

Capa de enlace, red y capa de Aplicación

Santiago Botero García

Laura Natalia Perilla Quintero

Escuela Colombiana de Ingeniería Julio Garavito

AYSR-1L: Arquitectura y Servicios de Red

Ing. Jhon Alexander Pachón Pinzón

Diciembre 06, 2025

Resumen

El presente informe tiene como objetivo revisar la operación de redes Ethernet y WiFi, así como la interconexión de equipos en redes locales (LAN) y redes de área amplia (WAN). Se enfocará en la integración de diversos servicios de la capa de aplicación, con énfasis en el uso de protocolos como DHCP, EIGRP y OSPF para el enrutamiento dinámico. A través de este informe, se explorarán conceptos fundamentales sobre el diseño, configuración y administración de redes, utilizando herramientas como Packet Tracer.

Durante el desarrollo del trabajo, se simulará una infraestructura de red típica, que incluye tanto redes alámbricas como inalámbricas, y la interconexión de equipos mediante switches de capa 2 y capa 3, routers y puntos de acceso WiFi. Se abordarán aspectos como la configuración de direccionamiento IP, la implementación de VLANs para segmentación de redes, y la verificación de la conectividad a través de pruebas como ping, tracert y navegación web.

Se utilizará el protocolo DHCP para asignar direcciones IP dinámicamente a los equipos en la red. En cuanto al enrutamiento, se configurarán y compararán los protocolos EIGRP y OSPF, con el fin de analizar su desempeño y las diferencias en sus métricas de enrutamiento. Se pondrá a prueba la conectividad entre diversas LANs y se verificarán las rutas de los paquetes en caso de caída de enlaces.

Además, se integrarán servicios de la capa de aplicación, como los servidores DNS y Web, asegurando que los equipos de la red puedan acceder a estos servicios tanto por IP como por nombre de dominio.

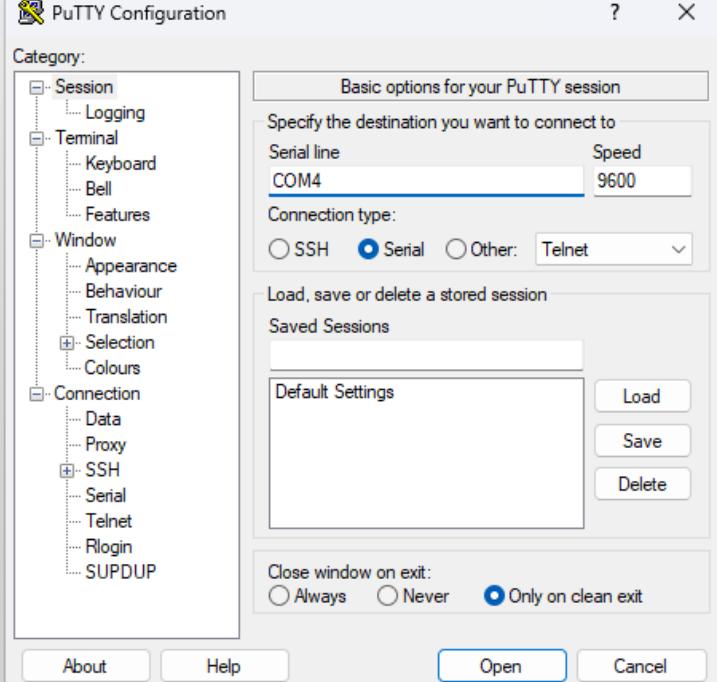
Palabras clave. Redes Ethernet y WiFi, Enrutamiento dinámico (EIGRP, OSPF), Protocolos de capa de aplicación (DHCP, TELNET), VLANs y direccionamiento IP, Switches, routers, routers inalámbricos, Subnetting y diseño de redes, Simulaciones en Packet Tracer

Contenido

Resumen.....	2
Montaje final	5
Simulaciones	9
Enrutamiento Dinámico	9
Implementación Santiago	9
Implementación Natalia.....	14
EIGRP	19
Conclusiones	23

Montaje final

En el desarrollo del montaje final, se llevará a cabo la implementación completa de la red propuesta en conjunto con los compañeros de laboratorio. Se configurarán los dispositivos de acuerdo con los rangos de direccionamiento IP utilizados en prácticas anteriores, asegurando la correcta asignación para cada segmento de red. Además, se establecerán las VLAN necesarias para garantizar la separación entre la red privada y la red WAN, verificando la conectividad interna y las restricciones de acceso. Se aplicarán las configuraciones del servidor DNS para que todos los equipos puedan resolver nombres y realizar pruebas de conectividad mediante ping y traceroute. Finalmente, se validará el funcionamiento de las redes cableadas e inalámbricas, asegurando que los equipos cumplan con los parámetros definidos y presentando el montaje completo al profesor para su revisión.

Acción Realizada	Captura de pantalla
Se realizó la configuración inicial en PuTTY para conectarse a un dispositivo de red mediante una sesión Serial y se debió especificar el puerto COM4	 The screenshot shows the PuTTY Configuration dialog box. The left pane is a tree view of categories: Session, Logging, Terminal, Window, Connection, and others. The 'Session' category is expanded, showing 'Serial line' set to 'COM4' and 'Speed' set to '9600'. The 'Connection type:' section has 'Serial' selected. The right pane contains sections for 'Basic options for your PuTTY session', 'Specify the destination you want to connect to', 'Saved Sessions', and 'Default Settings'. At the bottom, there are buttons for 'About', 'Help', 'Open', and 'Cancel'.

<p>Esta configuración inicial prepara el switch para aplicar la dirección IP del rango 90.0.0.8/29 y las interfaces mencionadas en la tabla, asegurando la conectividad con el gateway y los equipos del laboratorio.</p>	<pre>Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname boteroperilla boteroperilla(config)#banner motd #Exclusive use for AYSR students# boteroperilla(config)#line console 0 boteroperilla(config-line)#logging synchronous boteroperilla(config-line)#exit boteroperilla(config)#no ip domain-lookup</pre>
<p>Esta configuración corresponde al esquema IP definido previamente (red 90.0.0.8/29) donde cada usuario tiene una dirección asignada, y el switch se conecta al router por FastEthernet0/5 para la salida hacia el gateway 90.0.0.9.</p>	<pre>boteroperilla(config)#interface FastEthernet0/1 boteroperilla(config-if)#description connected to Natalia boteroperilla(config-if)#exit boteroperilla(config)#interface FastEthernet0/2 boteroperilla(config-if)#description connected to Brayan boteroperilla(config-if)#exit boteroperilla(config)#interface FastEthernet0/3 boteroperilla(config-if)#description connected to Daniel boteroperilla(config-if)#exit boteroperilla(config)#interface FastEthernet0/4 boteroperilla(config-if)#description connected to Santiago boteroperilla(config-if)#exit</pre>
<p>Esta configuración asegura que tanto el acceso local como remoto al switch esté protegido, cumpliendo con buenas prácticas de seguridad en la red 90.0.0.8/29.</p>	<pre>boteroperilla(config)#enable secret E boteroperilla(config)#line console 0 boteroperilla(config-line)#password C boteroperilla(config-line)#login boteroperilla(config-line)#logging synchronous boteroperilla(config-line)#exit boteroperilla(config)#line vty 0 4 boteroperilla(config-line)#password T boteroperilla(config-line)#login boteroperilla(config-line)#logging synchronous boteroperilla(config-line)#exit</pre>

Se asignó la IP 90.0.0.10 con máscara 255.255.255.248, correspondiente al rango /29 definido para la red. El gateway se configuró como 90.0.0.9, que es la dirección del router para salida hacia otras redes, y el DNS preferido también apunta a 90.0.0.9, permitiendo la resolución de nombres. Esta configuración asegura que el equipo identificado como “Natalia” pueda comunicarse correctamente dentro de la subred y acceder a servicios internos y externos según el diseño del laboratorio. Los equipos del laboratorio fueron configurados con direcciones IP dentro del rango 90.0.0.8/29, asignadas de la siguiente manera: Natalia en la interfaz FastEthernet0/1 con IP 90.0.0.10, Santiago en FastEthernet0/4 con IP 90.0.0.11, Brayan en FastEthernet0/2 con IP 90.0.0.12 y Daniel en FastEthernet0/3 con IP 90.0.0.13

Edit IP settings

Manual

IPv4

On

IP address

90.0.0.10

Subnet mask

255.255.255.248

Gateway

90.0.0.9

Preferred DNS

90.0.0.9

DNS over HTTPS

Off

Alternate DNS

Save

Cancel

El resultado indica que se enviaron 4 paquetes y se recibieron los 4 sin pérdida (0% loss), con un tiempo de respuesta mínimo y máximo de 1 ms, lo que confirma que ambos equipos están correctamente configurados dentro de la subred 90.0.0.8/29, con comunicación estable a través del switch y el gateway definido.

```
C:\Users\Redes>ping 90.0.0.11
Pinging 90.0.0.11 with 32 bytes of data:
Reply from 90.0.0.11: bytes=32 time=1ms TTL=128
Reply from 90.0.0.11: bytes=32 time=1ms TTL=128
Reply from 90.0.0.11: bytes=32 time<1ms TTL=128
Reply from 90.0.0.11: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 90.0.0.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\Users\Redes>
```

Esta configuración garantiza que el puerto pertenezca exclusivamente a la VLAN PRIVADA, aislando el tráfico de este equipo del resto de la red y evitando que tenga acceso a la red WAN.

```
boteroperilla(config)#vlan 35
boteroperilla(config-vlan)#name PRIVADA
boteroperilla(config-vlan)#exit
boteroperilla(config)#interface FastEthernet0/4
boteroperilla(config-if)#switchport mode access
boteroperilla(config-if)#switchport access vlan 35
boteroperilla(config-if)#exit
boteroperilla(config)
```

Esta configuración es esencial para que el tráfico de la VLAN PRIVADA pueda comunicarse con otros dispositivos que también soporten VLANs, manteniendo la segmentación lógica de la red y cumpliendo con el diseño del laboratorio.

Se muestra la configuración del puerto GigabitEthernet0/1 del switch, esto permite que el enlace transporte múltiples VLANs. Luego se habilita la VLAN 35 en el trunk con switchport trunk allowed vlan 35, asegurando que el tráfico de la VLAN PRIVADA pueda pasar por este enlace hacia otros dispositivos que soporten VLANs.

```
botoperilla(config)#interface FastEthernet0/5
botoperilla(config-if)#switchport mode trunk
botoperilla(config-if)#
*Mar 1 01:20:52.725: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
botoperilla(config-if)#
*Mar 1 01:20:52.725: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
botoperilla(config-if)#switchport trunk allowed vlan 35
botoperilla(config-if)#
botoperilla(config)#

```

```
botoperilla(config)#interface GigabitEthernet0/1
botoperilla(config-if)#switchport mode trunk
botoperilla(config-if)#
*Mar 1 02:09:33.177: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
botoperilla(config-if)#
*Mar 1 02:09:36.197: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
botoperilla(config-if)#switchport trunk allowed vlan 35
botoperilla(config-if)#
botoperilla(config)#

```

Simulaciones

Enrutamiento Dinámico

En esta etapa del laboratorio se realizará la configuración completa de una red compleja utilizando Packet Tracer, aplicando técnicas avanzadas de enrutamiento dinámico. Se llevará a cabo el proceso de subnetting basado en los rangos y cantidades de hosts definidos para cada ciudad, garantizando una correcta asignación de direcciones IP. Posteriormente, se configurará el protocolo DHCP en los routers para automatizar la entrega de direcciones a los equipos de cada LAN. Además, se implementarán los protocolos de enrutamiento dinámico EIGRP y OSPF, verificando sus métricas y tablas de enrutamiento para comparar su comportamiento. Finalmente, se comprobará la conectividad entre todos los dispositivos mediante pruebas de ping y traceroute, asegurando que la red funcione de manera óptima y que los equipos puedan comunicarse entre sí bajo las configuraciones establecidas.

Implementación Santiago

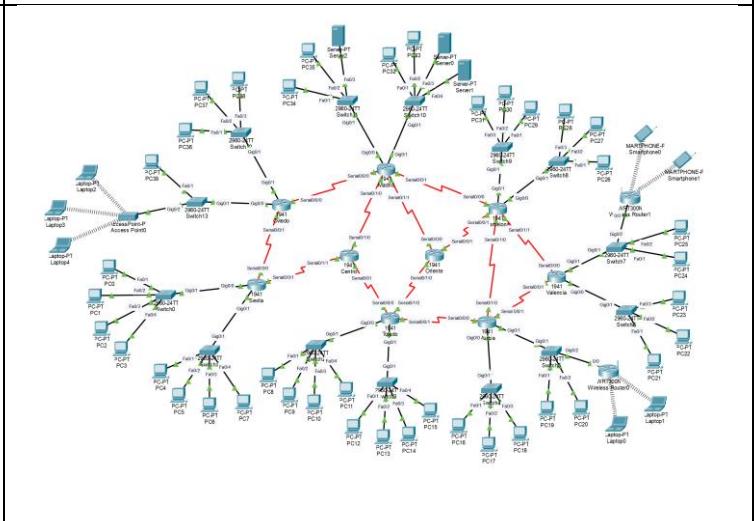
Antes de proceder a dividir la red de Santiago en subredes, es importante comprender la estructura básica de la red principal:

- Red de Santiago: 123.89.128.0/20
- Binario: 01111011.01011001.1000|0000.00000000
- Host: 123.89.128.0
- Broadcast: 123.89.143.255

Con esta información, se puede planificar adecuadamente la creación de subredes, asignando bloques de direcciones IP de manera eficiente según las especificaciones.

Ciudad	LAN	Numero de direcciones	Binario	Red	Rango	Mascara
Sevilla	Switch0	$54 \leq 2^6 - 2$	0000.01 000000	123.89.128.64/26	123.89.128.65 ----- 123.89.128.126	255.255.255.192
	Switch1	$160 \leq 2^8 - 2$	0001 .00000000	123.89.129.0/24	123.89.129.1 ----- 123.89.129.254	255.255.255.0
Toledo	Switch2	$200 \leq 2^8 - 2$	0010 .00000000	123.89.130.0/24	123.89.130.1 ----- 123.89.130.254	255.255.255.0
	Switch3	$243 \leq 2^8 - 2$	0011 .00000000	123.89.131.0/24	123.89.131.1 ----- 123.89.131.254	255.255.255.0
Murcia	Switch4	$30 = 2^5 - 2$	0000.001 00000	123.89.128.32/27	123.89.128.33 ----- 123.89.128.62	255.255.255.224
	Switch5	$80 \leq 2^7 - 2$	0000.1 0000000	123.89.128.128/25	123.89.128.129 ----- 123.89.128.254	255.255.255.128
Valencia	Switch6	$300 \leq 2^9 - 2$	010 0.00000000	123.89.132.0/23	123.89.132.1 ----- 123.89.133.254	255.255.254.0
	Switch7	$600 \leq 2^{10} - 2$	10 00.00000000	123.89.136.0/22	123.89.136.1 ----- 123.89.139.254	255.255.252.0
Barcelona	Switch8	$128 \leq 2^8 - 2$	0110 .00000000	123.89.134.0/24	123.89.134.1 ----- 123.89.134.254	255.255.255.0
	Switch9	$60 \leq 2^6 - 2$	0111.00 000000	123.89.135.0/26	123.89.135.1 ----- 123.89.135.62	255.255.255.192
Madrid	Switch10	$100 \leq 2^7 - 2$	0111.1 0000000	123.89.35.128/25	123.89.35.129 -----	255.255.255.128

					123.89.35.254	
	Switch11	$40 \leq 2^6 - 2$	1100.00 000000	123.89.140.0/26	123.89.140.1 ----- 123.89.140.62	255.255.255.192
Oviedo	Switch12	$32 \leq 2^6 - 2$	0111.11 000000	123.89.135.192/26	123.89.135.193 ----- 123.89.135.254	255.255.255.192
	Switch13	$20 \leq 2^5 - 2$	1100.010 000000	123.89.140.64/27	123.89.140.65 ----- 123.89.140.94	255.255.255.224

Acción Realizada	Captura de pantalla
<p>Se diseñó e implementó la topología de red, definiendo la interconexión de switches y routers para garantizar la conectividad entre las distintas subredes y permitir la simulación de un entorno de red completo y funcional.</p>	

Se configuraron los switches, asignando el nombre de host, contraseñas de consola y VTY, habilitando mensajes de banner de acceso exclusivo y desactivando la resolución de nombres innecesaria.

Se aplicaron buenas prácticas de seguridad y se guardó la configuración en la memoria de arranque para asegurar su persistencia.

Se procedió a configurar los routers, definiendo el nombre de host, contraseñas y banners de acceso. Se habilitó CEF, se configuraron los servicios DHCP con exclusiones y pools específicos para cada subred, y se establecieron direcciones helper para permitir la retransmisión de solicitudes DHCP entre redes. Toda la configuración se guardó en memoria de arranque para mantener la estabilidad de la red.

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch0
Switch0(config)#banner motd #Exclusive access for AYSR students#
Switch0(config)#no ip domain-lookup
Switch0(config)#enable secret E
Switch0(config)#line console 0
Switch0(config-line)#password C
Switch0(config-line)#login
Switch0(config-line)#logging synchronous
Switch0(config-line)#exit
Switch0(config-line)#line vty 0 4
Switch0(config-line)#password T
Switch0(config-line)#login
Switch0(config-line)#logging synchronous
Switch0(config-line)#exit
Switch0(config)#exit
Switch0#
*SYS-5-CONFIG_I: Configured from console by console

Switch0#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch0#

```

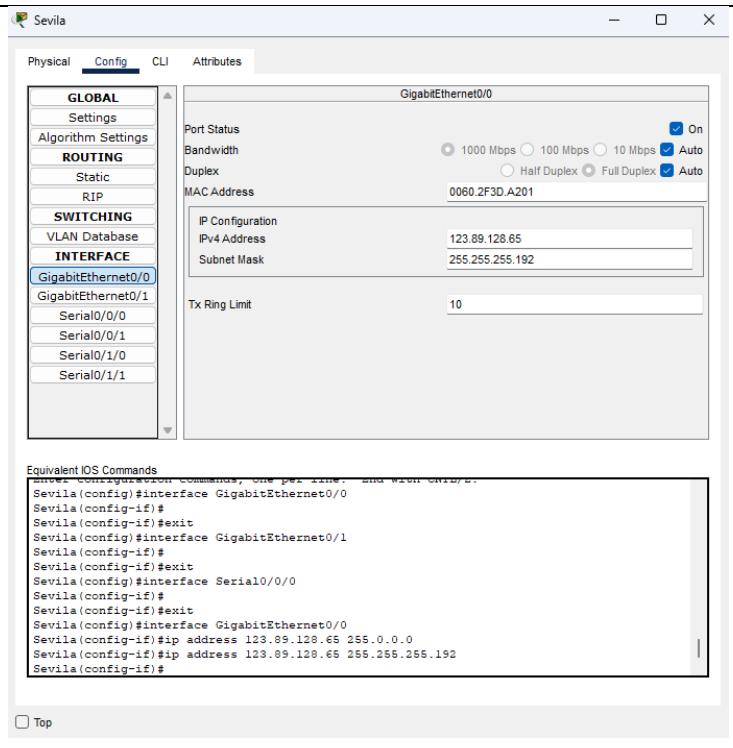
```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Murcia
Murcia(config)#banner motd #Exclusive access for AYSR students#
Murcia(config)#no ip domain-lookup
Murcia(config)#enable secret E
Murcia(config)#line console 0
Murcia(config-line)#password C
Murcia(config-line)#login
Murcia(config-line)#logging synchronous
Murcia(config-line)#exit
Murcia(config-line)#line vty 0 4
Murcia(config-line)#password T
Murcia(config-line)#login
Murcia(config-line)#logging synchronous
Murcia(config-line)#exit
Murcia(config)#service dhcp
Murcia(config)#ip dhcp excluded-address 123.89.128.33 123.89.128.62
Murcia(config)#ip dhcp pool MURCIA4
Murcia(dhcp-config)#network 123.89.128.32 255.255.255.224
Murcia(dhcp-config)#default-router 123.89.128.33
Murcia(dhcp-config)#exit
Murcia(config)#ip dhcp excluded-address 123.89.128.129 123.89.128.254
Murcia(config)#ip dhcp pool TOLEDOS
Murcia(dhcp-config)#network 123.89.128.32 255.255.255.128
Murcia(dhcp-config)#default-router 123.89.128.129
Murcia(dhcp-config)#exit
Murcia(config)#exit
Murcia#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Murcia#
*SYS-5-CONFIG_I: Configured from console by console

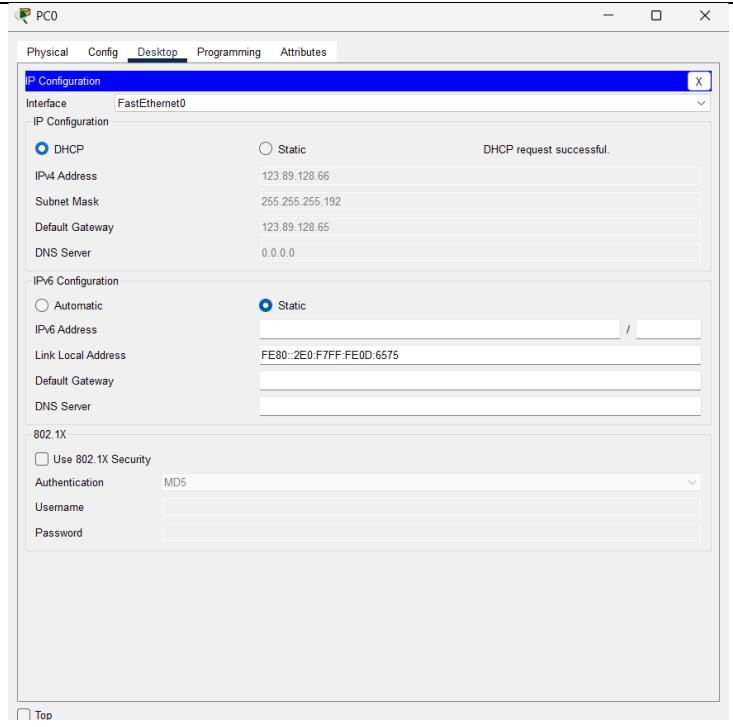
Murcia#

```

Se asignó la IP inicial configurada en los routers como gateway por defecto a los switches, asegurando que cada dispositivo contara con conectividad básica y pudiera comunicarse con el resto de la red.



Se activó el servicio DHCP en los equipos finales, permitiendo la obtención automática de direcciones IP, máscara de subred y gateway, lo que facilitó la integración de los dispositivos a la red sin necesidad de configuraciones manuales y garantizó la correcta asignación de recursos.



Implementación Natalia

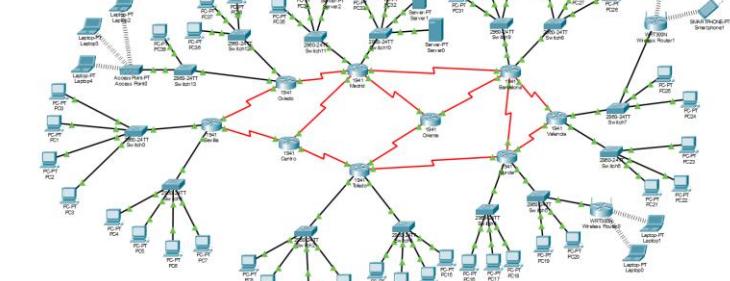
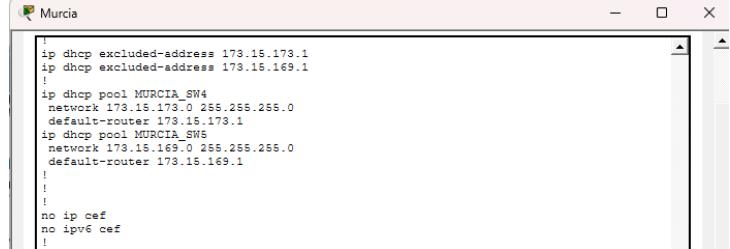
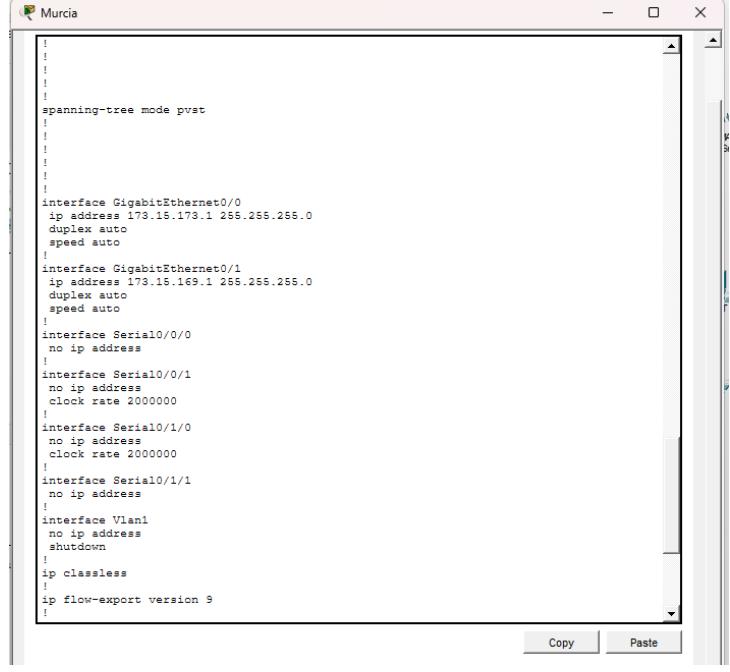
Antes de proceder a dividir la red de Natalia en subredes, es importante comprender la estructura básica de la red principal:

- Red de Natalia: 173.15.160.0/20
- Binario: 10101101.00001111.1010|0000.00000000
- Host: 173.15.160.1
- Broadcast: 173.15.175.255

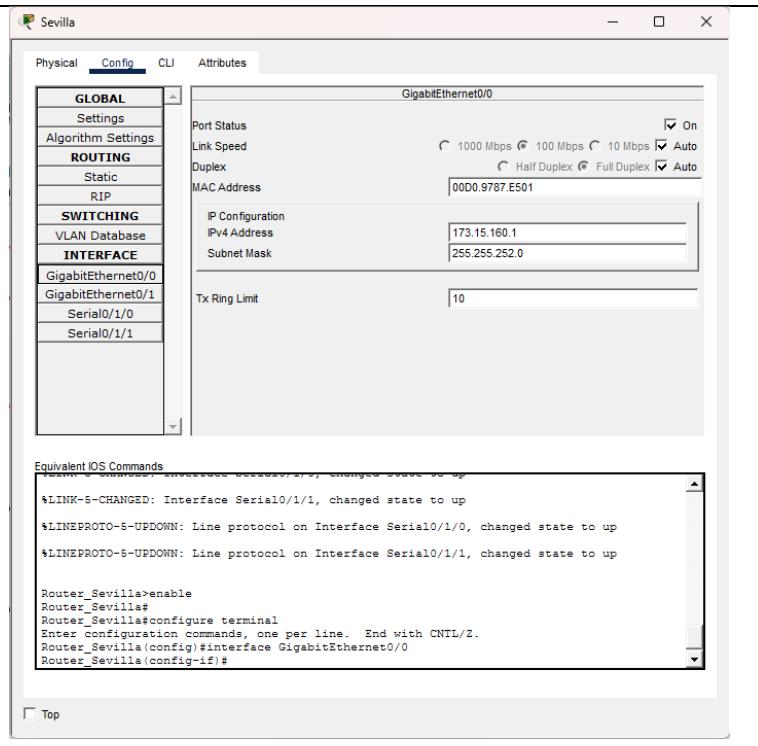
Con esta información, se puede planificar adecuadamente la creación de subredes, asignando bloques de direcciones IP de manera eficiente según las especificaciones.

Ciudad	LAN	Numero de direcciones	Binario	Red	Rango	Mascara
Sevilla	Switch0	$2^{10} - 2 \geq 700$	00 00.00000000	173.15.160.0/22	173.15.160.1 ----- 173.15.163.254	255.255.252.0
	Switch1	$2^8 - 2 \geq 189$	0001 00000000	173.15.171.0/24	173.15.171.1 ----- 173.15.171.254	255.255.255.0
Toledo	Switch2	$2^{10} - 2 \geq 550$	10 00.00000000	173.15.164.0/22	173.15.164.1 ----- 173.15.167.254	255.255.252.0
	Switch3	$2^7 - 2 \geq 80$	0000.1 0000000	173.15.174.128/25	173.15.174.129 ----- 173.15.174.254	255.255.255.128
Murcia	Switch4	$2^8 - 2 \geq 130$	0010 00000000	173.15.173.0/24	173.15.173.1 ----- 173.15.173.254	255.255.255.0
	Switch5	$2^8 - 2 \geq 220$	0011 00000000	173.15.169.0/24	173.15.169.1	255.255.255.0

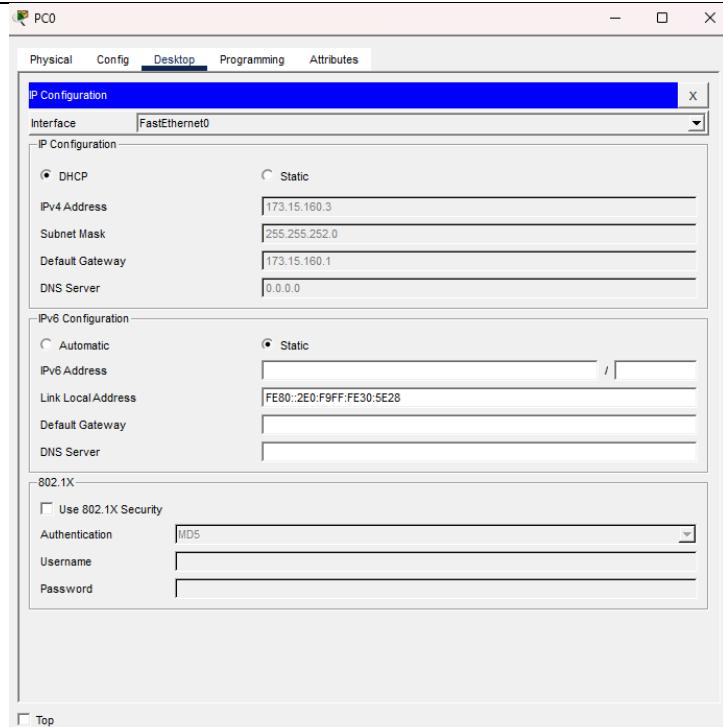
					----- 173.15.172.254	
Valencia	Switch6	$2^8 - 2 \geq 140$	0110 00000000	173.15.172.0/24	173.15.172.1 ----- 173.15.166.254	255.255.255.0
	Switch7	$2^6 - 2 \geq 60$	0000.01 000000	173.15.175.0/26	173.15.175.1 ----- 173.15.175.62	255.255.255.192
Barcelona	Switch8	$2^6 - 2 \geq 50$	0000.11 000000	173.15.175.128/26	173.15.175.129 ----- 173.15.175.190	255.255.255.192
	Switch9	$2^6 - 2 \geq 40$	0111.00 000000	173.15.175.192/26	173.15.175.192 ----- 173.15.175.254	255.255.255.192
Madrid	Switch10	$2^8 - 2 \geq 200$	0101 00000000	173.15.170.0/24	173.15.170.1 ----- 173.15.170.254	255.255.255.0
	Switch11	$2^8 - 2 \geq 230$	1000 00000000	173.15.171.0/24	173.15.171.1 ----- 173.15.171.254	255.255.255.0
Oviedo	Switch12	$2^6 - 2 \geq 55$	1001.00 000000	173.15.175.64/26	173.15.175.65 ----- 173.15.175.126	255.255.255.192
	Switch13	$2^7 - 2 \geq 99$	1010.0 0000000	173.15.174.0/25	173.15.174.1 ----- 173.15.174.126	255.255.255.128

Acción Realizada	Captura de pantalla
<p>Al inicio del laboratorio se diseñará e implementará una topología compleja en Packet Tracer que representará la interconexión de varias ciudades mediante routers y switches. Esta base será fundamental para realizar las configuraciones posteriores de DHCP, enrutamiento y pruebas de conectividad.</p>	
<p>Esta configuración permitirá que los dispositivos conectados a los switches SW4 y SW5 obtengan automáticamente su dirección IP, máscara y gateway, facilitando la administración de la red.</p>	 <pre> ip dhcp excluded-address 173.15.173.1 ip dhcp excluded-address 173.15.169.1 ! ip dhcp pool MURCIA_SW4 network 173.15.173.0 255.255.255.0 default-router 173.15.173.1 ip dhcp pool MURCIA_SW5 network 173.15.169.0 255.255.255.0 default-router 173.15.169.1 ! ! no ip cef no ipv6 cef !</pre>
<p>Esta configuración permitirá que el router gestione el tráfico entre las redes locales y facilite la entrega de direcciones IP mediante el protocolo DHCP previamente configurado.</p>	 <pre> spanning-tree mode pvst ; interface GigabitEthernet0/0 ip address 173.15.173.1 255.255.255.0 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 173.15.169.1 255.255.255.0 duplex auto speed auto ! interface Serial0/0/0 no ip address ! interface Serial0/0/1 no ip address clock rate 2000000 ! interface Serial0/1/0 no ip address clock rate 2000000 ! interface Serial0/1/1 no ip address ! interface Vlan1 no ip address shutdown ! ip classless ! ip flow-export version 9 !</pre>

En esta parte se configurará la interfaz GigabitEthernet0/0 del router de Sevilla, asignándole la dirección IP 173.15.160.1 con máscara 255.255.252.0, correspondiente a la subred calculada para el switch SW0 durante el proceso de subnetting. Esta configuración es fundamental para que el router pueda interactuar con el protocolo DHCP y posteriormente con los protocolos de enrutamiento dinámico (EIGRP y OSPF), asegurando la conectividad entre las diferentes ciudades de la topología.



En esta etapa se verificará el funcionamiento del protocolo DHCP configurado previamente en los routers. Para ello, se seleccionará la opción DHCP en la configuración de la interfaz del PC, permitiendo que el equipo obtenga automáticamente su dirección IP, máscara de subred y puerta de enlace. Como resultado, el PC recibirá la dirección 173.15.160.3, con máscara 255.255.252.0 y gateway 173.15.160.1, que corresponde a la red asignada al switch SW0 en Sevilla. Este proceso confirma que el servicio DHCP está funcionando correctamente y que



los dispositivos pueden integrarse a la red sin necesidad de configuraciones manuales, optimizando la administración y reduciendo errores en la asignación de direcciones.

EIGRP

Acción Realizada	Captura de pantalla
<p>Esta evidencia demuestra que EIGRP está funcionando correctamente, ya que la presencia de vecinos indica que los routers están intercambiando información de enrutamiento de manera dinámica.</p>	<pre>Seville# show ip eigrp neighbors IP-EIGRP neighbors for process 1 H Address Interface Hold Uptime SRTT RTO Q Seq 0 10.0.0.6 Se0/1/0 12 01:09:15 40 1000 0 68</pre>
<p>La salida del comando show ip route confirma que el router Sevilla ha aprendido rutas dinámicas mediante el protocolo EIGRP, identificadas con la letra D. En la tabla se observan múltiples redes del backbone, como 10.0.0.0/30, 10.0.0.4/30, y otras, que se alcanzan a través de la interfaz Serial0/1/0 con una métrica compuesta (por ejemplo, [90/3703856], donde 90 es la distancia administrativa y el segundo valor corresponde a la métrica calculada por EIGRP). Además, se incluyen las redes locales conectadas directamente, marcadas con la letra C, como 173.15.160.0/22, y las direcciones locales (L) asignadas a las interfaces. Esta evidencia demuestra que el router no solo mantiene conectividad con sus redes locales, sino que también intercambia información con otros routers del dominio EIGRP, permitiendo la comunicación entre todas las ciudades de la topología.</p>	<pre>Seville# show ip route Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is now set 10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks D 10.0.0.0/30 [90/3703856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.4/30 [90/3703856] via 10.0.0.6, 01:14:08, Serial0/1/0 L 10.0.0.5/32 is directly connected, Serial0/1/0 D 10.0.0.8/32 [90/3133856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.12/30 [90/2681856] via 10.0.0.6, 01:14:11, Serial0/1/0 D 10.0.0.16/30 [90/2681856] via 10.0.0.6, 01:14:11, Serial0/1/0 D 10.0.0.20/30 [90/3193856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.24/30 [90/3193856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.28/30 [90/3193856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.32/30 [90/3193856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.36/30 [90/3705856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.40/30 [90/3705856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.44/30 [90/3705856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 10.0.0.48/30 [90/3705856] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.160.0/16 is variably subnetted, 16 subnets, 2 masks C 173.15.160.0/22 is directly connected, GigabitEthernet0/0 L 173.15.160.1/32 is directly connected, GigabitEthernet0/0 D 173.15.164.0/22 [90/2684416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.168.0/24 [90/2684416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.169.0/24 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.170.0/24 [90/2684416] via 10.0.0.6, 01:14:08, Serial0/1/0 C 173.15.171.0/24 is directly connected, GigabitEthernet0/1 L 173.15.171.1/32 is directly connected, GigabitEthernet0/1 D 173.15.172.0/24 [90/3708416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.173.0/24 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.174.0/24 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.174.128/24 [90/2684416] via 10.0.0.6, 01:14:08, Serial0/1/0 D 173.15.175.0/24 [90/3708416] via 10.0.0.6, 01:14:08, Serial0/1/0</pre>

La salida del comando show ip protocols confirma que el router Sevilla tiene habilitado el protocolo EIGRP con número de sistema autónomo 1. En la información se observa la métrica utilizada por el algoritmo, donde los valores K1 y K3 están en 1 (bandwidth y delay), mientras que K2, K4 y K5 permanecen en 0, lo que indica que la métrica compuesta se basa únicamente en el ancho de banda y el retardo. También se muestra que la auto-sumarización está deshabilitada, lo que permite mantener la precisión en el direccionamiento VLSM. Además, se listan las redes anunciadas por el router, como 173.15.160.0/22 y varias subredes del backbone (10.0.0.0/30, 10.0.0.4/30, etc.), junto con la distancia administrativa (90 para rutas internas) y el número de vecinos activos. Esta evidencia demuestra que la configuración de EIGRP es correcta y que el router participa activamente en el intercambio de rutas dinámicas.

```

Sevilla
Physical Config CLI Attributes

IOS Command Line Interface

D 173.15.174.0/25 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0
D 173.15.174.128/25 [90/2684416] via 10.0.0.6, 01:14:08, Serial0/1/0
D 173.15.175.0/26 [90/3708416] via 10.0.0.6, 01:14:08, Serial0/1/0
D 173.15.175.64/26 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0
D 173.15.175.128/26 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0
D 173.15.175.192/26 [90/3196416] via 10.0.0.6, 01:14:08, Serial0/1/0

Sevilla#show ip protocols

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 1
    EIGRP-IPv4 Protocol for AS(1)
      Metric weights: K1=1, K2=0, K3=1, K4=0, K5=0
      NSF-aware route hold timer is 240
      Router-ID: 10.0.0.5
      Topology (base)
        Active Timer: min
        Distance: internal 90 external 170
        Maximum path: 4
        Maximum hopcount 100
        Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
    173.15.160.0/22
    173.15.171.0/24
    10.0.0.0/30
    10.0.0.4/30
  Routing Information Sources:
    Gateway          Distance      Last Update
    10.0.0.6           90          5586
  Distance: internal 90 external 170

Sevilla#

```

La salida del comando `show ip eigrp topology` muestra las redes conocidas por el router Sevilla dentro del proceso EIGRP con AS 1. Cada entrada indica una red, el número de sucesores (rutas válidas) y la métrica factible (FD), que se calcula principalmente en función del ancho de banda y el retardo acumulado. Además, se muestra la interfaz de salida (Serial0/1/0) y las métricas asociadas, confirmando que el router ha aprendido rutas dinámicas y mantiene una topología completa para la conmutación eficiente de paquetes. Esta evidencia demuestra que EIGRP está funcionando correctamente y que el router conoce múltiples rutas hacia diferentes destinos.

```

Sevilla#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address           Interface      Hold Uptime   SRTT    RTO     Q Seq
  0  10.0.0.6        Se0/1/0       12  01:09:15  40  1000  0  69

Sevilla#show ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(173.15.171.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/30, 1 successors, FD is 3705856
via 10.0.0.6 (3705856/3193856), Serial0/1/0
P 10.0.0.4/30, 1 successors, FD is 2681856
via Connected, Serial0/1/0
P 10.0.0.8/30, 1 successors, FD is 3193856
via 10.0.0.6 (3193856/2681856), Serial0/1/0
P 10.0.0.12/30, 1 successors, FD is 2681856
via 10.0.0.6 (2681856/2169856), Serial0/1/0
P 10.0.0.16/30, 1 successors, FD is 2681856
via 10.0.0.6 (2681856/2169856), Serial0/1/0
P 10.0.0.20/30, 1 successors, FD is 3193856
via 10.0.0.6 (3193856/2681856), Serial0/1/0
P 10.0.0.24/30, 1 successors, FD is 3193856
via 10.0.0.6 (3193856/2681856), Serial0/1/0
P 10.0.0.28/30, 1 successors, FD is 3193856
via 10.0.0.6 (3193856/2681856), Serial0/1/0
P 10.0.0.32/30, 1 successors, FD is 3193856
via 10.0.0.6 (3193856/2681856), Serial0/1/0
P 10.0.0.36/30, 1 successors, FD is 3705856
via 10.0.0.6 (3705856/3193856), Serial0/1/0
P 10.0.0.40/30, 1 successors, FD is 3705856
via 10.0.0.6 (3705856/3193856), Serial0/1/0
P 10.0.0.44/30, 1 successors, FD is 3705856
via 10.0.0.6 (3705856/3193856), Serial0/1/0
P 10.0.0.48/30, 1 successors, FD is 3705856
via 10.0.0.6 (3705856/3193856), Serial0/1/0
P 173.15.169.0/22, 1 successors, FD is 28150

```

En esta captura se muestra la ejecución del comando ping desde el equipo PC0 hacia la dirección 173.15.169.3, perteneciente a otra red dentro de la topología. El resultado indica que se enviaron 4 paquetes y se recibieron los 4 correctamente, con un tiempo de respuesta promedio de 15 ms y sin pérdida de paquetes (0%). Esta evidencia confirma que la configuración del protocolo EIGRP está funcionando adecuadamente, ya que permite la comunicación entre dispositivos ubicados en diferentes segmentos de red, demostrando que las rutas dinámicas aprendidas por el

```

C:\>ping 173.15.169.3

Pinging 173.15.169.3 with 32 bytes of data:
Reply from 173.15.169.3: bytes=32 time=17ms TTL=124
Reply from 173.15.169.3: bytes=32 time=13ms TTL=124
Reply from 173.15.169.3: bytes=32 time=19ms TTL=124
Reply from 173.15.169.3: bytes=32 time=12ms TTL=124

Ping statistics for 173.15.169.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 19ms, Average = 15ms

```

router son efectivas para garantizar la conectividad extremo a extremo.

Revise las tablas de enrutamiento generadas con EIGRP. ¿Qué métrica usa para calcular la mejor ruta?

El protocolo EIGRP emplea una métrica compuesta para determinar la ruta óptima hacia cada destino. Por defecto, esta métrica se calcula a partir de dos parámetros principales: ancho de banda (bandwidth) y retardo (delay), con los valores K1 y K3 establecidos en 1, mientras que K2, K4 y K5 permanecen en 0. Esto significa que la elección de la mejor ruta se basa en la combinación del ancho de banda disponible en el enlace y el retardo acumulado a lo largo del trayecto. En la práctica, EIGRP seleccionará la ruta que ofrezca el mayor ancho de banda y el menor retardo, garantizando así un camino eficiente para la transmisión de datos. Esta información puede verificarse mediante el comando `show ip eigrp topology`, donde se muestran las métricas calculadas para cada red conocida por el protocolo.

Conclusiones

El estudio y la implementación de redes Ethernet y WiFi permitió consolidar una comprensión profunda de la capa de enlace, capa de red y capa de aplicación, evidenciando cómo interactúan para garantizar conectividad, eficiencia y seguridad. La correcta segmentación mediante VLANs, junto con un direccionamiento IP planificado y el uso de DHCP, mostró la importancia de automatizar y optimizar la gestión de direcciones y servicios de red.

El análisis de enrutamiento dinámico con EIGRP y OSPF reforzó la capacidad de diseñar topologías escalables y resilientes, comprendiendo cómo las métricas de ancho de banda y retardo influyen en la selección de rutas óptimas. La integración de servicios de la capa de aplicación, como DNS y servidores web, permitió valorar la relación entre conectividad y disponibilidad de servicios, destacando que una infraestructura de red eficiente requiere planificación tanto en el plano físico como lógico.

En conjunto, este desarrollo fortaleció habilidades en diseño, configuración y administración de redes, consolidando un enfoque estratégico para crear arquitecturas robustas, seguras y adaptables a necesidades empresariales.