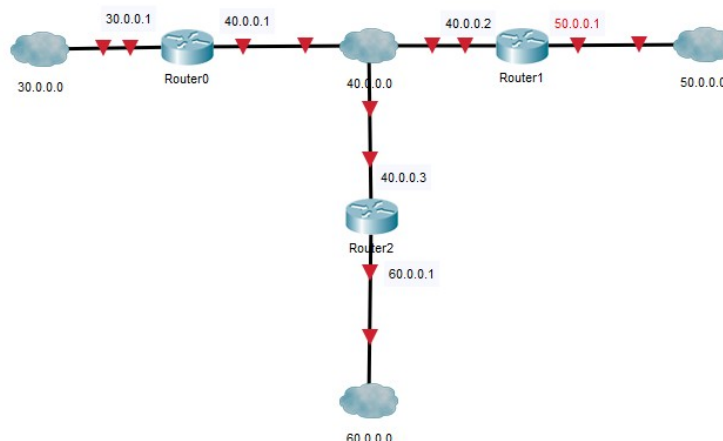


## Ejercicio 6: Tablas de enrutamiento.

a) Completa las tablas de enrutamiento estático de cada uno de los routers de esta LAN:



Como ejemplo, la tabla del Router0 se muestra ya completada. Recuerda que una tabla de encaminamiento tiene tantas filas como todas las posibles redes destino (estén cerca o lejos del router), y ha de indicarse la IP tanto de la red destino como la IP del router al cual se enviarán los datos para acercarlo a esa red destino.

Router R0		
Red destino	Máscara de subred	Siguiente salto
30.0.0.0	255.0.0.0	30.0.0.1
40.0.0.0	255.0.0.0	40.0.0.1
50.0.0.0	255.0.0.0	40.0.0.2
60.0.0.0	255.0.0.0	40.0.0.3

Las filas de esta tabla se interpretan como:

- Desde el router R0, para ir a la red 30.0.0.0, hay que enviar los paquetes a la IP 30.0.0.1 (que es una de las IP de R0 ya que él está directamente conectado a la red 30.0.0.0)
- Desde el router R0, para ir a la red 40.0.0.0, hay que enviar los paquetes a la IP 40.0.0.1 (que es una de las IP de R0 ya que él está directamente conectado a la red 40.0.0.0)
- Desde el router R0, para ir a la red 50.0.0.0, hay que enviar los paquetes a la IP 40.0.0.2 (que es la IP de R1, conectado a la red 50.0.0.0)
- Desde el router R0, para ir a la red 60.0.0.0, hay que enviar los paquetes a la IP 40.0.0.3 (que es una IP de R2, conectado a la red 60.0.0.0)

Observa bien las IP que se ponen en la columna “Siguiente salto”. Como R0 está conectado a las redes 30.0.0.0 y 40.0.0.0, solo podemos usar IP de esos rangos (por eso aparecen 30.0.0.1, 40.0.0.1, 40.0.0.2 y 40.0.0.3). No se pueden usar IP de otros rangos.

En resumen, para rellenar la columna “Siguiente salto”:

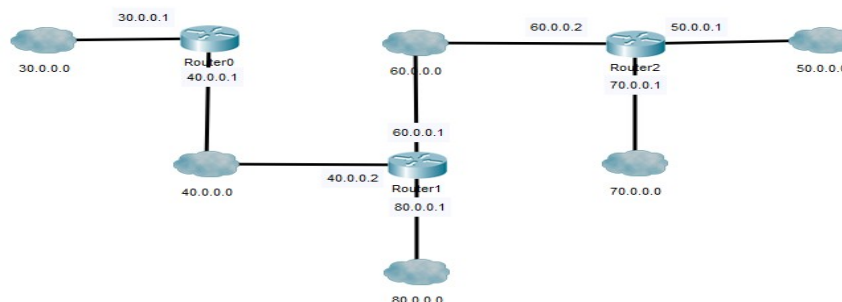
- Si el destino es una red directamente conectada al router X, el siguiente salto es la IP del router X correspondiente a la red a la que queremos ir
- Si el destino no es una red directamente conectada al router X, se pone la IP del siguiente router cercano al que saltar (teniendo en cuenta que solo podemos usar IP en los rangos que conoce el router X)

Completa ahora todas las tablas del resto de routers de la red:

Router R1		
Red destino	Máscara de subred	Siguiente salto
50.0.0.0	255.0.0.0	50.0.0.1
30.0.0.0	255.0.0.0	40.0.0.1
40.0.0.0	255.0.0.0	40.0.0.2
60.0.0.0	255.0.0.0	40.0.0.3

Router R2		
Red destino	máscara de subred	Siguiente salto
60.0.0.0	255.0.0.0	60.0.0.1
40.0.0.0	255.0.0.0	40.0.0.3
50.0.0.0	255.0.0.0	40.0.0.2
30.0.0.0	255.0.0.0	40.0.0.1

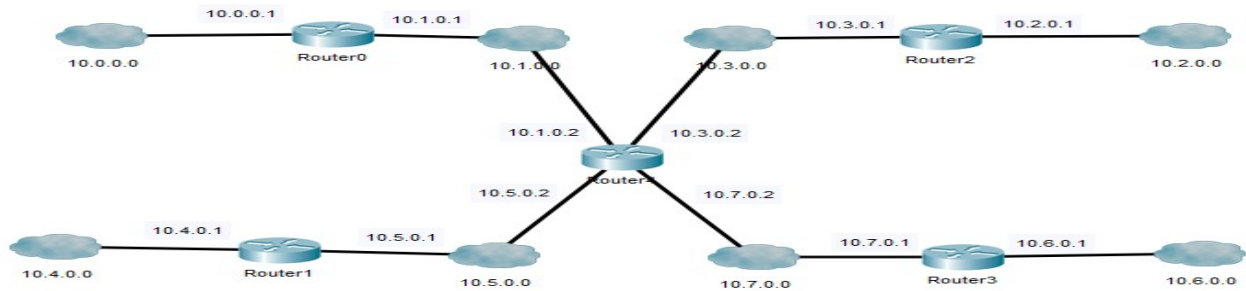
b) Escribe las tablas de enrutamiento estático de todos los routers de esta red:



**AQUÍ LA MÁSCARA DE SUBRED SERÁ 255.0.0.0**

Router 0		Router 1		Router 2	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
30.0.0.0	30.0.0.1	30.0.0.0	40.0.0.1	30.0.0.0	60.0.0.1
40.0.0.0	40.0.0.1	40.0.0.0	40.0.0.2	40.0.0.0	60.0.0.1
50.0.0.0	40.0.0.2	50.0.0.0	60.0.0.2	50.0.0.0	50.0.0.1
60.0.0.0	40.0.0.2	60.0.0.0	60.0.0.1	60.0.0.0	60.0.0.2
70.0.0.0	40.0.0.2	70.0.0.0	60.0.0.2	70.0.0.0	70.0.0.1
80.0.0.0	40.0.0.2	80.0.0.0	80.0.0.1	80.0.0.0	60.0.0.1

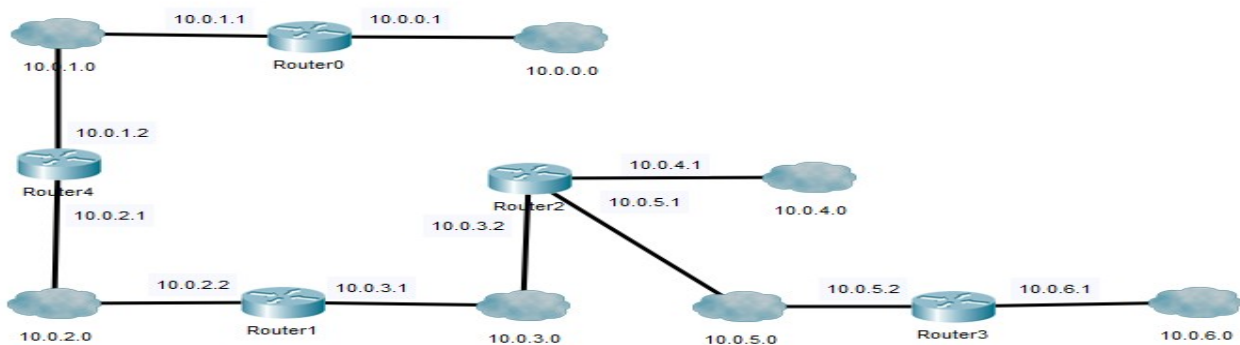
c) Escribe las tablas de enrutamiento estático de todos los routers de esta red:



AQUÍ LA MÁSCARA DE SUBRED SERÁ 255.255.0.0

Router 0		Router 1		Router 2		Router 3		Router 4	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.0.0	10.0.0.1	10.0.0.0	10.5.0.2	10.0.0.0	10.3.0.2	10.0.0.0	10.7.0.2	10.0.0.0	10.1.0.1
10.1.0.0	10.1.0.1	10.1.0.0	10.5.0.2	10.1.0.0	10.3.0.2	10.1.0.0	10.7.0.2	10.1.0.0	10.1.0.2
10.2.0.0	10.1.0.2	10.2.0.0	10.5.0.2	10.2.0.0	10.2.0.1	10.2.0.0	10.7.0.2	10.2.0.0	10.3.0.1
10.3.0.0	10.1.0.2	10.3.0.0	10.5.0.2	10.3.0.0	10.3.0.1	10.3.0.0	10.7.0.2	10.3.0.0	10.3.0.2
10.4.0.0	10.1.0.2	10.4.0.0	10.4.0.1	10.4.0.0	10.3.0.2	10.4.0.0	10.7.0.2	10.4.0.0	10.5.0.1
10.5.0.0	10.1.0.2	10.5.0.0	10.5.0.1	10.5.0.0	10.3.0.2	10.5.0.0	10.7.0.2	10.5.0.0	10.5.0.2
10.6.0.0	10.1.0.2	10.6.0.0	10.5.0.2	10.6.0.0	10.3.0.2	10.6.0.0	10.6.0.1	10.6.0.0	10.7.0.1
10.7.0.0	10.1.0.2	10.7.0.0	10.5.0.2	10.7.0.0	10.3.0.2	10.7.0.0	10.7.0.1	10.7.0.0	10.7.0.2

d) Escribe las tablas de enrutamiento estático de todos los routers de esta red:



AQUÍ LA MÁSCARA DE SUBRED SERÁ 255.255.255.0

Router 0		Router 1		Router 2		Router 3		Router 4	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.0.0	10.0.0.1	10.0.0.0	10.0.2.1	10.0.0.0	10.0.3.1	10.0.0.0	10.0.5.1	10.0.0.0	10.0.1.1
10.0.1.0	10.0.1.1	10.0.1.0	10.0.2.1	10.0.1.0	10.0.3.1	10.0.1.0	10.0.5.1	10.0.1.0	10.0.1.2
10.0.2.0	10.0.1.2	10.0.2.0	10.0.2.2	10.0.2.0	10.0.3.1	10.0.2.0	10.0.5.1	10.0.2.0	10.0.2.1
10.0.3.0	10.0.1.2	10.0.3.0	10.0.3.1	10.0.3.0	10.0.3.2	10.0.3.0	10.0.5.1	10.0.3.0	10.0.2.2
10.0.4.0	10.0.1.2	10.0.4.0	10.0.3.2	10.0.4.0	10.0.4.1	10.0.4.0	10.0.5.1	10.0.4.0	10.0.2.2
10.0.5.0	10.0.1.2	10.0.5.0	10.0.3.2	10.0.5.0	10.0.5.1	10.0.5.0	10.0.5.2	10.0.5.0	10.0.2.2
10.0.6.0	10.0.1.2	10.0.6.0	10.0.3.2	10.0.6.0	10.0.5.2	10.0.6.0	10.0.6.1	10.0.6.0	10.0.2.2

e) Ahora escribe la tabla de encaminamiento de un host para cada “nube” de cada una de las redes de a), b), c) y d). Por ejemplo, esta sería la tabla de enrutamiento del host cuya IP es 30.0.0.2, de la red del apartado a)

Las tablas de los host son muy sencillas. Un host solo está conectado a una red, por tanto, únicamente hay dos opciones: o entrega a alguien de su misma red (primera fila, entrega directa) o lo envía al router que hace de puerta de enlace (segunda fila, línea default). La IP del host (30.0.0.2) es cualquiera que pertenezca a esa red excepto la 30.0.0.1, que ya está ocupada por el router. Podríamos haber usado 30.0.0.20 o 30.0.0.18, por ejemplo. Las tablas de encaminamiento de todos los host de una misma “nube” son idénticas. Puedes imaginarte cada “nube” como un switch al que están conectados un conjunto de equipos. Para simplificar el diseño, en el enrutamiento se usan “nubes” para representar las subredes dentro de una red.

Incluye aquí la tabla de encaminamiento para cada host de cada subred de cada una de las cuatro LAN anteriores. En total, son 24 tablas.

a) **Tabla de la LAN del punto a) LA MÁSCARA DE SUBRED SERÁ 255.0.0.0**

Host 30.0.0.15		Host 40.0.0.15		Host 50.0.0.15		Host 60.0.0.15	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
30.0.0.0	directa	30.0.0.0	40.0.0.1	50.0.0.0	directa	60.0.0.0	directa
default	30.0.0.1	40.0.0.0	directa	default	50.0.0.1	default	60.0.0.1
		50.0.0.0	40.0.0.2				
		60.0.0.0	40.0.0.3				

b) **Tabla de la LAN del punto b) LA MÁSCARA DE SUBRED SERÁ 255.0.0.0**

Host 30.0.0.20		Host 40.0.0.20		Host 50.0.0.20	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
30.0.0.0	directa	30.0.0.0	40.0.0.1	50.0.0.0	directa
default	30.0.0.1	40.0.0.0	directa	default	50.0.0.1
		default	40.0.0.2		

Host 60.0.0.20		Host 70.0.0.20		Host 80.0.0.20	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
50.0.0.0	60.0.0.2	70.0.0.0	directa	80.0.0.0	directa
60.0.0.0	directa	default	70.0.0.1	default	80.0.0.1
70.0.0.0	60.0.0.2				
default	60.0.0.1				

c) Tabla de la LAN del punto c) LA MÁSCARA DE SUBRED SERÁ 255.255.0.0

Host 10.0.0.101		Host 10.1.0.101		Host 10.2.0.101		Host 10.3.0.101	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.0.0	directa	10.0.0.0	10.1.0.1	10.2.0.0	directa	10.2.0.0	10.3.0.1
default	10.0.0.1	10.1.0.0	directa	default	10.2.0.1	10.3.0.0	directa
		default	10.1.0.2			default	10.3.0.2

Host 10.4.0.101		Host 10.5.0.101		Host 10.6.0.101		Host 10.7.0.101	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.4.0.0	directa	10.4.0.0	10.5.0.1	10.6.0.0	directa	10.6.0.0	10.7.0.1
default	10.4.0.1	10.5.0.0	directa	default	10.6.0.1	10.7.0.0	directa
		default	10.5.0.2			default	10.7.0.2

d) Tabla de la LAN del punto d) LA MÁSCARA DE SUBRED SERÁ 255.255.255.0

Host 10.0.0.110		Host 10.0.1.110		Host 10.0.2.110		Host 10.0.3.110	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.0.0	directa	10.0.0.0	10.0.1.1	10.0.0.0	10.0.2.1	10.0.0.0	10.0.3.1
default	10.0.0.1	10.0.1.0	directa	10.0.1.0		10.1.0.0	
		default	10.0.1.2	10.0.2.0	directa	10.2.0.0	
				default	10.0.2.2	10.3.0.0	directa
						10.4.0.0	10.0.3.2
						10.5.0.0	
						10.6.0.0	

Host 10.0.4.110		Host 10.0.5.110		Host 10.0.6.110	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.4.0	directa	default	10.0.5.1	10.0.6.0	directa
default	10.0.4.1	10.0.5.0	directa	default	10.0.6.1
		10.0.6.0	10.0.5.2		

f) Añade a **todas** las tablas de encaminamiento obtenidas una columna nueva llamada máscara, como en el ejemplo siguiente, para que tanto routers como hosts sepan qué parte de la IP corresponde a la subred:

Router R0		
Red destino	Máscara de subred	Siguiente salto
30.0.0.0	255.0.0.0	30.0.0.1
40.0.0.0	255.0.0.0	40.0.0.1
50.0.0.0	255.0.0.0	40.0.0.2
60.0.0.0	255.0.0.0	40.0.0.3

La máscara será 255.0.0.0, 255.255.0.0 ó 255.255.255.0, dependiendo de si en las IP la parte de la subred ocupa uno, dos o tres bytes. (Este concepto será ampliado con detalle en la unidad siguiente)

(No copies y pegues todas las tablas de nuevo aquí, puedes añadir directamente la columna nueva a cada una de las tablas ya obtenidas)

g) Supongamos que en la red del apartado c) se realiza un cambio: añadir un nuevo router (Router5) entre las subredes 10.0.0.0 y 14.0.0.0. ¿Qué modificaciones habría que hacer para que las tablas de enrutamiento reflejaran este cambio? Copia aquí las tablas que han de modificarse, resaltando en amarillo las filas que han cambiado. Incluye también la tabla del nuevo router.

LA MÁSCARA DE SUBRED SERÁ 255.255.0.0					
Router 0		Router 1		Router 5	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.0.0	10.0.0.1	10.0.0.0	10.4.0.2	10.0.0.0	10.0.0.2
10.1.0.0	10.1.0.1	10.1.0.0	10.5.0.2	10.1.0.0	10.0.0.1
10.2.0.0	10.1.0.2	10.2.0.0	10.5.0.2	10.2.0.0	10.0.0.1
10.3.0.0	10.1.0.2	10.3.0.0	10.5.0.2	10.3.0.0	10.0.0.1
10.4.0.0	10.0.0.2	10.4.0.0	10.4.0.1	10.4.0.0	10.4.0.2
10.5.0.0	10.1.0.2	10.5.0.0	10.5.0.1	10.5.0.0	10.4.0.1
10.6.0.0	10.1.0.2	10.6.0.0	10.5.0.2	10.6.0.0	10.4.0.1
10.7.0.0	10.1.0.2	10.7.0.0	10.5.0.2	10.7.0.0	10.4.0.1

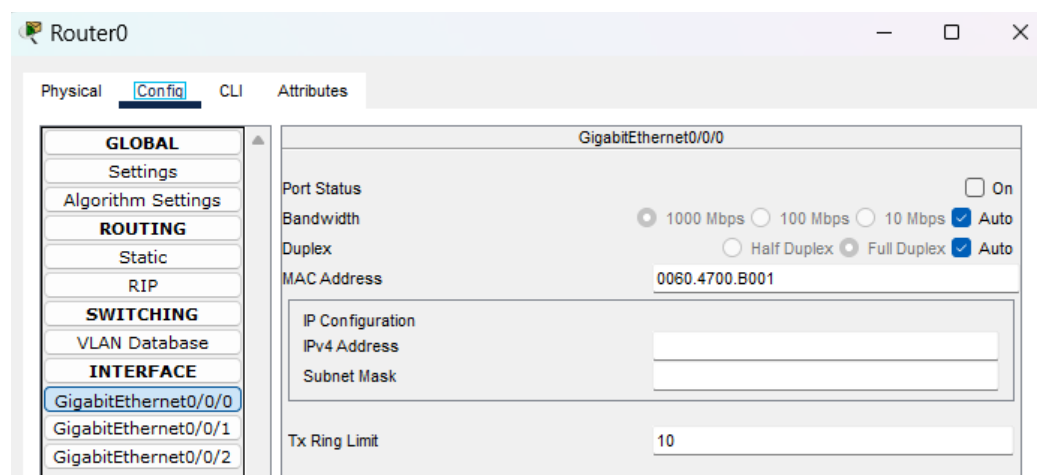
h) Supongamos que en la red del apartado d) se realizan dos cambios: añadir un nuevo router (Router5) entre las subredes 10.0.0.0 y 10.0.4.0, y eliminar el cable entre el Router2 y la subred 10.0.4.0. ¿Qué modificaciones habría que hacer para que las tablas de enrutamiento reflejaran estos cambios? Copia aquí las tablas que han de modificarse, resaltando en amarillo las filas que han cambiado. Incluye también la tabla del nuevo router.

LA MÁSCARA DE SUBRED SERÁ 255.255.255.0					
Router 0		Router 2		Router 5	
Red destino	Siguiente salto	Red destino	Siguiente salto	Red destino	Siguiente salto
10.0.0.0	10.0.0.1	10.0.0.0	10.0.3.1	10.0.0.0	10.0.0.2
10.0.1.0	10.0.1.1	10.0.1.0	10.0.3.1	10.0.1.0	10.0.0.1
10.0.2.0	10.0.1.2	10.0.2.0	10.0.3.1	10.0.2.0	10.0.0.1
10.0.3.0	10.0.1.2	10.0.3.0	10.0.3.2	10.0.3.0	10.0.0.1
10.0.4.0	10.0.0.2	10.0.4.0	10.0.3.1	10.0.4.0	10.0.4.1
10.0.5.0	10.0.1.2	10.0.5.0	10.0.5.1	10.0.5.0	10.0.0.1
10.0.6.0	10.0.1.2	10.0.6.0	10.0.5.2	10.0.6.0	10.0.0.1

## Ejercicio 7: Práctica: Enrutamiento estático y dinámico con Packet Tracer

### Parte 1: Asignación de direcciones IP a dispositivos

Para asignarle una IP y una máscara a un router, basta con seleccionarlo, ir a la sección Config, luego al apartado Interface, escoger la tarjeta de red Ethernet, y allí escribiríamos tanto la IP como la máscara del equipo (esta última suele autocompletarse con la máscara que PT cree que nos puede interesar):



Recuerda que las tarjetas de red de un router han de estar activadas para que funcionen (es decir, en "Port Status" tiene que estar marcado el On), y que un router tiene tantas tarjetas de red (y por tanto, tantas IP) como redes a las que está conectado. Podemos añadir tarjetas de red cableadas si nos hiciera falta (del mismo modo que añadíamos tarjetas de red inalámbricas en los portátiles en la unidad 5 apagando el dispositivo y seleccionando y arrastrando el módulo adecuado).

*Añade un router (dispositivo PT-Router) en PT y asígnale la IP 10.0.0.1 y máscara 255.0.0.0.*

(No es necesario que adjuntes pantallazos en este ejercicio durante las partes 1 y 2. El ejercicio a entregar está a partir de la parte 3)

De forma alternativa, asignar una IP y máscara a una conexión de un router puede configurarse también tecleando comandos en la sección CLI (Command Line Interface). Los comandos para asignar una IP a una conexión de un router son, primero, `interface` (tarjeta) y después `ip address` (direcciónIP) (máscara). Por ejemplo:

```
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 10.0.0.3 255.0.0.0
```

*Prueba desde el CLI a asignarle la IP 20.0.0.3 y máscara 255.0.0.0 a la segunda tarjeta de red del router anterior.*

Para averiguar la IP de un router no hace falta ir de nuevo a su configuración, simplemente dejando el ratón quieto unos instantes sobre el router aparecerán los nombres internos de cada tarjeta de red, y para cada una de ellas, si están activadas o no (Up/Down), su IP, su máscara en formato CIDR (por ejemplo, en lugar de 255.0.0.0 aparece /8) y su MAC:



R

Device Name: Router0

Device Model: ISR4331

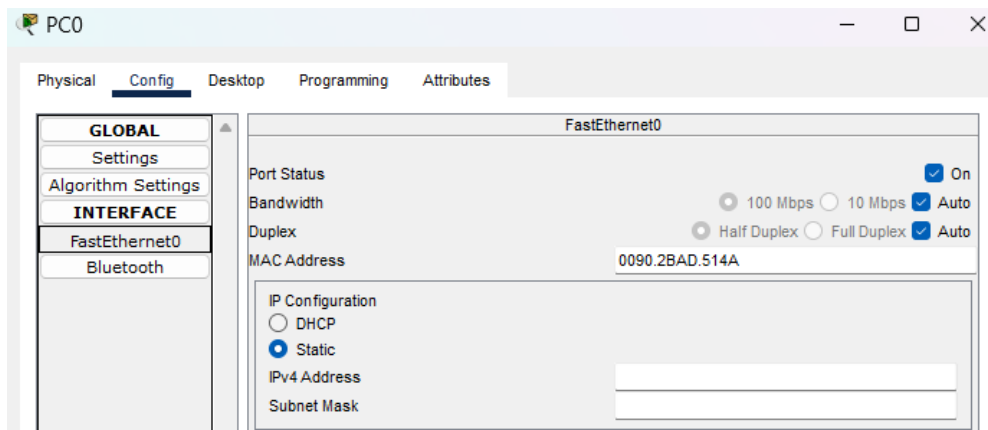
Hostname: Router

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0/0	Up	--	10.0.0.1/8	<not set>	0060.4700.B001
GigabitEthernet0/0/1	Up	--	20.0.0.3/8	<not set>	0060.4700.B002
GigabitEthernet0/0/2	Down	--	<not set>	<not set>	0060.4700.B003
Vlan1	Down	1	<not set>	<not set>	000C.CF33.E46C

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0

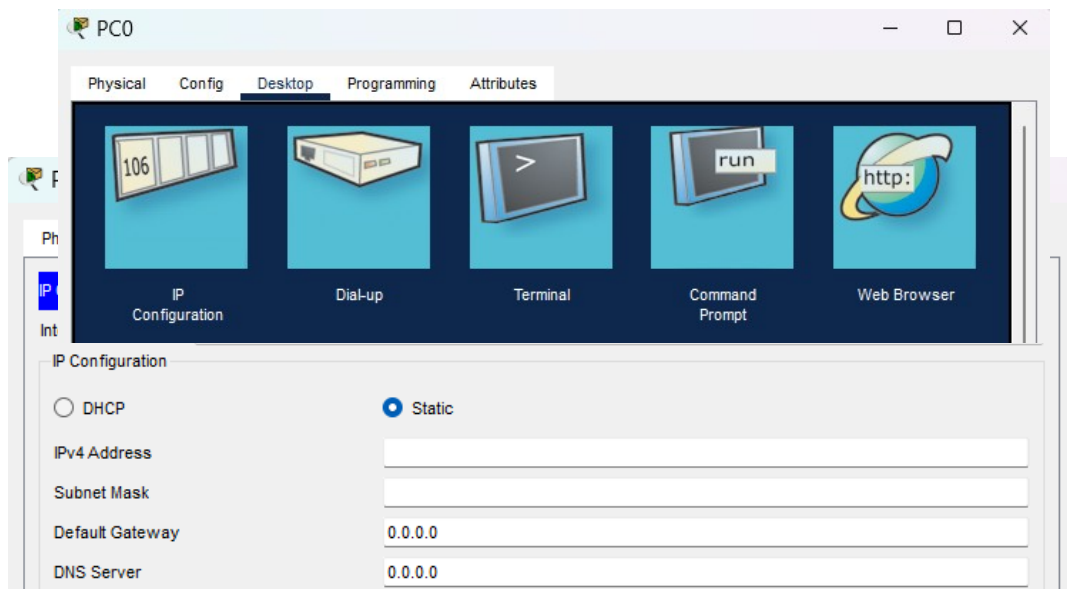
En el caso de PC, servidores o portátiles, se siguen los mismos pasos: Config, Interface, escoger la tarjeta Ethernet y teclear su IP y máscara. En estos dispositivos tiene que estar marcado el apartado Static (pese a la coincidencia de nombre, no tiene ninguna relación con el enrutamiento estático):





*Asigna la IP 15.0.0.7 y máscara 255.0.0.0 a un PC.*

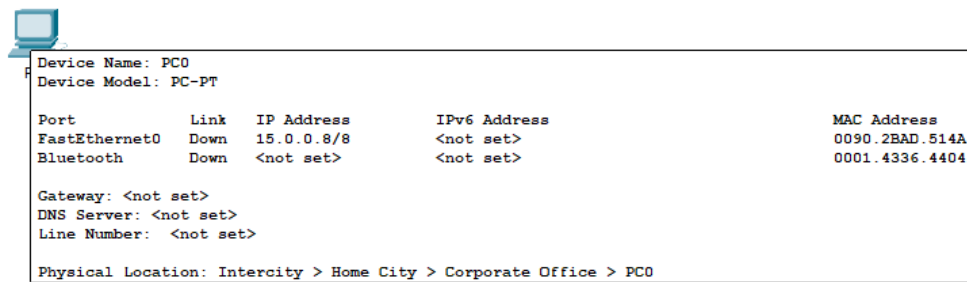
De forma alternativa, también podemos ir a la sección Desktop, IP Configuration, donde además se puede indicar la puerta de enlace y el servidor DNS que usará el equipo (también aquí tiene que estar marcado Static):



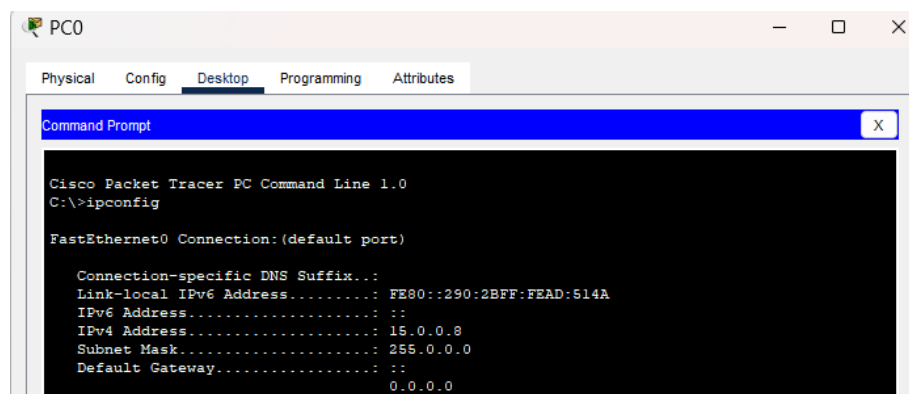
*Cambia la IP del PC anterior a 15.0.0.8 y asígnale la puerta de enlace 15.0.0.1*

Ten en cuenta que los dispositivos finales (PC, portátiles, servidores) no pueden configurarse mediante comandos CLI, sólo los routers o switches Cisco.

Para averiguar la IP, máscara o puerta de enlace con el exterior (gateway) de un equipo, podemos dejar el ratón quieto sobre el dispositivo:



O también, accediendo a Desktop, Command Prompt y tecleando ipconfig, como harías en la consola de un PC:



## **Parte 2: Uso del modo Simulación**

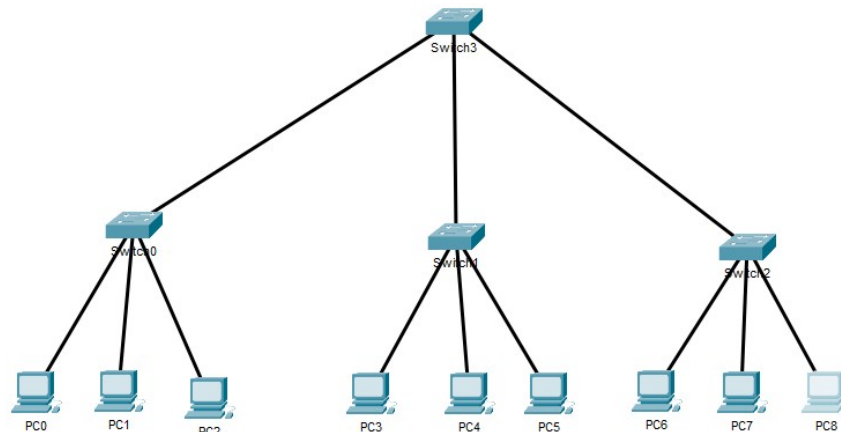
El contenido de esta parte puedes hacerlo indistintamente con la explicación que verás a continuación, o bien, de manera opcional, siguiendo la práctica 5 (el PDF con el manual de CISCO está en el aula virtual):

- ***Práctica 5. Exploring Network Functionality Using PDUs***
  - Para esta práctica necesitarás haber completado la práctica 4 de la unidad anterior.

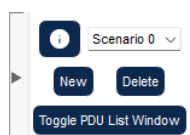
PT permite ver exactamente por dónde van circulando los paquetes de datos cuando dos equipos cualesquiera se comunican. Al ver claramente la ruta escogida, podemos saber exactamente dónde está el fallo en el caso de que haya problemas en la red, ya que, en caso de redes complejas, el camino entre emisor y receptor puede incluir muchos dispositivos, y si no visualizamos la ruta, puede resultar complicado localizar en qué dispositivo intermedio está el error.

*Para probar esta funcionalidad de PT, primero crea una LAN de prueba, con 9 equipos y 4 switches 2960 interconectados por par trenzado como en la imagen siguiente. Asigna las IP 10.0.0.1 a 10.0.0.9 de manera manual a los PC. Todos tienen la misma máscara: 255.0.0.0.*

Recuerda que este mapa de red es el diseño lógico. En la realidad (diseño físico) haría falta añadir paneles de parcheo, rosetas, racks, etc, como se vio en unidades anteriores. En esta unidad usaremos solamente el diseño lógico para simplificar.



Ahora, haz clic en los botones Simulation y Event List para que aparezcan dos nuevas secciones en la pantalla: escenario de la simulación (aparecerá en la parte inferior de la pantalla) y listado de eventos (aparecerá en la parte derecha).



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
------	-----------	-------------

Reset Simulation ☒ Constant Delay Captured to: (no captures)

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, RADIUS, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Estas nuevas secciones nos van a indicar en tiempo real qué va a ir sucediendo paso a paso en nuestra red cuando realizamos un envío de prueba, así como para inspeccionar cada paquete que viaje.

Ahora vamos a realizar una prueba de envío desde el equipo 10.0.0.1 hasta el 10.0.0.9. La prueba consistirá en enviar un ping de un equipo al otro. El ping viajará por la red hasta el destinatario, y luego volverá al emisor.

El comando ping (presente en Windows y Linux) simplemente comprueba si hay algún camino disponible entre dos equipos, enviando cuatro mensajes de prueba al equipo y comprobando si se reciben mensajes de vuelta. Basta con especificar la IP del receptor al introducir el comando para que se envíen paquetes de datos desde el origen hasta el destinatario.

*Para probarlo, haz clic en el botón con el sobre cerrado, luego en el equipo origen y después en el destinatario.*



*Verás que ha aparecido un sobre cerrado en el origen, que representa el paquete a enviar, y se han actualizado las secciones de Simulación y Lista de Eventos. Para que la simulación empiece, dale al botón de Play en la Lista de Eventos y observa qué sucede.*



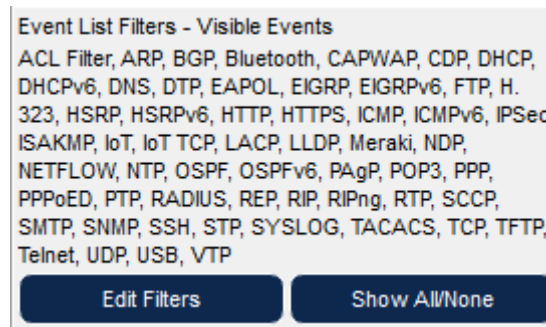
*Verás el camino que recorre el paquete, paso a paso. Puedes aumentar o disminuir la velocidad a la que se reproduce la simulación arrastrando a la derecha o a la izquierda el control que está justo debajo del botón del Play.*

La lista de eventos se actualizará con cada paso nuevo que se haga, mostrando el tiempo y el nombre de cada dispositivo por los que pasa el paquete:

Event List		
Vis.	Time(sec)	Last Device
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.003	Switch3
	0.004	Switch2
	0.005	PC8
	0.006	Switch2
	0.007	Switch3
	0.008	Switch0

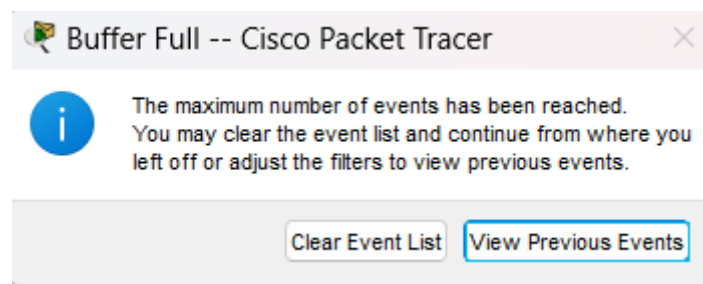
Sin embargo, la simulación no se detiene. Cuando el ping vuelve al emisor, siguen

apareciendo otros paquetes de datos correspondientes a otros protocolos, que dificultan la comprensión de lo que está sucediendo. En el listado de eventos aparecen todos los protocolos que se mostrarán (que por defecto son todos). (¿Cuántos protocolos del siguiente listado reconoces?)



*Detén la simulación dándole al botón de Pausa. Y ahora, vamos a ocultar los paquetes de los protocolos que no nos interese ver. Para ello, en el listado de eventos, haz clic en el botón Show All/None, para que pase de mostrar todos los protocolos a no mostrar ninguno, y luego ve a Edit Filters y deja marcado únicamente ICMP (que es el protocolo asociado al ping). Ahora ve a Reset Simulation para volver a simular desde el principio, y dale de nuevo al Play. Ya no deberían aparecer otros paquetes tras la vuelta del ping.*

Si durante una simulación aparece este mensaje, significa que la simulación ha acabado.



Puedes hacer clic en View Previous Events para examinar el listado de eventos o Clear Event List si no te interesa verlos (por ejemplo, cuando vayas a resetear y volver a simular).

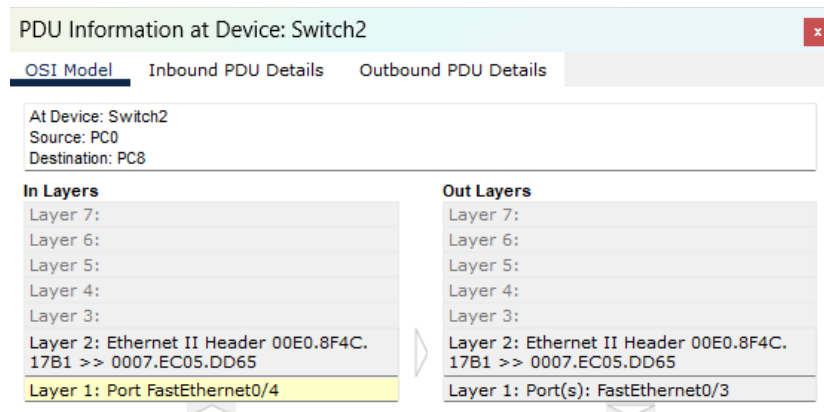
En la zona inferior aparece el resumen de la simulación en todo momento (indicando origen, destino, protocolo usado, y si tuvo éxito o no).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC8	ICMP		0.000	N	0	(edit)	

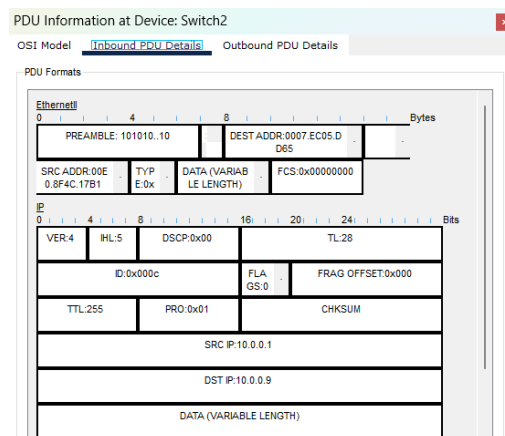
Y si haces clic sobre un evento del listado...

Event List		
Vis.	Time(sec)	Last Device
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.003	Switch3
	0.004	Switch2
	0.005	PC8
	0.006	Switch2
	0.007	Switch3
	0.008	Switch0

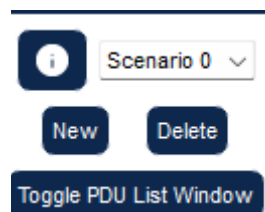
...aparecerá una ventana donde podrás ver los 7 niveles OSI del paquete. En el ejemplo, aparece la MAC origen, la MAC destino y las tarjetas de red de los dos PC.



También puedes ver el contenido exacto de cada campo de cada cabecera (de manera parecida a Wireshark). En el ejemplo se muestran las cabeceras Ethernet e IP del ping enviado. La diferencia entre Inbound y Outbound es que uno muestra el paquete que entra al dispositivo en ese paso seleccionado, y el otro, el paquete que sale. En algunas ocasiones (sobre todo cuando los datos pasan a través de routers) el paquete que entra no es exactamente el mismo que el paquete que sale (por ejemplo, los routers decrementan en uno el campo TTL), por lo que así podríamos ver los cambios realizados por el dispositivo en el paso seleccionado de la simulación.



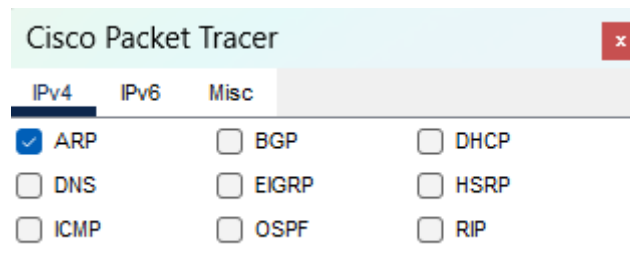
*Vamos a realizar otra simulación en la misma red. Para ello, vamos a borrar la que hemos realizado dándole a Delete.*



*Simularemos el uso de ARP, que como sabes, es un protocolo que emplea broadcast (difusión) para los envíos. Para ello, primero vamos a borrar la caché ARP del PC con IP 10.0.0.1, para así forzar el uso de ARP. Ve al PC, Desktop, Command Prompt y teclea estos comandos (el primero para borrar la tabla ARP y el segundo para comprobar que está vacía):*

```
C:\>arp -d
C:\>arp -a
No ARP Entries Found
```

Ahora haz que solo se muestren los paquetes ARP (desde Edit Filters):

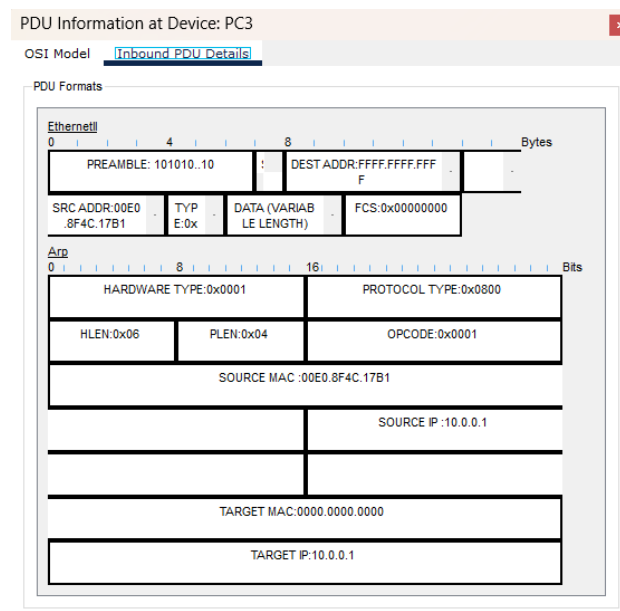


Y de nuevo desde la consola del PC con IP 10.0.0.1 teclea ping 10.0.0.9 y dale al Play. Deberías ver cómo primero se difunde la consulta ARP por todos los switches y PC. Aquellos que no sean el destinatario recibirán un sobre con una marca roja indicando que no está destinado a ellos, y solo el 10.0.0.9 responderá.

El equipo con la IP 10.0.0.1 tendrá actualizada su caché ARP al final del proceso:

```
C:\>arp -a
Internet Address      Physical Address      Type
10.0.0.9              0007.ec05.dd65       dynamic
```

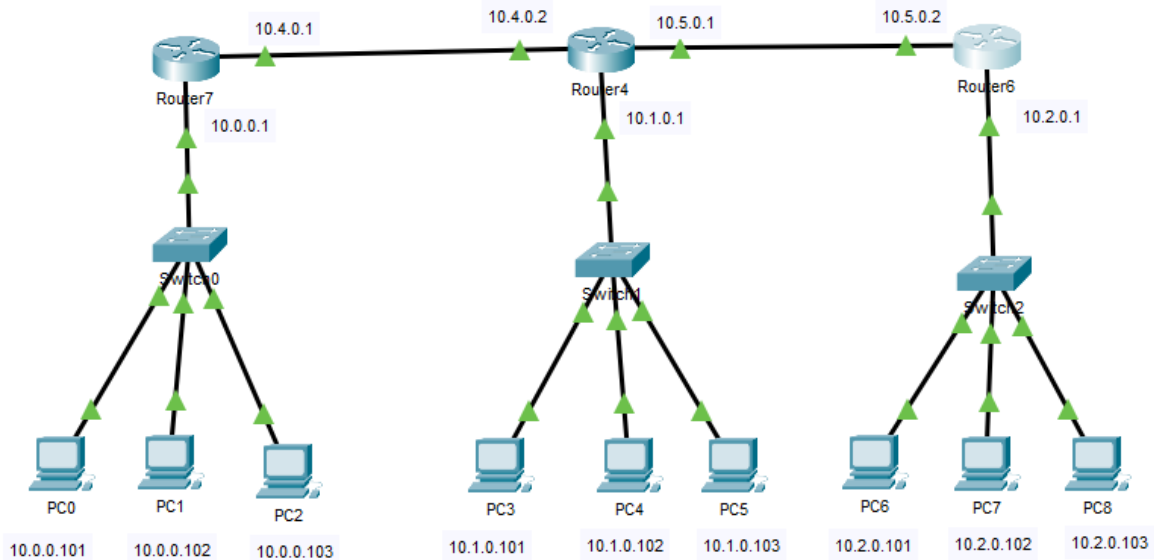
Y podemos ver el contenido de cada paquete ARP, campo por campo, seleccionando un evento del listado:



Como ves, la simulación en PT es muy útil y nos ayuda a entender qué pasa exactamente en una red, paso a paso. En el caso del enrutamiento, nos permitirá ver claramente por dónde van eligiendo los routers los caminos para los paquetes de acuerdo al contenido de su tabla de enrutamiento, como verás en la parte siguiente.

### Parte 3: Enrutamiento estático

Para probar el enrutamiento, modifica la red anterior para que sea como la de la siguiente figura.



Modificaciones que se han realizado:

- Se ha eliminado el switch superior.
- Se han añadido tres routers. **No se han usado los routers PT-Router**, pues solo tienen dos tarjetas Fast Ethernet. En su lugar, se ha preferido usar los routers de tipo PT-Empty, que inicialmente están vacíos, y a los que se les ha añadido dos o tres (según el router) módulos PT-ROUTER-1CGE, que son Gigabit Ethernet.
- En cuanto a las conexiones, los switches se han unido a los routers usando el puerto Gigabit, **no el Fast**, ya que por ese cable deben circular los datos a mayor velocidad porque recoge todo el tráfico de toda esa parte de la red. Entre routers la conexión también es Gigabit.
- Se han modificado prácticamente todas las IP y máscaras. Hay tres subredes: 10.0.0.0, 10.1.0.0 y 10.2.0.0. Fíjate bien en la máscara que autocompleta PT, ahora no podemos usar /8 sino /16. La máscara es /16 en todos (o 255.255.0.0), ya que ahora son los dos primeros bytes de las IP son los que indican la subred en la que estamos.
- La puerta de enlace de cada PC es su correspondiente router.
- Los routers laterales tienen dos IP (porque están conectados a dos redes) y el central tiene tres (está a la vez en tres redes). En la imagen puedes ver las IP que corresponden a cada router. Ten cuidado al asignar IP a los routers, **has de asignar la IP adecuada en la conexión o cable adecuado**. Para saber el nombre exacto de un cable, deja el ratón un instante sobre el cable o el triángulo verde.



En resumen:

- Subred izquierda: PC 10.0.0.101, 10.0.0.102, 10.0.0.103 y router 10.0.0.1
- Subred central: PC 10.1.0.101, 10.1.0.102, 10.1.0.103 y router 10.1.0.1
- Subred derecha: PC 10.2.0.101, 10.2.0.102, 10.2.0.103 y router 10.2.0.1

Como puedes ver, las IP se han repartido en cada subred de manera ordenada: las primeras IP de cada rango se reservan para routers, y a partir de la 101 para PC. **Es muy importante que en una red real el administrador de una LAN reparta de manera organizada las IP, para que, simplemente viendo el número de una IP se sepa si corresponde a un PC o un router. Si nos limitamos a repartirlas siempre en orden creciente desde el 1, puede inducir a confusión.**

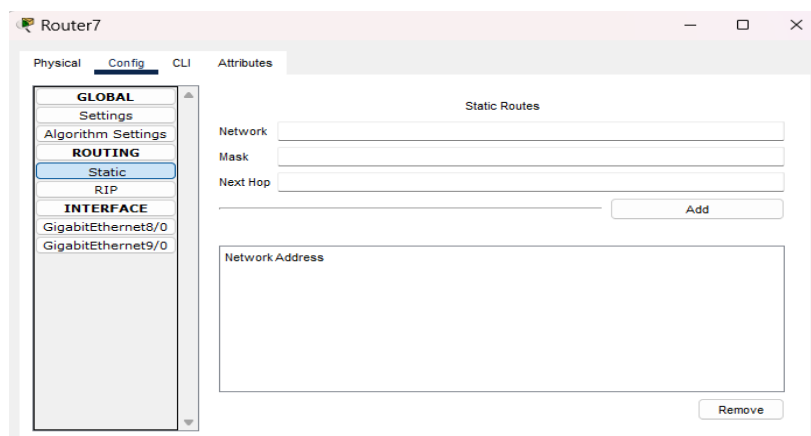
Entre routers también hay subredes:

- Subred superior izquierda: router 10.4.0.1 y router 10.4.0.2
- Subred superior derecha: router 10.5.0.1 y router 10.5.0.2

Asegúrate de que **todas** las IP, máscaras y puertas de enlace de los PC, así como las IP y máscaras de los routers están bien antes de seguir. Un solo fallo en una IP o máscara puede hacer que no funcione el enrutamiento, y deberás volver a repasar cada dirección.

Si ahora hiciéramos ping entre dos equipos lejanos, no funcionaría, ya que en cuanto el mensaje con el ping llegue a un router, no sabrá a donde dirigirse ya que están vacías las tablas de encaminamiento.

Para rellenar las tablas de encaminamiento estático, has de ir en cada router al apartado Config, Routing, Static.



De manera similar a como has hecho en el ejercicio 6 de esta misma unidad, primero deberás pensar el contenido de las tablas. Por suerte, en PT las filas de las tablas correspondientes a la entrega directa no es necesario añadirlas. Por ejemplo, en la tabla de encaminamiento del router de la izquierda no hay que añadir filas ni para 10.0.0.0 ni para 10.4.0.0, aunque sí para las 3 redes restantes.

Cuando añades una fila a una tabla, aparece debajo el comando CLI correspondiente. También puedes ver el contenido actual de una tabla en el CLI con el comando `show ip route`.

El ejercicio estará completo cuando las tablas de encaminamiento de los 3 routers estén rellenas con los valores correctos y se respondan pings entre dos PC cualesquiera (o entre PC y routers). Es probable que al principio, al hacer ping a otro equipo, falle alguno de los 4 mensajes de prueba que se lanzan en cada ping, como puedes ver en la siguiente figura, donde hay dos que no vuelven (time out) y dos que sí (tardan menos de 1 ms). Esto es normal. Pasado un tiempo, deberían siempre volver los 4 pings.

```
C:\>ping 10.1.0.101

Pinging 10.1.0.101 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.1.0.101: bytes=32 time<1ms TTL=126
Reply from 10.1.0.101: bytes=32 time<1ms TTL=126

Ping statistics for 10.1.0.101:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Puedes ayudarte de las herramientas de simulación explicadas en la parte 2 para observar el camino que siguen los paquetes y así poder detectar errores en las rutas. Si deseas ver rápidamente las respuestas a tus pings, haz clic en Realtime para abandonar el modo simulación. Alterna entre Realtime y Simulation si lo necesitas.



- ➔ Como resolución de esta actividad, adjunta a tu entrega el fichero .pkt con la red final (no olvides añadir etiqueta con nombre y fecha, así como poner etiquetas con las IP de todos los PC y routers).

Además, escribe aquí los comandos CLI para configurar las tres tablas de encaminamiento:

Router izquierdo:

```
configure terminal
ip route 10.1.0.0 255.255.0.0 10.4.0.2
ip route 10.2.0.0 255.255.0.0 10.4.0.2
ip route 10.5.0.0 255.255.0.0 10.4.0.2
```

Router derecho:

```
configure terminal
ip route 10.0.0.0 255.255.0.0 10.5.0.1
ip route 10.1.0.0 255.255.0.0 10.5.0.1
ip route 10.4.0.0 255.255.0.0 10.5.0.1
```

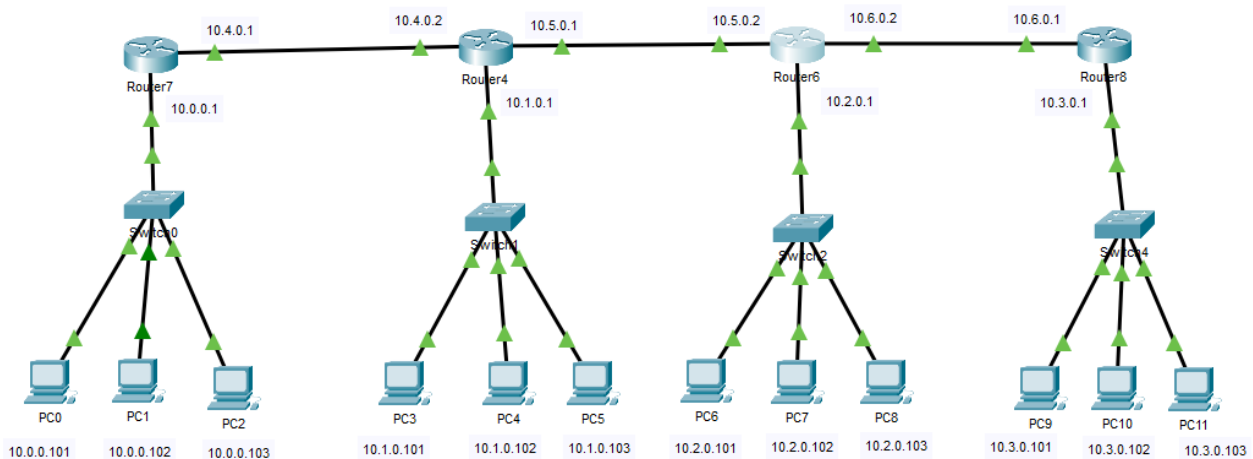
Router central:

```
configure terminal
ip route 10.0.0.0 255.255.0.0 10.4.0.1
ip route 10.2.0.0 255.255.0.0 10.5.0.2
```

#### Parte 4: Enrutamiento dinámico

Mientras que en el enrutamiento estático has tenido que añadir a mano las filas de cada tabla de encaminamiento en cada router, usando protocolos de enrutamiento dinámico las tablas se rellenan automáticamente gracias al uso de protocolos como RIP.

Para probarlo en PT, haz una copia del fichero anterior y en la copia añade a tu red una nueva subred a la derecha, con la misma estructura (un switch, tres PC con IP 10.3.0.101 a la 10.3.0.103, etc), haciendo las modificaciones que consideres necesarias.



Ahora en todos los routers, ve a Config, Routing, RIP y añade únicamente la nueva red: 10.3.0.0. Prueba ahora a hacer pings desde varios PC de varias subredes a un equipo de la red nueva, y al cabo de unos instantes, debería funcionar, aunque no hayas rellenado la tabla del router nuevo.

¿Qué comando CLI se ha ejecutado al añadir una fila en la sección RIP de cada router?

```
router rip
network 10.0.0.0
```