

Acerca de las redes de ordenadores y conexiones a DVR de SEGURIDAD por Internet:

Los ordenadores tienen la facultad de poder comunicarse entre sí, para ello pueden utilizar diversos tipos de "idiomas" de entre los cuales nos centraremos en unas nociones del protocolo TCP-IP ya que es el que nos interesa.

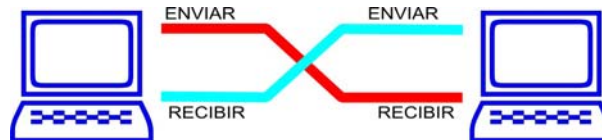
Para que los ordenadores puedan comunicarse, necesitan estar conectados entre ellos. Esta interconexión de ordenadores se denomina **RED**.

Los sistemas para conectar los ordenadores en red pueden ser muchos (cable coaxial, cable serie, vía radio (hoy en día esta de moda), ADSL, modem, satélite, etc.). De todos estos sistemas vamos a ver el que más nos afecta que es la conexión habitual de ordenadores mediante cable UTP y conectores RJ45 (que es como vienen equipados los DVR de SEGURIDAD y la mayoría de ordenadores que vamos a encontrar)

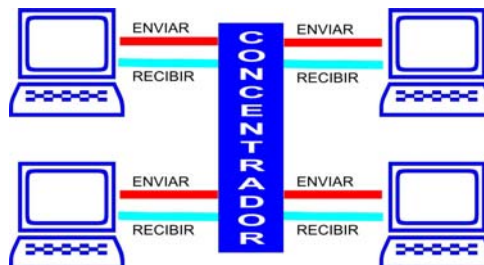
Que es una RED

Cuando encontramos dos equipos informáticos conectados entre sí para intercambiar datos ya estamos en presencia de una RED. La más básica de las redes se forma por dos ordenadores (vamos a considerar que todos tienen una tarjeta de red para protocolo TCP-IP con salida por conector RJ45) conectados mediante un cable.

En el conector RJ45, se hallan dos canales el de hablar (enviar datos) y el de escuchar (recibir datos). Es por eso que para interconectar sin más dos ordenadores necesitaremos un cable que se denomina "**CRUZADO**" este cable lo que hace es conectar las "orejas" con la "boca" y la "boca" con las "orejas" de manera que la comunicación sea posible.



Cuando tenemos más de dos equipos informáticos conectados entre sí, ya no podemos utilizar este tipo de cable y debemos emplear un equipo intermedio que es el que se encarga de interconectar los envíos con las recepciones. Este dispositivo se denomina **HUB** (concentrador) o **SWITCHER** (intercambiador).



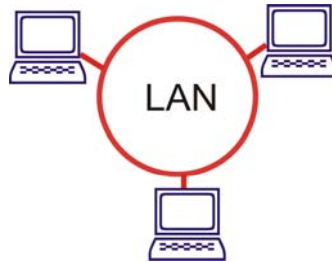
Como podemos comprobar en el esquema anterior, aquí ya no necesitamos el cable "cruzado" ya que el cruce de las comunicaciones lo realiza el concentrador debemos utilizar un cable Directo o **PARALELO**.

Este inciso nos debe servir para comprender que cada uno de los dos tipos de cables debe utilizarse **ÚNICA Y EXCLUSIVAMENTE PARA SU FIN**. Es decir que una conexión directa entre dos equipos informáticos con un cable que no sea "cruzado" **NUNCA** funcionará, del mismo modo si conectamos un equipo informático a un concentrador con un cable "cruzado" **NUNCA** funcionará.

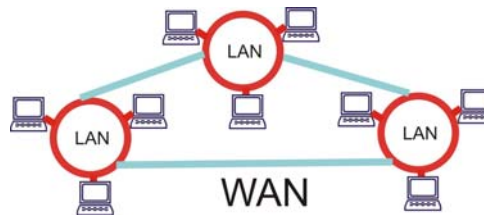
Los concentradores los hay actualmente de tres tipos: HUBS, cada vez se utilizan menos pues son mas lentos ya que cuando reciben datos de un ordenador conectado a ellos lo reenvían a todos los canales al mismo tiempo. SWITCHERS, son los que se están utilizando hoy en día y la ventaja que tienen es que cuando reciben datos de un ordenador conectado son capaces de identificar a que otro ordenador de los conectados está destinado y solo se lo envían a él, entre los SWITCHERS actualmente hay dos variedades: los "duplex" envían datos o reciben datos como un "walkie-talkie" y los "full-duplex" pueden enviar y recibir al mismo tiempo como un teléfono. Como es lógico estos últimos son mas veloces (y también más caros).

Tipos de redes según su tamaño.

Las redes de ordenadores, según su tamaño y ámbito se vienen a dividir en varios grupos. El grupo básico se entiende como una RED LOCAL (LAN) que está formada por varios ordenadores conectados a un concentrador y como ejemplo podemos poner unas oficinas o un negocio.

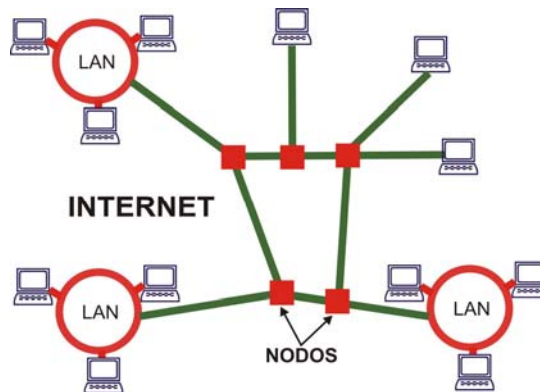


Una red media sería por ejemplo distintas delegaciones de una empresa con su red local en cada delegación y una extra red (WAN) que interconectaría todas las delegaciones. Este servicio se ofrece también mediante INTERNET para las empresas por los proveedores de servicios (Telefónica, Wanadoo, etc.) con el nombre de "VPN" (red privada virtual) creando un "camino" de conexión directa entre las redes locales de la empresa utilizando la estructura de Internet.



Y la red más importante que nos interesa que es INTERNET donde una serie de centros de distribución que llamaremos NODOS se encargan de conectar entre sí a usuarios de todo el mundo.

INTERNET fue creado por el gobierno americano hace años para proporcionar un medio seguro de comunicación a sus servicios militares y de espionaje en todo el mundo, pero nunca se hubieran imaginado a donde iba a llegar.



La comunicación entre ordenadores TCP IP

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPAnet) que conectaba redes de ordenadores de varias universidades y laboratorios en investigación en Estados Unidos. World Wide Web que conocemos hoy (las famosas **WWW**) se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear.

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

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos. Los dos protocolos más importantes son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto.

Dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos tienen una serie de características.

La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro. Los ordenadores que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen *IP mueve los paquetes de datos a granel, mientras TCP se encarga del flujo y asegura que los datos estén correctos.*

Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino.

Los datos no tienen que enviarse directamente entre dos ordenadores. Cada paquete pasa de ordenador en ordenador hasta llegar a su destino. Éste, claro está, es el secreto de cómo se pueden enviar datos y mensajes entre dos ordenadores aunque no estén conectados directamente entre sí. Lo que realmente sorprende es que sólo se necesitan algunos segundos para enviar un archivo de buen tamaño de una máquina a otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples ordenadores. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje.

Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando enviamos un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

Después de este breve inciso sobre las comunicaciones a través de Internet, vamos de nuevo a centrarnos en el conocimiento más básico que aquí nos interesa.

Las Direcciones IP

Los ordenadores, para poder comunicarse mediante los protocolos TCP-IP necesitan tener un identificador que los distinga de los demás. Algo así como un número de teléfono que permita saber a quien se dirigen las llamadas y los mensajes.

Este número es la **dirección IP**.

Hoy en día, se utilizan para las direcciones IP, unas cadenas de 4 bloques con 3 dígitos cada una desde 0 a 255.

XXX.XXX.XXX.XXX

Las posibilidades de combinaciones son muchas, pero debido al crecimiento de la cantidad de ordenadores que se van interconectando en todo el mundo, esta gran cantidad de direcciones IP se va quedando pequeña y está a punto de instaurarse un nuevo sistema de direcciones IP que constará de 6 bloques de 4 dígitos.

XXXX.XXXX.XXXX.XXXX.XXXX.XXXX

Este nuevo sistema es considerado como inagotable ya que según los cálculos efectuados se podría llegar en toda la superficie mundial, una vez organizadas de forma práctica y jerárquica, en el peor de los casos a 1.564 direcciones IP por cada metro cuadrado,

Centrándonos en las direcciones IP actuales diremos que estos números de que consta cada bloque, no son arbitrarios si no que están definidos de forma muy importante.

El primer bloque de 3 dígitos identifica el tipo de red en tres grandes grupos que se definieron en un principio:

Grupo A: formado por las direcciones IP que en sus primeros tres dígitos están comprendidas entre 1 y 126 (ambos inclusive) Este primer bloque identifica la red, mientras que los otros tres bloques identifican a cada uno de los ordenadores en cada red. Esto quiere decir que en cada una de estas redes podemos identificar más de 16 millones de ordenadores pero solo pueden haber 126 redes de este tamaño.

Grupo B: formado por las direcciones IP que sus primeros tres dígitos están comprendidos entre 128 y 191 (ambos inclusive) y que para poder alcanzar un número mayor de redes se compone la identificación de la red por los dos primeros bloques, pudiendo ir desde 128.1 hasta 191.254 haciendo un total de 16.000 redes con un máximo en cada una de 64.516 ordenadores

Grupo C: en este caso el valor del primer bloque estará formado por un valor comprendido entre 192 y 223, identificándose la red por los tres primeros bloques y permitiendo un máximo de 254 ordenadores en cada red.

Además quedan reservadas las direcciones con el primer bloque superior a 223 para los grupos D y E que aun no han sido definidos y el valor 127 que se utiliza para propósitos especiales en algunos sistemas; también es importante notar que los valores 0 y 255 en cualquiera de los bloques no se utilizan normalmente pues tienen unas funciones específicas, el 0 se utilizaría para máquinas que aun no tienen una dirección asignada y el 255 para hacer una especie de llamada general a todas las máquinas de una red.

En definitiva las redes en las que nos vamos a mover nosotros normalmente van a ser del tipo C y el resto de grupos los vamos a dejar para que los gestionen las empresas que nos van a proporcionar acceso a internet o a conectarnos externamente a otra red de grupo C en otro lugar.

Cuando configuramos un ordenador o un DVR nos encontramos con que hemos de rellenar tres casillas que son las siguientes:

Dirección IP
Máscara de red
Puerta de enlace

La dirección IP es como hemos visto anteriormente el "**NOMBRE**" único en la red de un determinado ordenador. Normalmente el rango que encontraremos en una red para los equipos conectados será de 192.168.255.001 hasta 192.168.255.254.

La máscara de red es una cadena similar a una dirección IP que sirve para delimitar el número de ordenadores que componen la red, siendo normalmente 255.0.0.0 para una red de clase "A" 255.255.0.0 para una red de clase "B" y 255.255.255.0 para una red de clase "C".

Esta última es la que habitualmente encontraremos. Solo cuando la red está dividida en varias sub-redes podremos encontrar máscaras de red como 255.255.60.0, lo que limitaría la capacidad de esta red a 60 ordenadores.

Queda así claro que para que dos ordenadores se "VEAN" en una misma red deberán tener la MISMA máscara de red y una dirección IP con los tres primeros bloques iguales y el tercero diferente. Por ejemplo:

Ordenador 1 = Máscara de red 255.255.255.0 Dirección IP 192.168.255.001

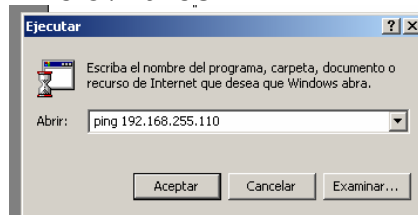
Ordenador 2 = Máscara de red 255.255.255.0 Dirección IP 192.168.255.002

Ordenador 3 = Máscara de red 255.255.255.0 Dirección IP 192.168.255.012

Estos tres ordenadores están en la misma red y cada uno se identifica individualmente en ella.

Existe en los ordenadores un comando que se llama PING (es una onomatopeya del sonido que habréis visto en las películas de submarinos cuando con el radar o sonar envían una señal para esperar si rebota en algún cuerpo que quieren detectar esperando su rebote) cuando ejecutamos este comando seguido de la dirección IP que estamos comprobando, el ordenador nos dice si hay respuesta y nos muestra la velocidad a que se ha recibido esta respuesta.

Este sería el comando que encontramos en INICIO / EJECUTAR



Y este sería el resultado de una conexión correcta

```
C:\WINNT\system32\ping.exe
Haciendo ping a 192.168.255.110 con 32 bytes de datos:
Respuesta desde 192.168.255.110: bytes=32 tiempo=20ms TTL=255
Respuesta desde 192.168.255.110: bytes=32 tiempo<10ms TTL=255
Respuesta desde 192.168.255.110: bytes=32 tiempo<10ms TTL=255
```

La respuesta si no se encuentra el ordenador que buscamos sería:

```
C:\WINNT\system32\ping.exe
Haciendo ping a 192.168.255.115 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
```

Con esta simple prueba podemos asegurarnos de que la comunicación entre dos ordenadores es la correcta, están bien los cables y las direcciones IP.

Con esto podemos dar por finalizada la explicación de una red sencilla de dos ordenadores o una pequeña red local de unas oficinas y pasar a ver de que más equipos consta el acceso a INTERNET o sea la comunicación entre redes distantes.

Puerta de enlace (o la puerta por la que una red de ordenadores se conecta a Internet)

Para poder unir dos o mas redes necesitamos un equipo que puede ser un MODEM o puede ser un ENRUTADOR (ROUTER).

El Modem (cuyo nombre viene de MODulador DEModulador) es un equipo que se encarga de convertir las señales digitales del ordenador en otras que se pueden transmitir por la líneas telefónicas (modular) y a su vez recibir las señales que vienen por las líneas telefónicas y convertirlas en señales inteligibles para el ordenador (demodular). Se conocen también con este nombre actualmente equipos capaces de convertir señales que no provienen de las conexiones que hemos visto anteriormente (RJ45) si no que provienen de los puertos de ordenador USB o SERIE (que utilizan otros protocolos diferentes al TCP-IP) en señales TCP-IP. Estos modems ADSL que algunos proveedores de ADSL ofrecen en

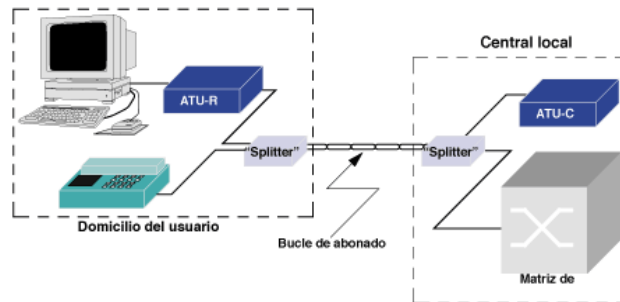
sus paquetes, son adecuados en instalaciones en que solo tengamos un ordenador, por lo cual mientras que servirán para recibir de internet datos o imágenes de un DVR, no son adecuados para los lugares en que vayamos a instalar un DVR de SEGURIDAD.

Normalmente los DVR de SEGURIDAD únicamente se van a conectar utilizando TCP-IP por RJ-45, una ADSL con Modem USB **NUNCA** la podremos utilizar para conectar a internet un DVR de SEGURIDAD.

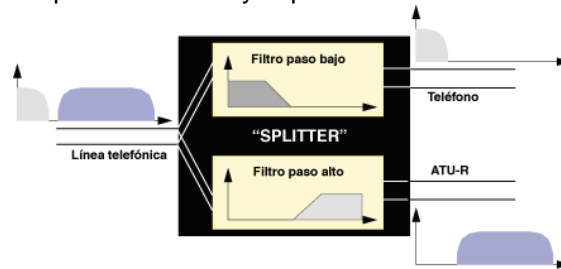
Vamos a centrarnos en los ROUTERS. Estos equipos se conectan a la línea de teléfono (o de cable) en la cual el proveedor de acceso a internet nos envía la señal y nos permite conectar mediante un puerto RJ-45 en la red.

Si únicamente dispone de un puerto, lo deberemos conectar a un HUB o SWITCHER para poder dar acceso a internet a más de un equipo.

Normalmente en una línea con ADSL sobre la línea de teléfono existente nos encontramos con la siguiente disposición:



La línea de teléfono existente (o bucle de abonado) se configura en la central mas próxima de teléfonos para inyectarle mediante un Splitter (filtro separador) la señal ADSL sobre la señal existente de voz y conviven en el mismo cable hasta el interior del domicilio del usuario en que son separadas ambas señales mediante otro Splitter. En casa del usuario se conecta la parte de ADSL resultante del Splitter al Router y la parte de Voz al teléfono.



Hoy también podemos encontrar que en vez de un Splitter en la entrada, se conecte toda la señal al Router y se conecten en paralelo los teléfonos incorporando a cada teléfono un "Micro Filtro" para eliminar el ruido causado por el componente ADSL.



"Micro Filtro"

Una vez comprendido esto, ya tenemos la línea ADSL en el Router.

Como es lógico, en este Router (que no es más que un pequeño ordenador) tenemos que tener una dirección IP que es con la que se reconocerá nuestra pequeña red en Internet. Esta dirección IP puede ser de dos tipos: Estática (FIJA) o Dinámica (VARIABLE) dependerá de nuestro proveedor de internet.

¿Por qué y como una dirección IP dinámica?

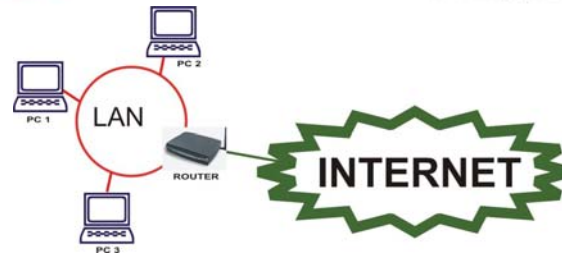
Como hemos visto al principio, las direcciones IP actualmente son un número finito y escaso, la mayoría de los usuarios de Internet utilizan solo su acceso a Internet para recibir cosas y eventualmente enviar algo, además no siempre están conectados.

Esto es utilizado por los proveedores de Internet para aprovechar al máximo las direcciones IP de que disponen, de modo que cuando una dirección IP no está en uso puede ser utilizada por otro usuario y con una buena gestión de los muchos horarios y puntos del planeta, poder dar servicio a mas público con menos gasto (para ellos).

PERO para poder tener un punto totalmente disponible desde Internet (como puede ser un Servidor de contenidos, un ordenador con ficheros que queremos que puedan acceder nuestros clientes, o nuestro **DVR de SEGURIDAD**) NECESITAMOS que esta dirección IP sea **FIJA**, es decir necesitamos saber siempre a que número tenemos que llamar para que nuestro DVR de SEGURIDAD nos conteste.

Ya tenemos una dirección IP FIJA y ya tenemos un Router en la entrada de nuestra instalación. ¿Qué nos falta?

La **puerta de enlace** para entrar y salir de Internet.



Tal como decía anteriormente el Router es un ordenador y como tal tiene también una dirección IP. Esto no es cierto pues no tiene una si no que tiene DOS. Una es la dirección IP PÚBLICA (es decir la que tiene nuestra red hacia el exterior, la que se "VE" desde Internet) y la otra es la dirección IP PRIVADA (o sea la que hace que el Router se "VEA" desde nuestros ordenadores en la red).

Por lo tanto el Router tendrá una dirección IP y una máscara de red públicas (que nos proporciona nuestro proveedor de Internet) y una dirección IP y una máscara de red privadas (que se deberá configurar como hemos visto anteriormente, misma máscara de red que los demás equipos y dirección IP igual a las de los equipos con el último bloque de tres dígitos diferente).

Con esto ya es el Router visible desde Internet y desde nuestra red. Ahora solo falta decirles a los ordenadores de nuestra red que la puerta de enlace para acceder a Internet es LA DIRECCIÓN IP PRIVADA que le hemos puesto al Router.

En el ejemplo de la pequeña red dibujada sobre estas líneas, una correcta configuración sería:

EQUIPO	DIRECCION IP	MASCARA DE RED	PUERTA DE ENLACE
PC 1	192.168.255.1	255.255.255.0	192.168.255.50
PC 2	192.168.255.2	255.255.255.0	192.168.255.50
PC 3	192.168.255.12	255.255.255.0	192.168.255.50
ROUTER	192.168.255.50	255.255.255.0	NO TIENE

Ya está la configuración completa y los tres PC's tienen acceso a Internet, pero todavía nos falta un detalle:

Cuando nosotros desde un PC nos conectamos a Internet, le indicamos mediante el Navegador de Internet o mediante el programa que utilicemos para ver nuestro DVR una dirección IP o un nombre de una página web a donde dirigir la llamada de nuestro ordenador.

Pero que ocurre si lo que queremos es desde el exterior conectarnos con un PC (o en nuestro caso con un DVR de SEGURIDAD) que está conectado al Router y del que sabemos la dirección IP pública.

Si hacemos una llamada, responderá el Router pero no el equipo que nos interesa. Para ello debemos activar la "Telefonista" que incluye el Router en su interior (conocida como NAT o Network Adress Translator (Traductora de Direcciones de Red))

En el protocolo TCP-IP, además del camino por el que se envían los datos, existen también unas canalizaciones que utiliza cada programa exclusivamente para sus datos. Estas canalizaciones se denominan **PUERTOS**. Hay programas muy extendidos y que utilizan unos puertos estandarizados universalmente para permitir que programas estandares puedan acceder a la información que fluye por esos puertos, por ejemplo el puerto 21 para los correos electrónicos y el puerto 80 para los servidores WEB. También cada fabricante de programas utiliza los puertos que le son mas interesantes.

Si tomamos por ejemplo un DVR X, el fabricante nos indica que el puerto necesario para la comunicación es el **TCP 5365** (hay dos tipos de puertos TCP y UDP, dependiendo de los fabricantes ya que TCP-IP como hemos dicho incluye muchos y diversos protocolos) esto quiere decir que le hemos de indicar al Router que cuando reciba una llamada en la dirección IP pública con este puerto (es la llamada que hará el programa de visión de este DVR) la redirija a la dirección IP en que tenemos configurado el DVR.

El comportamiento es como si se tratara de una centralita de teléfonos inteligente, el programa quiere hablar con el departamento de ver cámaras que tiene la extensión 5365, al hacer la llamada al número de teléfono de la centralita, la operadora automática reconoce por el puerto de llamada que tiene que dirigir esa llamada a la extensión (dirección IP) del departamento de ver cámaras (el DVR de SEGURIDAD).

Varios datos que deben quedar claros para que a un DVR DE SEGURIDAD se pueda acceder desde el exterior:

- ✓ 1º La dirección IP pública debe ser FIJA y se debe conocer
- ✓ 2º La ADSL debe disponer de un Router con salida de red RJ45
- ✓ 3º El Router debe estar en modo MULTIPUESTO (es decir que permita conectar varios ordenadores y configurar puertos (NAT)
- ✓ 4º Deben poderse abrir los puertos que se indiquen
- ✓ 5º No deben haber filtros que impidan acceso desde el exterior o en su caso estos deben estar bien configurados