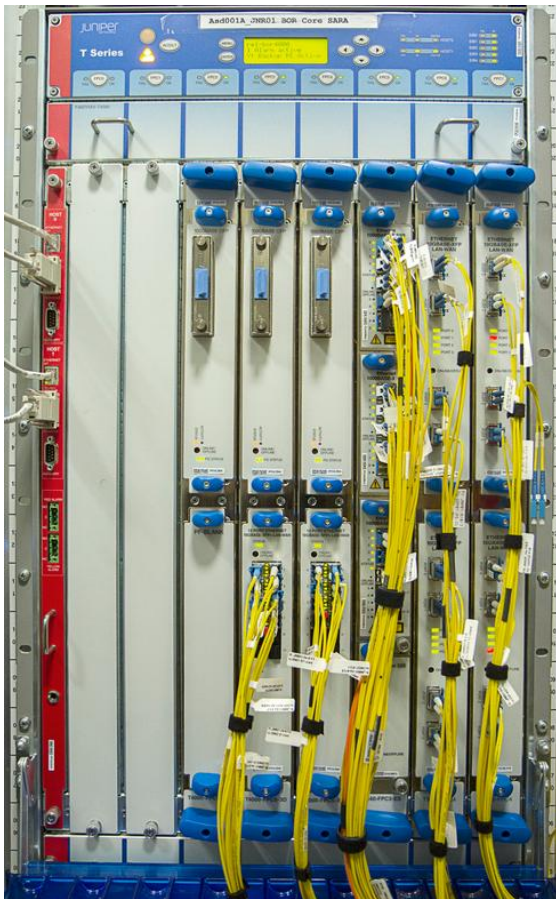


# **Configuración y administración de routers**

## Contenido

1. Introducción .....	2
2. Componentes del router .....	3
3. Los routers en las LAN y en las WAN .....	5
Routers en las LAN .....	6
Routers en las WAN .....	8
4. Formas de conexión al router .....	9
Conexión al router vía puerto de consola .....	10
Conexión al router vía SSH o Telnet .....	10
Conexión al router vía web .....	12
5. Configuración y administración del router .....	13
Configuración y administración del router por comandos .....	14
Configuración y administración del router vía web .....	14
6. Listas de control de acceso (ACL) .....	18



### 1. Introducción

## Caso práctico

Avanza el curso, Luisa cada vez está más ilusionada.

Luisa: Vamos a ver los routers en la asignatura ¿Qué te parece?

Juan: El router es el elemento clave de la red

Luisa: ¿Por qué?

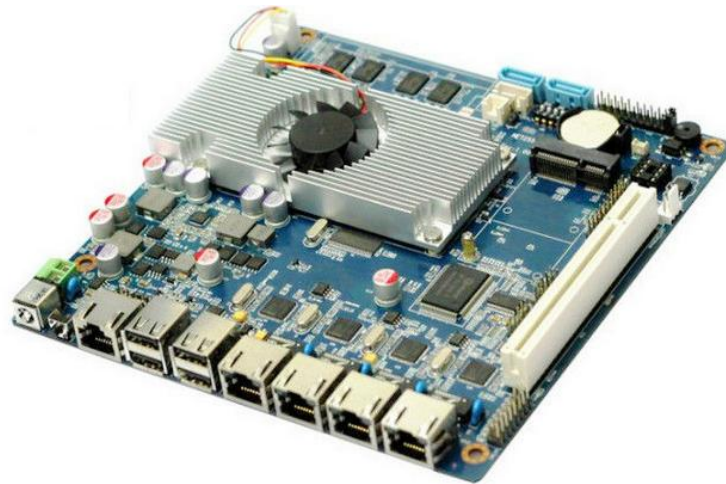
Juan: Es el dispositivo donde se controla normalmente toda la red y con el que vas a trabajar más a menudo.

Luisa: ¿y cómo son?

Juan: Uf, los hay de todas las clases, tienes por ejemplo el tipo router-ADSL, también puede ser un ordenador con dos conexiones de red, y puede ser un router empresarial con una gran cantidad de conexiones y difícil de configurar.

## 2. Componentes del router

Desde el punto de vista del hardware, los componentes básicos de un router son prácticamente los mismos que los de un ordenador: CPU, memoria, buses, distintas interfaces de entrada/salida y fuente de alimentación.



Desde el punto de vista del software ocurre algo similar, el router tiene un sistema operativo (de red) como base y sobre este se pueden montar diferentes servicios, por ejemplo, el servicio web para configuración.

- Chasis: En el caso de routers modulares, grandes routers, podemos encontrar diferentes chasis, donde iremos encajando las diferentes placas que adquiramos, las dos imágenes corresponden a un chasis Cisco y otro Juniper.



- Módulos, placas o tarjetas que encajamos:



- CPU: Al igual que en los ordenadores personales, es un microprocesador que ejecuta las instrucciones del sistema operativo, la inicialización del sistema, funciones de enrutamiento y el control de las interfaces de red.
- MEMORIA: Dentro de un router podemos encontrar diferentes tipos de memoria:
  - RAM: Esta memoria se utiliza principalmente para gestionar el almacenamiento de las tablas de enrutamiento y la configuración del router.
  - Flash: Almacena una imagen del software del sistema operativo.
  - NVRAM: Es una memoria RAM no volátil. Se utiliza para guardar la configuración de inicio.
  - ROM: Se utiliza para almacenar el diagnóstico del hardware durante el arranque del router.
- BUS: Es el canal que comunica la CPU con los demás componentes del router y transporta los datos y las instrucciones de control.
- INTERFACES: Son las conexiones con el exterior, pueden ser RJ-45 (Red Ethernet), RJ-11 (Cable telefónico), Fibra óptica, serie, etc.



- FUENTE DE ALIMENTACION: Es la parte que se encarga de suministrar la energía eléctrica necesaria para el funcionamiento del router.

### 3. Los routers en las LAN y en las WAN

Los routers son dispositivos que operan en la capa 3 del modelo OSI. Los routers son máquinas, que como los ordenadores, tienen su CPU, memoria y sistema operativo.



Router empresarial (usados en WAN)



Router doméstico (usados en LAN)

La función principal del router es separar redes y comunicarlas. ¿Y para que separarlas si después queremos comunicarlas?, pues porque desde el router el administrador controla toda la red, decide por donde debe viajar los datos, que accesos están permitidos, etc.

Un router es un dispositivo que tiene varias interfaces, cada una de estas interfaces está en una red IP distinta. Cuando un router recibe un paquete IP en una interface, determina la interface por la que debe enviar el paquete hacia su destino (esta acción es la que se conoce como encaminar o enrutar)

En general los routers no se limitan a enrutar los datos, entre las funcionalidades habituales nos encontramos:

- Servidor DHCP
- Filtrado de datos (ACL)
- Traducción de direcciones (NAT)
- Diferentes formas de configuración: vía Web, telnet, SSH, SNMP.
- Redes privadas virtuales (VPN)

## Routers en las LAN

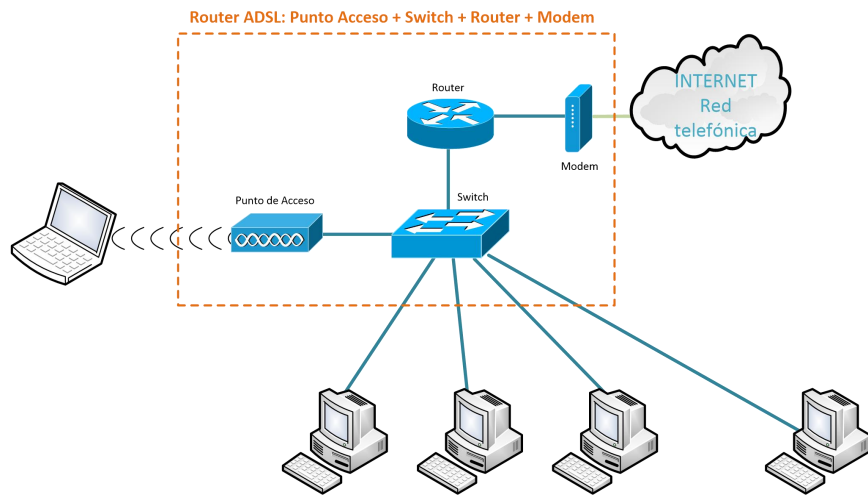
Se caracterizan en que todos usan la técnica NAT porque separan una red privada (donde están los PCs) de una red pública (la del proveedor de servicios de internet, ISP). Como cualquier router tiene una CPU, memoria y un sistema operativo. Estos sistemas operativos suelen estar basados en Linux.

El uso de routers en LAN más habitual es para la conexión a internet, y lo más común es una conexión ADSL.



El router-ADSL típico dispone de una conexión RJ-11 que se conecta a la línea telefónica, a través de esta conexión se recibe IP pública, y utilizando la tecnología NAT comparte esta IP pública a una red local a la que se pueden conectar dispositivos alámbricos (suelen traer 4 conexiones RJ-45) o inalámbricos (mediante el punto de acceso incorporado).

Suelen venir configurados de fábrica para conectar y funcionar sin necesidad de cambiar ningún parámetro. La configuración habitual es asignar IPs a la red local mediante el servicio DHCP que viene activado y recibir una IP dinámica del proveedor de internet. La señal WIFI suele venir activada y la clave para conectarse impresa en el exterior del dispositivo. Un esquema del interior del dispositivo sería el siguiente:



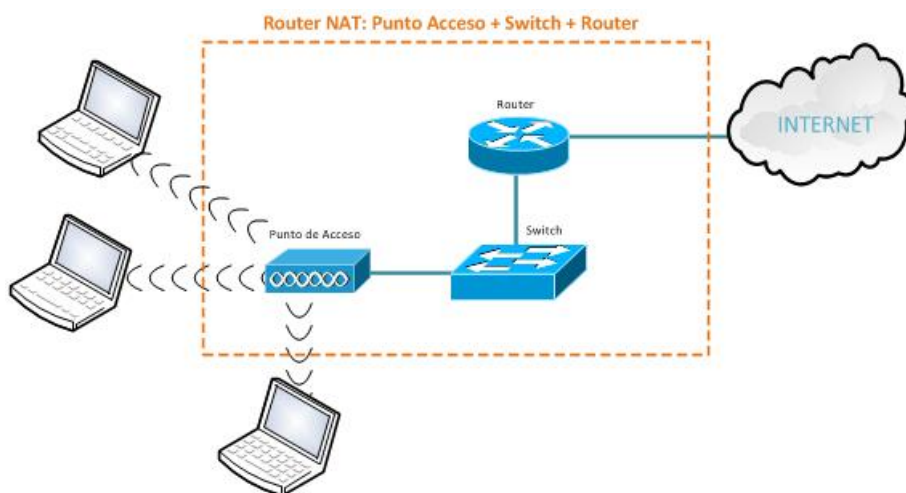
Como se trata de un router, separa redes, en este caso 2 redes: WAN y LAN. Por tanto tiene 2 IPs una IP pública asociada a la interfaz WAN y una IP privada asignada a la interfaz LAN.

Sobre este primer router podemos hacer diferentes combinaciones que también son frecuentes de encontrar en las redes locales:

Sin modem, **router-NAT**:



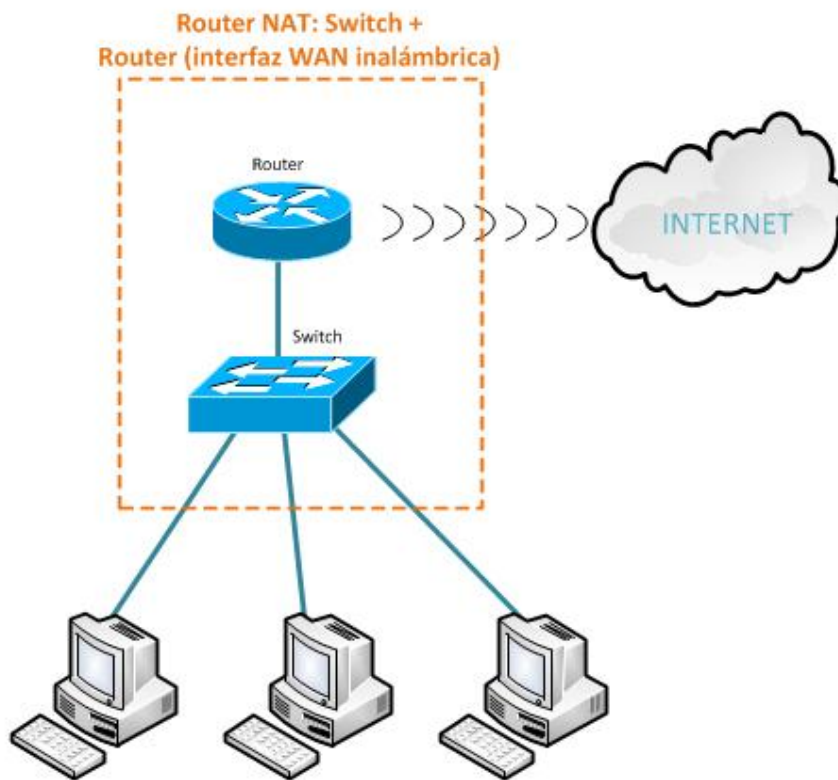
En este caso cambia el tipo de conexión WAN de RJ-11 (cable telefónico) a RJ-45 (cable de red), el esquema del dispositivo multifunción sería:



Router receptor de señal WIFI, **router cliente WISP:**



En este caso la señal inalámbrica está asociada al puerto WAN y sirve para recibir internet por señal inalámbrica de un proveedor de internet (WISP). Es habitual encontrar este modelo en forma de antena sectorial para recibir señal desde largas distancias. El esquema sería:



Podemos encontrar más variedades de estos routers, por ejemplo, incorporando un adaptador para tarjeta SIM, recibir internet 4G y repartir a la red local.

## Router en las WAN

Los routers en las redes WAN tienen como principal función enrutar los paquetes





Mientras que una LAN los routers se comunican con otros dispositivos como PC, hubs o conmutadores siguiendo el estándar Ethernet, en una red WAN se comunican básicamente con otros routers y los estándares seguidos son muy variados.

Al igual que todos los routers son máquinas con CPU, memoria y sistema operativo, aunque en este caso los sistemas operativos suelen ser diseñados por los diferentes fabricantes. El sistema operativo de red más conocido es el IOS de Cisco, de hecho, es un estándar.

Este sistema operativo permite introducir comandos a través del intérprete de línea de comando (CLI) para configurar el funcionamiento de los routers. La mayoría de los routers también admiten configuración a través de herramientas gráficas, entorno web, SNMP, etc.

Como decimos cada fabricante tiene su propio sistema operativo, pero como estos routers se comunican entre ellos deben utilizar “idiomas” entendidos por todos: los protocolos. Evidentemente los protocolos más importantes utilizados por los routers son los protocolos de enrutamiento.

Los protocolos de enrutamiento permiten que los routers conectados creen un mapa de comunicaciones que permite que en cada momento se seleccione la mejor ruta, estos mapas forman parte de las tablas de enrutamiento que manejan cada uno de los routers.

#### 4. Formas de conexión al router

Al igual que ocurre con los switches hay varias formas de conexión al router, desde las más tradicionales como es el puerto de consola a lo más actual como es vía web.



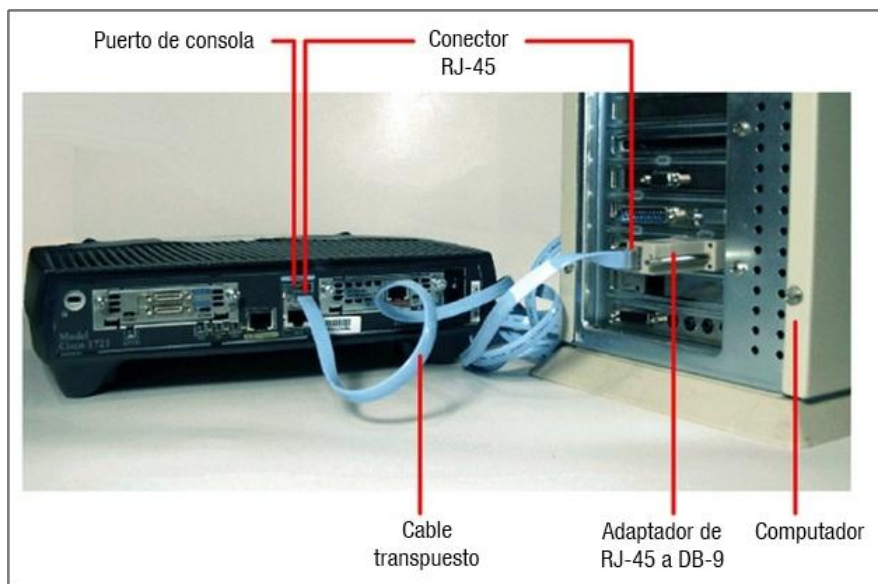
## Conexión al router vía puerto de consola.

El puerto de consola es una conexión específica para administración que incorporan muchos routers, principalmente, routers empresariales.

Las tres formas más comunes para acceder a la línea de comandos del router son por el puerto de consola, por el auxiliar o por un puerto LAN con una sesión Telnet. Si es la primera vez que se accede, es fácil acceder por el puerto consola. Para poder hacerlo, debemos utilizar un programa para emular el terminal puerto serie (Hyperterminal, TeraTerm, CRT, PuTTY, Reflection, minicom) junto con un cable de administración.



La forma de conectar los dispositivos es como se ve en la figura, unimos un puerto serie del PC al puerto consola del router mediante el cable de administración.



## Conexión al router vía SSH o Telnet

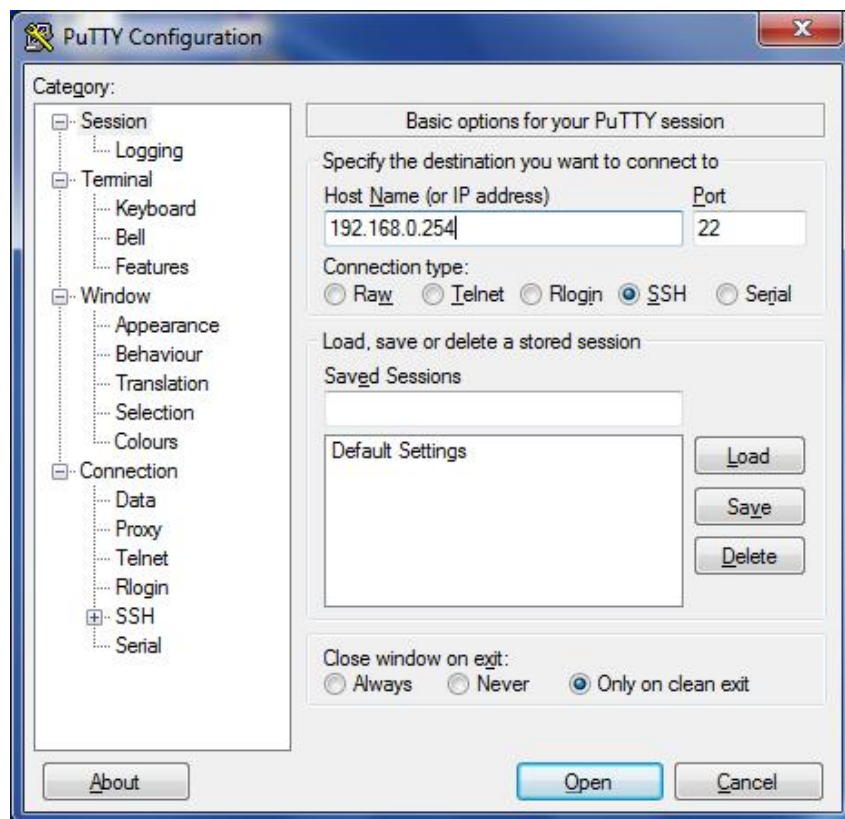
Otra forma de acceder a los routers es a través de la línea de comandos con los protocolos telnet o SSH. Esta forma no es muy habitual en routers domésticos como los mencionados en apartado los routers en las LAN.

Conectamos un cable, normalmente RJ-45, desde el ordenador de trabajo al router directamente o a la red del router (si, por ejemplo, este está conectado a un switch bastaría con conectar nuestro ordenador de trabajo al switch).

Para saber la IP a la que debemos conectarnos tenemos varias opciones: manual del fabricante donde viene la IP de fábrica o, si viene con servicio DHCP activado de fábrica solicitar una IP desde nuestro PC y comprobar que puerta de enlace nos asigna:

```
C:\>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Conexión de área local:
Dirección IPv4 . . . . . : 192.168.0.101
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.0.254
C:\>telnet 192.168.0.254
```

Si nuestro sistema operativo no dispone del comando telnet o la conexión es via ssh podemos utilizar putty:



Dependiendo del modelo de router utilizaremos unos comandos u otros (podemos probar con help o ? son bastante habituales):

```

_{root}=>help
Following commands are available :

help          : Displays this help information
menu         : Displays menu
?            : Displays this help information
exit        : Exits this shell.
..         : Exits group selection.
saveall     : Saves current configuration.
ping       : Send ICMP ECHO_REQUEST packets.
traceroute  : Send ICMP/UDP packets to trace the ip path.

Following command groups are available :

firewall      service      autopvc      connection   cwnmp
dhcp          dns             dsd          dyndns       eth
adsl         atm            config      debug        env
expr         grp            hostmgr     ids          igmp
interface    ip             ipqos       label        language
mbus         memm          mlp         nat          ppp
pftp        script        snmp        sntp software
system      systemlog    upnp        user wireless

_{root}=>

```

## Conexión al router vía web

Actualmente la forma de conexión a routers para configuración más habitual es vía Web. Las ventajas de esta forma de conexión son no necesitar ningún software especial (basta un navegador), no tener que conocer los comandos de configuración (algo tedioso) y una interfaz intuitiva y de fácil manejo.

Una vez sepamos la IP de nuestro router basta con teclearla en la barra de navegación. Cada fabricante suele diseñar la web de configuración a su manera. En estos enlaces hay simuladores de las pantallas web de configuración de diferentes dispositivos:

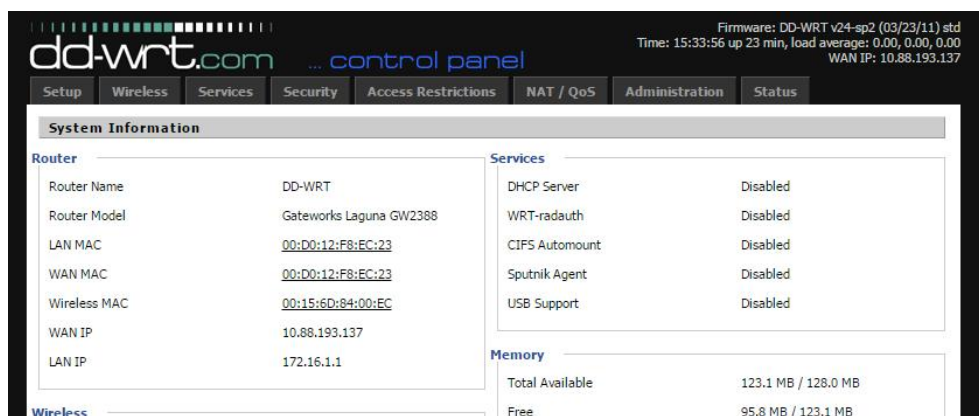
[Tp-link](#)

[Linksys](#)

[Netgear](#)

[Cisco](#)

También existen algunos firmware (sistema operativo que instalamos en el router) que son libres, como openwrt, dd-wrt o tomatos:




Estos firmware suelen traer más herramientas instaladas que los firmware de los fabricantes y permiten configurar diferentes marcas con el mismo entorno.

El acceso vía web, como otros, se puede realizar de manera inalámbrica si el router soporta esta funcionalidad. Esto implica la conveniencia de configurar el usuario y la contraseña del administrador del router de manera que sean diferentes a los valores de fábrica ya que de lo contrario cualquier persona en el radio de acción del router podría acceder a su configuración.

## 5. Configuración y administración del router

### Caso práctico



Luisa ya tiene su router, pero ¿por dónde empezar? ¿Qué cable conecto?

La teoría nos va a enseñar como configurar routers pero la realidad es que cada router tiene sus peculiaridades. Vamos a ver algunas configuraciones via web y también algunas configuraciones con comandos.

Cada router tiene unos parámetros configurables diferentes, depende del fabricante, del firmware, etc.

En la configuración por comandos suele haber respuesta tecleando **?** o **help**, y se ofrece un listado de todos los comandos disponibles.

Los parámetros configurables más comunes de un router son:

- Nombre del router
- Nombre de usuario
- Contraseña
- Parámetros de red: IP, máscara, etc.
- Características de interfaces.
- Protocolos de enrutamiento.
- Cortafuegos
- Servicios disponibles (QoS, DHCP, FTP, etc)

Para poder configurar un parámetro del router hay que conectarse al router vía SSH, telnet o web. Y por supuesto tener los permisos necesarios (usuario y clave) para poder realizar los cambios.

## Configuración y administración del router por comandos

Cada sistema operativo tiene sus comandos y además suelen ser una lista larga, de forma que sería imposible tratar aquí todos los sistemas y sus comandos. Nos centraremos en los comandos del sistema IOS de Cisco por tratarse de un referente a nivel mundial.

Para trabajar con un dispositivo en IOS hay tres entornos, dependiendo de los privilegios que tengamos, usuario, privilegiado y configuración global

El modo usuario (prompt > ) me permite solamente consultar el estado de configuración, el nivel superior es el modo privilegiado (prompt #), para una configuración completa el modo configuración global (prompt Router(config)#) y modo configuración de interfaces (prompt Router(config-if)#)

Para cambiar entre los diferentes modos:

```
router> enable
router# configure terminal
router(config)# interface fa0/0
router(config-if)# exit
router(config)# exit
router# exit
router>
```

Para poner nombre al router:

```
router> enable
router# configure terminal
router(config)# hostname ASIR_PAR
```

Para poner una clave de acceso al modo privilegiado:

```
router(config)# enable password clave_elegida
```

Para asignar IP a una interface:

```
router(config)# interface Gi0/0
router(config-if)# ip address 192.168.0.1 255.255.255.0
router(config-if)# no shutdown
```

Para hacer una copia de seguridad de la configuración:

```
router# copy running-config startup-config
```

Mostrar la tabla de enrutamiento:

```
router# show ip route
```

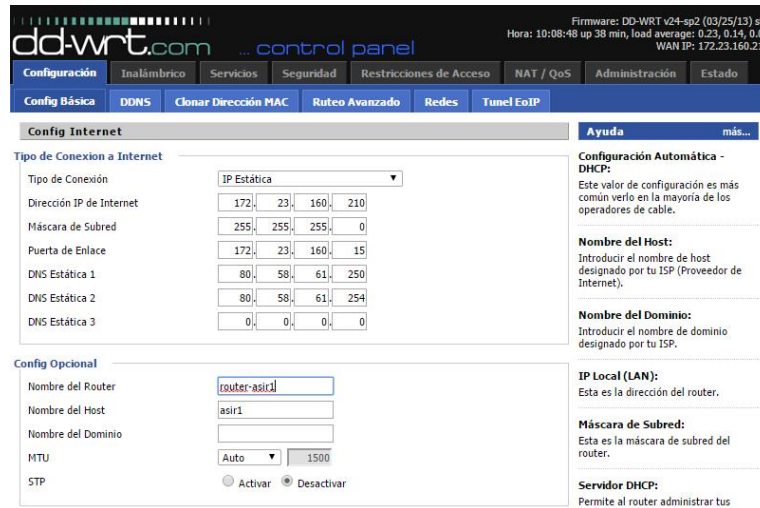
## Configuración y administración del router vía web

Al igual que sucede con los comandos, la configuración vía web está basada en las páginas web que cada fabricante diseña, evidentemente cada fabricante plantea los menús, los parámetros, etc. como le parece conveniente. La única ventaja es que cada fabricante suele usar diseños

muy similares para los diferentes dispositivos, con lo cual los dispositivos que tenemos son de una sola marca o de muy pocas solo tendremos que aprender a manejar unas pocas páginas web.

Para mostrar las configuraciones usaremos dd-wrt, es un firmware que podemos instalar de diferentes dispositivos y que tienen bastante auge.

Para cambiar el nombre del router basta con acceder a la configuración básica y escribir en la casilla nombre del router:



Cambio de contraseña, se haría en la opción de administración, este entorno, como la mayoría de los routers domésticos solo hay un tipo de usuario que tiene acceso a la configuración completa del router.



En el caso de router domésticos la configuración de las interfaces se realiza vía web, los tipos más habituales son:

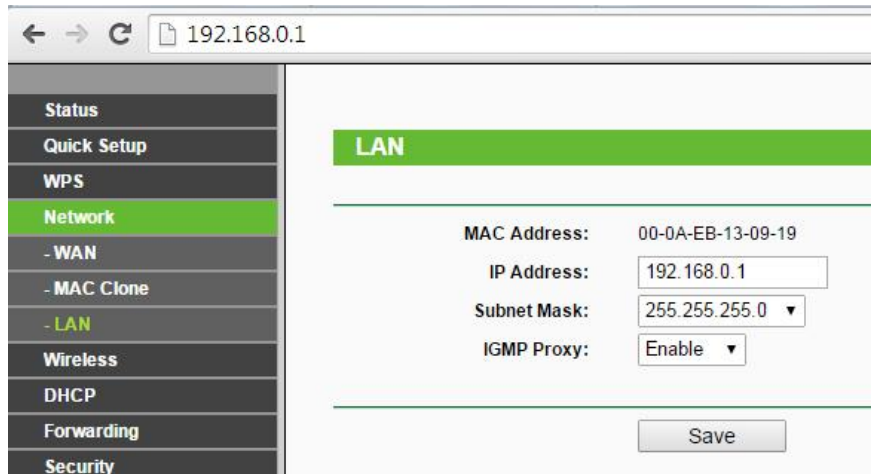
- Ethernet, las cuales no suelen admitir más configuración que la relacionada con la dirección IP.
- Inalámbricas, donde podemos configurar el nombre de la WIFI, los parámetros de seguridad, etc.



- PPP, es usado en varios tipos de redes físicas como cable serial, línea telefónica, telefonía móvil. PPP también es usado en las conexiones de acceso a internet. Los ISP han usado PPP para que accedan a internet los usuarios de línea telefónica:

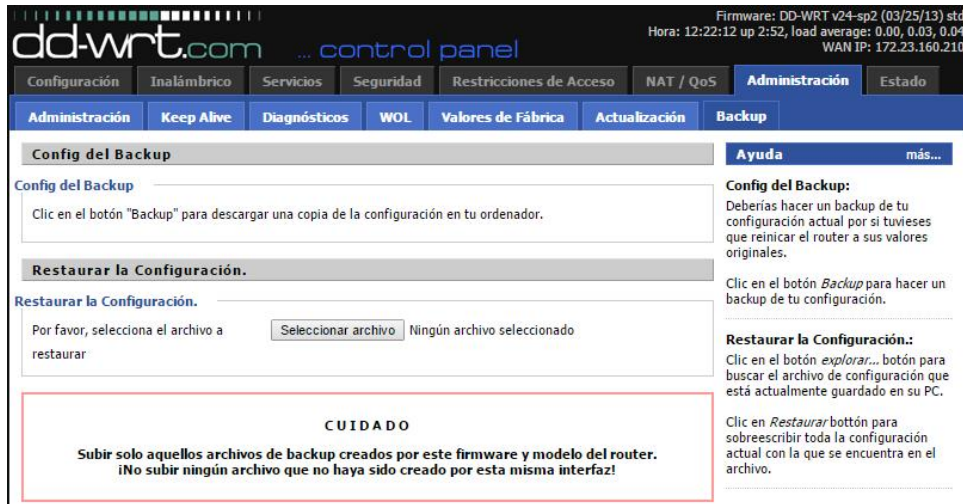
WAN Configuration			
Interface	VPI/VCI	Encap	Protocol
vc0	8/32	LLC	rt1483

En el caso de router domésticos, la interfaz LAN suele traer una configuración de fábrica (habitualmente una IP 192.168.x.x) y la interfaz WAN suele venir configurada en IP dinámica con todos los parámetros necesarios. No obstante, si deseamos podemos cambiar la configuración de estos parámetros a través del entorno gráfico:

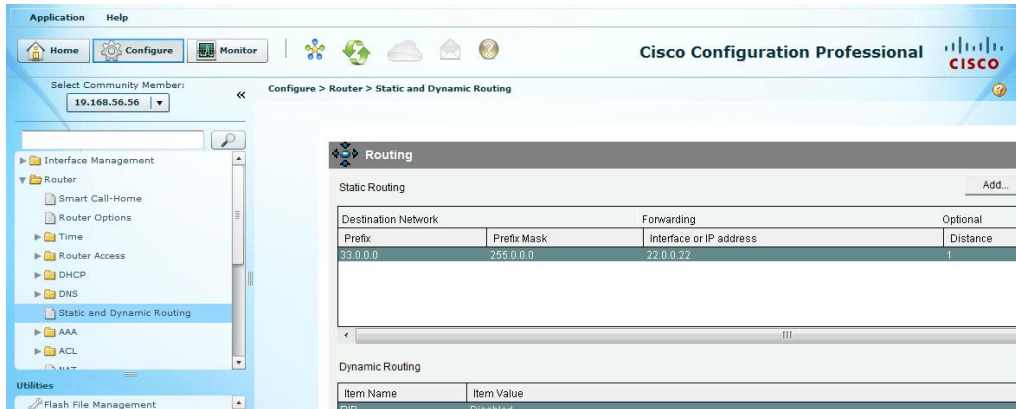


Hacer una copia de seguridad de la configuración:





Mostrar la tabla de enrutamiento en CCP:



Actualización del firmware:

En el caso de routers domésticos, el firmware o software que maneja el dispositivo, se actualiza normalmente a través de una pantalla web, pero cuidado, **no actualizar nunca desde una conexión WIFI** porque podemos perder la conexión en mitad de la subida del nuevo firmware y averiar el dispositivo:

## 6. Listas de control de acceso (ACL)

### Caso práctico



Luisa tiene dos hijos adolescentes que por las tardes entran en su cuarto a “estudiar” pero ella sabe que lo que realmente hacen es visitar web de redes sociales. Ha oído que desde su router puede bloquear los accesos a determinados contenidos y está dispuesta a aprender cómo hacerlo para que realmente estudien sus hijos.

De forma genérica, una lista de control de acceso o ACL (access control list) es una lista de reglas que definen la política de tráfico permitido en un router.

Este control del tráfico se puede hacer a muchos niveles, el más conocido por todos es el cortafuegos que puede tener el sistema operativo o el programa antivirus.

En los routers podemos hacer lo mismo con el tráfico, estas ACLs se pueden aplicar en cualquiera de los interfaces del router por donde pasa el tráfico. De forma resumida tenemos que saber que:

- Una ACL es una relación de reglas (no una sola regla).
- Al aplicar una ACL se va comprobando una a una las reglas, cuando llegamos a una regla que se debe aplicar terminamos, es decir, a partir de esta regla se ignoran todas las reglas restantes.
- En una ACL primero se indican las reglas más concretas y después las más genéricas (Por ejemplo, si queremos bloquear una red entera y dentro de esa red permitir un equipo, la regla del equipo va antes que la regla de la red, puesto que si lo hacemos al contrario se aplicaría la regla de red y no se leería la regla del equipo)
- En la mayoría de los sistemas todo lo que no está indicado en las reglas de la ACL se bloquea, por tanto en estos casos, siempre habrá que poner al menos una regla permisiva porque si no todo es negado.
- La ACL se aplica en un interfaz y se puede aplicar en dirección salida o en dirección entrada.

Veamos un ejemplo de bloqueo de todos los equipos para el acceso al servidor (88.2.188.98), esta ACL tiene 2 reglas, la primera deniega (deny) el acceso desde cualquier PC (source any) al servidor (destination 88.2.188.98) de todos tipos de accesos (IP, también se puede bloquear otros protocolos), la segunda regla debe permitir todo el tráfico que no cumpla la primera regla porque si no por defecto se bloquearía.

Access Rules							
Name/Number	Used by	Type	Description				
BloqueoServidor		Extended	Bloqueo de acceso al Servidor 88.2.188.98				

Action	Source	Destination	Service	Log	Attributes	Description
Deny	any	88.2.188.98	ip			Bloqueo desde cualquier PC al servidor
Permit	any	any	ip			Permitir el resto

Pero además de definir las reglas hay que indicar en que interfaz queremos aplicarlo (Fastethernet 0/1) y si es al entrar el tráfico por la interfaz o al salir (al entrar Inbound):

Interface	IP	Type	Slot	Status	Description
FastEthernet0/0	19.168.56.56	FastEthernet	0	Up	
FastEthernet0/1	22.22.22.22	FastEthernet	0	Up	
FastEthernet1/0	no IP address	FastEthernet	1	Up	
FastEthernet1/1	no IP address	FastEthernet	1	Up	
FastEthernet1/2	no IP address	FastEthernet	1	Up	
FastEthernet1/3	no IP address	FastEthernet	1	Up	
FastEthernet1/4	no IP address	FastEthernet	1	Up	
FastEthernet1/5	no IP address	FastEthernet	1	Up	
FastEthernet1/6	no IP address	FastEthernet	1	Up	
FastEthernet1/7	no IP address	FastEthernet	1	Up	
FastEthernet1/8	no IP address	FastEthernet	1	Up	
FastEthernet1/9	no IP address	FastEthernet	1	Up	
FastEthernet1/10	no IP address	FastEthernet	1	Up	
FastEthernet1/11	no IP address	FastEthernet	1	Up	

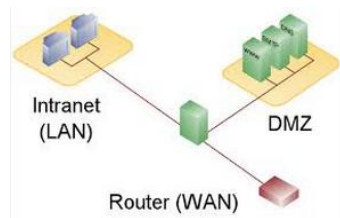
Item Name	Item Value
IP address/subnet mask	22.22.22.22/255.0.0.0
NAT	<None>
Access Rule - inbound	BloqueoServidor
Access Rule - outbound	<None>
IPSec Policy	<None>

En los routers domésticos es diferente, cada fabricante diseña pantallas de bloqueo propias, la configuración suele ser más sencilla y cercana al usuario. Habitualmente se permite:

- bloqueo por MAC
- bloqueo por IP
- bloqueo por puertos (TCP – UDP)
- bloqueo por palabras
- bloqueo por dominios
- configuración del horario de bloqueo, etc.

En la siguiente imagen podemos ver las restricciones de acceso en dd-wrt donde se puede aplicar varias políticas simultaneas, en cada política podemos bloquear determinados equipos, se puede indicar el horario de bloqueo.

Un concepto muy relacionado con la protección es **DMZ** zona desmilitarizada (sigla en inglés de demilitarized zone).



Es una red que está entre la red interna de una organización y una red externa, o sea Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la

DMZ solo se permitan a la red externa. El objetivo es evitar conexiones desde el exterior a la red interna pero si permitirlos a la DMZ.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

Los routers domésticos suelen incluir esta opción, en este caso consiste en indicar la IP de un equipo que va a ser accesible desde internet (es la opción más rápida para abrir los puertos a un equipo).