# Routing IP entre VLANs de un site

*Guillermo Pérez Trabado* *©2016-2022*

**Diseño de Infraestructuras de Redes**

**Depto. de Arquitectura de Computadores - Universidad de Málaga**

## Verificación previa del Escenario

En esta etapa ya tenemos una red de site configurada correctamente a nivel 2 del modelo OSI (Ethernet). Resumimos aquí todas las modificaciones hechas hasta el momento.

- Nuestra red tiene forma de árbol con doble raíz (core switches redundantes) y enlaces troncales duplicados para cada repartidor secundario (trunks redundantes).
- Todos los enlaces entre switches están en modo Trunk. Hay que recordar que por defecto, los switches usan en todos sus interfaces el modo **Dynamic Auto**, que implica un papel **pasivo** en la negociación del modo **trunk**. Es decir, si dos switches conectados por un enlace tienen la configuración por defecto, ninguno de ellos toma la iniciativa y el enlace queda en modo **access**. Al menos uno de ellos debe estar en modo T**runk** o **Dynamic Desirable**. Lo recomendable es que **todo core switch debe tener todos sus interfaces en modo Trunk y los switches de los repartidores secundarios deben poner sus enlaces inter-switch en modo Trunk**.
- El VTP ha sido configurado para propagar la información de VLANs a todos los switches de la red de forma que podamos transportar el tráfico de cualquier VLAN a cualquier punto de nuestro árbol. El VTP solo negocia a través de los enlaces que están en modo **trunk** y nunca en los enlaces en modo access (ver el punto anterior).
- El core switch primario ha sido configurado como root primario de STP para todas las VLANS. El core switch secundario ha sido configurado como root secundario de STP para todas las VLANs. De este modo, STP negociará una topología lógica (árbol MST) de forma que coincida con nuestro árbol físico de repartidores. Todos los terminales estarán a menos de 3 hops del core switch 1.
- Todos los switches usarán RSTP en lugar de STP para negociar rápidamente el árbol MST y modificarlo rápidamente en caso de modificación de la topología.
- Todos los switches del nivel de acceso han activado el modo PortFast para evitar negociar RSTP con los terminales (servidores y PCs).
- El edificio ha sido dividido en departamentos y a cada uno se le ha asignado una VLAN.
- Los puertos de acceso de los switches han sido configurados para conectar cada terminal a la VLAN del departamento al que pertenece.

La conclusión es que tenemos una red aislada en departamentos que funciona óptimamente a nivel 2. Sin embargo, si recordamos la red inicial, existía una sola VLAN y un servidor DHCP que asignaba sus direcciones a todos los equipos de la red. Incluso existía un servidor DNS y varios servidores de aplicaciones.

Sin embargo, ahora mismo nuestra red está dividida en VLANs aisladas ya que no existe ningún router. Eso quiere decir que:

- Los PCs no pueden ver al servidor DHCP y por tanto no pueden conseguir su configuración inicial de red.
- Si tuvieran dirección, serían incapaces de dialogar con otros equipos fuera de su VLAN, sobre todo los servidores de aplicaciones, que serán usados por varios departamentos.

Por tanto, necesitamos añadir urgentemente dos elementos:

- Un router para interconectar las VLANs.
- Un servidor DHCP en cada VLAN.

En los tutoriales realizados, ya hemos visto que el propio router puede ofrecer el servicio DHCP a cada VLAN a la que está conectado. Por tanto, el mismo equipo va a servir para todas las funciones a la vez.

## 1. Conexión del router

A la hora de conectar el router tenemos que distinguir la estructura física de su conexión a la red y la estructura lógica, que son totalmente distintas aunque están relacionadas.

### *Estructura física de la conexión*

Recuerda que un router puede tener uno o varios **interfaces físicos**. Cada interfaz físico tiene un circuito transmisor y receptor (el propio interface), un conector y un medio de transmisión que se conecta a dicho conector. Cada interfaz físico puede configurarse con una **dirección IP y una máscara** que determinan el rango de direcciones IP que pueden estar conectadas a este interfaz (**la subred** IP).

La **estructura física** de la conexión está reflejada por los cables que interconectan el router con otros equipos y por los interfaces físicos que se usan para conectar dichos cables. La capacidad de mover tráfico está determinada por el tipo de interfaz. Por ejemplo, si usamos un puerto Fast Ethernet 100BaseT, podrá mover hasta 100Mbps en cada dirección (si el puerto es FDX), mientras que un puerto 1000BaseT podrá mover hasta 1Gbps en cada dirección.

### *Estructura lógica de la conexión*

Sin embargo, en cada interfaz físico se pueden definir varios **subinterfaces o interfaces lógicos**. Para ello basta que el enlace tenga definidas varias VLANs y que cada subinterfaz use un identificador de VLAN distinto. Físicamente, todos los subinterfaces de un interfaz físico comparten el mismo enlace, por lo que compiten por los mismos recursos.

Recuerda que no hay paralelismo entre subinterfaces de un mismo interfaz físico. Tan solo se trata de una **multiplexación en el tiempo**. Los paquetes de los distintos subinterfaces se encolan en la cola de salida del único transmisor existente y los paquetes son transmitidos secuencialmente por el transmisor. Lo mismo ocurre durante la recepción. Los paquetes son recibidos secuencialmente y separados según el identificador de VLAN. Un interfaz físico que usa varios interfaces de VLAN se llama un enlace troncal (**trunk**) y puede estar conectado a un puerto de un switch (en modo trunk) o también directamente a un puerto de otro router que tenga definidos los mismos subinterfaces.

Por tanto, los subinterfaces no son más que varias **colas software** separadas que comparten una única **cola hardware** (el interfaz físico).

Sin embargo, los subinterfaces pueden ser configurados igual que los interfaces con una IP y una máscara, por lo que la configuración tanto de interfaces como de subinterfaces es idéntica.

### *Función de Forwarding*

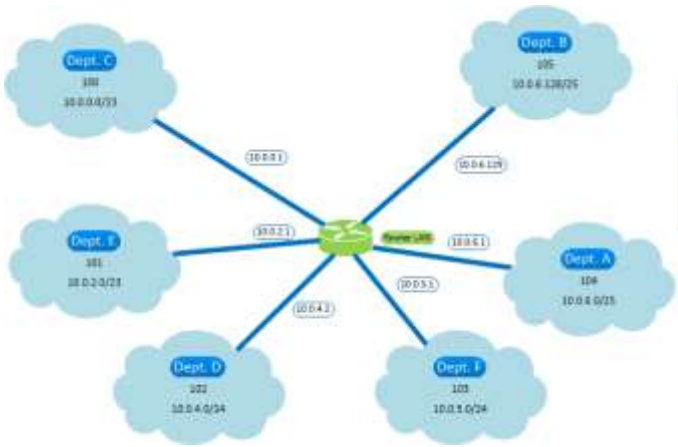
En un router se llama **forwarding** a la funcionalidad de reenviar por un interfaz un paquete que ha sido recibido por otro. Por defecto, todo interfaz (físico o subinterfaz) activo y con una IP y máscara válidas participa en el algoritmo de **forwarding** de forma homogénea.

La consecuencia más importante de ésta homogeneidad entre interfaces físicos y subinterfaces es la flexibilidad. El router hace forwarding entre todos sus interfaces independientemente del tipo de interfaz. Evidentemente, los enlaces multiplexados son mucho más flexibles para el diseño ya que si añadimos VLANs, tan solo tenemos que añadir nuevos subinterfaces, y no hay que cambiar ni el cableado ni añadir puertos físicos al router.

## 2. Diseño del router LAN de un único site

La interconexión a nivel IP de las VLANs de un solo site suele ser bastante simple, de forma que suele ser un árbol de un solo nivel. Evidentemente estamos hablando de la estructura lógica formada por el router y las VLANs de los distintos departamento.

Al ser suficiente el uso de un único router como raíz de este árbol, se denomina **"LAN router"**, debido a que su función únicamente es hacer forwarding entre distintas VLANs. Este nombre indica su contraposición al **WAN router**, que introduciremos más tarde para interconectar varios sites entre sí. El esquema lógico tendrá el aspecto siguiente:



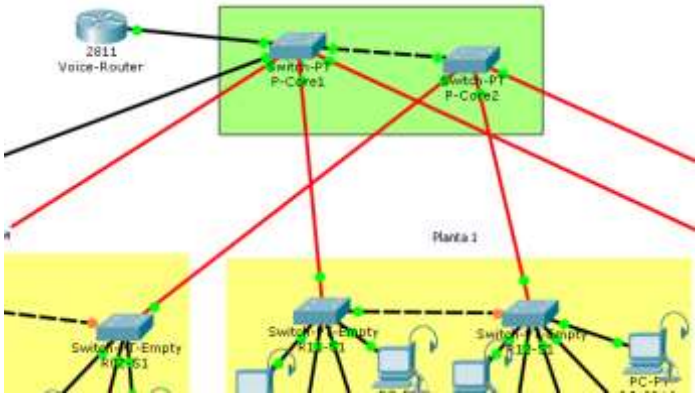

*Informe_VLANs*

| Descripción de VLAN | ID de VLAN | Nombre de VLAN | Rango IP |
|---|---|---|---|
| Fabrica | 100 | Dept. C | 10.0.0.0/23 |
| Almacén | 101 | Dept. E | 10.0.2.0/23 |
| Departamento de contabilidad | 102 | Dept. D | 10.0.4.0/24 |
| Departamento de informática | 103 | Dept. F | 10.0.5.0/24 |
| Departamento de publicidad | 104 | Dept. A | 10.0.6.0/25 |
| Departamento de dirección | 105 | Dept. B | 10.0.6.128/25 |

Cuando representamos la estructura de nuestra red a nivel IP, no estamos mostrando los equipos reales, sino la **estructura lógica** del forwarding entre VLANs. Efectivamente sabemos que una VLAN (representada por una nube azul) puede en realidad extenderse a lo ancho de varios switches, o que un router puede tener un solo interfaz físico multiplexado entre varios de subinterfaces de VLAN. El esquema lógico **no está mostrando la conectividad física**, sino lógica. El símbolo del router mostrado en el esquema lógico no es realmente un equipo físico sino una abstracción del forwarding.

Sin embargo, la estructura física de la red muestra dónde se ubica realmente el router LAN y cómo se conecta a otros equipos. Si vemos el papel central del forwarding en la estructura lógica, intuiremos que el sitio más eficiente para conectar el router LAN es al Core switch

primario ya que la distancia de todos los terminales hasta este punto es uniforme (STP ha minimizado el diámetro del MST desde este punto). Además, gracias a los enlaces en modo trunk, con un solo enlace físico el router LAN dispone de todos los subinterfaces que necesite para implementar el esquema lógico anterior.




### *Ubicación física*

Dado que el router LAN tiene un funcionalidad central crítica (raíz de un árbol de VLANs) similar a la del core switch (raíz de un árbol de switches), y que ambos deben estar interconectados, este router se ubicará en el mismo armario que el core switch. Es decir, dentro del repartidor primario, y deseablemente en el data center para protegerlo físicamente de accesos no autorizados.

### *Level 3 switches*

Dado que todo el tráfico que pasa de una VLAN a otra distinta debe pasar del Core Switch al Router LAN y luego volver otra vez al Core Switch para llegar a su destino, la conexión entre Switch y Router se convierte en un cuello de botella para el intercambio de tráfico entre VLANs. Para eliminar esta limitación, los fabricantes venden switches de gama alta llamados *Level 3 switches*, o *switches con servicios de nivel 3* y muchos otros nombres comerciales.

Lo que quiere decir esto es que es un equipo que integra las funciones de **forwarding de nivel 3** junto con las de **switching de nivel 2** en el mismo core switch. Es decir, que el mismo equipo es capaz de decidir si un paquete que entra por un puerto debe salir por otro puerto tras ser conmutado a nivel 2 dentro de la misma VLAN o bien enrutado a nivel 3 al cambiar de VLANs.

Los fabricantes de L3 switches incluyen optimizaciones con soporte hardware para acelerar las decisiones y que el Routing de nivel 3 sea tan rápido como el switching de nivel 2. Por ejemplo Cisco ofrece lo que denomina *Cisco Express Forwarding* (CEF), que incluye una cache que guarda decisiones de Routing de paquetes precedentes. Esta cache está implementada en hardware y permite encontrar la decisión que fue tomada para un paquete anterior con las mismas IPs y MACs de origen y destino de forma mucho más rápida que un algoritmo software, lo que permite enrutar paquetes a velocidades de 100Gbps.

## 3. Pasos para configurar el router LAN

***Elige en la paleta un router modelo Cisco 2811 y conéctalo a un puerto de cobre de tu Core Switch1.***

Una vez conectado el router LAN al core switch por un cable hay que configurar los interfaces para construir el esquema lógico anterior. Para ello tenemos que realizar los siguientes pasos:

- **En el core switch:**
  - Configurar el interfaz al router en modo trunk.
  - Para cada VLAN:
    - Verificar que la VLAN ya existe en el core switch.
- **En el router LAN:**
  - Activar el interfaz físico del enlace al core switch.
  - Para cada VLAN:
    - Crear el subinterfaz en la VLAN con el nombre <interfaz>.<id>
    - Definir el tipo de encapsulamiento usado por el subinterfaz como 802.1Q y asignar el identificador de VLAN.
    - Asignar la dirección IP y máscara del router en la VLAN.

La secuencia de comandos anterior **para el router** quedaría algo parecida a esto:

```
interface FastEthernet0/0
  no shutdown
interface FastEthernet0/0.100
  encapsulation dot1Q 100
  ip address 10.0.0.1 255.255.254.0
interface FastEthernet0/0.101
  encapsulation dot1Q 101
  ip address 10.0.2.1 255.255.254.0
```

## 4. Definición del servidor DHCP para cada VLAN

Una vez definidos los subinterfaces, necesitamos definir el servicio DHCP para cada VLAN ya que el router puede ofrecer este servicio sin necesidad de instalar un servidor para cada una.

Para ello tan solo hay que definir un pool para cada VLAN indicando el rango y la máscara de cada una y el router por defecto.

```
ip dhcp pool pool100
 network 10.0.0.0 255.255.254.0
 default-router 10.0.0.1
ip dhcp pool pool101
 network 10.0.2.0 255.255.254.0
 default-router 10.0.2.1
```

Con esta información, cada cliente DHCP puede obtener los tres datos fundamentales que necesita:

- Su **dirección IP** y la **máscara** que determina qué direcciones son locales.
- La **dirección IP del gateway** que permite alcanzar las direcciones que no son locales.
- También se puede añadir la dirección del servidor DNS, pero como no hemos decidido ni siquiera el rango para el Data Center, por lo que es prematuro configurarlo ahora.

Por último, no olvides configurar **y actualizar cada vez que haga falta** la lista de direcciones que el router no debe dar dinámicamente a ningún cliente. Estas son las direcciones que están ocupadas por algún equipo que no usa DHCP, como por ejemplo, el propio router, o algún servidor de la propia red que deba tener una dirección prefijada.

Por ejemplo, imagina que en la VLAN101, hay un servidor DNS cuya dirección 10.0.2.2 es estática para que todos los clientes puedan encontrarlo. El router tiene que excluir su propia dirección del pool (10.0.2.1) y la dirección del servidor DNS.

```
ip dhcp excluded-address 10.0.2.1
ip dhcp excluded-address 10.0.2.2
```

## 5. Esquema de la estructura lógica

Como puedes vez, la estructura física y la lógica son tan dispares que un plano de la estructura física de la red no permite deducir la estructura lógica.

La lista de VLANs que habíamos elaborado es una parte importante de la documentación ya que nos ha permitido sistematizar la partición de la red. Sin embargo, la lista no refleja la topología de interconexión entre las LANs y los routers. En este momento, solo hay un router y la topología es muy sencilla, pero en el momento en que haya más de un router, tendremos problemas para deducir la topología a partir de la tabla. Por tanto, es necesario mantener un **mapa de la estructura lógica**.

Para ello, vamos a usar Microsoft Visio, un programa profesional muy usado en las empresas para hacer esquemas. Este programa permite definir paletas de plantillas a medida del tipo de diagrama que vamos a hacer. Además, en Visio los símbolos tienen asociados atributos (parecidos a los de una base de datos) que permiten que el esquema además sea una base de datos.

Para hacer tu esquema descarga la plantilla de Visio que puedes encontrar en el campus virtual (GIC-DIR-EL1_LANs_v4.zip). Descomprime este directorio **debajo del mismo directorio donde estás haciendo tu diseño con Packet Tracer** de forma que mantengas unida la documentación con tu implementación. **La entrega se realizará conjuntamente**.

Una vez abierto el archivo Visio, encontrarás a la izquierda una paleta de iconos listos para usar. Cada vez que añades un icono a tu diseño, Visio abre un cuadro de datos para pedirte la información necesaria. **No te saltes el cuadro. Tu esquema no es correcto si la información está en blanco.** Sigue las instrucciones que encontrarás en el propio esquema. Cuando tengas terminado el esquema actualiza las hojas de cálculo para que muestren correctamente la información resumida del esquema.

La entrega se realiza junto con la implementación al comprimir el directorio que ahora contiene todo.

## 6. Data Center y DNS

De momento no hemos configurado los servidores ni las VLANs del data center ni el servicio DNS. No te preocupes por ellos ya que tendrán su propio apartado de configuración cada uno.