está desactivada. También debemos elegir esta opción si estamos conectado directamente a Internet sin usar un router, o si tiene una conexión de banda ancha móvil.

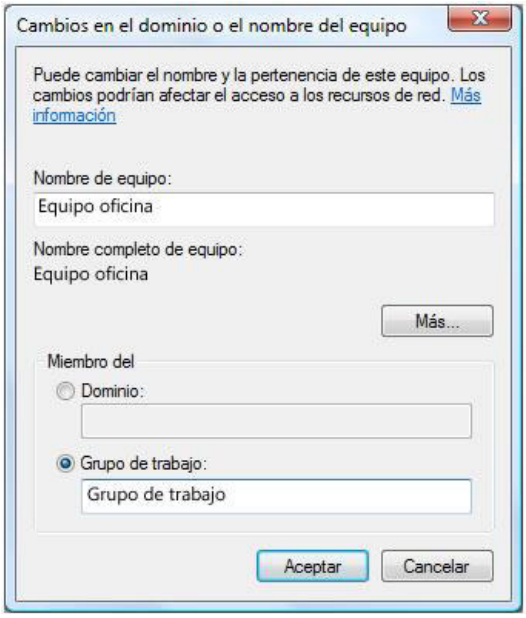
04 Grupo de trabajo

Cuando configuramos una red, Windows crea automáticamente un grupo de trabajo y le da un nombre. Podemos unirnos a un grupo de trabajo existente de una red o crear uno nuevo. Este grupo de trabajo nos va a permitir compartir recursos entre todos los equipos que pertenecen a él:

- Hacer clic en el botón **Inicio**, en **Panel de control** y, a continuación, en **Sistema**.



- En **Configuración de nombre**, dominio y grupo de trabajo del equipo, hacer clic en **Cambiar la configuración**.
- Seleccionar la ficha **Nombre del equipo** y, a continuación, pinchar en **Cambiar**.
- En **Miembro de**, hacemos clic en **Grupo de trabajo** y realizamos una de las acciones siguientes:
    - Para unirse a un grupo de trabajo existente, escribir el nombre del grupo de trabajo al que queremos pertenecer.
    - Para crear un nuevo grupo de trabajo, escribir el nombre del grupo de trabajo que queremos crear.



- Si el equipo formaba parte de un dominio antes de unirse al grupo de trabajo, se quitará del dominio y la cuenta del equipo en ese dominio se deshabilitará.

El uso de grupos de trabajo está indicado para redes domésticas o redes profesionales muy sencillas, para entornos empresariales más estructurados lo mejor es la utilización de dominios.

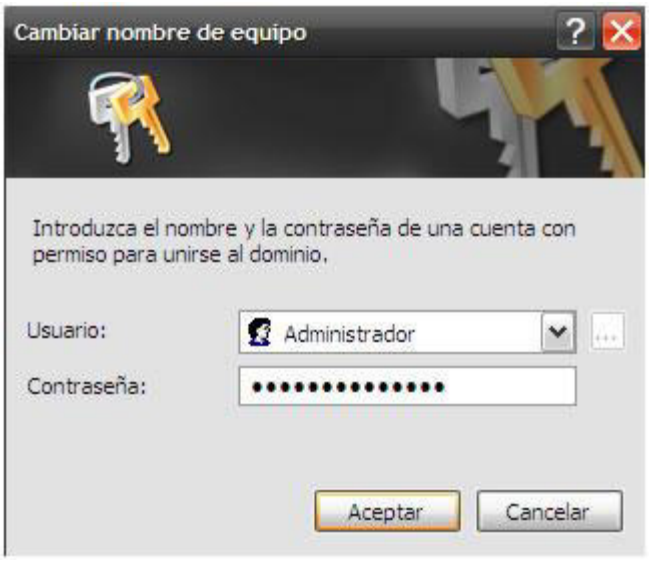
05 Dominios

Un dominio es un conjunto de ordenadores cuyas directrices, permisos, cuentas de usuarios y pertenencia están supeditados a uno o varios servidores denominados **Controladores de Dominio** que se encargan de gestionar el dominio.

Se utiliza en entornos profesionales y permite que un administrador de dominio gestione qué personas o grupos pueden hacer qué operaciones en la red, desde qué equipos y bajo qué circunstancias.

De esta manera, a diferencia del grupo de trabajo donde simplemente se permitía la interconexión entre ordenadores, un dominio resulta mucho más eficaz a la hora de gestionar los recursos de la red y evitar que un usuario malintencionado tenga acceso a información protegida (por ejemplo: podríamos evitar que cualquier empleado de una empresa accediera a los datos confidenciales del departamento de recursos humanos que están compartidos en la red).

El mecanismo para añadir un equipo a un dominio es el mismo que para añadirlo a un grupo de trabajo pero escribiendo el nombre del dominio en la casilla correspondiente, no obstante, para hacer efectivo el ingreso en el dominio se nos solicitará el nombre de usuario y la contraseña de una cuenta del dominio autorizada para hacer esta operación.



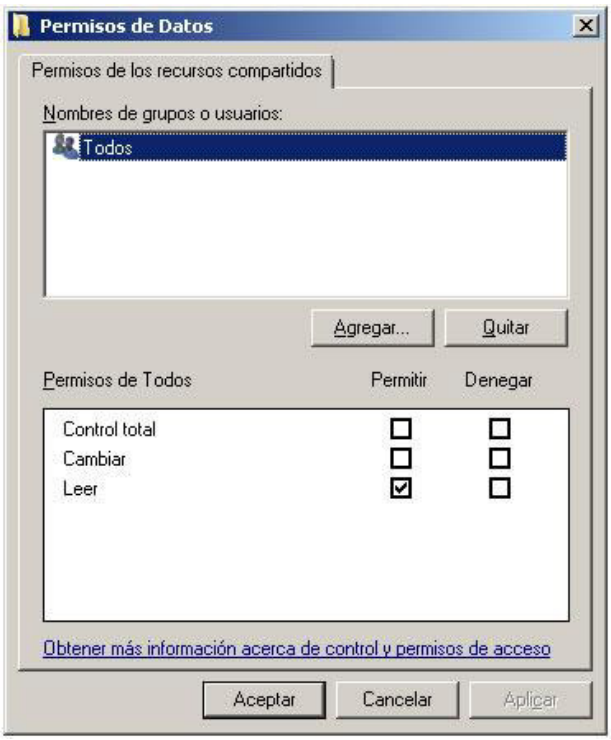
06 Compartir recursos

Para acceder a la herramienta **Compartir archivos**, tenemos que acceder teniendo previamente seleccionada la carpeta que deseamos compartir, hacemos clic sobre ella con el botón secundario del ratón, seleccionamos la opción **Propiedades** y marcamos **Compartir**.

Una vez que tenemos la ventana abierta, pincharemos sobre la opción **Uso compartido avanzado**, que es donde asignaremos el nombre del perfil de la regla, los usuarios que podrán acceder a la carpeta compartida y los permisos de gestión de ficheros que estos tendrán.

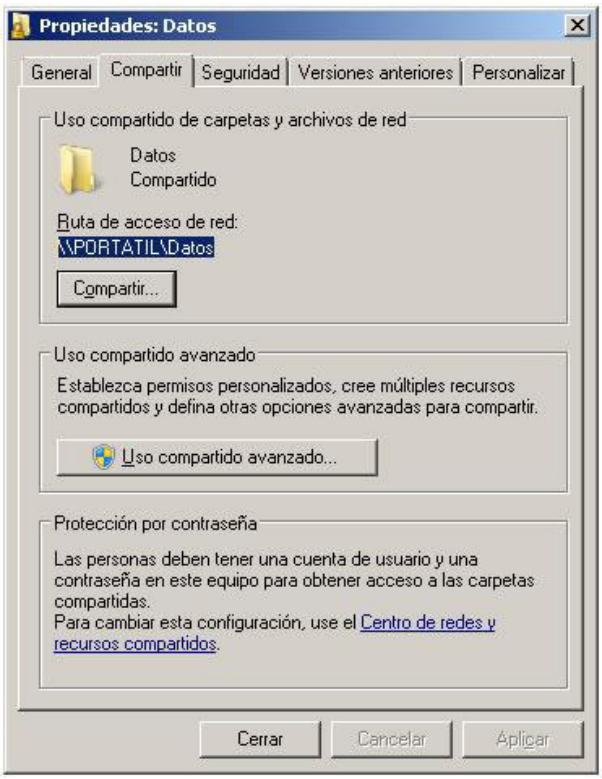
En el panel de control de la pestaña **Compartir** en Windows 7, encontraremos tres parámetros básicos a configurar. En primer lugar, seleccionaremos el nombre de la regla que usaremos para compartir dicha carpeta, ya que podremos crear varias reglas independientes, a las que asignarles distintos usuarios asociados, distintos permisos, etc.

Una vez creado el nombre del perfil, haremos clic en permisos y se abrirá una nueva ventana. En esta, podremos seleccionar que usuarios queremos que puedan acceder a nuestras carpetas, y además, estableceremos los permisos requeridos para cada uno de ellos.



Si lo que queremos es compartir archivos en red en Windows 7 con usuarios que sólo puedan ver nuestros archivos, seleccionaremos **Leer**. Si damos el permiso para que también puedan almacenar archivos en la carpeta compartida, activaremos también la casilla de **Cambiar**, y si queremos permitir que el usuario tenga el mismo poder de gestión de los ficheros que el administrador, marcaremos la opción **Control total**.

Una vez que establezcamos todos los parámetros de configuración para compartir carpetas en red con Windows 7, aceptaremos los cambios y el sistema operativo asignará una ruta de red para que los demás ordenadores puedan acceder a nuestra carpeta compartida.



En mi caso, la ruta que deberé escribir en el explorador de Windows 7 o en el navegador, será: \\PORTATIL\DATOS

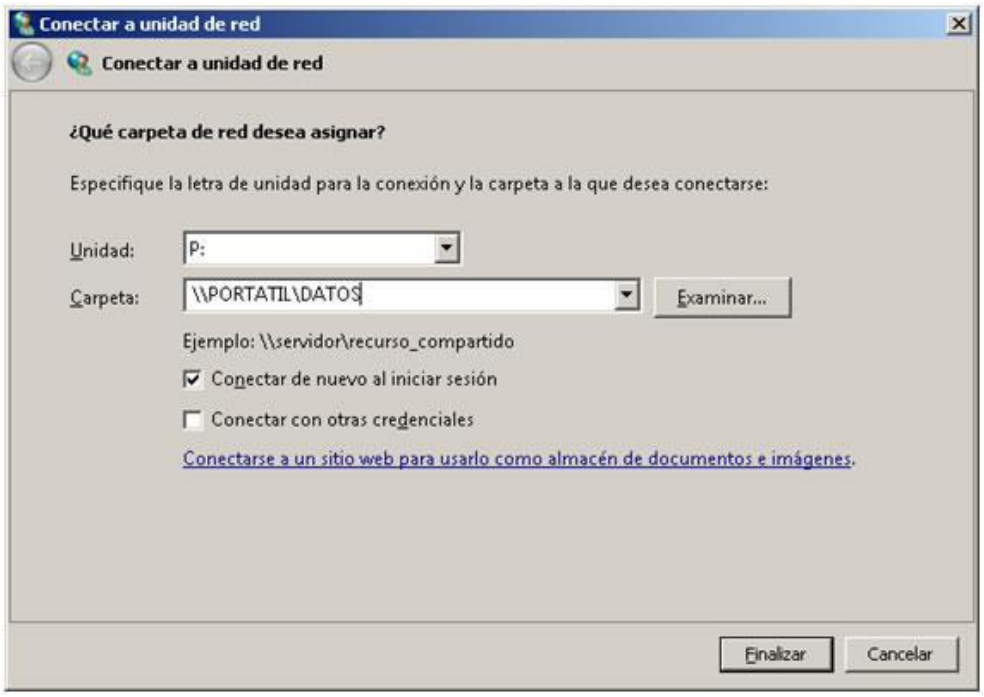
Si ahora abrimos el explorador y trazamos esa ruta desde otro equipo con el usuario asociado a la red, veremos cómo tenemos acceso directo a la carpeta compartida, y en definitiva a sus archivos contenidos.

07 Conectar unidades de red

Si queremos que nuestro equipo tenga acceso permanente a una carpeta compartida en otro equipo, podemos conectar esa carpeta a una unidad lógica de nuestro equipo y asignarle la letra de unidad que deseemos.

Para ello lo más sencillo es abrir el componente Equipo y pinchar en el botón **Conectar a una unidad de red.**

En la ventana que aparece podremos seleccionar la letra de la unidad que deseamos y la ruta de acceso a la carpeta compartida.



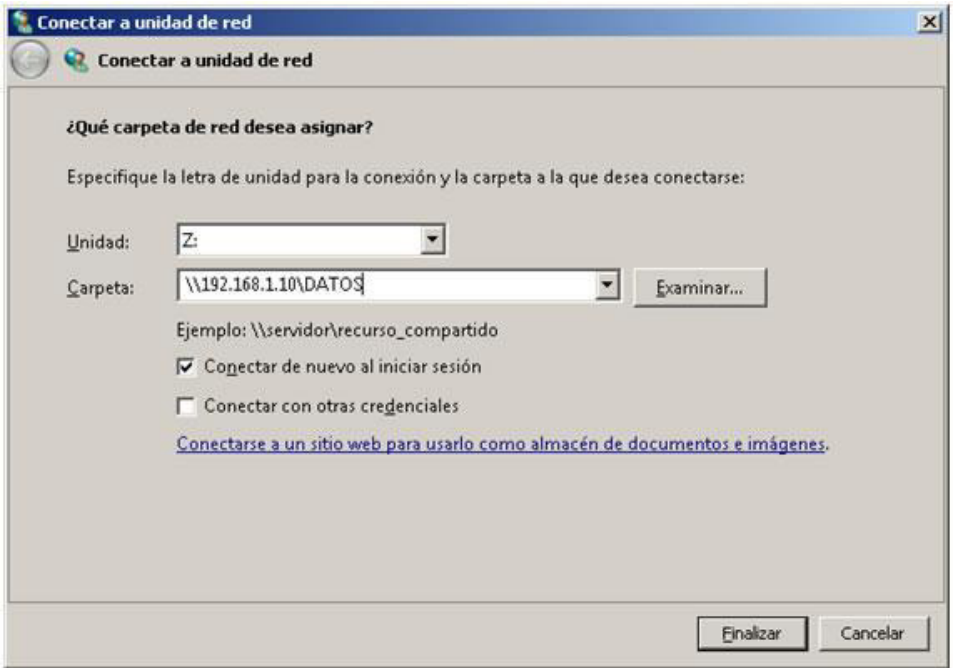
Si queremos que esta conexión aparezca la próxima vez que encendamos nuestro ordenador, debemos dejar marcada la opción **Conectar de nuevo al iniciar sesión**.

De esta manera, la unidad "P:\" de mi ordenador accede directamente a la carpeta que hemos compartido en otro equipo.

01 Práctica: Compartir y conectar una carpeta

En esta práctica vamos a probar cómo compartir una carpeta en un equipo, y posteriormente, conectarla desde otro como una unidad.

- Crear la carpeta C:\Datos en un equipo y copiar dentro dos o tres ficheros diversos (video, audio, texto,…)
- Compartir esta carpeta dando permisos de lectura a Todos los usuarios.
- Desde otro equipo en la misma red probar a acceder a \\Nombrede1ºequipo\datos o a \\DirecciónIPde1ºequipo\Datos
- Una vez hayamos accedido, conectar esa ruta a la unidad Z:\
- Probar que accedemos a Z:\ y podemos abrir los ficheros, pero no podemos modificarlos ni cambiar sus nombres.
- Desde el primer equipo, cambiar los permisos de compartición y dar acceso de escritura a Todos.
- Comprobar que en el segundo equipo podemos acceder a Z:\ y modificar los ficheros o cambiar sus nombres.



Tema 8

Comandos y herramientas

En esta unidad, hablaremos de las herramientas que pueden ayudarnos a la hora de localizar problemas o de revisar configuraciones, todas ellas se ejecutarán desde una ventana de comando a la que accederemos ejecutando el comando CMD.

Índice

01 IPCONFIG

Esta herramienta nos permite visualizar de manera directa la configuración de TCP/IP que tenemos en nuestro equipo:

Estos son algunos de los modificadores con los que se puede ejecutar este comando para realizar distintas acciones:

Ipconfig /all: Muestra toda la información de configuración.

Ipconfig /release: Libera la concesión DHCP de la dirección IP.

Ipconfig /renew: Solicita una nueva dirección IPv4 al servidor DHCP.

Ipconfig /renew6: Solicita una nueva dirección IPv6 al servidor DHCP.

Ipconfig /flushdns: Purga la caché de resolución de DNS.

Ipconfig /registerdns: Envía al servidor DNS la información IP para registrar el equipo con ella.

Ipconfig /displaydns: Muestra el contenido de la caché de resolución DNS.

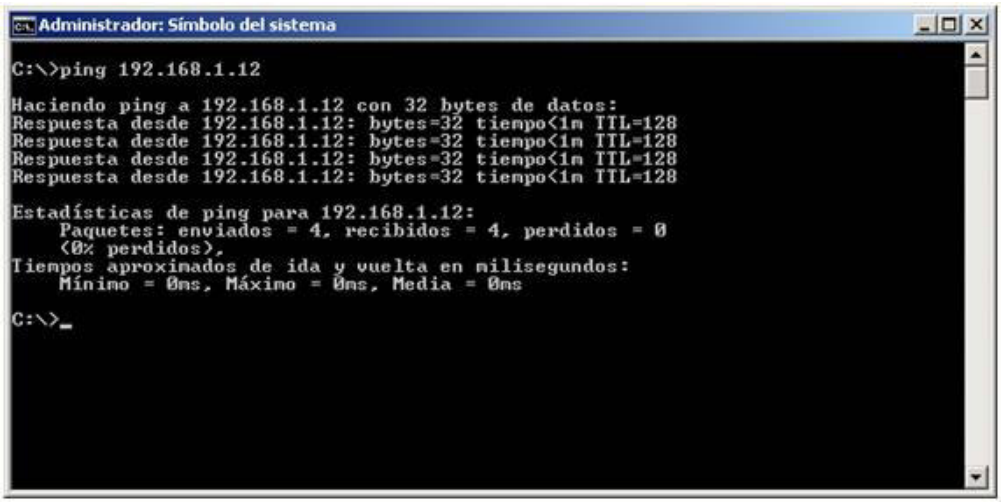
02 PING

Cuando hacemos ping a un equipo (ejecutamos el comando ping) o a una dirección IP lo que hace el sistema es enviar a esa dirección una serie de paquetes (normalmente cuatro) de un tamaño total de 64 bytes (salvo que se modifique) y queda en espera del reenvío de estos (eco), por lo que se utiliza para comprobar que la comunicación a través de la red entre nuestro equipo y otro dispositivo funciona correctamente.

También resulta muy útil para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.

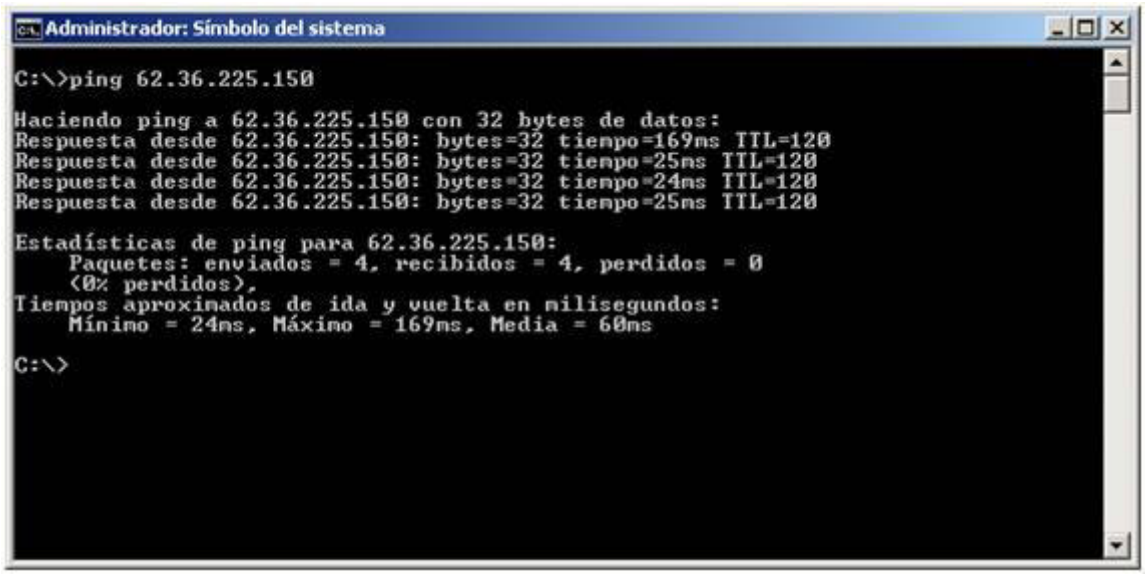
Para comprobar el correcto funcionamiento de los elementos de nuestra red podemos hacer tres ping en el orden que se especifica:

Un primer ping a nuestra IP local, con lo que comprobamos que nuestra tarjeta de red funciona correctamente (en este caso hacemos PING 192.168.1.12).



Un segundo ping a nuestra Puerta de enlace, con lo que comprobamos que nuestro equipo se comunica correctamente con nuestro router (en este caso hacemos PING 192.168.1.1).

Un tercer ping a la IP de nuestro servidos DNS, con lo que comprobamos que nuestro router se conecta correctamente con el exterior, es decir, con Internet (en este caso hacemos PING 62.36.225.150).



Para comprobar la nuestra conexiones de red podemos hacer ping a cualquier equipo de nuestra red, con lo que podemos comprobar si estamos realmente conectados a ese equipo, ya que en esta prueba no nos va a afectar ni configuraciones de Firewall (salvo que lo configuremos expresamente para no admitirlos) ni permisos de acceso al sistema, puesto que el ping se hace directamente sobre la tarjeta.

También podemos hacer PING a una dirección de una World Wide Web determinada. Por ejemplo, podemos hacer ping www.google.es y el efecto será el mismo, siempre y cuando nuestro servicio DNS funcione correctamente.

Al igual que ocurre con el comando IPConfig el comando PING tiene también una serie de modificadores que en un momento dado nos pueden ser de utilidad.

Algunos de estos modificadores son:

Ping –t: Hacer ping al host especificado hasta que se detenga.

Ping –a: Resolver direcciones en nombres de host.

Ping -n XX: Número de solicitudes de eco para enviar.

Ping -w XXX: Tiempo de espera en milisegundos para esperar cada respuesta.

Ping -S srcaddr: Dirección de origen que se desea usar (sólo en IPv6).

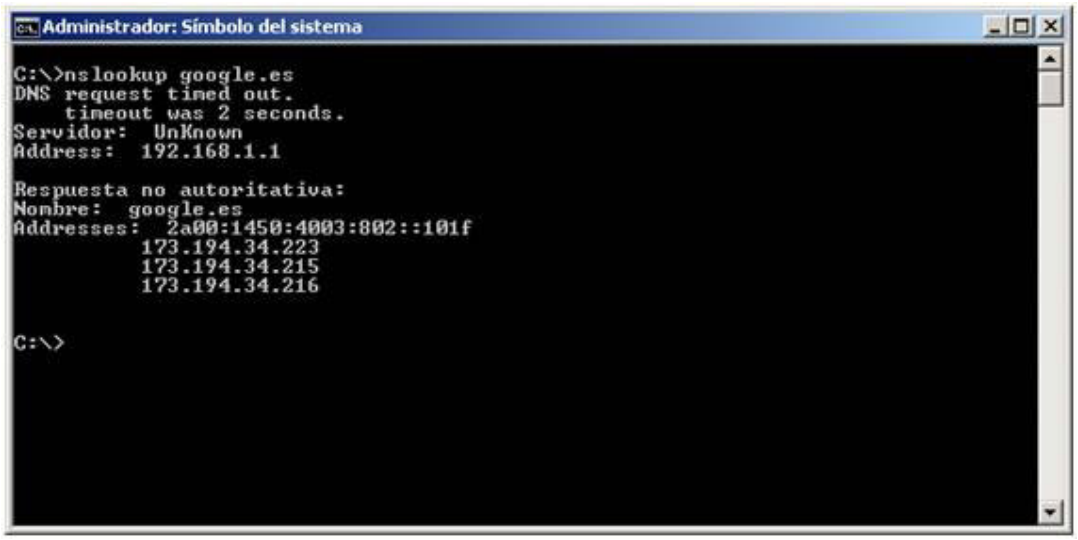
Ping -4: Forzar el uso de IPv4.

Ping -6: Forzar el uso de IPv6.

03 NSLOOKUP

El comando **NSLOOKUP** permite realizar consultas al servidor DNS para saber con qué direcciones IP está registrado un equipo o servicio determinado.

También se puede utilizar para realizar búsquedas inversas, es decir, saber a qué equipo o servicio corresponde una IP determinada.

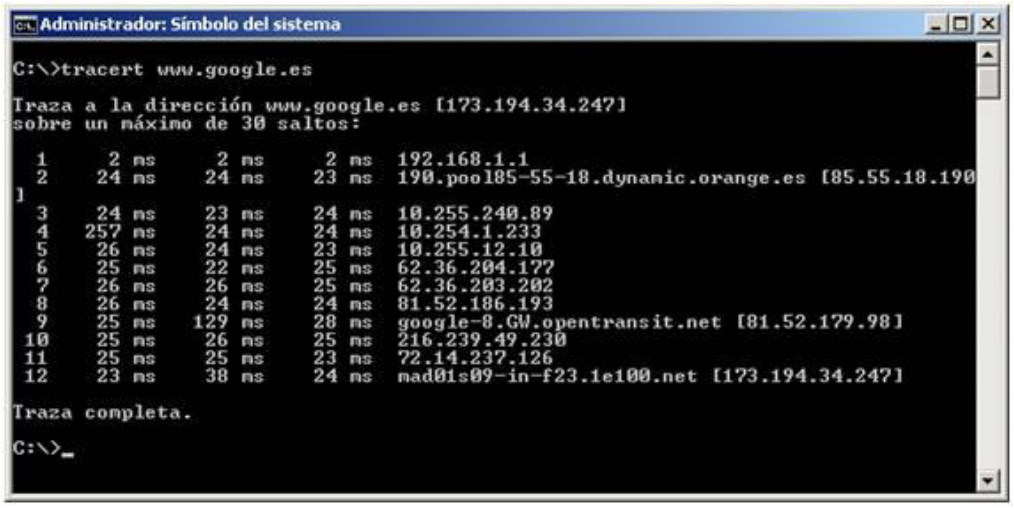


04 TRACERT

El comando **TRACERT** o **TRACEROUTE** permite visualizar el camino que se sigue a través de una red para llegar a un dispositivo seleccionado.

De esta manera podemos diagnosticar en qué punto podemos tener un problema de enrutamiento si nuestro equipo es incapaz de conectar con otro nodo de la red (por ejemplo mediante el comando PING)

Por defecto se hace esta ruta con un máximo de 30 saltos entre nodos.



En la sintaxis para ejecutarlo se pueden incluir varias opciones:

-d: Especifica que no se resuelvan las direcciones en nombres de host (no ponerlo puede hacer que la ejecución de la traza sea bastante lenta)

-h: XX: Especifica el número máximo de saltos para alcanzar el destino.

-w XXX Espera el número de milisegundos especificado de tiempo para cada.

De esta manera, una ejecución de este comando sería:

tracert [-d] [-h saltos_máximos] [-w tiempoDeEspera] nombre_destino

05 TELNET

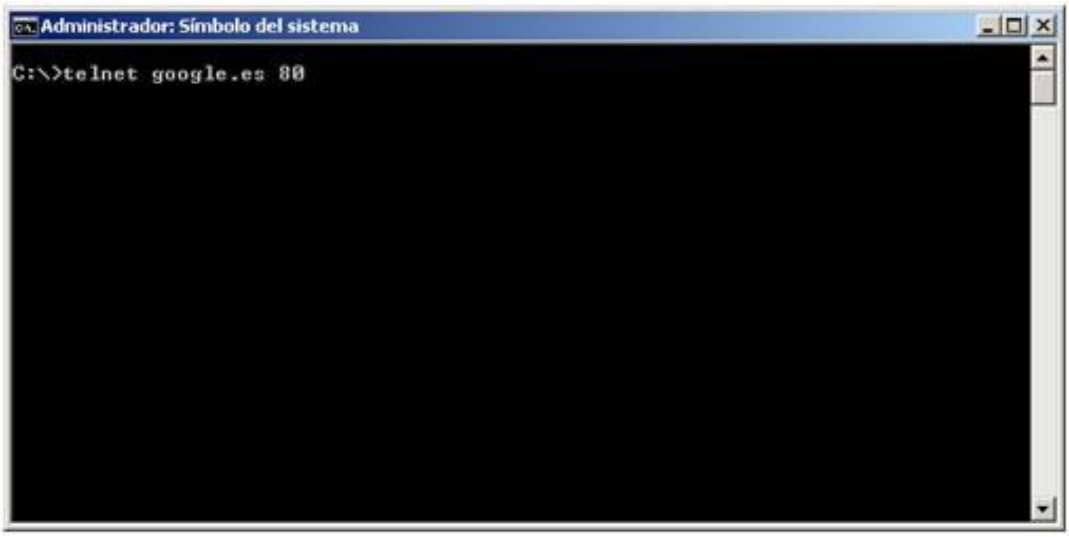
Telnet es una herramienta de terminal remota muy potente y con varios usos diferentes de lo que vamos a tratar aquí.

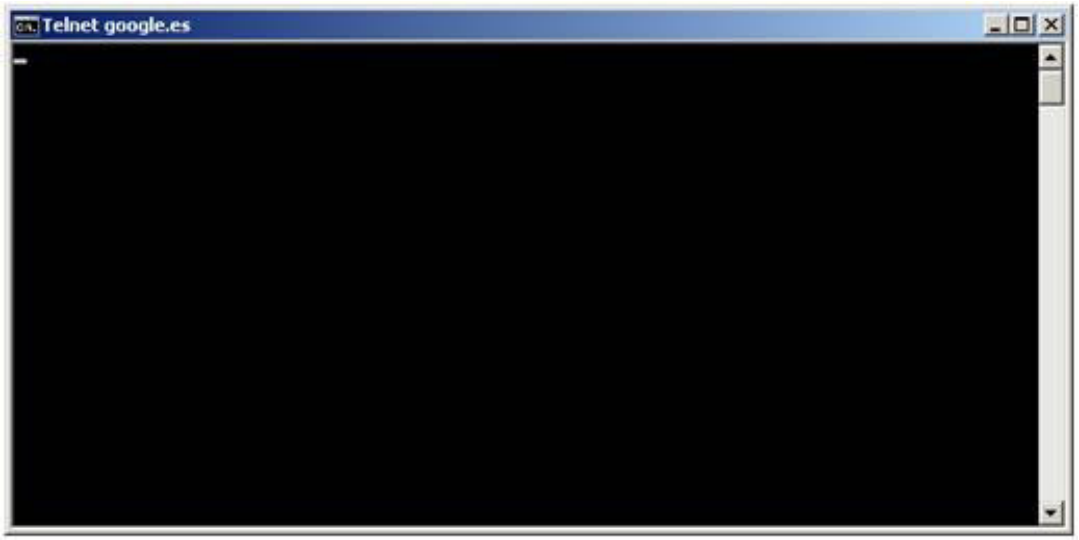
En nuestro caso, esta herramienta nos va a ayudar a diagnosticar si un equipo remoto es accesible por un puerto determinado.

De esta manera podremos saber por ejemplo si el no poder acceder a un servidor web determinado se debe a problemas de conectividad de nuestra red o si puede estar causado por algo más sencillo como una configuración errónea en nuestro navegador de Internet.

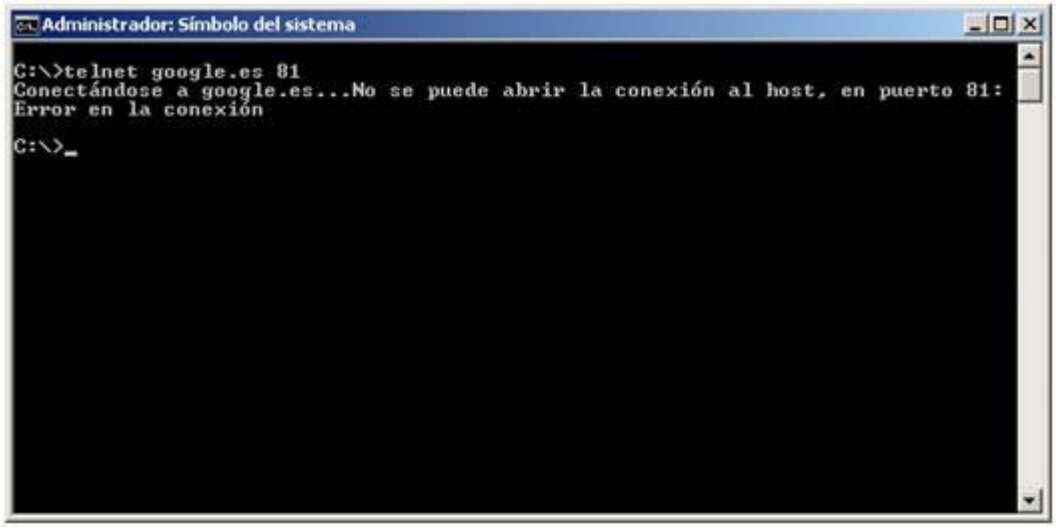
Para ejecutarlo debemos escribir telnet seguido del servidor remoto y el número de puerto al que queremos acceder (si es un servidor web http por defecto será el 80)

Si después de ejecutarlo la pantalla se queda negra con un cursor esperando un comando, entonces es que funciona, el equipo remoto es accesible por ese puerto, también es posible que el equipo remoto conteste con algún texto de entrada o nos cambie el cursor.





En cambio, si se queda intentando la conexión y al final da un fallo, eso significa que, al menos desde nuestro equipo, el nodo remoto no es accesible por ese puerto.



05 FTP

Permite conectarse a otra máquina a través del protocolo FTP para transferir archivos.

05 GETMAC

Muestra las direcciones MAC de los adaptadores de red que tengamos instalados en el sistema.

05 NBTSTAT

Muestra las estadísticas y las conexiones actuales del protocolo NetBIOS sobre TCP/IP, los recursos compartidos y los recursos que son accesibles.

05 NET

Permite administrar usuarios, carpetas compartidas, servicios, etc. Para un listado completo de todas las opciones, escribir net sin ningún argumento. Para obtener ayuda sobre alguna opción en concreto, escribir net help opción.

05 NETSH

Este programa en modo consola permite ver, modificar y diagnosticar la configuración de la red.

05 PATHPING

Muestra la ruta que sigue cada paquete para llegar a una IP determinada, el tiempo de respuesta de cada uno de los nodos por los que pasa y las estadísticas de cada uno de ellos.

05 MSG

Envía un mensaje a unos o varios usuarios determinados mediante su nombre de inicio de sesión o el identificador de su sesión.