

## **UD5.3. Enrutamiento Dinámico**

### **1. Rutas dinámicas. Protocolos**

### **2. Protocolos de enrutamiento dinámico**

- 2.1. Protocolos interiores y exteriores
- 2.2. Protocolos basados en vector – distancia
- 2.3. Protocolos basados en el estado del enlace
- 2.4. Protocolos híbridos

### **3. Parámetros de un protocolo de enrutamiento dinámico**

- 3.1. Métrica
- 3.2. Equilibrado de carga
- 3.3. Bucles de enrutamiento. Time to live (TTL)
- 3.4. Distancia administrativa
- 3.5. Entradas de la tabla de enrutamiento

### **4. Protocolo RIP (Routing Information Protocol)**

### **5. Caso práctico: Configuración de RIP**

### **6. Protocolo OSPF (Open Shortest Path First)**

### **7. Caso práctico: Configuración de OSPF**

## 1. Rutas dinámicas. Protocolos

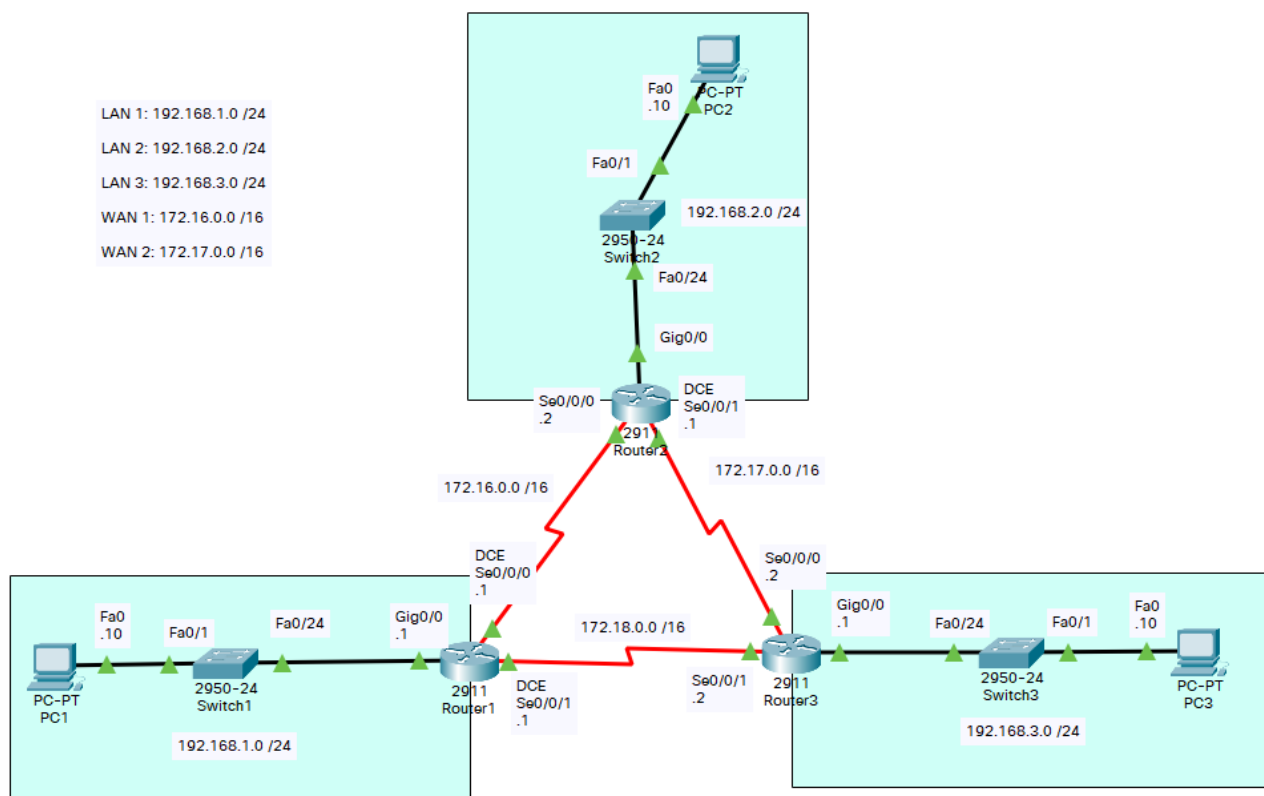


Imagen 1. Topología de ejemplo

Los protocolos de enrutamiento dinámico generalmente se usan en redes de mayor tamaño para facilitar la sobrecarga administrativa y operativa que implica el uso de rutas estáticas.

Normalmente, una red usa una combinación de un protocolo de enrutamiento dinámico y rutas estáticas, así como rutas por defecto.

En la mayoría de las redes, se usa un único protocolo de enrutamiento dinámico, sin embargo, hay casos en que las distintas partes de la red pueden usar diferentes protocolos de enrutamiento.

Uno de los primeros protocolos de enrutamiento fue el **Protocolo de información de enrutamiento (RIP)**. RIP ha evolucionado a una nueva versión, el **RIPv2**. Sin embargo, esta nueva versión no se escala a implementaciones de redes más extensas (como máximo 15 saltos).

Para abordar las necesidades de redes más amplias, se desarrollaron dos protocolos de enrutamiento avanzados: **Open Shortest Path First (OSPF)** e **Intermediate System-to-Intermediate System (ISIS)**. Cisco desarrolló el protocolo de enrutamiento de gateway interior (**IGRP**) y el IGRP mejorado (**EIGRP**), que también se adapta bien en implementaciones de redes más grandes.

Asimismo, surgió la necesidad de interconectar diferentes internetworks y proveer el enrutamiento entre ellas. El protocolo de enrutamiento de gateway fronterizo (**BGP**) ahora se usa entre los ISP, y entre ISP y sus clientes privados más grandes para intercambiar información de enrutamiento.

A fin de sostener la comunicación basada en IPv6, se han desarrollado versiones más nuevas de los protocolos de enrutamiento IPv4.

## 2. Protocolos de enrutamiento dinámico

Los objetivos de un protocolo de enrutamiento dinámico son:

- **Mejor ruta:** Es el objetivo primordial y depende del criterio escogido, que puede ser la distancia (número de saltos intermedios), ruta con menor tráfico, enlaces con mayor capacidad,...
- **Simplicidad:** Este objetivo pretende que el algoritmo utilizado no consuma grandes recursos de memoria y procesador.
- **Robustez:** El protocolo debe contener mecanismos que eviten el bloqueo ante cualquier fallo o situación inesperada, permitiendo que el router siga dando servicio.
- **Rapidez de aprendizaje:** Cuando se produce un cambio en la red, todos los routers deben conocerlo cuanto antes y modificar sus tablas para alcanzar rápidamente el estado de convergencia.

No existe un protocolo de enrutamiento dinámico que cumpla todos los objetivos de forma óptima. Lo que si hay son protocolos que se ajustan mejor que otros a determinadas situaciones.

Existen diversas características que permiten catalogar los protocolos, algunas de ellas son:

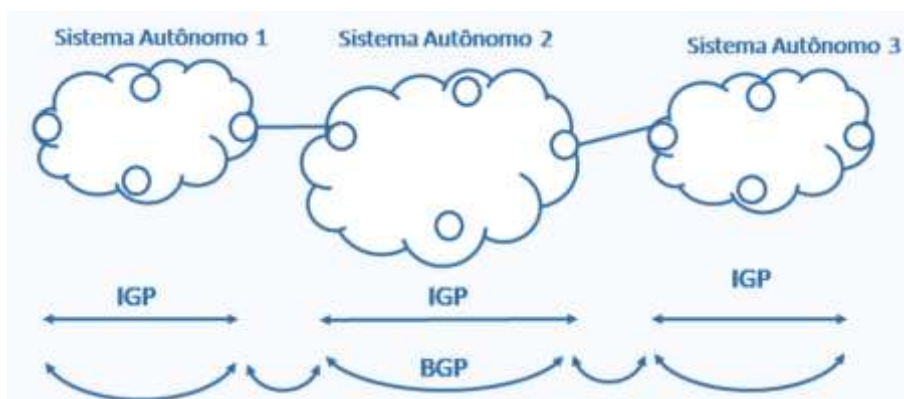
### 2.1. Protocolos interiores y exteriores

Se define un sistema autónomo (AS – Autonomous System) como una red dentro de Internet cuya administración y mantenimiento pertenece a una sola empresa, que suele ser un ISP o un organismo público.

Un sistema autónomo está perfectamente delimitado del resto de la WAN a la que pertenece. La ICANN es la encargada de identificar estos AS a través de sus registros internacionales.

Dependiendo de si un protocolo funciona dentro o fuera de un SA se clasifica en:

- **IGP** (Interior Gateway Protocol): Protocolos que funcionan dentro del ámbito de un sistema autónomo. Son los protocolos RIP, RIPv2, RIPv6, IGRP, EIGRP, OSPF, IS-IS.
- **EGP** (Exterior Gateway Protocol): Protocolos que enrutan los paquetes entre sistemas autónomos. El más importante es BGP.



## 2.2. Protocolos basados en vector - distancia

Con estos protocolos cada router se preocupa solamente de enviar información a sus vecinos más próximos, de forma que no conocen la topología del resto de la red, lo que mantiene son las distancias entre ellos.

Son protocolos lentos y fáciles de manejar, adecuados para redes con pocos equipos.

A esta familia pertenecen los protocolos **RIP, RIPv2, RIPv3 e IGRP**.

## 2.3. Protocolos basados en el estado del enlace

Estos protocolos se caracterizan por tener complejas tablas de enrutamiento que almacenan toda la topología de la red, no solo la de sus vecinos.

Cada router, con la información que recibe, confecciona un árbol jerárquico que identifica todos los destinos y los routers intermedios. Esto hace que cada router sea autónomo para calcular el siguiente salto, sea cual sea el nodo de destino. La ruta final calculada estará compuesta de las mejores rutas intermedias entre los nodos.

La ejecución de estos algoritmos exige mayores capacidades de procesamiento y memoria.

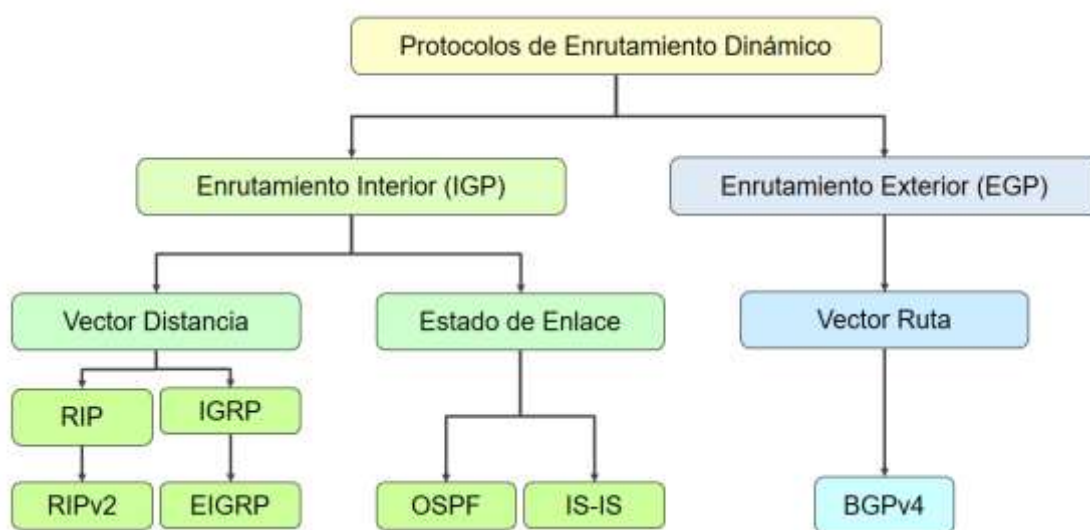
A esta familia pertenece el protocolo **OSPF**.

## 2.4. Protocolos híbridos

Se trata de una situación intermedia entre los dos anteriores.

Estos protocolos solo envían información a los demás routers cuando se produce un cambio en la topología de la red. Además utilizan métricas más sofisticadas que el simple cálculo de saltos.

A esta familia pertenecen los protocolos **EIGRP e IS-IS**.

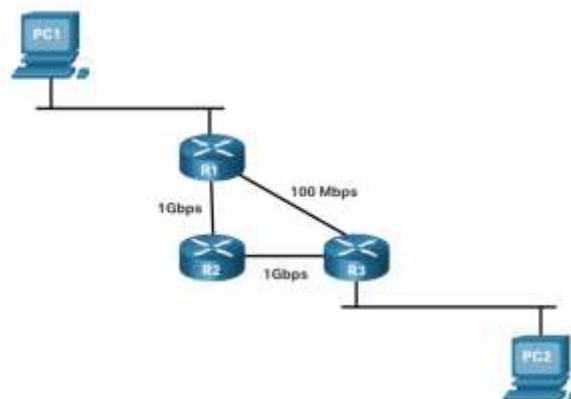


### 3. Parámetros de un protocolo de enrutamiento dinámico

#### 3.1. Métrica

Todos los protocolos dinámicos valoran, entre todas las rutas posibles a un destino, cuál es la mejor en términos de rapidez y/o fiabilidad. Esta valoración es un valor numérico cuantificable que se llama **métrica**.

Para calcular la métrica se deben tener en cuenta diversos parámetros como **número de saltos** (routers) intermedios para alcanzar el destino, **velocidad de transmisión** del enlace en bps, **tráfico del enlace** medido en número de mensajes que circulan por la ruta, **fiabilidad del enlace**, medida como la tasa de mensajes que alcanzan su destino frente a los perdidos,....



En el ejemplo anterior, para enviar un mensaje desde PC1 a PC2:

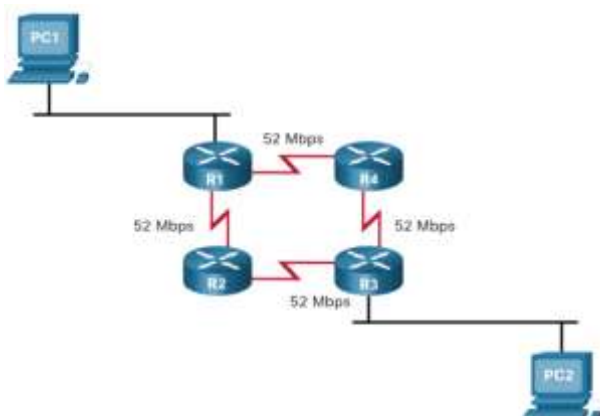
- Si elegimos el menor número de saltos, el camino sería: R1 → R3 (1 salto)
- Si elegimos la velocidad, el camino sería: R1 → R2 → R3 (1 Gbps – 1 Gbps)

#### 3.2. Equilibrado de carga

La mayoría de los protocolos dinámicos permiten incluir, en su tabla de enrutamiento, varias entradas para el mismo destino, con el mismo o distinto valor de la métrica.

De esta forma se puede lograr un equilibrado de carga (**tráfico**), porque el router envía los paquetes de forma alternativa por las distintas rutas posibles al mismo destino. Esto evita la **saturación de una ruta** y redundancia en la mejora de toda la red.

La distribución de los paquetes por las posibles rutas depende del protocolo de enrutamiento.



La comunicación entre PC1 y PC2 sería utilizando los dos enlaces alternativamente

### 3.3. Bucles de enrutamiento. Time to live (TTL)

Cuando un conjunto de routers está aprendiendo la topología de la red, puede contener en sus tablas de enrutamiento entradas incoherentes.

Hasta alcanzar el **estado de convergencia**, es decir, hasta que todas las tablas de enrutamiento de los diferentes routers contienen información consistente, se pueden dar situaciones de bucle, donde los paquetes no alcanzan su destino, sino que permanecen dando vueltas.

Para ello se establece el TTL para cada paquete transmitido. Cuando un paquete llega a un router, antes de reenviarlo por la interfaz correspondiente, disminuye el valor de su TTL en uno. Esto permite a un router descartar el paquete si su TTL tiene un valor de cero.

### 3.4. Distancia administrativa

Cuando existen distintos protocolos de enrutamiento en una red, la decisión de cuál es la ruta mejor (cuando existen varias hacia un mismo destino) se complica.

Este valor es **implícito al protocolo** utilizado. Cuanto más pequeño es el valor, más confianza ofrece el protocolo y antes es elegido.

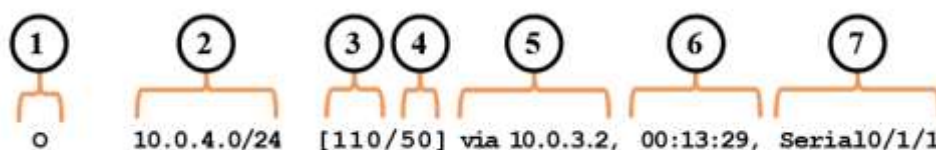
Red directamente conectada	0
Ruta estática	1
EIGRP sumarización (valor local)	5
eBGP	20
EIGRP interno	90
OSPF	110
Intermediate System - Intermediate System	115
RIP	120
EIGRP externo	170
iBGP	200

El valor de la distancia administrativa es el criterio que utiliza un router cuando dos o más protocolos ofrecen una ruta al mismo destino

### 3.5. Entradas de la tabla de enrutamiento

A modo de ejemplo, veamos la siguiente entrada:

Tabla de enrutamiento IPv4



- 1 – Indica el protocolo de enrutamiento utilizado, en este ejemplo sería OSPF
- 2 – Indica la dirección de la red remota, así como su máscara de red
- 3 – Indica la distancia administrativa, en OSPF tiene un valor de 110
- 4 – Indica la métrica, es decir, el coste para llegar al destino
- 5 – Indica la dirección del siguiente salto, es decir, la dirección IP del router siguiente para reenviar el paquete
- 6 – Indica el tiempo transcurrido desde que se descubrió la ruta
- 7 – Indica la interfaz de salida a utilizar

## 4. Protocolo RIP

---

Es un protocolo de puerta de enlace interior (**IGP** - Interior Gateway Protocol) utilizado por los routers para intercambiar información acerca de redes IP a las que se encuentran conectados.

Su algoritmo de encaminamiento está basado en el **vector distancia**, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar.

El **límite máximo** de saltos en RIP es de **15** (lo que indica el estándar), de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable.

A diferencia de otros protocolos, RIP **es un protocolo libre** es decir que puede ser usado por diferentes routers y no únicamente por un solo propietario como es el caso de los protocolos propietarios, como por ejemplo EIGRP que pertenece a CISCO Systems.

Actualmente existen 3 versiones, **RIPv1** (es un protocolo que trabaja exclusivamente con direcciones IPv4 con clase), **RIPv2** (trabaja con IPv4 y soporta subredes – CIDR y VLSM) y **RIPng** (trabaja con IPv6).

Para no tener problemas, nosotros trabajaremos con RIPv2.

Básicamente, lo que este protocolo hace es anunciar a sus vecinos las redes a las que él está conectado.

## 5. Caso práctico: Configuración de RIP

---

Vamos a trabajar con la **topología de ejemplo de la imagen 1**.

Supongamos que los tres routers pertenecen al mismo Sistema Autónomo y por tanto somos nosotros, como los administradores de la red, los que podemos y debemos hacer el enrutamiento entre ellos que consideremos mejor.

Imaginemos que son los routers de las tres sedes que mi empresa tiene en España (R1 está en Sevilla, R2 está en Madrid y R3 está en Barcelona).

Lo primero que debemos hacer es **Crear un archivo en Packet Tracer denominado "Rutas dinámicas con RIP"** y seguir los siguientes pasos:

- Implementar la red que tenemos en la **imagen 1**
- Configura el nombre de cada router con el nombre de la ciudad donde se encuentra (hostname)
- Configura las interfaces de los routers (Dir IPv4 y máscara de red)
- Configura los ETD (Dir IPv4, máscara de red y Gateway)
- Comprueba la configuración de cada uno de los routers  
`Sevilla#show running-config`
- Configura el router de Sevilla para que trabaje con RIPv2, indicando las redes que conoce.

```

Sevilla(config)#router rip
Sevilla(config-router)#version 2
Sevilla(config-router)#no auto-summary
Sevilla(config-router)#network 192.168.1.0
Sevilla(config-router)#network 172.16.0.0
Sevilla(config-router)#network 172.18.0.0

```

- g) Configura el router de Madrid para que trabaje con RIPv2, indicando las redes que conoce.
- h) Configura el router de Barcelona para que trabaje con RIPv2, indicando las redes que conoce.
- i) Guarda la configuración actual de cada uno de los tres routers (copy)
- j) Comprueba las tablas de enrutamiento de cada uno de los routers (show ip route) y determina la distancia administrativa y la métrica asignada, así como el tiempo en qué fue asignado.
- k) Vamos a comprobar si desde cada una de las LAN tenemos conectividad al resto (desde el Command Prompt):
  - ping de PC1 a PC2
  - ping de PC1 a PC3
  - ping de PC2 a PC3

```

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time=2ms TTL=126
Reply from 192.168.2.10: bytes=32 time=12ms TTL=126
Reply from 192.168.2.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 5ms

```

- l) Vamos a comprobar el camino que sigue esa conectividad, debemos asegurarnos que sigue el camino más corto:
  - tracert de PC1 a PC2
  - tracert de PC1 a PC3
  - tracert de PC2 a PC3

```

C:\>tracert 192.168.3.10

Tracing route to 192.168.3.10 over a maximum of 30 hops:

  0  0 ms    1 ms    1 ms    192.168.1.1
  1  1 ms    1 ms    2 ms    172.18.0.2
  2  *        2 ms    0 ms    192.168.3.10

Trace complete.

```

- m) Para asegurarnos de que RIP funciona, vamos a “tirar el enlace” entre Sevilla y Barcelona, para ello apaga una interfaz, por ejemplo, la interfaz de router de Barcelona que une a Sevilla.
- n) Realiza la comprobación de conectividad entre Sevilla y Barcelona, comprueba que existe con ping y después con tracert.
- o) Activa de nuevo la interfaz



## 6. Protocolo OSPF

Es un protocolo de puerta de enlace interior (**IGP** - Interior Gateway Protocol) utilizado por los routers para intercambiar información acerca de redes IP a las que se encuentran conectados y el estado de sus enlaces.

El protocolo OSPF es un protocolo de enrutamiento de **estado de enlace** que se desarrolló como una alternativa al Protocolo de Información de Enrutamiento del Vector de Distancia (RIP).

RIP fue un protocolo de enrutamiento aceptable en los primeros días de las redes e Internet. Sin embargo, el hecho de que RIP dependiera del conteo de saltos como única métrica para determinar la mejor ruta, rápidamente, se volvió problemático. El uso del conteo de saltos no escala bien en redes más grandes con varias rutas de distintas velocidades. El OSPF tiene ventajas significativas sobre el RIP en el sentido que **ofrece una convergencia más rápida y se escala a implementaciones de redes mucho más grandes**.

**OSPF es un protocolo de enrutamiento de estado de enlace** que utiliza el concepto de **áreas**. Un administrador de red puede dividir el dominio de enrutamiento en áreas distintas que ayudan a controlar el tráfico de actualización de enrutamiento. Un vínculo es también un segmento de red que conecta dos routers, o una red auxiliar, como una LAN Ethernet que está conectada a un único router. La información sobre el estado de un enlace se conoce como estado de enlace. Toda la información del estado del enlace incluye el prefijo de red, la longitud del prefijo y el costo.

Este módulo cubre implementaciones y configuraciones básicas de OSPF de área única.

Para poder trabajar con este protocolo, es necesario conocer lo que es la **wildcard**, que sería la inversa a la máscara de red, es decir, cambiar 0's por 1's y viceversa.

### Que es el Wildcard Cisco

Fundamentos de networking

Una máscara **Wildcard Cisco**, es una máscara de bits que indica qué partes de una dirección de IP son relevantes para la ejecución de una determinada acción.

Otra forma de decirlo es que el Wildcard es la representación de bits significativos (generalmente los bits de red) y no significativos (generalmente los bits de host), se escribe exactamente al contrario de una máscara de subred, algunos ejemplos:

**10.0.0.0 /24 mascara: 255.255.255.0 wildcard 0.0.0.255**

**192.168.1.0 /28 mascara: 255.255.255.240 wildcard 0.0.0.15**

En la parte matemática podemos usar un método abreviado que es restar la máscara de subred a 255.255.255.255 de la siguiente manera:

**Ejemplo 1: El Wildcard para la máscara de red 255.255.255.0**

255	255	255	255
— 255	255	255	0
			255

Wildcard: 0.0.0.255

**Ejemplo 2: El Wildcard para la máscara de red 255.255.255.240**

255	255	255	255
— 255	255	255	240
			15

Wildcard: 0.0.0.15

**Ejemplo 2: El Wildcard para la máscara de red 255.255.254.0**

255	255	255	255
— 255	255	254	0
		1	255

Wildcard: 0.0.1.255

## 7. Caso práctico: Configuración de OSPF

Vamos a trabajar con la **topología de ejemplo de la imagen 1**.

Supongamos que los tres routers pertenecen al mismo Sistema Autónomo y por tanto somos nosotros, como los administradores de la red, los que podemos y debemos hacer el enrutamiento entre ellos que consideremos mejor.

Imaginemos que son los routers de las tres sedes que mi empresa tiene en España (R1 está en Sevilla, R2 está en Madrid y R3 está en Barcelona).

Lo primero que debemos hacer es **Crear un archivo en Packet Tracer denominado “Rutas dinámicas con OSPF”** y seguir los siguientes pasos:

- Implementar la red que tenemos en la **imagen 1**
- Configura el nombre de cada router con el nombre de la ciudad donde se encuentra (hostname)
- Configura las interfaces de los routers (Dir IPv4 y máscara de red)
- Configura los ETD (Dir IPv4, máscara de red y Gateway)
- Comprueba la configuración de cada uno de los routers

`Sevilla#show running-config`

- El enrutamiento OSPF necesita un **Process ID** (identificador de proceso). Este ID va desde 1 hasta 65535. En este ejemplo usaremos el **Process ID 1** en todos los routers.

g) También necesitamos un **Area ID** (identificador de área) entre 0 y 4294967295. En este ejemplo usaremos el valor **Area ID 1** en todas las redes que configuremos para OSPF.

h) Configura el router de Madrid para que trabaje con OSPF, indicando las redes que conoce.

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 1
R2(config-router)#network 172.16.0.0 0.0.255.255 area 1
R2(config-router)#network 172.17.0.0 0.0.255.255 area 1
```

i) Configura el router de Sevilla para que trabaje con OSPF, indicando las redes que conoce. Mantén el mismo número de proceso (Process ID) y el mismo número de área (Area ID)

j) Configura el router de Barcelona para que trabaje con OSPF, indicando las redes que conoce. Mantén el mismo número de proceso (Process ID) y el mismo número de área (Area ID)

k) Guarda la configuración actual de cada uno de los tres routers (copy)

l) Comprueba las tablas de enrutamiento de cada uno de los routers (show ip route) y determina la distancia administrativa y la métrica asignada, así como el tiempo en qué fue asignado.

```
Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/16 is directly connected, Serial0/0/0
L       172.16.0.2/32 is directly connected, Serial0/0/0
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.17.0.0/16 is directly connected, Serial0/0/1
L       172.17.0.2/32 is directly connected, Serial0/0/1
O       172.18.0.0/16 [110/128] via 172.16.0.1, 00:03:58, Serial0/0/0
        [110/128] via 172.17.0.1, 00:03:58, Serial0/0/1
O       192.168.1.0/24 [110/65] via 172.16.0.1, 00:04:54, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/65] via 172.17.0.1, 00:03:58, Serial0/0/1
```

m) Vamos a comprobar si desde cada una de las LAN tenemos conectividad al resto (desde el Command Prompt):

- ping de PC1 a PC2
- ping de PC1 a PC3
- ping de PC2 a PC3

```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time=2ms TTL=126
Reply from 192.168.2.10: bytes=32 time=12ms TTL=126
Reply from 192.168.2.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 5ms
```

n) Vamos a comprobar el camino que sigue esa conectividad, debemos asegurarnos que sigue el camino más rápido: (Adjunta las tres capturas de pantalla)

- tracert de PC1 a PC2
- tracert de PC1 a PC3
- tracert de PC2 a PC3

```
C:\>tracert 192.168.3.10

Tracing route to 192.168.3.10 over a maximum of 30 hops:

  1  0 ms      1 ms      1 ms      192.168.1.1
  2  1 ms      1 ms      2 ms      172.18.0.2
  3  *          2 ms      0 ms      192.168.3.10

Trace complete.
```

- o) Para asegurarnos de que OSPF funciona, vamos a “tirar el enlace” entre Sevilla y Barcelona, para ello apaga una interfaz, por ejemplo, la interfaz de router de Barcelona que une a Sevilla.
- p) Realiza la comprobación de conectividad entre Sevilla y Barcelona, comprueba que existe con ping y después con tracert.
- q) Activa de nuevo la interfaz

---

Por defecto, OSPF viaja a través del camino más rápido. Si hacemos un PING desde el PC2 de MADRID hasta PC3 de BARCELONA, el tráfico irá siempre desde el router de MADRID hasta el router de BARCELONA, nunca irá por SEVILLA a no ser que el enlace entre MADRID y BARCELONA esté caído.

Pero OSPF tiene otra **característica**, cuanto **más ancho de banda** disponga un enlace, éste será prioritario **aunque el camino sea más largo**.

Vamos a configurar el ancho de banda en cada tramo con la opción de "**bandwidth**" en cada una de las interfaces, medidas en kbps.

- Vamos a **configurar el enlace entre Madrid y Sevilla** con un ancho de banda (velocidad) de 50 kbps (la idea es que sea un enlace muy lento).
- Vamos a **configurar el enlace entre Madrid y Barcelona** con un ancho de banda (velocidad) de 10000 kbps (la idea es que sean uno enlace muy rápido).
- Vamos a **configurar el enlace entre Sevilla y Barcelona** con un ancho de banda (velocidad) de 10000 kbps (la idea es que sean un enlace muy rápido).

Para configurar un enlace entre dos routers, basta con configurar la interface en uno de ellos ya que el otro ajustará su velocidad a la interface más lenta.

---

- r) Configura la interface del router de Madrid que une con Sevilla para que tenga un ancho de banda de 50 kbps.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0/0
R2(config-if)#bandwidth 50
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

- s) Configura el resto de las interfaces de los routers necesarias con las configuraciones indicadas anteriormente.
- t) Vamos a comprobar si desde cada una de las LAN seguimos teniendo conectividad al resto (desde el Command Prompt):
- ping de PC1 a PC2
  - ping de PC1 a PC3
  - ping de PC2 a PC3
- u) Vamos a comprobar el camino que sigue esa conectividad, debemos asegurarnos que sigue el camino más rápido: (Adjunta las tres capturas de pantalla)
- tracert de PC1 a PC2
  - tracert de PC1 a PC3
  - tracert de PC2 a PC3