

## Caso práctico



María ha ampliado su academia con 2 aulas más, ha instalado equipos conectados en red en ambas aulas, para la instalación se asesoró por un técnico de sistemas microinformáticos y redes. Todo el cableado acaba en un cuarto de comunicaciones, pero quiere separar las diferentes aulas, es decir, que no comuniquen los equipos de las diferentes aulas entre sí. Le han comentado que puede utilizar routers o crear VLANs.



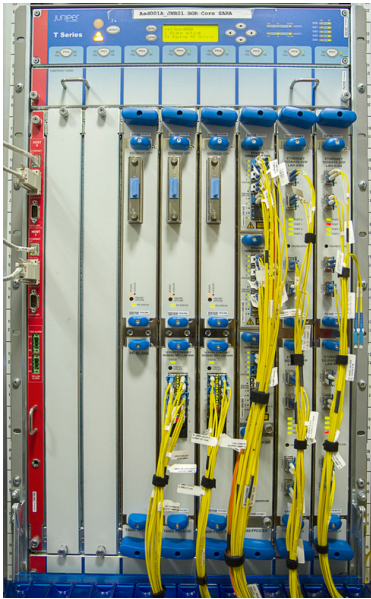
[Ministerio de Educación y Formación Profesional](#). (Dominio público)

**Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.**

[Aviso Legal](#)

# 1.- Introducción

---



En este tema vamos a tratar dos temas principales, las VLANs (Virtual LAN) y comenzar el estudio de uno de los elementos clave en la administración de redes: el router.

Hay que tener en cuenta que los dispositivos finales, como por ejemplo los PCs, suelen configurar sus parámetros de red forma dinámica.

Otros dispositivos muy frecuentes en la red son los switches, donde se configuran las VLANs.

Aunque la mayor parte de la configuración de red suele realizarse en su mayoría sobre routers.

En cuanto, a los routers, tenemos mucha variedad: el típico router-fibra, 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.- VLAN

---

Las VLAN se crearon para separar de forma lógica una red física. Se instala y cablea toda la red uniendo todos los dispositivos, y posteriormente utilizando VLANs se separa la red de forma lógica según decida el administrador de la red, por tanto, las VLANs permiten una gran versatilidad sin necesidad de cambiar físicamente la red.

En una red habrá varias VLANs, cada dispositivo comunica con los que estén en su VLAN. Es decir, en una red sin VLAN un paquete puede llegar a todos los dispositivos, en cambio en una red con VLAN un paquete solo puede llegar a los dispositivos de su VLAN.

Las VLAN pueden ser, siguiendo los niveles OSI:

- De nivel 1, son las más habituales, es cuando se asocia cada puerto de un switch a una VLAN. Al principio todos los puertos están en la VLAN 1, que es la VLAN predeterminada.
- De nivel 2, se asocia cada MAC a una VLAN

De nivel 3 y 4, se asocia cada protocolo o servicio a una VLAN.

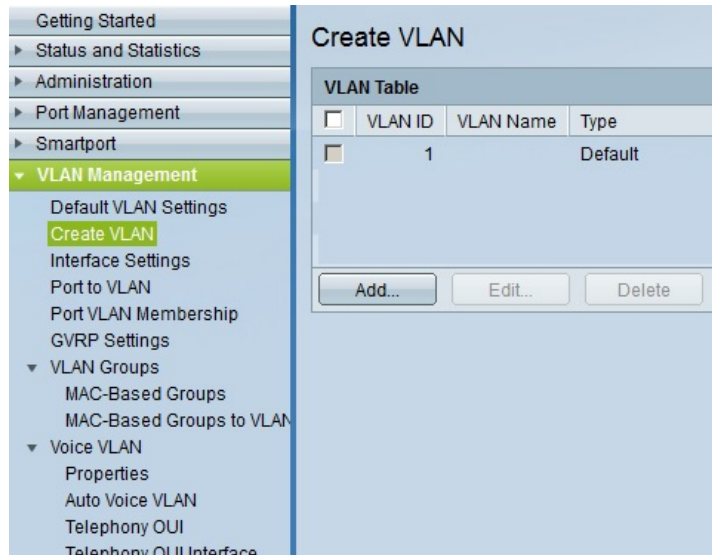
## 2.1.- ¿Cómo se crea una VLAN?

Para crear una VLANs basta con indicar los elementos que componen cada VLAN. En el caso de las VLANs de nivel 1 consiste en asociar cada puerto del switch a una VLAN. Debemos tener en cuenta que la mayoría de los switches tienen una lista de VLANs admitidas, de fábrica solo suelen tener una VLAN en su base de datos, la VLAN 1, que es la VLAN predeterminada. Esto supone que, en un principio, todos los puertos están en la VLAN 1, es decir, que solo hay una división lógica de la red donde se encuentran todos los elementos.

Por tanto, para crear VLAN, lo primero es añadir las nuevas VLANs a la lista de VLANs admitidas. Lo segundo, asignar los elementos a cada VLAN.

Para configurarlas, aunque depende del fabricante, la mayoría facilitan una configuración vía web, para una configuración básica (un solo switch):

1. Situación inicial, solo la VLAN predeterminada:

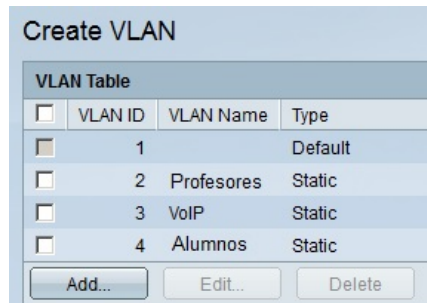


The screenshot shows a web interface for creating VLANs. On the left is a navigation menu with 'VLAN Management' expanded and 'Create VLAN' selected. The main area is titled 'Create VLAN' and contains a 'VLAN Table' with the following data:

<input type="checkbox"/>	VLAN ID	VLAN Name	Type
<input type="checkbox"/>	1		Default

Below the table are three buttons: 'Add...', 'Edit...', and 'Delete'.

2. Se añaden a la lista de VLANs las nuevas VLANs:

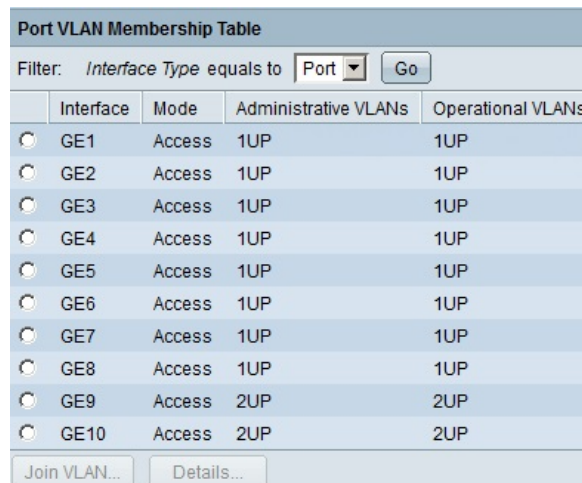


The screenshot shows the 'Create VLAN' web interface with a 'VLAN Table' containing four entries:

<input type="checkbox"/>	VLAN ID	VLAN Name	Type
<input type="checkbox"/>	1		Default
<input type="checkbox"/>	2	Profesores	Static
<input type="checkbox"/>	3	VoIP	Static
<input type="checkbox"/>	4	Alumnos	Static

Below the table are three buttons: 'Add...', 'Edit...', and 'Delete'.

3. Asignamos las interfaces a las diferentes VLANs:



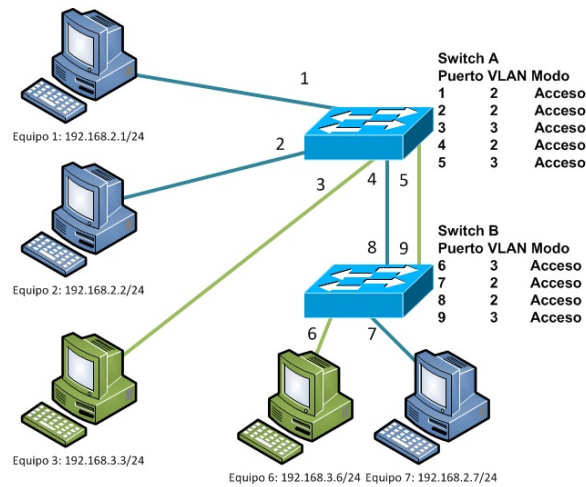
The screenshot shows the 'Port VLAN Membership Table' web interface. It includes a filter: 'Interface Type equals to Port' and a 'Go' button. The table below shows the following data:

	Interface	Mode	Administrative VLANs	Operational VLANs
<input type="radio"/>	GE1	Access	1UP	1UP
<input type="radio"/>	GE2	Access	1UP	1UP
<input type="radio"/>	GE3	Access	1UP	1UP
<input type="radio"/>	GE4	Access	1UP	1UP
<input type="radio"/>	GE5	Access	1UP	1UP
<input type="radio"/>	GE6	Access	1UP	1UP
<input type="radio"/>	GE7	Access	1UP	1UP
<input type="radio"/>	GE8	Access	1UP	1UP
<input type="radio"/>	GE9	Access	2UP	2UP
<input type="radio"/>	GE10	Access	2UP	2UP

At the bottom are two buttons: 'Join VLAN...' and 'Details...'.

## 2.2.- Enlaces troncales

En una red con varios switches la configuración de VLANs se complica un poco, habría que hacer una unión por cada VLAN entre los switches. En la figura el switch A, cuando recibe un dato por el puerto 1 (que pertenece a la VLAN 2) enviará este dato por el resto de puertos que pertenecen a la VLAN 2, es decir, 2 y 4 (que conecta con el switch B); de igual forma sucederá con los puertos que pertenecen a la VLAN 3. Es como si hay dos redes independientes (azul y verde). Pero esta solución supone un exceso de cableado entre switches.

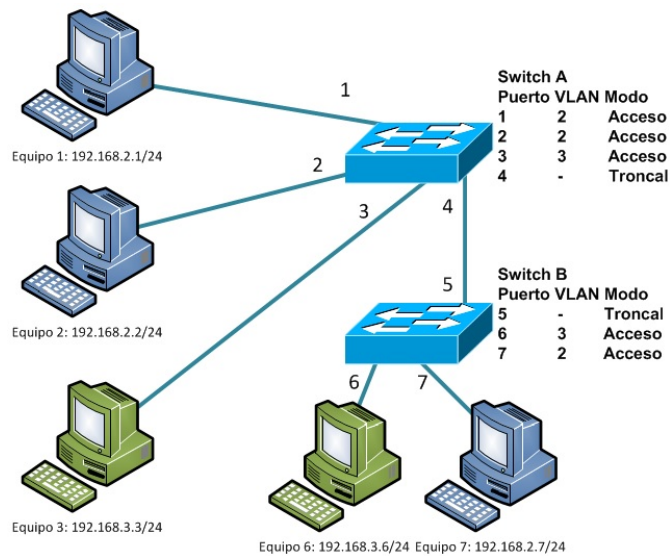


Para solucionar este problema se configura el modo de funcionamiento de cada puerto:

- **Modo Acceso.-** El puerto está asociado a una VLAN, el tráfico que llega al switch por este puerto es enviado a los demás puertos asociados a la VLAN asociada y a los puertos troncales. El tráfico llega sin etiquetar, sin información sobre la VLAN
- **Modo Troncal.-** El puerto admite tráfico de diferentes VLANs, el tráfico que llega al switch por este puerto es analizado para conocer la VLAN a que pertenece y es enviado por los puertos asociados a esa VLAN y a los puertos troncales. El tráfico en principio llega etiquetado, pero en switches más modernos se admite que si no tiene etiqueta es asignado a una VLAN, la VLAN nativa.

Aunque estos son los dos modos de funcionamiento básicos, los fabricantes suelen incluir otros tipos como general o personalizados que permiten combinaciones de tráfico etiquetado de diferentes VLANs o no etiquetado, e indicar que tipo de tráfico se admite y cual no.

Por tanto en la configuración de VLANs hay que tener en cuenta un parámetro más: Indicar si el puerto es troncal o de acceso. El esquema de red anterior con este planteamiento quedará:



### Reflexiona

¿Tiene sentido un enlace troncal en un puerto si solo disponemos de un único switch y elementos finales?

Mostrar retroalimentación

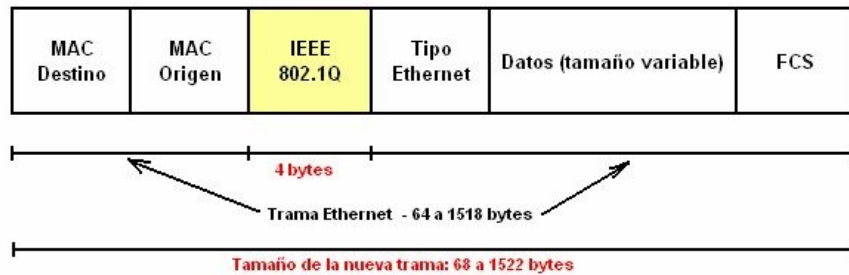
No, puesto que un enlace troncal se usaría si por una de las conexiones del switch en concreto hubiera elementos de diferentes VLANs, pero para ello en esa conexión debería estar conectado otro switch.

## 2.3.- Etiquetado de tramas. Protocolo IEEE802.1Q

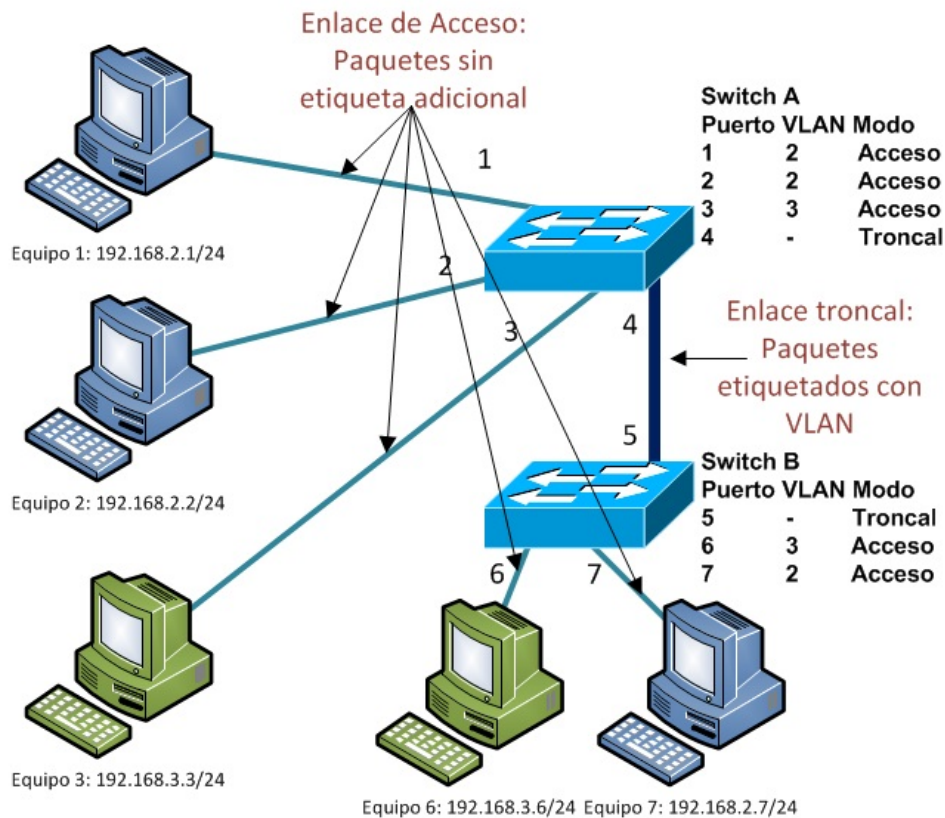
Como se indicó anteriormente, cuando en una determinada conexión se pretende que puedan viajar paquetes de diferentes VLANs se debe establecer esta conexión como troncal.

Para distinguir la VLAN a la que pertenecen los paquetes es necesario manipular estos paquetes e incluir el código de VLAN al que pertenece. Esto es lo que se conoce como etiquetado IEEE 802.1Q o dot1Q, su función es poder compartir un canal entre diferentes redes. Es el estándar que deben cumplir todos los dispositivos de interconexión que soportan VLAN.

ESTRUCTURA DE LA TRAMA IEEE 802.1Q



El etiquetado consiste en que cuando un paquete entra en un canal troncal, se manipula y se le añade la información de la VLAN a la que pertenece, cuando el paquete sale del canal, es analizado para comprobar su VLAN, manipulado para eliminar la etiqueta dot1Q y enviado a los puertos de esa VLAN.



## 2.4.- VLAN nativa, administrativa y predeterminada

En los puertos troncales se pueden recibir paquetes sin etiquetar, en tal caso, como no se conoce la VLAN a la que pertenecen se les asigna una VLAN por defecto, esta es la VLAN nativa.

Para que todo funcione correctamente a ambos lados de un cable troncal deben de coincidir el número de VLAN nativa.

Al iniciar algunos switches nos podemos encontrar con una configuración como la de la imagen:

Port VLAN Membership Table				
Filter: <i>Interface Type</i> equals to <input type="text" value="Port"/> <input type="button" value="Go"/>				
	Interface	Mode	Administrative VLANs	Operational VLANs
<input type="radio"/>	GE1	Trunk	1UP	1UP
<input type="radio"/>	GE2	Trunk	1UP	1UP
<input type="radio"/>	GE3	Trunk	1UP	1UP
<input type="radio"/>	GE4	Trunk	1UP	1UP
<input type="radio"/>	GE5	Trunk	1UP	1UP
<input type="radio"/>	GE6	Trunk	1UP	1UP
<input type="radio"/>	GE7	Trunk	1UP	1UP
<input type="radio"/>	GE8	Trunk	1UP	1UP

Esta configuración nos indica que en un principio todos los puertos están en la VLAN 1 pero no están en modo acceso sino en modo troncal porque todo lo que llega sin etiquetar se asigna a la VLAN nativa.

La VLAN administrativa es una VLAN que se utiliza para fines de configuración del switch

La VLAN predeterminada es la VLAN a la que pertenecen todos los puertos cuando aún no se les ha asignado una VLAN en concreto, normalmente la VLAN 1.

### Reflexiona

Si queremos crear 3 VLANs en una empresa ¿podríamos usar la VLAN 1 para una de ellas?

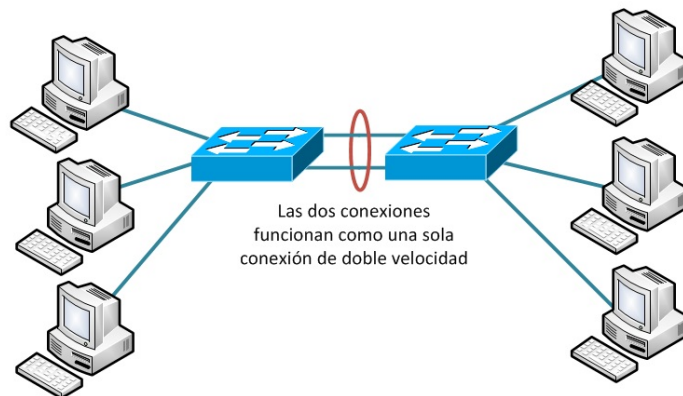
Si, podríamos, pero no es aconsejable porque de entrada todos los puertos están en la VLAN predeterminada y si al crear las VLANs no programamos algunos puertos estos ya, de entrada, estarán en una de las VLANs. Es decir, los puertos que no programemos pueden ser asignados de forma no deseada a la VLAN 1.



### 3.- Agregación de enlaces. Protocolo IEEE802.3ad

---

La agregación de enlaces (protocolo IEEE802.3ad) consigue utilizar varios enlaces entre dos dispositivos como si se tratase de un único enlace, es una forma muy económica de realizar un enlace de alta velocidad.



Una vez configurados los dos switches del esquema correctamente para la agregación de enlaces estos utilizarán los dos cables que les unen como una sola conexión al doble de velocidad, con lo cual el protocolo STP no anulará ningún bucle de datos.

## 4.- 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)

## 4.1.- Routers en las LAN

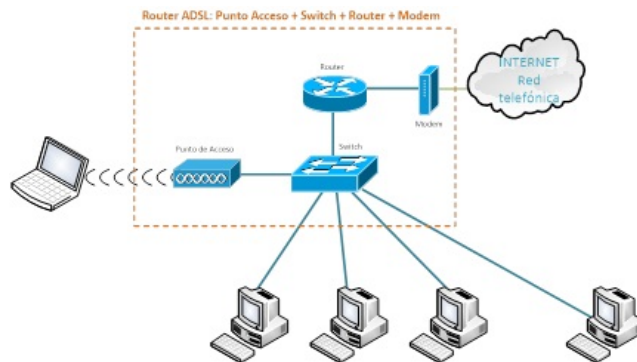
Se caracterizan en que todos usan la técnica NAT porque separan una red privada (donde están los PCs) de una red pública (la del proveedor de servicios de internet, ISP). Como cualquier router tiene una CPU, memoria y un sistema operativo. Estos sistemas operativos suelen estar basados en Linux.

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



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.

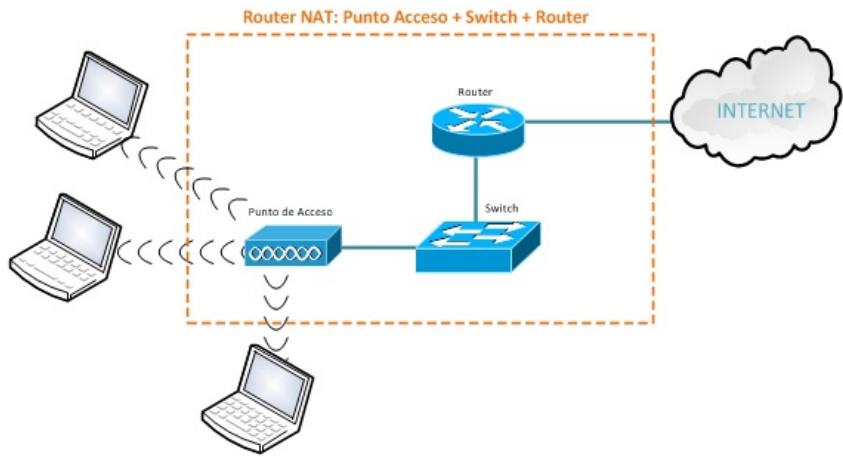
**Router de Fibra**, es exactamente igual al anterior pero sustituimos el modem por el ONT, es decir, cambia el dispositivo que transforma la señal porque en este caso llegaría la señal por un cable de fibra en vez de por un cable RJ11.

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

Sin modem, **router-NAT**:



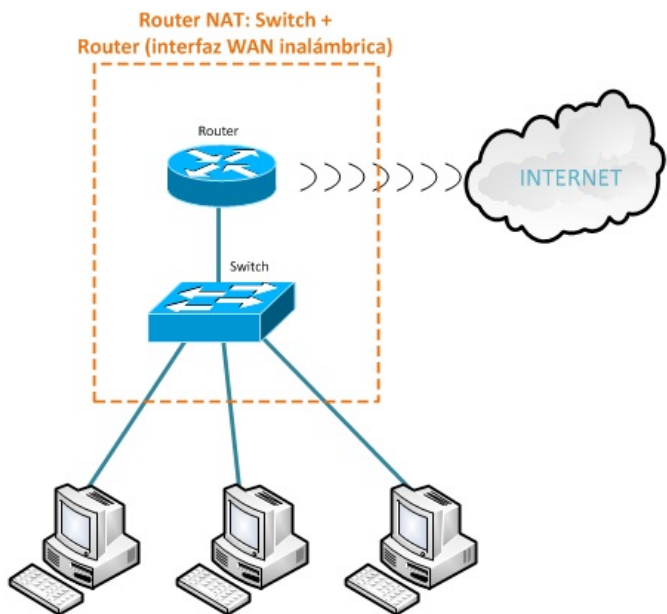
En este caso cambia el tipo de conexión WAN de RJ-11 (cable telefónico) a RJ-45 (cable de red), el esquema del dispositivo multifunción sería:



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.

## 4.2.- Routers 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.

### Autoevaluación

Entre los componentes de un router está:

- Pantalla
- CPU
- Teclado
- Lector CD

Incorrecto

Correcto

Incorrecto

Incorrecto

### Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

# 4.3.- 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.



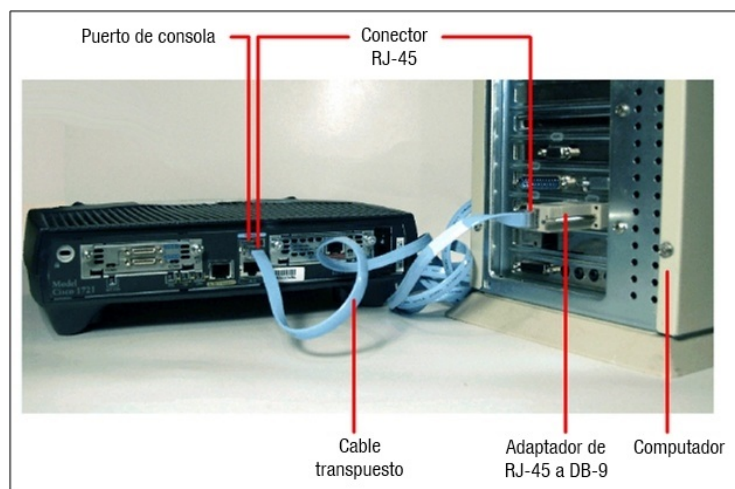
## 4.3.1.- Conexión al router vía puerto de consola.

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.





## 4.3.2.- Conexión al router vía SSH o Telnet

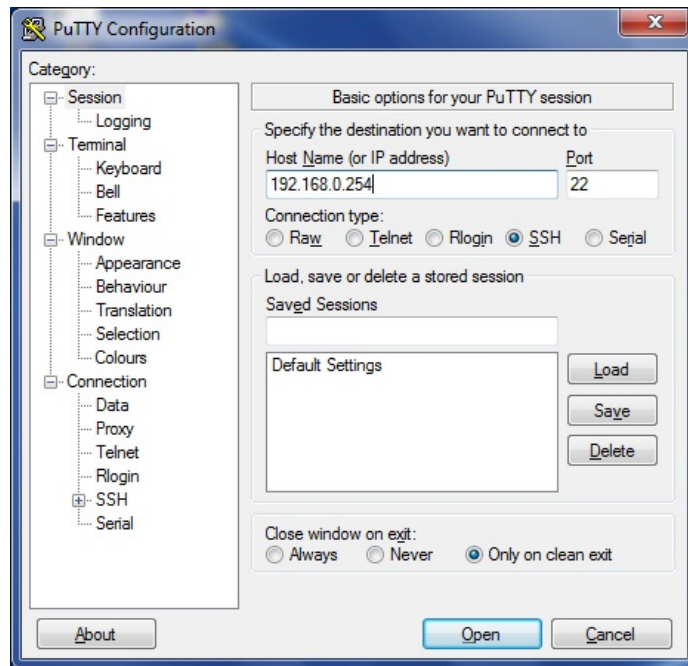
Otra forma de acceder a los routers es a través de la línea de comandos con los protocolos telnet o SSH. Esta forma no es muy habitual en routers domésticos como los mencionados en apartado los routers en las LAN.

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   cwmpp
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
pptp         script       snmp         snmp software
system       systemlog    upnp         user wireless

_{root}>=
```

## Autoevaluación

El proceso de conexión con SSH:

- Tenemos que conocer la IP del router

- Es habitual en routers domésticos
- Muestra una web para configuración

Opción correcta

Incorrecto

Incorrecto

## Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

## 4.3.3.- 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](#) [Cisco](#)

### Para saber más

Actualmente, todos nuestros routers domésticos se configuran por vía web. Los pasos para acceder a esta configuración:

- Comprobar cual es la IP de nuestra puerta de enlace
- Teclear esta IP en el navegador
- Introducir las credenciales (suelen venir anotadas en el router)

## 4.4.- Configuración y administración del router

---

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.

## 4.4.1.- 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:

Firmware: DD-WRT v24-sp2 (03/25/13) std  
Hora: 10:08:48 up 38 min, load average: 0.23, 0.14, 0.09  
WAN IP: 172.23.160.210

Configuración Inalámbrico Servicios Seguridad Restricciones de Acceso NAT / QoS Administración Estado

Config Básica DDNS Clonar Dirección MAC Ruteo Avanzado Redes Tunnel EoIP

**Config Internet**

Tipo de Conexión a Internet

Tipo de Conexión: IP Estática

Dirección IP de Internet: 172.23.160.210

Máscara de Subred: 255.255.255.0

Puerta de Enlace: 172.23.160.15

DNS Estática 1: 80.58.61.250

DNS Estática 2: 80.58.61.254

DNS Estática 3: 0.0.0.0

**Config Opcional**

Nombre del Router: router-asis1

Nombre del Host: asis1

Nombre del Dominio:

MTU: Auto 1500

STP:  Activar  Desactivar

**Ayuda** más...

**Configuración Automática - DHCP:**  
Este valor de configuración es más común verlo en la mayoría de los operadores de cable.

**Nombre del Host:**  
Introducir el nombre de host designado por tu ISP (Proveedor de Internet).

**Nombre del Dominio:**  
Introducir el nombre de dominio designado por tu ISP.

**IP Local (LAN):**  
Esta es la dirección del router.

**Máscara de Subred:**  
Esta es la máscara de subred del router.

**Servidor DHCP:**  
Permite al router administrar tus...

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.

Firmware: DD-WRT v24-sp2 (03/25/13) std  
Hora: 10:20:44 up 50 min, load average: 0.00, 0.03, 0.05  
WAN IP: 172.23.160.210

Configuración Inalámbrico Servicios Seguridad Restricciones de Acceso NAT / QoS Administración Estado

Administración Keep Alive Diagnósticos WOL Valores de Fábrica Actualización Backup

**Administración Router**

Clave del Router

Usuario del Router: \*\*\*\*\*

Clave del Router: \*\*\*\*\*

Re-introducir Clave: \*\*\*\*\*

**Acceso Web**

Protocolo:  HTTP  HTTPS

Auto-Refresco (en segs): 3

Activar la página Info:  Activar  Desactivar

**Ayuda** más...

**Auto-Refresco:**  
Ajusta el intervalo de actualización automática de la interfaz gráfica de la web (Web GUI). El valor 0 deshabilita esta función por completo.

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.

Firmware: DD-WRT v24-sp2 (03/25/13) std  
Hora: 11:51:20 up 2:21, load average: 0.04, 0.04, 0.04  
WAN IP: 172.23.160.210

Configuración Inalámbrico Servicios Seguridad Restricciones de Acceso NAT / QoS Administración Estado

Config Básica SuperChannel Seguridad Inalámbrica Filtrado MAC WDS

**Interfaz física WIFI ath0 [2.4 GHz]**

Interfaz Física ath0 - SSID [rtuyuu] HWAddr [B0:48:7A:E2:46:13]

Modo Inalámbrico: AP

Modo de Red WIFI: Desactivado

Anchura de canal: Completo (20 MHz)

Nombre de Red WIFI (SSID): redwifi

Broadcast SSID Inalámbrico:  Activar  Desactivar

Configuración Avanzada:

**Interfaz virtual**

Añadir

Guardar Config. Aplicar Configuración Cancelar Cambios

**Ayuda** más...

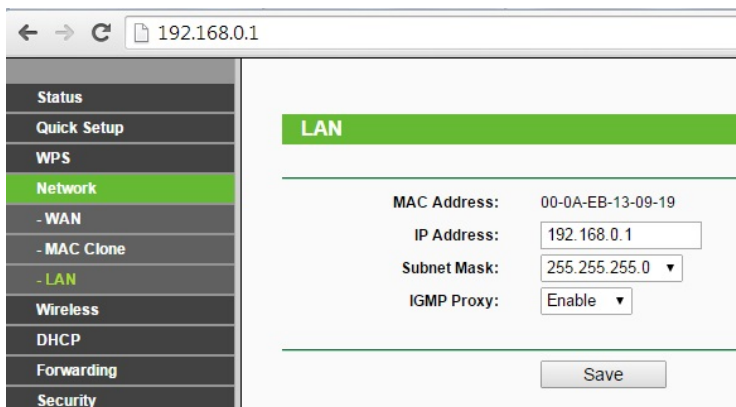
**Modo de Red WIFI:**  
Si deseas que excluyas a los clientes Wireless-G, debes elegir el modo *Solo-B*. Si lo que quieres es deshabilitar el acceso inalámbrico (cualquiera) debes escoger *Desactivar*.

**Rango Sensibilidad:**  
Ajusta el Tiempo de ACK (acknowledgement - reconocimiento). 0 deshabilita el Tiempo de ACK timing completamente.

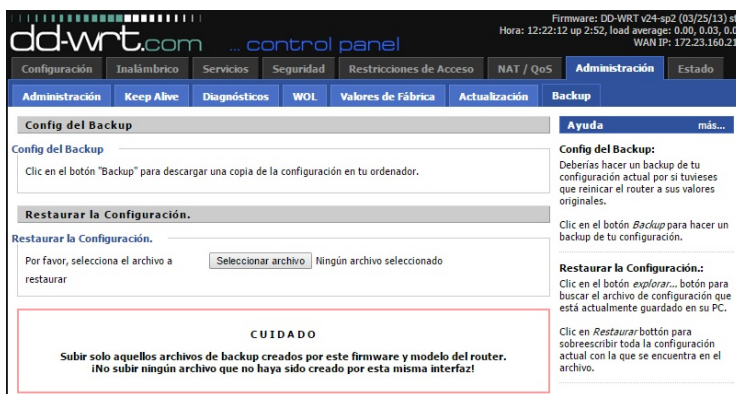
- PPP, es usado en varios tipos de redes físicas como cable serial, línea telefónica, telefonía móvil. PPP también es usado en las conexiones de acceso a internet. Los ISP han usado PPP para que accedan a internet los usuarios de línea telefónica:

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:

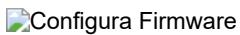


Hacer una copia de seguridad de la configuración:



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:



## 5.- Enrutamiento

Como vamos viendo hay una gran cantidad de opciones de configuración que tiene un router. Pero lo más interesante de los routers está por llegar. La principal función de un router es enrutar, es decir, dirigir el tráfico de internet.

El enrutamiento en redes consiste en encontrar el camino por el que deben ir los datos de un origen a un destino.

Todos los dispositivos toman estas decisiones, en nuestro PC hay una tabla de enrutamiento, que puede ser mostrada con el comando netstat -r, route, o route PRINT.

```
Administrador: C:\Windows\system32\cmd.exe
=====
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
0.0.0.0             0.0.0.0             192.168.0.254       192.168.0.76  266
127.0.0.0           255.0.0.0           En vínculo           127.0.0.1     306
127.0.0.1           255.255.255.255     En vínculo           127.0.0.1     306
127.255.255.255     255.255.255.255     En vínculo           127.0.0.1     306
192.168.0.0         255.255.255.0       En vínculo           192.168.0.76  266
192.168.0.76       255.255.255.255     En vínculo           192.168.0.76  266
192.168.0.255      255.255.255.255     En vínculo           192.168.0.76  266
224.0.0.0           240.0.0.0           En vínculo           127.0.0.1     306
224.0.0.0           240.0.0.0           En vínculo           192.168.0.76  266
255.255.255.255     255.255.255.255     En vínculo           127.0.0.1     306
255.255.255.255     255.255.255.255     En vínculo           192.168.0.76  266
=====
Rutas persistentes:
Dirección de red    Máscara de red      Dirección de puerta de enlace  Métrica
0.0.0.0             0.0.0.0             192.168.0.254                 Predeterminada
=====
```

En este caso, aunque pueda parecer muy complicada nos indica que en principio todo (0.0.0.0) se envía a la puerta de enlace (192.168.0.254) excepto lo que se detalla en las líneas siguientes:

- 127.0.0.0 es una dirección especial que se refiere a nuestro propio equipo
- 192.168.0.0/24 es nuestra red, en tal caso, no se envía a la puerta de enlace porque no tiene que salir al exterior.
- Resto de direcciones especiales.

Enrutamiento en el router: Un router conecta múltiples redes. Esto significa que tiene varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz usar para enviar el paquete hacia su destino. La interfaz que usa el router para enviar el paquete puede ser la red del destino final del paquete (la red con la dirección IP de destino de este paquete), o puede ser una red conectada a otro router que se usa para alcanzar la red de destino.

Cuando un router recibe un paquete, examina su dirección IP de destino y:

1. Si la dirección IP de destino no pertenece a ninguna de las redes del router conectadas directamente, el router debe enviar este paquete a otro router.
2. Si no es así se busca en la tabla de enrutamiento y si la ruta que coincide con la red de destino del paquete es una red remota, el paquete es reenviado a la interfaz indicada, encapsulado por el protocolo de la Capa 2 y enviado a la dirección del siguiente salto.
3. Si la tabla de enrutamiento no contiene una entrada de ruta más específica para un paquete que llega, el paquete se reenvía a la interfaz indicada por la ruta default, si la hubiere
4. Si, en cualquier router, no se encuentra una ruta para la red de destino en la tabla de enrutamiento y no existe una ruta default, ese paquete se descarta.

Los routers en una tabla de enrutamiento tienen cuatro características principales:

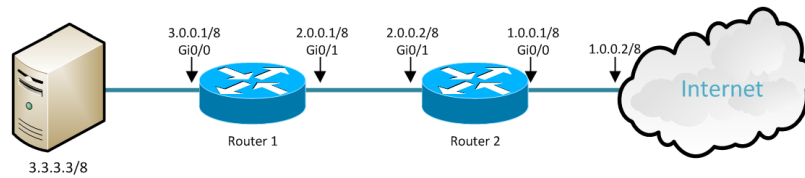
- Red de destino
- Máscara de red de destino
- IP del siguiente salto (puerta de enlace) o interfaz para su envío
- Coste de la ruta o métrica (se da preferencia a las métricas inferiores)

En una tabla de enrutamiento nos varios tipos de rutas:

1. A redes conectadas directamente (el router las añade automáticamente, las conoce porque cada una de sus interfaces tiene asignada IP y máscara)
2. A redes asignadas manualmente o estáticas
3. A redes aprendidas del entorno o dinámicas

## Ejercicio Resuelto

Tenemos el siguiente esquema de red:



¿Cuál sería la ruta para ir desde el PC a internet?

¿Cuál sería la ruta para ir desde el Router 1 a internet?

Se trata de buscar el siguiente salto o paso

Mostrar retroalimentación

El problema del enrutamiento siempre se soluciona buscando el paso o salto siguiente, no es cuestión de buscar todos los pasos para llegar a un destino.

Así para ir a internet desde el PC a internet el salto que hay que dar (la información debe enviarse a) es 3.0.0.1. Una vez llegue a este punto la información el router 1 se encargará de decidir el siguiente paso.

Para ir a internet desde el router 1 el siguiente salto será 2.0.0.2



## 5.1.- Rutas estáticas

---

Como ya hemos visto una ruta estática es una ruta que ha sido configurada manualmente en el dispositivo.

Es similar a cuando configuramos los parámetros IP manualmente en el PC, introduciendo la IP/máscara indicamos la ruta conectada directamente e introduciendo la puerta de enlace indicamos que en caso de ser un destino diferente a nuestra red se envíe a la puerta de enlace.

En los routers domésticos ocurre algo parecido a la configuración manual del PC, es decir, nos limitamos a indicar los parámetros de la configuración IP de las interfaces WAN LAN y el dispositivo construye la tabla de enrutamiento a partir de estos datos.

## 5.2.- Rutas predeterminadas

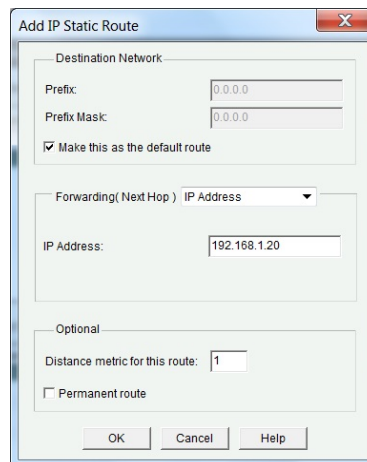
En internet existen infinidad de redes, por tanto, sería imposible indicar todas las redes en nuestras tablas de enrutamiento ya que estas serían larguísimas.

Para reducir el tamaño de estas tablas de enrutamiento se pueden resumir las redes, es decir, si varias redes consecutivas (y que formen una red superior) están por un mismo camino podemos anotar una sola entrada en la tabla de enrutamiento donde indiquemos una ruta a todas ellas.

Otra posibilidad para simplificar las tablas de enrutamiento es indicar una ruta por defecto o predeterminada de forma que cuando no hay ninguna referencia en la tabla de enrutamiento a una red se utiliza la ruta predeterminada para enviar los datos.

Para indicar la ruta predeterminada usamos la red 0.0.0.0/0 en IPv4 y la red ::/0 en IPv6

Gráficamente:



En el caso de router domésticos basta con indicar la puerta de enlace en la configuración IP de la interfaz WAN puesto que esta es la ruta por donde se van a enviar todos los paquetes con destino a cualquier red que no sea nuestra red local:



### Reflexiona

¿cuál es la ruta predeterminada de nuestro equipo?

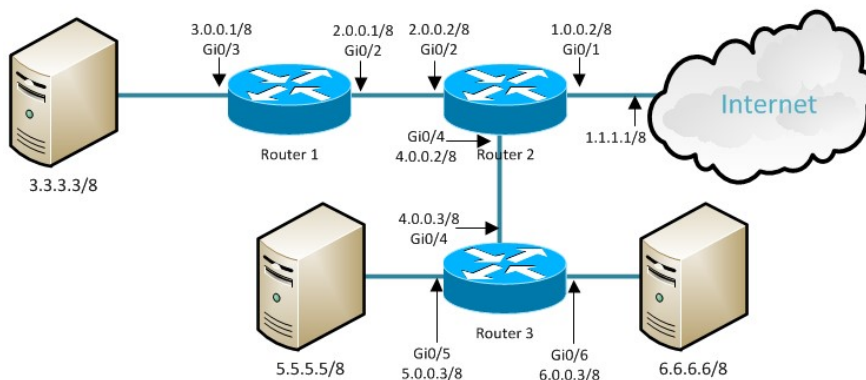
Mostrar retroalimentación

Nuestro equipo, como todo dispositivo conectado en red, tiene una tabla de enrutamiento, en este caso es muy básica:

- La información destinada a equipos de la propia red se envía directamente a cada equipo
- La información destinada a equipos de otras redes se envía a la puerta de enlace, **esta es la ruta predeterminada**

## 5.3.- Ejemplo de funcionamiento

Vamos a ver con un ejemplo como trabajan los routers, supongamos el siguiente esquema de una empresa, en la que hay 3 routers que separan varias redes dentro de la empresa (1.0.0.0/8, 2.0.0.0/8, 3.0.0.0/8, 4.0.0.0/8, 5.0.0.0/8 y 6.0.0.0/8)



Las tablas de enrutamiento de los 3 routers, donde se indica que ruta seguir en cada caso, son las siguientes:

### Router 1

Tipo de enrutamiento	Red	Interface	IP siguiente salto	Métrica
Conectada	3.0.0.0/8	Gi0/3	-	0
Conectada	2.0.0.0/8	Gi0/2	-	0
Estática	0.0.0.0/0	Gi0/2	2.0.0.2	1

### Router 2

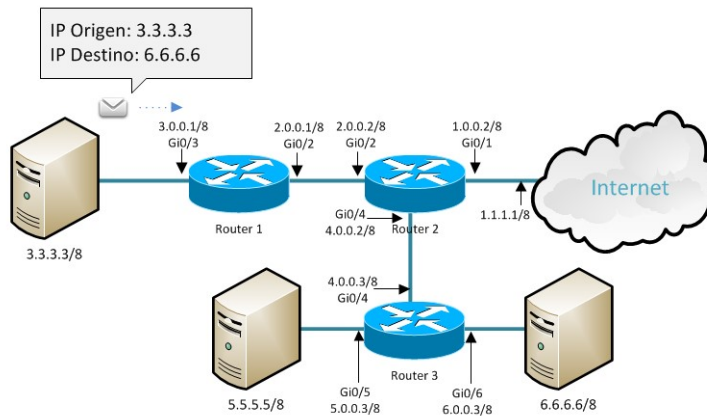
Tipo de enrutamiento	Red	Interface	IP siguiente salto	Métrica
Conectada	1.0.0.0/8	Gi0/1	-	0
Conectada	2.0.0.0/8	Gi0/2	-	0
Conectada	4.0.0.0/8	Gi0/4	-	0
Estática	3.0.0.0/0	Gi0/2	2.0.0.1	1
Estática	5.0.0.0/0	Gi0/4	4.0.0.3	1
Estática	6.0.0.0/0	Gi0/4	4.0.0.3	1
Estática	0.0.0.0/0	Gi0/1	1.1.1.1	1

### Router 3

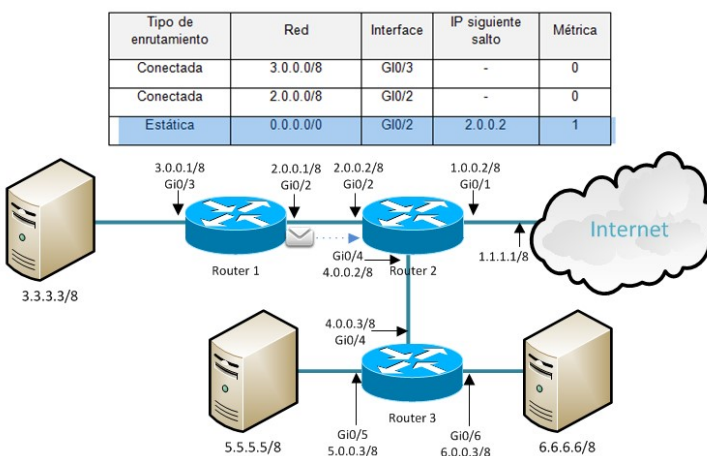
Tipo de enrutamiento	Red	Interface	IP siguiente salto	Métrica
Conectada	4.0.0.0/8	Gi0/4	-	0
Conectada	5.0.0.0/8	Gi0/5	-	0
Conectada	6.0.0.0/8	Gi0/6	-	0
Estática	0.0.0.0/0	Gi0/4	4.0.0.2	1

Supongamos que el equipo 3.3.3.3 quiere enviar un dato al equipo 6.6.6.6

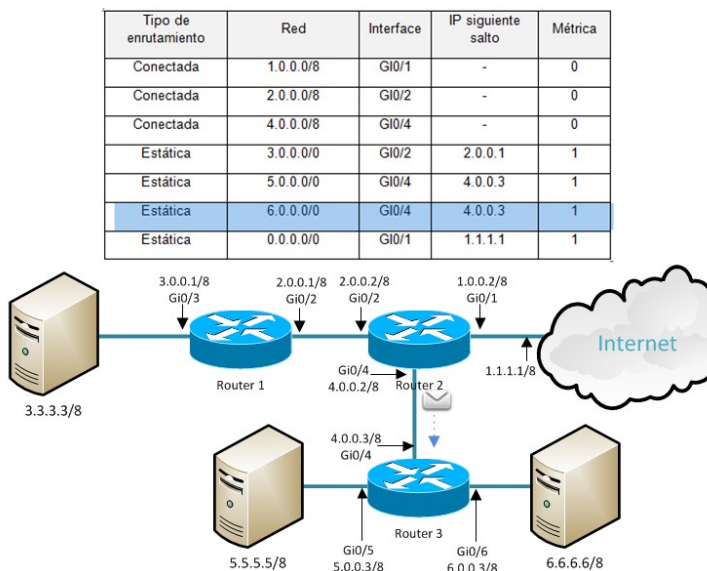
Paso 1: el equipo, como el destino no está en su red (3.0.0.0/8), envía el paquete a su puerta de enlace, el router 1.



Paso 2: El router 1 consulta su tabla de enrutamiento, como el destino es 6.6.6.6, no corresponde a ninguna de las dos primeras rutas (3.0.0.0 y 2.0.0.0), por tanto, envía el paquete a 2.0.0.2 como le indica la ruta predeterminada (0.0.0.0 = todas las rutas no indicadas).

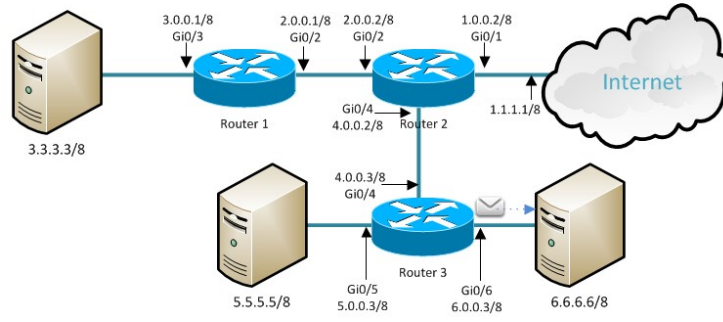


Paso 3: El router 2 busca en su tabla de enrutamiento, encuentra una ruta hacia la red 6.0.0.0, envía el paquete al siguiente salto 4.0.0.3, el router 3.



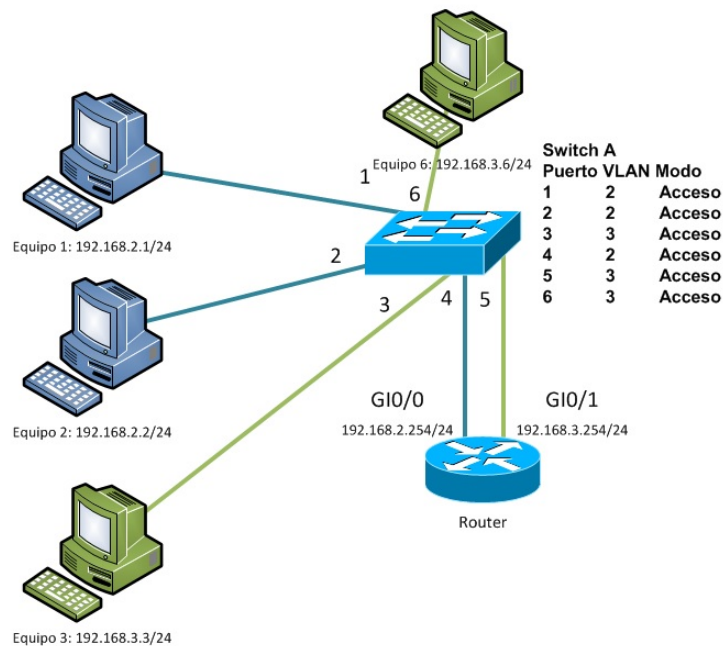
Paso 4: El router 3 busca en su tabla de enrutamiento y encuentra una ruta hacia la red 6.0.0.0, envía el paquete a su destino final.

Tipo de enrutamiento	Red	Interface	IP siguiente salto	Métrica
Conectada	4.0.0.0/8	Gi0/4	-	0
Conectada	5.0.0.0/8	Gi0/5	-	0
Conectada	6.0.0.0/8	Gi0/6	-	0
Estática	0.0.0.0/0	Gi0/4	4.0.0.2	1

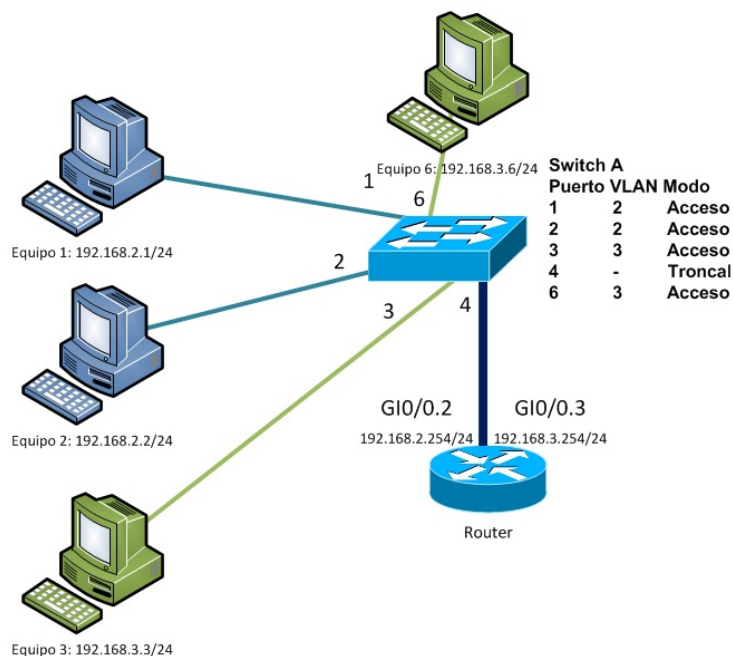


## 6.- Enrutamiento entre VLANs

En el siguiente esquema se representa como se enrutaría el tráfico entre 2 VLANs sin uso de subinterfaces (una subinterfaz es la división de una interface física en varias interfaces lógicas. En otras palabras es usar una interface real como si fueran varias interfaces diferentes), se necesitaría dos interfaces de un router, una en cada VLAN, para poder comunicar el tráfico entre las VLANs. La interface GI0/0 es la puerta de enlace de la VLAN 2 y la interface GI0/1 es la puerta de enlace de la VLAN 3.



Con el uso de subinterfaces el esquema quedará con una interface GI0/0 que se divide en dos subinterfaces GI0/0.2 y GI0/0.3. Como se puede observar el puerto 4 pasa a ser troncal, es decir, los paquetes enviados por este cable serán etiquetados con el número de VLAN al que pertenecen (2 o 3), en el router estos paquetes serán analizados para comprobar a que VLAN pertenecen y asociarlos a VLAN correspondiente.



¿Y después de haber realizado las VLANs y separar en dos redes, para que comunicaras?

Pues, aunque el objetivo de las VLANs es separar los dispositivos en bloques independientes, al comunicar las redes a través de un router se pueden aplicar diferentes políticas de acceso en router para determinar que dispositivos y que aplicaciones tienen acceso entre las VLANs, de forma que en el router se puede controlar la red.

# Anexo. Licencia de Recursos

## Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: Petr Josef Pár Licencia: CC0 1.0 Universal (CC0 1.0) Procedencia: <a href="https://www.publicdomainpictures.net/es/view-image.php?image=93744&amp;picture=redes">https://www.publicdomainpictures.net/es/view-image.php?image=93744&amp;picture=redes</a>		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: jedno urządzenie Licencia: CC0 1.0 Universal (CC0 1.0) Procedencia: <a href="https://digileaks.pl/2111-tp-link-td-w8970-jedno-urzadzenie-wiele-funkcji/">https://digileaks.pl/2111-tp-link-td-w8970-jedno-urzadzenie-wiele-funkcji/</a>		Autoría: Desconocido Licencia: Dominio público Procedencia: <a href="https://www.cisco.com/c/en/us/support/routers/7206vvr-router/model.html">https://www.cisco.com/c/en/us/support/routers/7206vvr-router/model.html</a>
	Autoría: Asiana Licencia: CC0 1.0 Universal (CC0 1.0) Procedencia: <a href="https://sp.depositphotos.com/2933255/stock-photo-optic-cables-connected-to-router.html">https://sp.depositphotos.com/2933255/stock-photo-optic-cables-connected-to-router.html</a>		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY

