

REDES COMPUTACIONALES

Laboratorio N.º 2

Profesor: Viktor Tapia

Alumno: Rodrigo Pereira

Ayudante: Luciano Yevenes

Fecha: 26/11/2025

1. Desarrollo paso a paso

El desarrollo de este laboratorio se divide en dos fases esenciales. La planificación y asignación de direcciones de red y la activación del protocolo de enrutamiento dinámico (OSPF).

1.1. El plan se basa en los siguientes criterios, definidos en el diseño de red:

Segmento	Red Base	Mascará Subred	IPs asignadas al router
LAN (Zona A)	192.168.10.0/28	255.255.255.240	192.168.10.1 (R1 F0/0)
LAN2 (Zona B)	192.168.20.0/28	255.255.255.240	192.168.20.1 (R2 F0/0)
LAN3 (Zona C)	192.168.30.0/28	255.255.255.240	192.168.30.1 (R3 F0/0)
Serial 1 (R1-R4)	10.0.1.0/30	255.255.255.252	10.0.1.1 (R1), 10.0.1.2 (R4)
Serial 2 (R2-R4)	10.0.2.0/30	255.255.255.252	10.0.2.1 (R2), 10.0.2.2 (R4)
Serial 3 (R3-R4)	10.0.3.0/30	255.255.255.252	10.0.3.1 (R3), 10.0.3.2 (R4)

1.2. Configuración de red en áreas locales

La configuración de los dispositivos finales (PCs) en las áreas locales (Zonas A, B y C) requiere que a cada uno se le asigne una dirección IP dentro de su subred correspondiente. Además, deben utilizar la interfaz FastEthernet del router local como su Puerta de Enlace por Defecto (Default Gateway).

A modo de ejemplo, solo se detallará la configuración de un PC por área, ya que el resto de las configuraciones son similares, variando únicamente la dirección IP.

Zona A:

Dispositivo	Dirección IP	Mascará de Subred	Gateway por Defecto
PC1	192.168.10.2	255.255.255.240	192.168.10.1

PC2	192.168.10.3	255.255.255.240	192.168.10.1
PC3	192.168.10.4	255.255.255.240	192.168.10.1

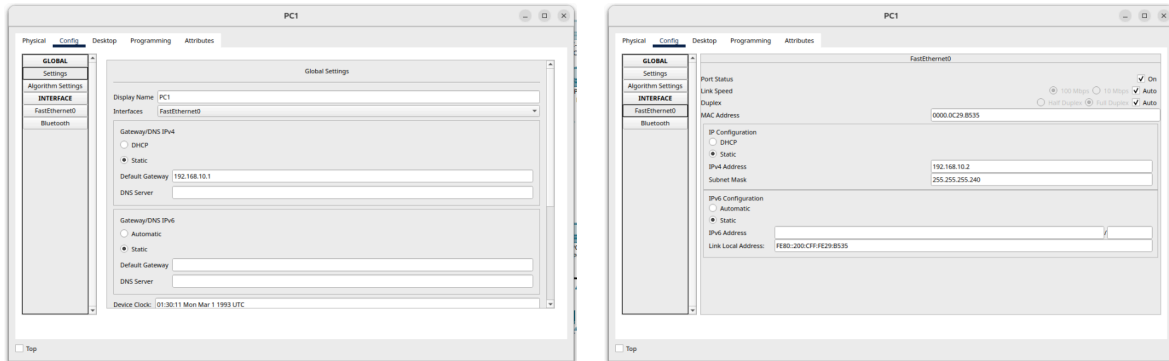


Figura 1, 2 - Asignación de Gateway por Defecto y dirección IP con Máscara de Subred en PC1 de zona A.

Zona B:

Dispositivo	Dirección IP	Mascará de Subred	Gateway por Defecto
PC4	192.168.20.2	255.255.255.240	192.168.20.1
PC5	192.168.20.3	255.255.255.240	192.168.20.1
PC6	192.168.20.4	255.255.255.240	192.168.20.1

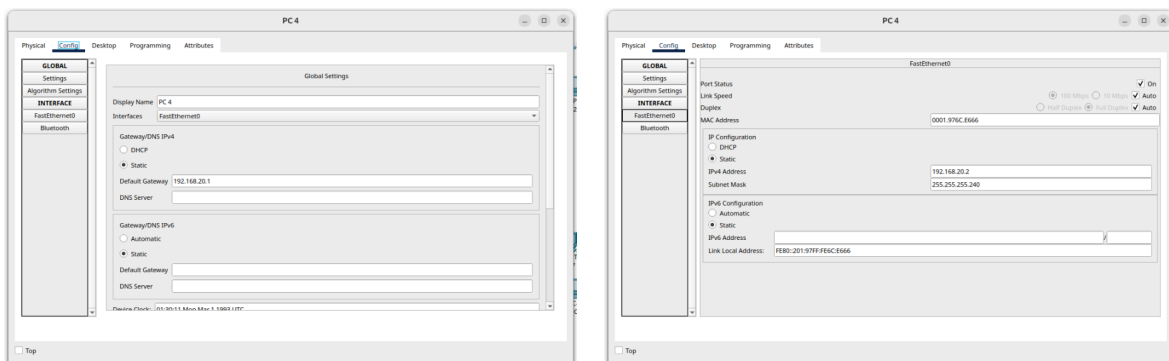


Figura 3, 4 - Asignación de Gateway por Defecto y dirección IP con Máscara de Subred en PC4 de zona B.

Zona C:

Dispositivo	Dirección IP	Mascará de Subred	Gateway por Defecto
PC7	192.168.30.2	255.255.255.240	192.168.30.1

PC8	192.168.30.3	255.255.255.240	192.168.30.1
PC9	192.168.30.4	255.255.255.240	192.168.30.1

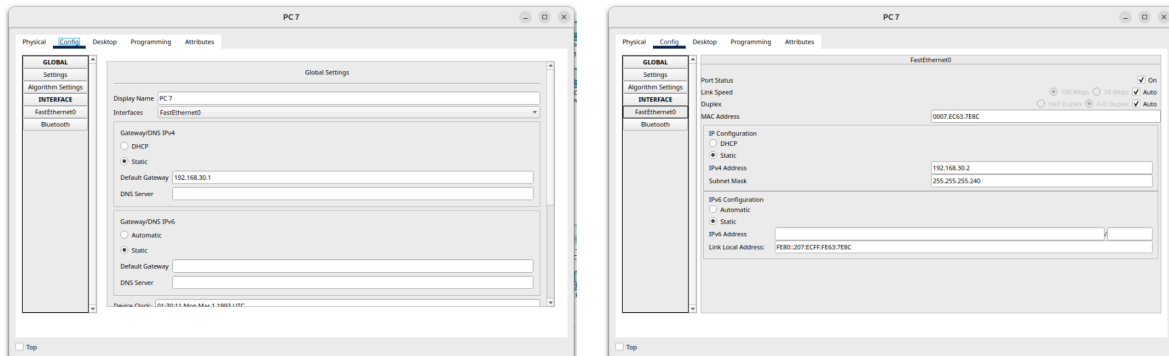


Figura 5, 6 - Asignación de Gateway por Defecto y dirección IP con Máscara de Subred en PC7 de zona C.

1.3. Configuración de interfaces en Routers

Se configura la dirección IP y la máscara de subred en todas las interfaces, estableciendo también la tasa de reloj (clock rate) en el lado DCE (Data Communications Equipment) de cada enlace serial.

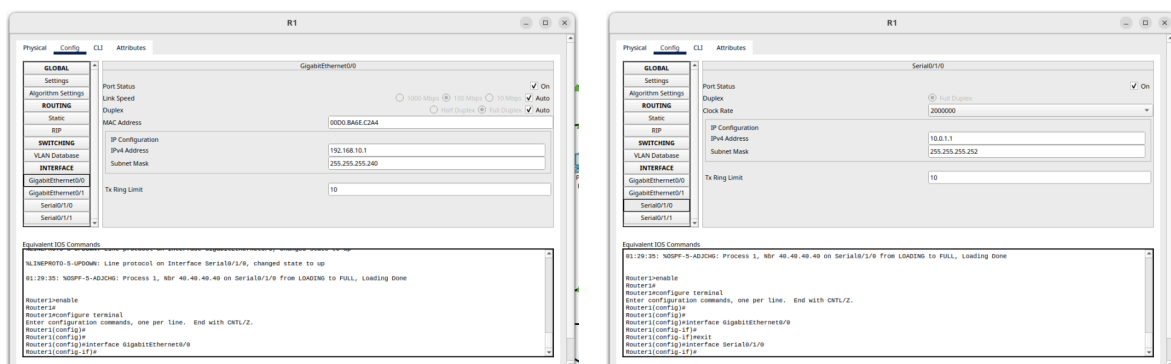


Figura 7, 8 - Configuración en Router 1.

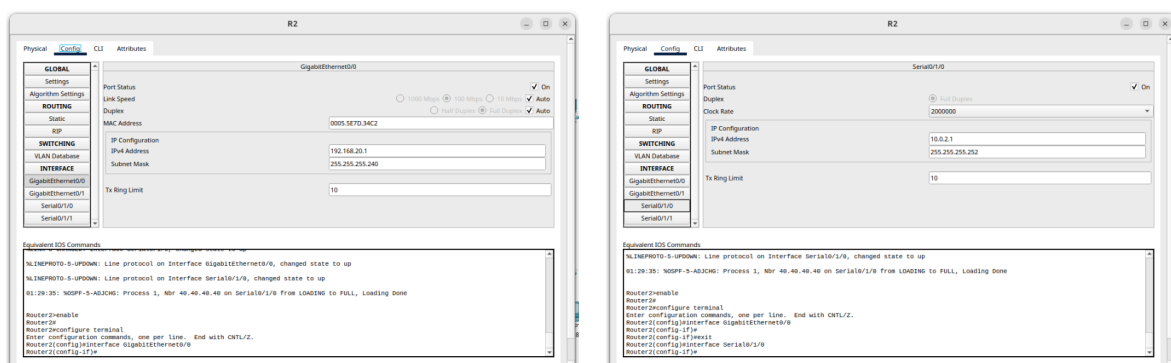


Figura 9, 10 - Configuración en Router 2.

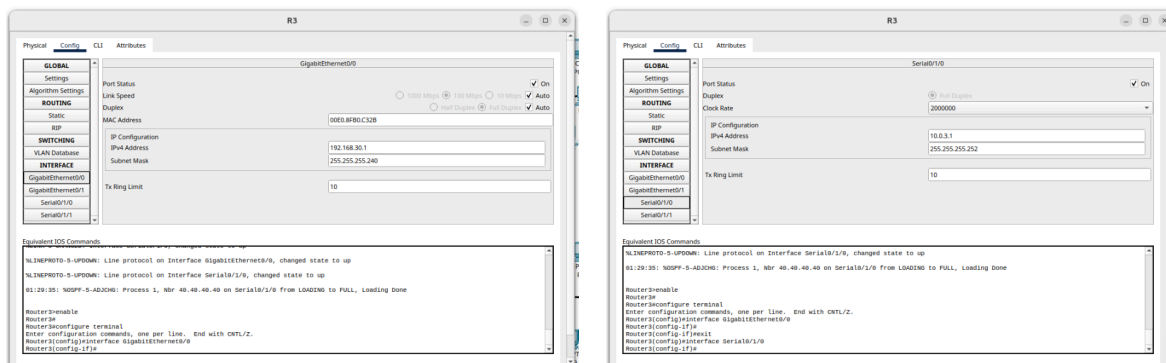


Figura 11, 12 - Configuración en Router 3.

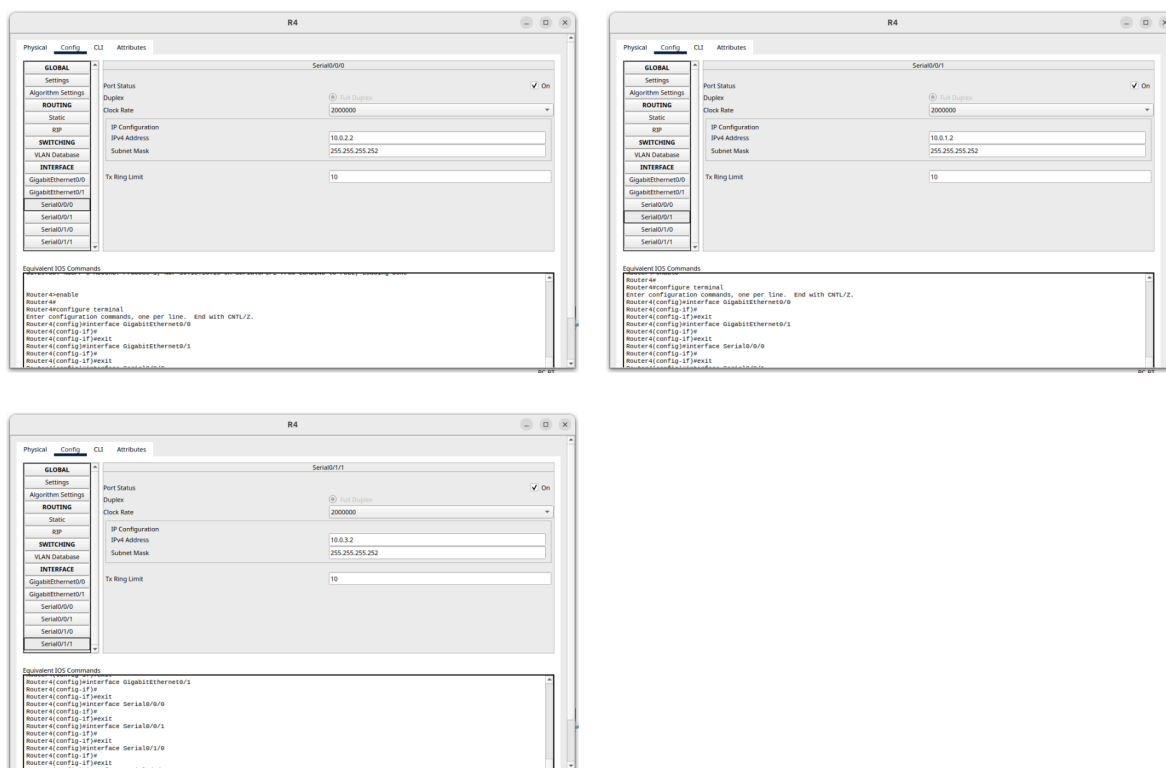


Figura 13, 14, 15 - Configuración en Router 4 (Nodo Central).

1.4. Configuración del Protocolo OSPF

El protocolo OSPF de estado de enlace se activa para permitir que los routes descubran automáticamente las rutas remotas y construyan la base de datos de estado de enlace (LSBD).

Cada router de zona debe anunciar su red LAN (192.168.XX.X) y su enlace serial (10.0.X.X) en el área. Se utiliza un Router ID (RID) único para cada proceso OSPF.

El comando network de OSPF requiere la máscara inversa (Wildcard Mask), que se calcula restando la máscara de subred de 255.255.255.255

Configuración en Router 1:

```
Router1(config-router)# end
```

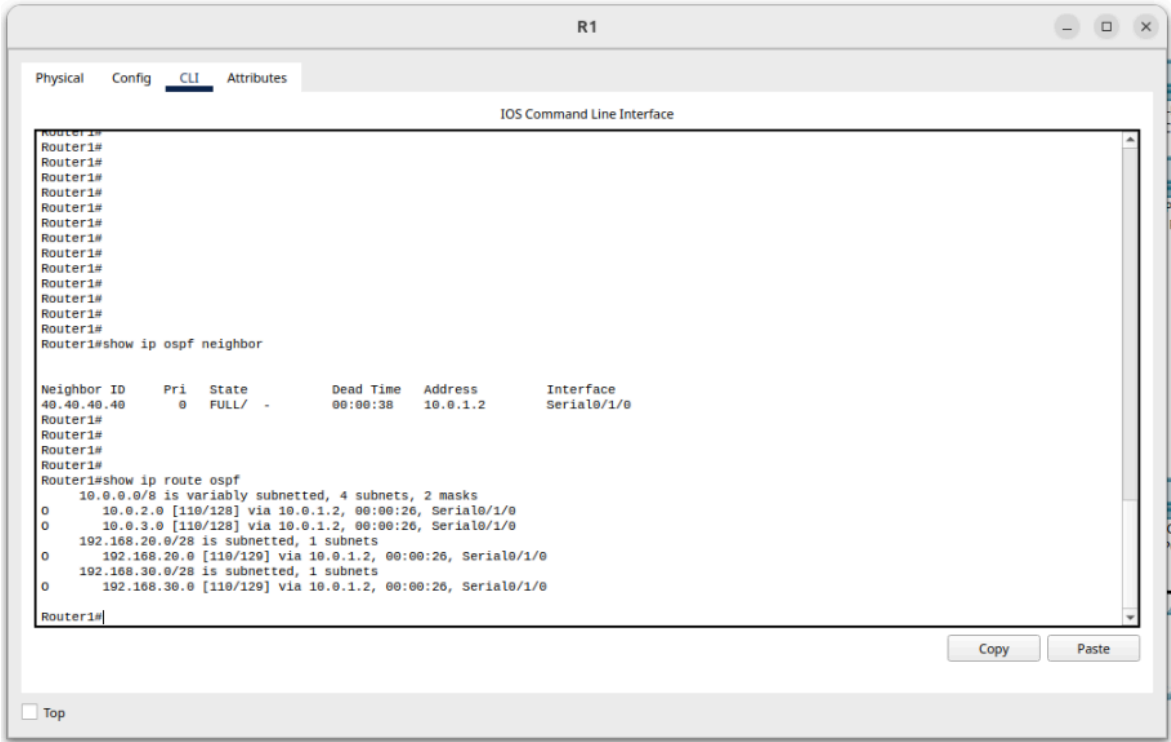


Figura 16 - Ejecución de comandos para adyacencia OSPF y tabla de enrutamiento en R1.

Configuración en Router 2:

```
Router2(config-router)# end
```

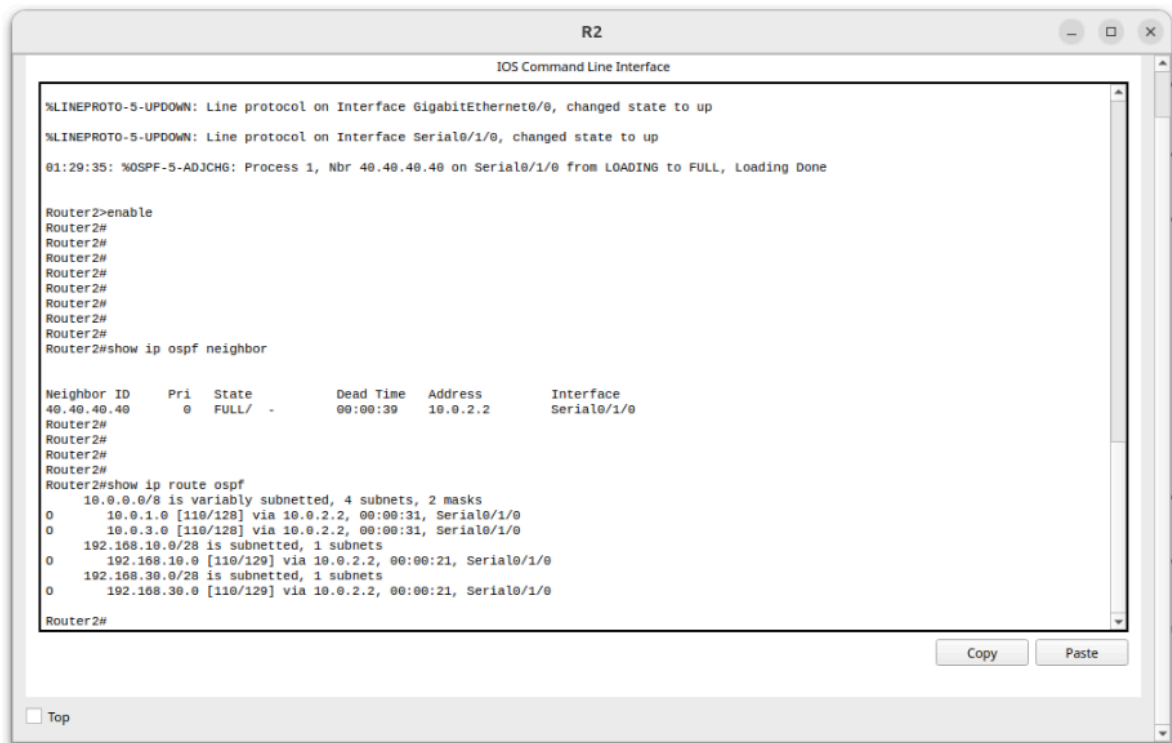


Figura 17 - Ejecución de comandos para adyacencia OSPF y tabla de enrutamiento en R2.

Configuración en Router 3:

Shell

Cisco CLI

Router3# configure terminal

Router3(config)# router ospf 1

Router3(config-router)# router-id 30.30.30.30

Router3(config-router)# network 192.168.30.0 0.0.0.15 area 1 # ← Anuncia LAN1 (/28)

Router3(config-router)# network 10.0.3.0 0.0.0.3 area 1 # ← Anuncia Serial a R4 (/30)

Router3(config-router)# end

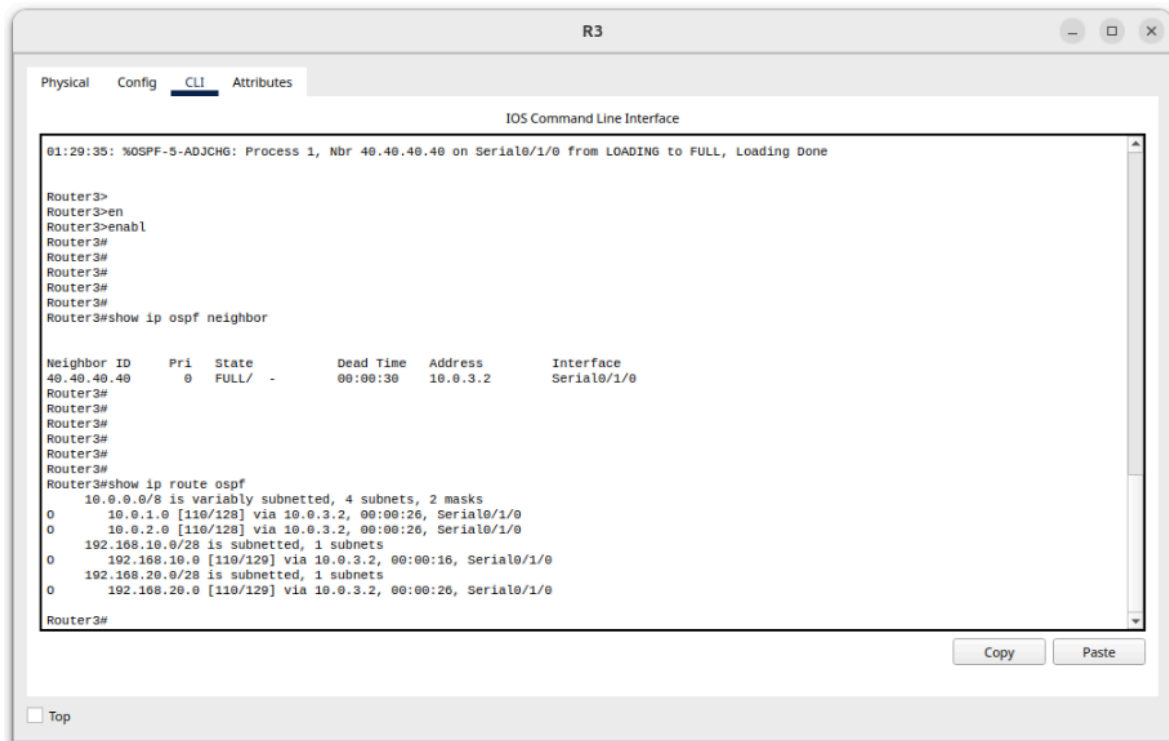


Figura 18 - Ejecución de comandos para adyacencia OSPF y tabla de enrutamiento en R3.

Configuración en Router 4:

Shell

Cisco CLI

Router4# configure terminal

Router4(config)# router ospf 1

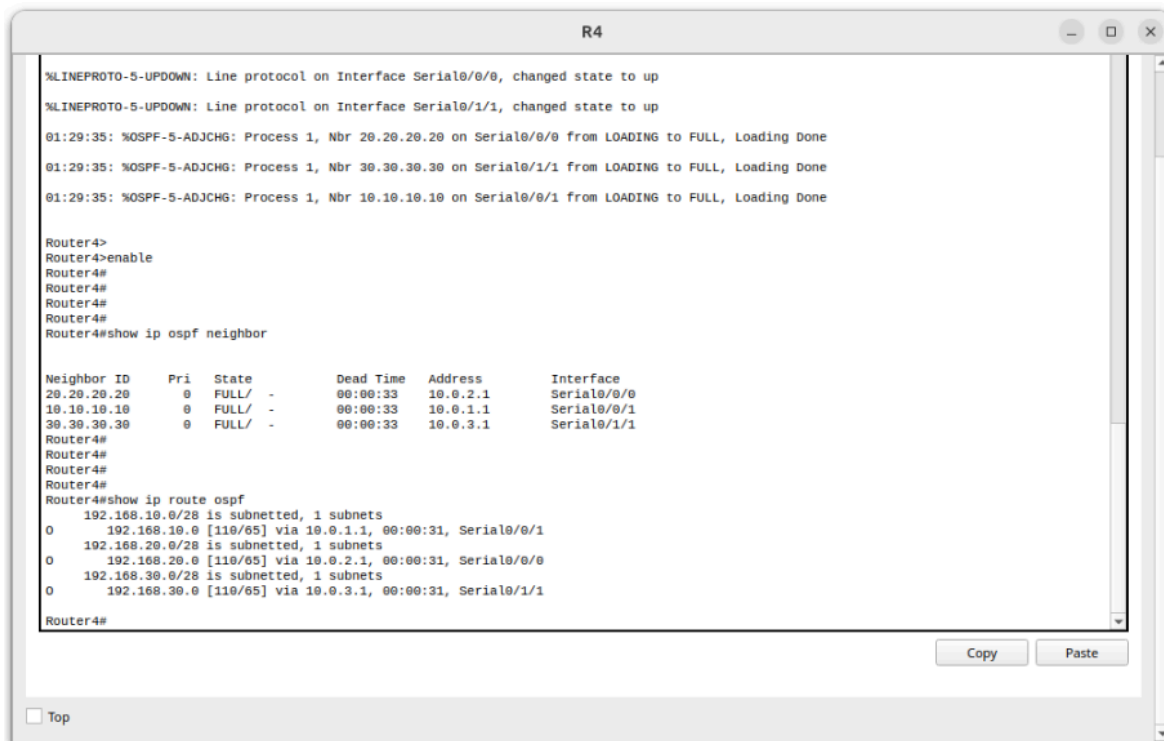
Router4(config-router)# router-id 40.40.40.40

Router4(config-router)# network 10.0.1.0 0.0.0.3 area 1 # ← Anuncia Serial a R1

Router4(config-router)# network 10.0.2.0 0.0.0.3 area 1 # ← Anuncia Serial a R2

Router4(config-router)# network 10.0.3.0 0.0.0.3 area 1 # ← Anuncia Serial a R3

Router4(config-router)# end



```

R4
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
01:29:35: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.20 on Serial0/0/0 from LOADING to FULL, Loading Done
01:29:35: %OSPF-5-ADJCHG: Process 1, Nbr 30.30.30.30 on Serial0/1/1 from LOADING to FULL, Loading Done
01:29:35: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

Router4>
Router4>enable
Router4#
Router4#
Router4#
Router4#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address        Interface
20.20.20.20     0 FULL/ -         00:00:33    10.0.2.1       Serial0/0/0
10.10.10.10     0 FULL/ -         00:00:33    10.0.1.1       Serial0/0/1
30.30.30.30     0 FULL/ -         00:00:33    10.0.3.1       Serial0/1/1
Router4#
Router4#
Router4#
Router4#show ip route ospf
192.168.10.0/28 is subnetted, 1 subnets
O       192.168.10.0 [110/65] via 10.0.1.1, 00:00:31, Serial0/0/1
192.168.20.0/28 is subnetted, 1 subnets
O       192.168.20.0 [110/65] via 10.0.2.1, 00:00:31, Serial0/0/0
192.168.30.0/28 is subnetted, 1 subnets
O       192.168.30.0 [110/65] via 10.0.3.1, 00:00:31, Serial0/1/1
Router4#
  
```

Figura 19 - Ejecución de comandos para adyacencia OSPF y tabla de enrutamiento en R4.

Como se observa en las figuras 16, 17, 18 y 19, se verifica la convergencia de OSPF.

- Comprobación de vecinos: El comando `show ip ospf neighbor` confirma que R4 es adyacente a R1, R2 y R3 en estado FULL, validando la comunicación OSPF.
- Comprobación de rutas: El comando `show ip route ospf` en cualquier router mostrará rutas o (OSPF intra-area) hacia las redes LAN remotas, lo que confirma el éxito del enrutamiento dinámico.

2. Simulaciones

2.1. Ping entre computadores de la Zona A (Pc1, Pc2, Pc3)

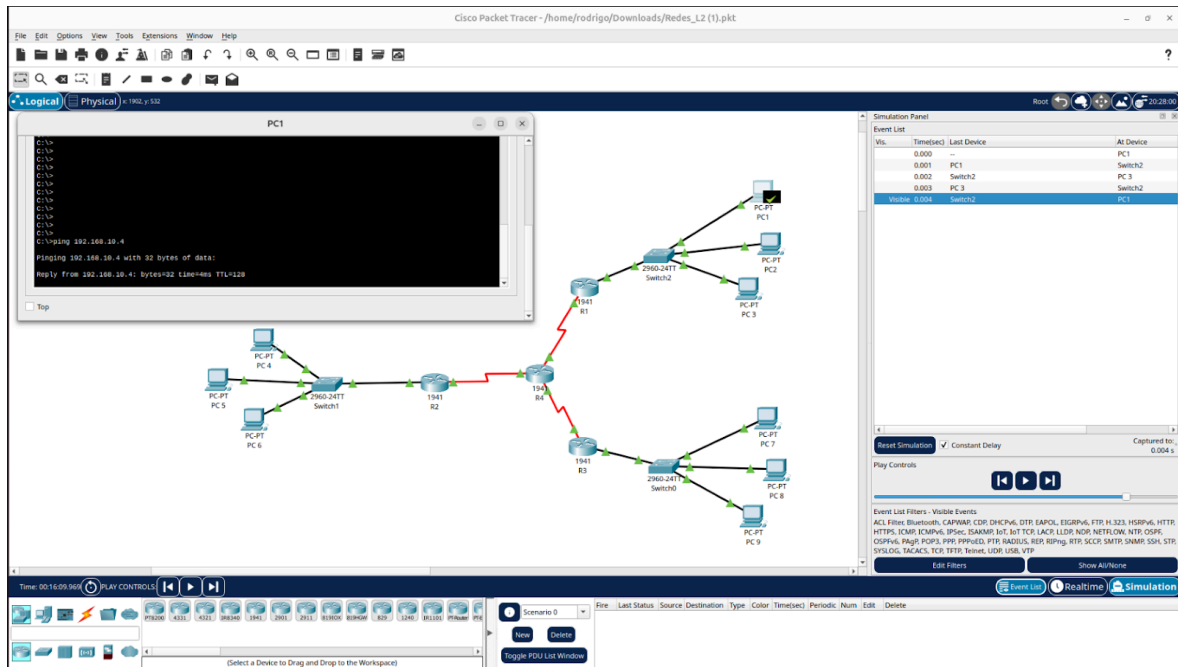


Figura 20.- Ping interno zona A, entre Pc1 y Pc3.

2.2. Ping entre un computador de la Zona A y uno de la Zona B (Pc1 a Pc4)

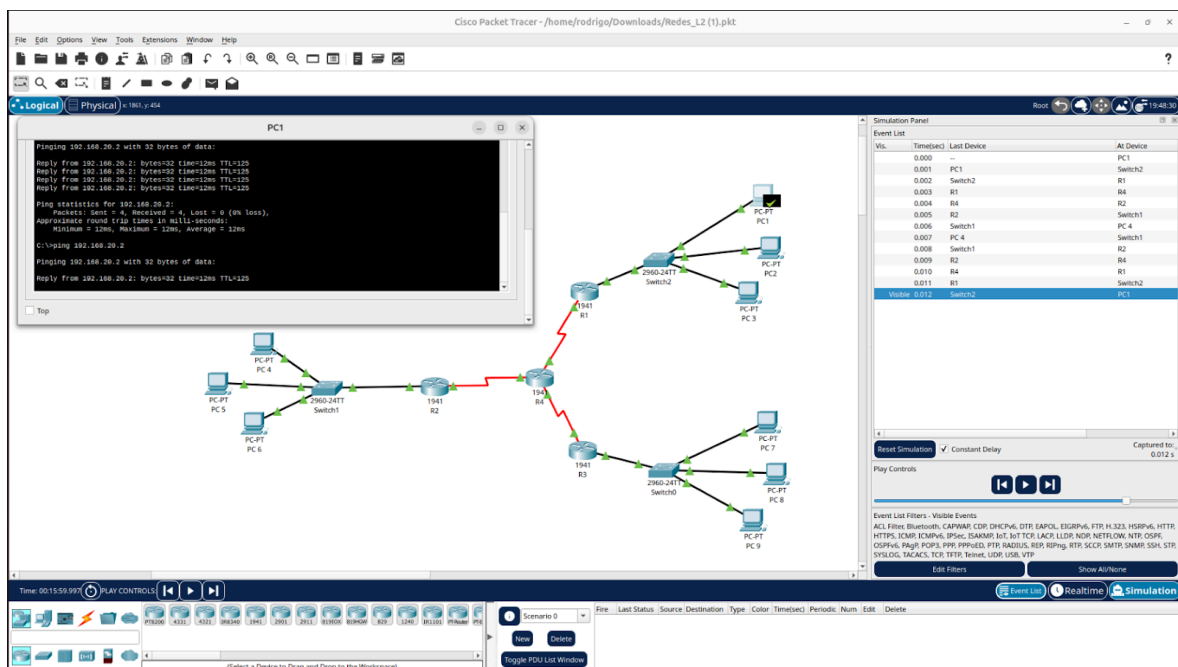


Figura 21.- Ping entre zonas A y B, desde Pc1 a Pc4

2.3. Ping entre un computador de la Zona B y uno de la Zona C (Pc4 a Pc7)

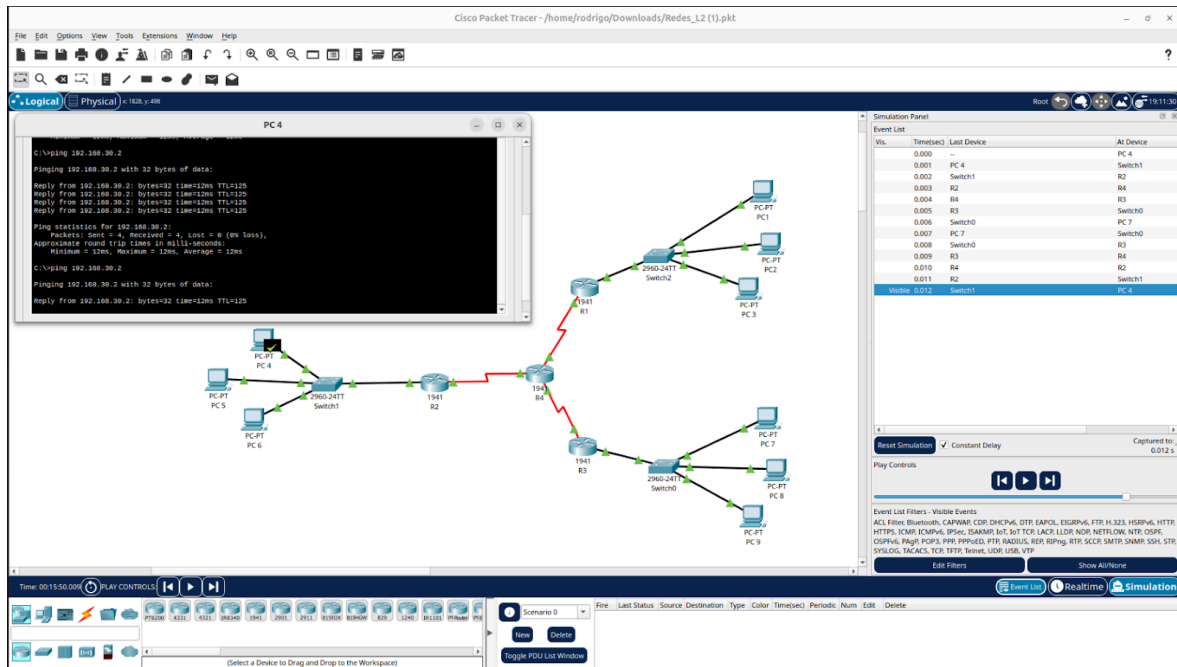


Figura 22.- Ping entre zonas B y C, desde Pc4 a Pc7

3. Preguntas

3.1. ¿Qué camino sigue un paquete enviado desde Pc1 (Zona A) hasta Pc7 (Zona C)? Justifique usando la tabla de enrutamiento y los saltos intermedios.

Basado en el diseño de la tabla de enrutamiento. El camino que sigue un paquete enviado desde Pc1 (Zona A) hasta Pc7 (Zona C) pasa por el router central R4 que es el nodo central de la topología de red utilizada y que es la que conecta las diferentes zonas (LANs) a través de enlaces seriales.

El camino que sigue el paquete con el uso de OSPF es:

1. Pc1. (Zona A 192.168.10.2/28) envía el paquete a su puerta de enlace Router 1 (192.168.10.1/28)
2. R1 consulta su tabla de enrutamiento OSPF. Dado que Pc7 no es local, R1 reenvía el paquete hacia el Router 4 (R4) a través del enlace serial que conecta R1 con R4 (10.0.1.2)
3. R4 recibe el paquete. Y evalúa cuál es el camino de menor costo hacia el destino (Pc7 Zona C) y determina que es a través del Router 3 (R3).
4. R4 reenvía el paquete a R3 a través del enlace serial que los conecta (10.0.3.1).
5. R3 recibe el paquete y lo entrega Pc7 conectado a la zona C (192.168.30.2/28)

El camino completo es: Pc1 \Rightarrow R1 \Rightarrow R4 \Rightarrow R3 \Rightarrow Pc7. Esta ruta es elegida por ser la única ruta de enrutamiento dinámico disponible y, por ende, la que OSPF calcula como la ruta de menor costo.

3.2. ¿Qué router centraliza las conexiones entre las zonas? ¿Cuál es su rol dentro del protocolo OSPF?

El Router 4 (R4) es la pieza central de la red, ya que centraliza todas las conexiones entre las zonas A, B y C. Su ubicación lo convierte en el principal punto de intercambio de tráfico entre las distintas redes de área local.

Dentro de la arquitectura OSPF (Open Shortest Path First), un protocolo de enrutamiento de tipo link-state que permite a los routers construir automáticamente sus tablas de rutas mediante el intercambio de información, el rol de R4 es crítico:

1. **Nodo de Tránsito Central:** R4 actúa como el punto de tránsito fundamental, haciendo posible la comunicación fluida entre las zonas A, B y C.
2. **Gestión de Rutas OSPF:** Al participar R4 en el protocolo OSPF y centralizar el intercambio de información con R1, R2 y R3, asegura que todos los routers de la red obtengan y mantengan una tabla de rutas completa y actualizada.

3.3. ¿Qué sucede si se elimina una de las conexiones seriales entre un router de zona y el router central? ¿Se pierde conectividad entre zonas? Justifique.

Sí, se produce una pérdida de conectividad para la zona afectada (Por ejemplo, Zona A).

La razón es que al eliminarse la única conexión serial ($R1 \Rightarrow R4$), se suprime la única ruta de salida de la Zona A para acceder a las demás zonas (Zona B y Zona C).

El protocolo OSPF, al ser un protocolo de enrutamiento dinámico de tipo link-state, detectará el fallo en el enlace. Esto permite a los routers construir un mapa completo de la red. En consecuencia, OSPF en R1 y R4 marcará ese enlace como caído y procederá a actualizar sus registros de estado de enlace y sus tablas de enrutamiento.

Debido a que R1 no dispone de otra ruta alternativa hacia R4 y, por ende, hacia las subredes de las Zonas B y C, la Zona A queda aislada del resto de la red. Por lo tanto, no podrá alcanzar las redes 192.168.20.0/28 (Zona B) ni 192.168.30.0/28 (Zona C).

3.4. ¿Que parámetros son fundamentales para establecer una conexión IP entre dos dispositivos de red?

Para la comunicación a nivel de red (Capa 3: Network Layer) los parámetros fundamentales son:

1. **Dirección IP (IP address):** Cada dispositivo en la red se identifica mediante una dirección IP. Esta dirección IP de 32 bits (IPv4) es utilizado por los routes para encaminar el paquete de datos desde el origen al destino.
2. **Mascará de subred (Subnet Mask):** La máscara de subred (por ejemplo: 255.255.255.240 para enlaces /28 o 255.255.255.252 para enlaces /30) es necesaria para que un host determine si el dispositivo se encuentra en la misma red local o si necesita ser enviado al gateway (puerta de enlace) para salir de la subred.

3. Gateway: Si el destino del paquete de datos no está en la red local del host, este debe conocer la dirección IP del router edge al que debe enviar el paquete de datos para que este comience su viaje a través de la red. La interfaz del router conectada al switch actúa como gateway para todos los Pc de cada zona (A, B y C).
4. Enlaces seriales: Los enlaces seriales utilizan subredes dedicadas (ej. 10.0.1.0/30). Estas subredes de enlaces están anunciadas y activadas en el protocolo OSPF para que los routers R1, R2, R3 y R4 puedan formar la adyacencia y así poder determinar la secuencia de enlace de comunicación que tomar el paquete de datos.

Por lo tanto, la dirección IP, mascarará y gateway son los parámetros lógicos que definen la comunicación IP, los enlaces seriales es la capa física que soporta la interconexión de los routers, haciendo posible que el algoritmo de enrutamiento (OSPF) trace la ruta de extremo a extremo.

3.5. ¿Por qué los switches envían mensajes incluso cuando no se están transmitiendo datos entre PCs? Nombre y explique brevemente los protocolos involucrados en esta comunicación.

Los switches envían mensajes constantemente, incluso cuando los PCs no están transmitiendo datos de aplicación, porque la infraestructura de la red debe mantener activamente su coordinación, estabilidad y conectividad operativa. Estos mensajes son generalmente tráfico de control generado por dispositivos (routers) conectados a los switches.

Los principales protocolos involucrados en esta comunicación de control son:

1. **Protocolo de Resolución de Direcciones (ARP - Address Resolution Protocol):** ARP es la función que mapea las direcciones IP de capa 3 a las direcciones MAC físicas de capa 2. Cuando la MAC de destino es desconocida, el dispositivo emisor inunda la LAN con un ARP Request. El dispositivo con la IP solicitada responde con una ARP Replay proporcionando su MAC. Este proceso es continuo, ya que las entradas de la caché ARP expiran y deben ser refrescadas, lo que genera tráfico de control constante.
2. **Protocolo de Árbol de Expansión (STP/RSTP - Spanning Tree Protocol):** La función principal de STP es prevenir la creación de bucles lógicos en la Capa 2, para evitar un colapso de la red. STP logra esto bloqueando lógicamente las rutas redundantes. Los switches intercambian periódicamente mensajes de control llamados Bridge Protocol Data Units (BPDUs). Estos mensajes se envían cada pocos segundos para que los switches negocien la topología activa y decidan que puertos deben bloquearse para mantener la estabilidad libre de bucles.